CYBER DEFENSE MAGAZINE

eMAGAZINE

JULY 2022

In This Edition

3 Ways Asset Management Companies Can Reduce Cyber Risk

A Modern Cybersecurity Fight Requires a Modern Approach to Regulatory Oversight

Apes Gone Phishing

…and much more…

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

We'll be celebrating our 10th Year in business unveiling the Top InfoSec Innovators in the World including Black Unicorns to the Top CISOs in the World at CYBERDEFENSECON 2022 – 10/27/22 – See You There!

Dear Friends,

Even in the most tumultuous times, with a 'soft' cyberwar waging behind the scenes, we at CDMG choose to focus on the innovations and next generation solutions in cyber defense that help protect our way of life, our data and our privacy.

Therefore, we have opened our Top InfoSec Innovators in the World, competition as part of our annual Black Unicorn awards. All innovative information security companies of any size may apply for this prestigious award. Cybersecurity companies that wish to apply may visit https://www.cyberdefenseawards.com/

In the cybersecurity industry, I coined the term black unicorn as a cybersecurity company that has the potential to reach a $1 billion dollar market value as determined by private or public investment. The Black Unicorn Awards are designed to help showcase companies with this kind of potential. Ultimately, the judging in our awards is tough and it's still up to the finalists and the winners to execute a flawless business model to reach this potential. It takes innovation, dedication, passion – the right team and the right cyber security solution, harmoniously executed to become a unicorn.

Cyber Defense Media Group (CDMG), having launched our 10th annual cybersecurity community awards this year, continues to seek nominees for our annual young Women in Cybersecurity scholarship program for entries. We have one scholarship open and remaining for the year. Any young woman in high school who will be entering college in 2022/2023 can apply now:

https://cyberdefenseawards.com/women-in-cybersecurity-scholarship-fund-for-2022/

Readers can learn about the prior winners, in 2020, Annabelle Klosterman, here: https://cyberdefenseawards.com/women-in-cybersecurity-scholarship-winner-for-2020/ in 2021, Olivia Gallucci, here: https://cyberdefenseawards.com/women-in-cybersecurity-2021-scholarship-winner/ and in 2022, Veronika (Nikki) Jack, here: https://cyberdefenseawards.com/women-in-cybersecurity-2022-scholarship-winner-1st-of-2/ who each remain an inspiration for other young women to enter the field of cybersecurity.

As in past years, a panel of judges will review each entry and choose one scholarship winner and a backup winner in case there are issues on the winner's college entry in 2022/2023. Now is an excellent time for young women to plan their future careers in cybersecurity. It's a hot field with hundreds of thousands of career openings and unlimited opportunities for those who wish to make a positive impact on today's digital world.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR-IN-CHIEF
Yan Ross, JD
Yan.Ross@cyberdefensemediagroup.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451

http://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
http://www.cyberdefensemagazine.com/about-our-founder/

10 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM
MAGAZINE TV RADIO AWARDS
PROFESSIONALS VENTURES WEBINARS
CYBERDEFENSECONFERENCES

Welcome to CDM's July 2022 Issue

From the Editor-in-Chief

Once again, this month the Editor's Welcome letter provides an overview of the topics and trends in the articles for the issue. As always, the articles reflect the authors' perceptions of the most pressing cybersecurity matters of the day.

The challenges and responses of the cybersecurity community are growing, as evidenced by the unusually large number of articles being submitted, reviewed, and published; this month we are pleased to include 50 impressive articles, all relevant to the most pressing cybersecurity issues of the day.

A brief review of this month's Table of Contents will demonstrate the breadth and importance of the topics chosen by our contributors and brought to you, our readers, to support your own cyber endeavors.

We live in an ever-changing and dynamic world of cyber players with a tremendous number of job opportunities in our field. Therefore, we launched https://www.cyberdefenseprofessionals.com to help job seekers find these opportunities. It's free to post and search for infosec related jobs.

The central role Cyber Defense Magazine plays in the breadth of activities conducted by the entire Cyber Defense Media Group means that we always select and publish the most actionable intelligence from the most knowledgeable writers in the field.

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemediagroup.com


SPONSORS

CYBER DEFENSE CONFERENCES

THREE EVENTS IN ONE

Orlando, Florida, USA | October 27-28, 2022

One of the most exclusive, fun and educational CISO conferences of the year!

Limited to our selection of the top 100 CISOs in the world, amazing speakers and insider threat mitigation training by a world reknown expert - meets 100 top cyber defense companies in an intimate, high value two day summit

www.cyberdefenseconferences.com

CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

• Deploy. • Manage. • Tune up. • Audit. • Defend. Report.

GET YOUR FREE eBook

Get https://cionsystems.com/


DATATRIBE
CYBER STARTUP FOUNDRY
Forging dominant companies from nation-state domain expertise
CAPITAL | RESOURCES | GUIDANCE | SUCCESS
HOME TO THE WORLD'S FASTEST GROWING CYBERSECURITY AND DATA SCIENCE COMPANIES
attila SECURITY
DRAGOS
ENVEIL ENCRYPTED VEIL
INERTIALSENSE
PREVAILION
the cyberwire
refirm labs
BlueRidge.ai
STRIDER
CodeDx
BLACKCLOAK™
SightGain
JOIN THE TRIBE
DATATRIBE.COM

Is your AI Secure?

BOSCH

Widespread AI adoption has profoundly exposed AI/ML models to adversarial attacks. Hackers can subvert AI/ML systems causing financial loss, reputational damage, loss of competitive advantage and intellectual property theft.

> **It's hard to patch or mitigate what you can't find**

Bosch AIShield

Cybersecurity solution for your AI assets

An industry-first, ready-to-deploy and production-optimized solution to secure AI systems against adversarial attacks such as model extraction, model evasion, data poisoning and model inference attacks

www.boschaishield.com

Consulting

Consulting led AI security impact assessment & mitigation plan

Services

Customized enterprise implementation service for AI security

Product

Leverage AIShield API every time a new AI/ML model is deployed or changed

+91 8951989144

AIShield.contact@bosch.com

Bosch Global Software Technologies
alt_future

CYBER CRIMINALS
DON'T GIVE A $#!T:

- ☐ About your project's scope.
- ☐ It's managed by a third party.
- ☐ It's a legacy system.
- ☐ It's "too critical to patch."
- ☐ About your outage windows.
- ☐ About your budget.
- ☐ That you've always done it that way.
- ☐ About your go-live date.
- ☐ It's only a pilot/proof of concept.
- ☐ About non-disclosure agreements.
- ☐ It wasn't a requirement in the contract.
- ☐ It's an internal system.
- ☐ It's really hard to change.
- ☐ It's due for replacement.
- ☐ You're not sure how to fix it.
- ☐ It's handled in the Cloud.
- ☐ About your Risk Register entry.
- ☐ The vendor doesn't support that configuration .
- ☐ It's an interim solution.
- ☐ It's [insert standard here] compliant.
- ☐ It's encrypted on disk.
- ☐ The cost-benefit doesn't stack up.
- ☐ "Nobody else could figure it out."
- ☐ You can't explain the risk to "The business."
- ☐ You've got other priorities.
- ☐ About your faith in the competence of your internal rules.
- ☐ You don't have a business justification.
- ☐ You can't show return on investment.
- ☐ That it's supposed to be "Air Gapped."

But we do, and we're here to help!

SCADAfence

The Most Comprehensive
OT & IoT
Cyber Security Platform For
Critical Infrastructure &
Enterprises

www.SCADAfence.com

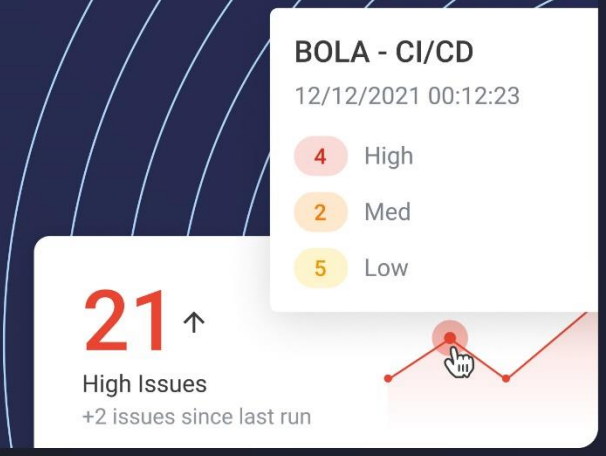
noname

The Complete, Proactive API Security Platform

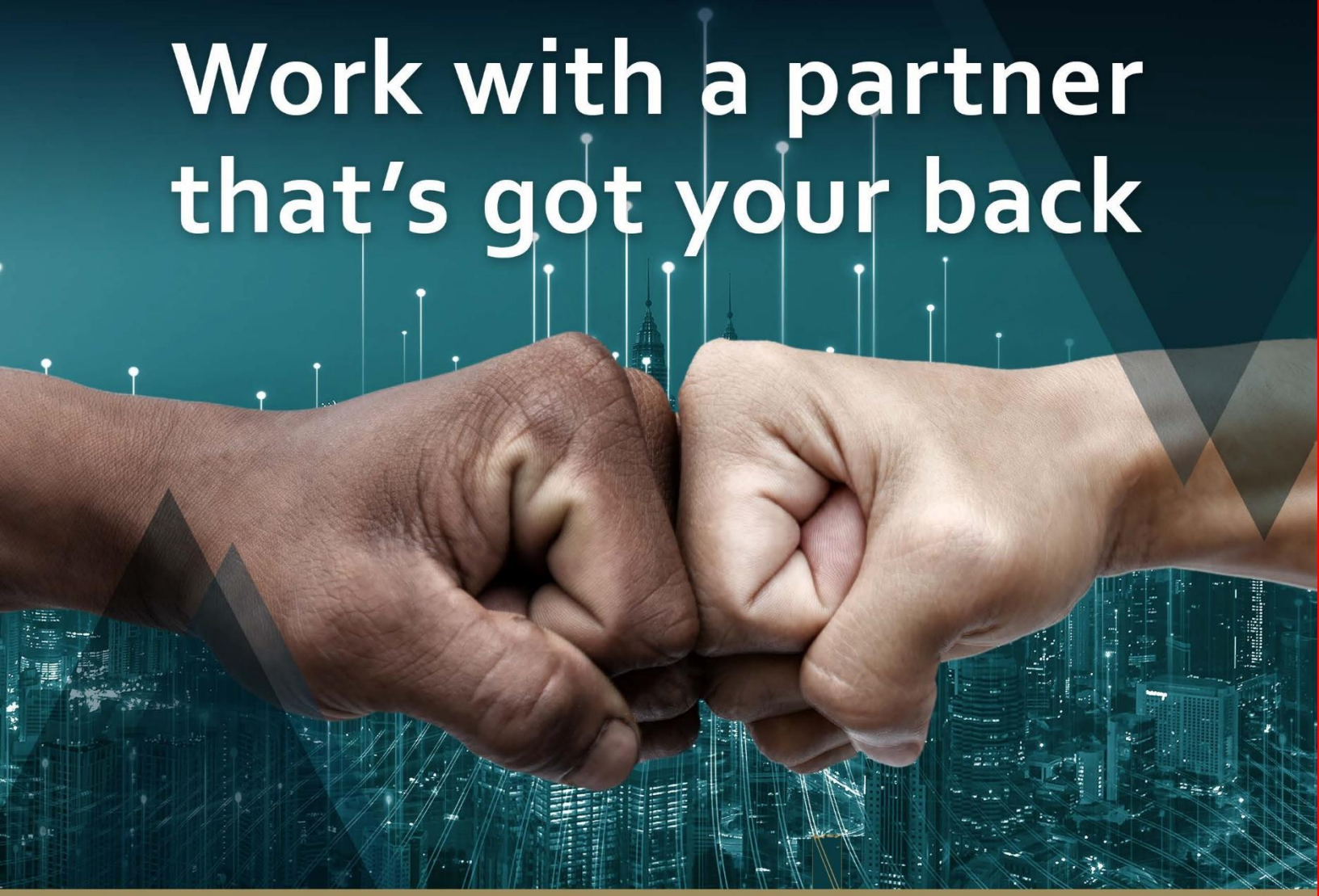
nonamesecurity.com >

Shift Left with **API Security Testing**

Industry-leading posture managment, runtime security and API security testing



Work with a partner that's got your back



Up Your Security Game

WITH A PARTNER 100% COMMITTED TO MICROSOFT SECURITY

MANAGED SIEM - powered by Microsoft Sentinel

MANAGED EDR - powered by Microsoft Defender for Endpoint

MDR FOR IT - powered by Microsoft Sentinel and Defender XDR Platform

MDR FOR OPERATIONAL TECHNOLOGY (OT) - powered by Microsoft Sentinel & Defender for IoT/OT

ADVANCED VULNERABILITY MANAGEMENT - powered by Microsoft Defender TVM

MICROSOFT SECURITY PROFESSIONAL SERVICES - Design, Implement, Configure & Optimize

DIFENDA

CONTACT A DIFENDA SECURITY EXPERT TODAY

Microsoft Partner

Microsoft

Gold Security
Gold Cloud Platform
Gold Application Development
Advanced Specialization - Threat Protection

Member of
Microsoft Intelligent Security Association

Microsoft

MYTH

Data can't protect itself from ransomware criminals.

FACT

Now it does! No matter where it goes in the world,
who has it or how many copies exist.

DATA ITSELF IS NOW ITS OWN FORTRESS

Learn more at Keyavi.com

keyavi

Making data self-protecting, intelligent and self-aware

Join the conversation!
#TransformCybersec, #TransformingCybersec

Transform your datasecurity strategy
with the power of Keyavi.

Download your free whitepaper

How People, Processes, and Technology Shape the Future of Cyber Security

By Milton Security

Start my **FREE** 15-day POV

In 2016, Gartner released their top 10 technologies for information security,[1] containing Intelligence-driven Security Operations Centers, which would shift the paradigm of threat detection and response by incorporating adaptive architecture and context-aware components. At this time, detection and response budgets were 30% of overall security budgets and were expected to double by 2020 because no amount of preventative security controls were able to catch all intrusions or attempts.[2]

These two reports paved the way for organizations to understand this dichotomy - the security of an organization can not rely solely on humans or tools. Milton Security has been preaching (and practicing) this shift since 2007 through Dynamic Threat Hunting. Dynamic Threat Hunting occurs when creative, human Threat Hunters are enhanced by AI/ML. Pair that with deep threat intelligence, telemetry, and billions of daily messages and you have an intelligent, context-aware, and just-in-time security operation to your organization protected.

Standing up a Dynamic Threat Hunting Team internally could lead to a few possible outcomes:

- Take decades to get it right, all while leaving your network vulnerable to threat actors;
- Completely burn out and decimate your team with data deluge; OR
- Increase your security budget to that of Amazon3 and still see threat groups slip through.[3]

In 2017, Gartner's principal research analyst Sid Deshpande wrote, "The shift to detection and response approaches spans people, process and technology elements and will drive a majority of security market growth over the next five years." Mr. Deshpande realized that PPT is essential to the future of cyber security, which is why Milton Security, over the last 15 years, has combined these three elements to pave the way in becoming the leader in Dynamic Threat Hunting. Sure, you could go at this alone and struggle with the three outcomes listed above, or you could sign up for a free 15-day Proof of Value trial from Milton Security and see for yourself how effective our Dynamic Threat Hunters are in protecting your brand.

About Milton Security

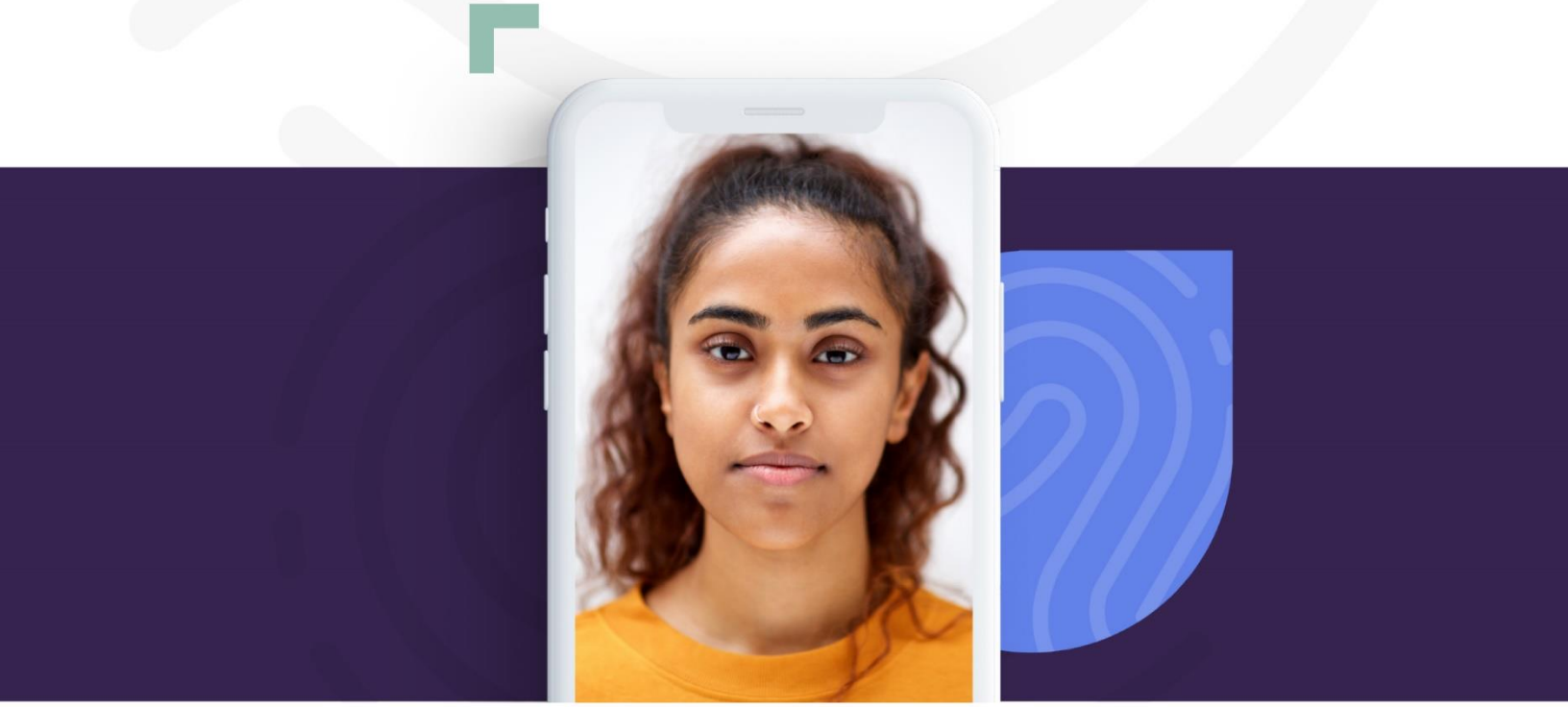
Milton Security is the global leader in Dynamic Threat Hunting. For over 15 years, Milton's team of Threat Hunters have stopped hundreds of thousands of threats and assisted organizations in protecting themselves around the clock. Milton focuses on the best combination of AI, ML, and Humans, to zero-in on threats, assist with remediation and incident response activities, and keep your brand protected.

1. https://www.gartner.com/smarterwithgartner/gartners-top-10-technologies-for-information-security
2. https://www.gartner.com/en/newsroom/press-releaes/2016-06-06-gartner-says-by-2020-60-percent-of-digital-businesses-will-suffer-major-service-failures-due-to-the-inability-of-it-security-teams-to-manage-digital-risk
3. https://blog.twitch.tv/en/2021/10/15/updates-on-the-twitch-security-incident/

1KOSMOS

Close the loopholes in passwordless logins with identity-based authentication

Defeat phishing, data breaches and ransomware while improving your user experience.



Experience BlockID

Use biometric authentication with flexible levels of identity assurance to secure workforce account access and eliminate the risk and inconvenience of passwords.

www.1kosmos.com/demo

COVIANT Software

Software Reviews CHAMPION 2021

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2021

Award-Winning, Secure File Transfer & Automation

Supports All Major Transfer Protocols

FTP, FTPS, SFTP, HTTP, HTTPS, AS2, Email, SMB, CIFS, NFS

Best In Class PGP Automation

Encrypt, decrypt, sign or verify encrypted files with a simple checkbox

Cloud Integration

Connect To A Range Of Cloud Storage Providers (Amazon S3, Microsoft Azure, Box, Citrix ShareFile, Dropbox, Google Cloud, Oracle Cloud and more)

RepliWeb Replacement

RepliWeb reached End of Life on 01/31/2022. This platform is no longer being supported. Our software, Diplomat MFT, is an ideal alternative to this popular solution.

FREE TRIAL

We offer a no obligation, free trial or demo. Please visit our website for more details or call us on: (210) 985-0985

www.coviantsoftware.com

Trustwave®

MANAGED DETECTION & RESPONSE

Give Your Security Team More Venom.

Detect with Accuracy

Defend Intelligently

Respond Quickly

www.trustwave.com

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

Founder & Managing Partner

SEAN DRAKE

U.S.ARMY

"At Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. "

Sean Drake
Managing Partner
Stony Lonesome Group LLC
203-247-2479
www.stonylonesomegroupllc.com

Database Cyber Security Guard

Don't be the next data breach. Equifax paid $575 million, British Airways $230 million and Marriott $124 million in fines.

Prevents confidential data theft by Hackers, Rogue Insiders, Phishing Emails, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks.

Product Features

- Detects Informix, MariaDB, MySQL, Oracle, SQL Server and Sybase data theft within milliseconds and shuts down Hackers immediately.
- Advanced SQL Behavioral Analysis of the database query activity learns the normal query patterns and detects database data theft.
- View all suspicious database activity and attempted data theft.
- Supports key GDPR compliance requirements. Non-intrusive detection of data theft. Runs on a network tap or proxy server.

Get a FREE COPY now.

www.DontBeBreached.com/Free

NIGHTDRAGON

"NightDragon *Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com


ARTICLES

3 Ways Asset Management Companies Can Reduce Cyber Risk

Fund managers should not get caught out thinking they are a low-priority target: here's how to identify risks and build resilience, to protect investor data and assets

By Roland Thomas, Corporate Development Manager, Thomas Murray

Conventional wisdom tells us that investment risk depends solely on the success or failure of a financial instrument. A higher risk appetite can reap higher rewards, but the value of an investment can be wiped out. This is true, but how many investors are aware of the huge array of other risks faced by their chosen funds? And how many investment management companies consider cyber risk to be an investment risk? In this article, we explain why cyber risk is an area of acute vulnerability for investment companies, and the steps firms can take to build security.

Banks are a harder target for threat actors

Asset management companies, like any other firm, and more than most, face unprecedented challenges to protect themselves from cyber criminals. The sector is under particular scrutiny because the banks –

historically a greater focus for hackers – have invested so heavily in security that they are generally well-protected against threats and are prepared to respond when attacks inevitably occur.

Most large global and regional banks now have dedicated Security Operations Centres, responsible for detecting, quantifying and responding to cyber threats and incidents. Even in spite of all this, according to analysis by Thomas Murray, 20% of banks still suffered cyber attacks in the last 12 months, with 8% refusing to disclose. Banks are still a target, especially via vulnerable supply chains, but it logically follows that cyber-criminals will increasingly pursue targets that are asset-rich but have weaker security.

Investment companies are vulnerable

With significant Assets Under Management (AUM) but often limited operational budgets, asset management companies are acutely vulnerable. Financial firms are 300 x more likely than other institutions to experience attacks, and the average cost of a data breach in 2021 was $4.23 million. While banks have the balance sheets to absorb these costs, few but the largest asset managers do. Companies are being targeted with a higher volume of attacks, by threat actors who are becoming more sophisticated, and asset managers are making themselves vulnerable by underinvesting in IT infrastructure, as well as by exposing themselves to a huge range of service providers.

Attack surfaces are growing

As asset managers responded to Covid by innovating with new digital services, they unwittingly grew their attack surfaces. The result has been that security has often not kept pace with digitisation, and performance has taken precedence over resilience. At the same time, investment firms have taken advantage of the efficiencies and expertise offered by outsourcing their middle and back office, exposing themselves – and their clients – to a larger number of third parties than ever before. These investment institutions should be bastions of security, safeguarding investors' and savers' assets as a minimum requirement, but they are faced with a perfect storm of growing attack surfaces, vulnerable supply chains, rising cyber criminality and complex regulation. Acknowledging the problem is the first step, but how can they respond to the challenge?

What can asset managers do?

There are three ways by which asset management companies can reduce cyber risk in the front, middle and back office – making security a C-Suite priority.

1. Learn who their third- and fourth- parties are

51% of organisations have experienced a data breach caused by a third party, according to the Ponemon Institute (2021). For investment firms, these third parties can include software providers, fund administrators, transfer agents, third-party management companies, distributors and a bewildering array of other firms – many of whom pose a risk of client data breaches and spillover cyber attacks. On top of

that, a fourth party is any provider to your providers, and is an often-neglected area of risk. Companies should maintain inventories of their providers and indirect exposures, and should seek to monitor all of them.

2. **Include cyber risk in investment due diligence**

Cyber due diligence is becoming a critical area of investment due diligence. Initial checks and ongoing monitoring of investment portfolio companies should be treated like AML and KYC checks: you would never work with sanctioned individuals or indirectly facilitate terrorist financing, so why would you expose your clients to unnecessary cyber risk?

This is a particularly pertinent point when it comes to Venture Capital and Private Equity firms with a small number of tech-enabled companies in their portfolios. Security is a potentially existential risk for such companies, particularly in their early stages, and a combination of due diligence and continuous threat intelligence can help a fund measure and mitigate these risks.

3. **Invest in IT Security teams & solutions**

A certain kind of asset manager has long considered IT to be a back-office function, neither seen nor heard. Today, IT Security needs to be recognised as a front, middle and back office investment. Without well-funded, competent teams, an investment company's IT infrastructure, staff awareness and third party exposure will suffer.

About the Author

Roland Thomas is the Corporate Development Manager at Thomas Murray. He is responsible for strategy and innovation. Roland is responsible for bringing to market Thomas Murray's award-winning AI Threat Intelligence and Cyber Security Ratings Platform, which launched in 2021. He and the Cyber Risk team at Thomas Murray have engaged with 100s of banks, funds, market infrastructures, government agencies and other organisations to help them build long-term security.

Roland can be reached on LinkedIn at https://www.linkedin.com/in/roland-thomas-60a6a3125 and on Thomas Murray's website https://thomasmurray.com

A Modern Cybersecurity Fight Requires a Modern Approach to Regulatory Oversight

By Charlie Moskowitz, Vice President, Policy and Public Sector at SecurityScorecard

Cybercriminals never stop. Often they are supported, tacitly or explicitly, by a nation-state, pitting individual company security executives against the full force of rogue nations.

Companies cannot win this fight if left to defend their infrastructure alone. To secure the nation's IT infrastructure, regulators must improve collaboration with the private sector and modernize their approach by bringing stronger cybersecurity tools to their oversight efforts.

The cyber threat landscape and companies' security posture changes daily, if not hourly, yet underfunded regulators do not have the resources to audit every company even once a year. Government agencies still rely on infrequent audits and examinations, limiting the government's understanding of the true nature of the threat we face and leaving companies highly vulnerable to attack.

Cyber examinations, in other words, are a yearly (if that) solution to an immediate and ever-evolving problem. Regulators should no longer rely on annual paperwork and box-checking exercises that amount to an illusion of security.

New York Opens an Eye to Cybersecurity Oversight

In May 2022, the New York Department of Financial Services (DFS) announced its intention to incorporate cybersecurity ratings into its regulatory process. DFS regards cybersecurity as the top threat facing these companies. This is excellent news for the 3,000 businesses and organizations regulated by

DFS – including top banks, insurers and other financial services companies doing business in the heart of America's financial system.

DFS began looking at real-time ratings as a key component to their work as early as December 2019, as New York implemented new cybersecurity rules while fighting against an exponential increase in cyber attacks.

The use of ratings – grades based on a wide array of data taken from public and open sources – has helped DFS evolve its oversight in several ways. DFS can use the grades to match its limited number of audits to the most vulnerable organizations. Once an examination starts, ratings on 10 different subfactors point to specific security vulnerabilities ranked by criticality so examiners can prioritize their attention.

Ratings provide this defined set of metrics from an outside, impartial source in an easy-to-navigate online interface. In addition to ongoing monitoring, information from the ratings platform can be used to verify data that an audited organization provides.

Most importantly, ratings provide a quantitative assessment of cyber risk that allow DFS and the companies it regulates to speak the same language. Any company can now see the exact same data that DFS is looking at. DFS can also now compare organizations objectively against consistent data points to understand what the risk landscape looks like across the entire financial services industry operating in New York State.

Using cybersecurity ratings as part of a regulatory approach helps re-orient evaluations from a point-in-time paperwork assessment to a collaborative dialogue between company and regulator. It also completes the 360-degree view of an organization's attack surface: Complementing the purely internal view of a company's vulnerabilities, security ratings provide a hacker's-eye view, allowing organizations to think like a threat actor and stay one step ahead. These simple-to-understand grades can show leaders, boards, IT practitioners, and more what the company's platform looks like to someone trying to break in, using clear language and grounding it in objective third-party, publicly available data.

Taking Cybersecurity Ratings Across 50 States

New York DFS is one of the world's most important regulators, overseeing companies at the heart of the global financial system, regardless of where they are headquartered. But what does all this mean outside of New York?

New York DFS is leading the way for other regulatory agencies across the country by putting a firm stake for regulatory modernization in the ever-evolving ground of cybersecurity. DFS is pointing to cybersecurity ratings as a must-have for regulators in other states.

Achieving that sort of coverage – across America's 50 states, 5,000 banks and savings institutions, and more – is a big, beneficial goal. The advantage is safety in numbers. Each state that modernizes oversight makes it easier for other states to patrol their networks. States that do not modernize, however, will

continue to rely primarily on the static, infrequently communicated viewpoints of individual, regulated entities to defend against an enemy that requires collective, ongoing action.

We are safer together.

With this in mind, regulatory agencies should modernize their oversight by adding cybersecurity ratings to their box of tools. Otherwise, the nation's IT infrastructure won't be safe.

About the Author

Charlie Moskowitz is Vice President, Policy and Public Sector at SecurityScorecard. Charlie brings over 15 years of policy and regulatory experience to SecurityScorecard. Charlie comes to SecurityScorecard after two years at Signal Group, a bipartisan public affairs firm in Washington where he represented a variety of clients on issues ranging from child abuse prevention to cybersecurity to bringing more data science rigor to federal policy. Before that he spent almost a decade on Capitol Hill in policy and investigatory roles, ultimately serving as the Chief Policy Counsel for the Democratic staff of the Senate Homeland Security and Governmental Affairs Committee under Senator Claire McCaskill (D-MO).

Charlie can be reached on LinkedIn https://www.linkedin.com/in/charlie-moskowitz-8905a5b/ and at https://securityscorecard.com

Apes Gone Phishing

BAYC Attack Leads to $250,000 Loss

By Ronghui Gu, CEO and cofounder at CertiK

NFTs are one of the most headline-grabbing topics in web3, with the most popular being sold for jaw-dropping prices and generating a dedicated following of fans and collectors.

Anyone still in disbelief about the monetary value of NFTs should take a look at the recent hack against Bored Ape Yacht Club (BAYC), where a hacker was able to make away with 32 NFTs, and sell them for 142 ETH (equivalent to over $250,000) in a phishing attack.

In the attack, the hacker shared a fake phishing site that impersonated the official BAYC site. This malicious site then promised that BAYC, MAYC, and OthersideMeta holders were able to claim a free NFT once they clicked on a link.

The victims of the attack can be forgiven for being duped– not only was the fake site a near duplicate of the official BAYC site, it was also distributed over the official BAYC discord server after a community manager's account was compromised.

Shockingly, this is the third time that the BAYC servers have been compromised this year, and the second which has led to losses. On April 1st a hacker was able to access the BAYC discord server, causing BAYC to issue a warning to its community. Then later in the same month on April 25th, BAYC was hit with another phishing attack on its Instagram account, this time leading to the theft of 91 NFTs, equivalent to over $1.3 million.

The web2 hangover

Despite NFTs being seen as one of the most definitive products of the web3 ecosystem, the fact that an attacker was able to successfully use a phishing attack shows how projects are *still* vulnerable to hacks typically associated with web2.

The continued success of such phishing attacks is frustrating for anyone working towards securing the web3 ecosystem, as part of the promise of the decentralized nature of web3 is that it can consign such attacks to the past. However, so long as there remains centralization in web3, there remains the chance for hackers to exploit the single-point of failure that it offers. A recent State of Defi report shows that 'centralization issues were the most common attack vector, with over $1.3 billion lost across 44 DeFi Hacks'.

In the case of phishing attacks such as the BAYC hack, this point of centralization came in the form of a community manager's account, which gave the hacker the illusion of authenticity and lent their malicious link credibility it would not otherwise have had.

What to do?

While it is likely that there will always be some aspects of centralization in web3, there are still ways of implementing practices of decentralization into a project's structure to boost security. For example, BAYC could have better protected itself by requiring multi-sig verification to access privileged accounts and also any time a post or change is made.

This effectively distributes the authority across multiple nodes, meaning that the hacker would have had to compromise multiple accounts before gaining privileged access to the BAYC's discord.

How to manage accounts with privileged access remains a problem for many web3 projects, and it continues to lead to major losses when an attacker strikes. Ongoing security audits are one of the best measures teams can take to ensure their project has the best defenses, as it will highlight any areas where a hacker can leverage centralization to conduct an attack as the project grows.

Yet the risk of centralization is only half of the story here. There is also a need to cultivate a better community understanding of the risks involved in web3, and the best ways to spot bad actors attempting to trick you into giving away your assets.

Whilst all projects have a responsibility to their communities to keep their social media platforms secure, NFT holders should also be highly suspicious of anyone claiming to offer free assets, as these can often be disguised phishing attacks.

In the case of BAYC's June 4th attack, the malicious site had a few small differences from the real one. Firstly, unlike the authentic site, the phishing site did not provide links to BAYC's social media sites. There was also an added tab titled "claim free land" that specifically targeted popular NFT projects.

While subtle, these differences should alert any user to potential malicious activity. At the very least, users engaging with such giveaways should always make an effort to confirm the legitimacy of the site by comparing it with a known and confirmed site and looking for any discrepancies.

Looking Ahead

The persistence of phishing attacks alongside more sophisticated web3 attacks highlights the multiple frontiers on which the web3 ecosystem must defend itself. Web3 has the potential to be the most secure iteration of the internet to date. But to get there, web3 projects have to take an ongoing, end-to-end approach to their security. This means making use of tools such as routine smart contract audits, blockchain analytics, and implementing practices of decentralization. As the BAYC hack shows, failure to do so spells disaster not only for the projects, but for their communities as well.

About the Author

Professor Gu is the Tang Family Assistant Professor of Computer Science at Columbia University and Co-Founder of CertiK. He holds a Ph.D. in Computer Science from Yale University and a Bachelor's degree from Tsinghua University. He is the primary designer and developer of CertiKOS and SeKVM. Gu has received: an SOSP Best Paper Award, a CACM Research Highlight, and a Yale Distinguished Dissertation Award. You can find more information about CertiK here: https://www.certik.com/

As The Pandemic Persists, Hospitals Face New Cyber Vulnerabilities

By Jack Chapman, VP of Threat Intelligence, Egress Software

Regardless of where you are, local hospitals are a vital part of every community. More so than at any point in our lifetime, the past three years have tested these institutions. Thankfully, the widespread resilience of doctors, nurses, and staff has provided the rest of us with a benchmark for human capabilities and important glimmers of hope for the future.

But just as we have learned to live with one crisis, a new threat has presented itself.

Most hospitals operate from a complex, technical ecosystem that supports important machinery alongside a range of legacy solutions. In order to operate, connect, and communicate these ecosystems are increasingly reliant on WiFi.

Indeed, hospitals are a treasure trove of the Internet of Things (IoT), which is both a blessing and a curse. While there are significant technical benefits to the IoT approach it must also be understood that these systems may be attracting unwanted attention.

The truth is that wireless networks are one of the biggest vulnerabilities in healthcare, and one that is regularly taken advantage of by cybercriminals. In most cases, hospitals are public places that readily allow anyone - including cybercriminals - to walk in, connect and gain access and compromise unsecured devices.

There's an obvious irony that the same devices that save patient lives can also be the weak link for an entire hospital's network. In the face of cyber threats, devices connected to wireless networks - like MRI machines - are necessary to a hospital's capabilities. The idea of having them rendered unusable is not negotiable - or is it?

Knowing this, threat actors seek to gain access to hospital networks with the purpose of hijacking vital machines in order to hold them to ransom. Due to the fact that healthcare technology is incredibly expensive, cybercriminals are counting on the added pressure to pay because it's often felt to be a cheaper and faster solution than replacing a machine. Despite this, decryption keys, supplied by attackers, only work around 20% of the time.

For cybercriminals, gaining control of these machines is just the beginning. It's not just ransom payments that hackers are interested in - it's also data. Once they've accessed a machine, they can access patient data stored on the device or move laterally through the network to access protected health information (PHI) on other systems.

So, in addition to holding devices ransom, gangs are increasingly using so-called double extortion schemes to turn up the pressure on victims by threatening to expose or sell this data. Some criminals go even further through a method of triple extortion that uses hacked patient data to turn the screws on hospitals and further increases the chance of being paid a ransom.

Three Steps Hospitals Can Take to Protect from Cyber Attacks

Teams responsible for the technical ecosystems operating within hospitals should be following these

three steps.

1. Understand Your Ecosystem

Healthcare organizations rely on a vast network of legacy and IoT devices to carry out day-to-day operations, which makes it incredibly difficult to protect without full visibility of its scope and assets.

As more connected devices are added to the network, it can be hard for healthcare Chief Information Security Officers (CISO) - if the hospital employs one - to have full visibility of the devices in use, despite their best efforts.

Regardless of the makeup of the personnel, a hospital's security teams must regularly carry out a full audit of all IoT devices to assess their level of risk to the organization. Further to this are risk assessments that must be performed and subsequent action is taken before new devices are connected to the network.

With a more comprehensive understanding of the landscape, healthcare CISOs and/or security teams can take important steps toward mitigating risks and identifying vulnerabilities.

2. Segment Your Networks

Healthcare CISOs must adopt a strategy of segmentation and isolation of vulnerable devices – particularly those that don't have endpoint security. If a device doesn't require access to the internet in order to carry out its main function, then turn off its access. Build an allowlist to ensure devices can only connect to the networks and other devices that they need to, and isolate public networks from the rest of the network.

Doing this will enable security teams to prevent threat actors from gaining access via devices before they move laterally through the organization's networks. However, it's important to find a balance between effective segmentation and the smooth running of operations. To do this ensure that devices and information are still accessible to those who need them.

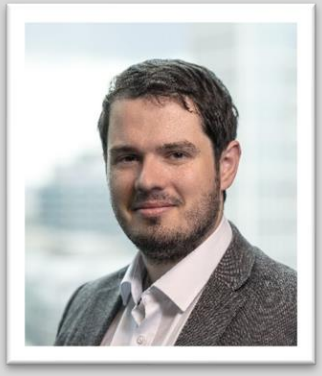
3. Patch, validate, and Test!

Healthcare organizations are increasingly appealing targets for cybercriminals. Because of this, it's a necessity that good security fundamentals are applied across not only technology but also people and processes throughout the organization.

These measures include patching, training, risk assessments, back-ups, disaster recovery, and prevention and protection software. However, often this is not enough.

Too often have organizations believed that they were properly protected when they were not. Due to the often complex and evolving nature of these organizations, it is also important to validate and test that the security that is in place achieves the objective.

About the Author



Jack Chapman, VP of Threat Intelligence at Egress Software. He is an experienced cybersecurity expert and serves as VP of Threat Intelligence at Egress, where he is tasked with deeply understanding the evolving cyber-threat landscape to remain one step ahead of cybercriminals. Leveraging these insights and his extensive R&D skillset, Jack oversees the product development for Egress Defend, an inbound threat detection, and prevention solution that mitigates all zero-day phishing attacks. Jack can be reached online at LinkedIn and at our company website https://www.egress.com/

Cyber EO One Year Later: Feds Weigh in On Progress, Areas For Improvement

By Brittany Johnston, Research Director, MeriTalk

In May 2021, President Biden issued the Executive Order on Improving the Nation's Cybersecurity (cyber EO), which included technology guidance and mandates pushing Federal agencies to improve their cybersecurity posture to better protect the American people.

The cyber EO came on the heels of several high-profile cyberattacks that plagued public and private sector organizations, including the Colonial Pipeline attack that caused gas shortages along the East Coast and the Solar Winds software breach that affected agencies and organizations across the public and private sectors. These incidents highlighted the cybersecurity vulnerabilities within government agencies and across our nation's critical infrastructure.

The cyber EO set a new tone for Federal cyber policy and aligned agencies under the same cybersecurity principals, including modernizing legacy technology, accelerating cloud migration, and implementing a zero trust architecture.

While the cyber EO provided direction, Federal cyber leaders were faced with work that needed to be done under accelerated timelines, limited budgets, and a shortage of trained technology experts in order to meet the mandates.

Even with that pressure, a new study from MeriTalk, underwritten by AWS, CrowdStrike, and Zscaler, found that 99 percent of Federal cyber decision makers say that the cyber EO had a positive impact on their agency, and 91 percent say that the cyber EO has made U.S. data and critical infrastructure safer. Most agree that the steps outlined in the cyber EO are necessary to protect our nation.

A Year of Progress

The study explores Federal technology leaders' perspectives on progress made against the cyber EO as we approached the one-year anniversary of its release. It identifies what agencies are doing differently and examines where agency cyber leaders say they need more help to succeed.

Over half of technology leaders confirm that IT management and staff are placing increased priority on cybersecurity. However, all agencies agree that progress against cyber EO goals is still in the early stages, with just 15 percent reporting tangible improvements because of cyber EO efforts to date. Agencies are making the most progress in creating a formal strategy, implementing endpoint detection and response solutions, improving software supply chain security, strengthening investigative and remediation capabilities, and migrating to the cloud.

While fewer than half rate of leaders rate their agencies' progress against key cyber EO goals as "excellent," a significant portion expects to see an impact within the next year.

Focus on Zero Trust

Many of the cyber EO mandates involve building a zero trust architecture, which is one that requires users and devices to be authenticated and authorized before accessing the agency network, applications, and data. A zero trust architecture includes several technology components including identity management, access control, and policy enforcement.

Ninety percent of technology leaders say that a zero trust architecture is an important factor for national cybersecurity, and 96 percent agree that the Office of Management and Budget's (OMB's) Federal Zero Trust Strategy is somewhat or very helpful.

Despite the high priority, just 30 percent of Federal cyber decisionmakers rate their zero trust progress as "excellent." Sixty-seven percent say the EO's three-year window for implementing a zero trust architecture is not realistic.

"Getting to zero trust is not easy. The detail provided in the multi-step guidance from OMB provides a path, but there is no single box you can buy to meet the varied needs of the five zero trust pillars," says Stephen Kovac, chief compliance officer and head of global government affairs, Zscaler. "You need multiple solutions from varying vendors that work together with seamless integration to achieve true zero trust – it is a team sport. OMB has done a good job in helping to define those rules, with rule one being to keep users off the network. If they can't reach you, they can't breach you."

When rating the most important factors in national cybersecurity going forward, technology leaders pointed to elements of a zero trust architecture, including multi-factor authentication and standardized event logging. Over the next five years, technology leaders point to endpoint detection and response capabilities – another element of a zero trust architecture – as the cyber EO requirement that will have the single greatest impact on improved cybersecurity.

"Zero Trust is the gold standard for cybersecurity, so we're encouraged to see the EO is prioritizing that approach," said Drew Bagley, vice president and counsel for Privacy and Cyber Policy, CrowdStrike. "In

addition, cloud-native endpoint detection and response capabilities can significantly strengthen the cybersecurity posture for the Federal government, especially when integrated with other security capabilities including identity security, threat intelligence, and managed threat hunting. These concepts have become cybersecurity best practices for the private sector's most technologically advanced businesses, and we encourage the public sector to continue to embrace these technologies and strategies."

Roadblocks to Achieving Cyber EO Mandates

While agencies are being asked to meet the aggressive mandates outlined in the cyber EO, just 14 percent report they have all funding needed to do so, and one-third say they have half, or less than half, of the funding needed.

"The sea change is the focus on comprehensive cyber resiliency," says Nicole Burdette, principal, MeriTalk. "The EO provided direction, but progress requires sustained funding and resource commitment. The research shows the gaps."

Eighty-seven percent of technology leaders also report negative impacts from the EO, including time-consuming proof of compliance requirements, moving IT staff from other projects to focus on the cyber EO requirements, confusion around competing priorities, and an increased cost with working with the private sector. Twenty-eight percent of technology leaders report that the cyber EO has created competition between agencies for trained staff or other resources, which is significant in today's environment where Federal agencies are already struggling to recruit technology talent away from the private sector.

To overcome resource issues, in addition to heavy recruiting and training, agencies should focus on automating repetitive tasks and minimizing any optional proof-of-compliance practices. Agencies should look to private-sector partners and utilize managed services for support where appropriate.

Private Sector's Role

When asked about the gaps in the cyber EO directives, 74 percent of technology leaders feel that the cyber EO should have been more authoritative with private-sector directives. After all, many critical infrastructure operators are privately held companies, like Colonial Pipeline.

"The U.S. Federal government is taking important steps to improve the nation's cybersecurity posture," said Dave Levy, Vice President of U.S. Government, Nonprofit, and Healthcare at Amazon Web Services. "In the cyber EO, the White House directs Federal agencies to adopt security best practices, implement zero trust architectures, and accelerate migration to secure cloud services. Organizations of all sizes should consider similar principles and practices to enhance their cybersecurity and protect employees and sensitive data against cyberattack."

In the year since the release of the cyber EO, progress has been made to share information with the private sector. The Cybersecurity and Infrastructure Agency has developed and implemented several

information sharing programs with the private sector and state, local, tribal, and territorial governments. Most recently, the U.S. Cyber Command has created a collaborative program called “Under Advisement” to share insights and information about critical cyber threats in an effort to further bolster national cybersecurity.

Sharing is a two-way street, and to help critical infrastructure operators that have experienced a breach, Congress included a mandatory reporting requirement in the Infrastructure Investment and Jobs Act.

A Look Ahead

Agencies that are behind the curve with EO implementation can accelerate their progress by appointing implementation leads with the authority to make bold changes. Agencies that graded their EO implementation as “excellent” were significantly more likely to have confidence in the cyber EO’s impact and report they are already experiencing the benefits.

With hackers constantly looking for new ways to outmaneuver existing security measures, agencies must continually prioritize cyber talent and adopt an active cyber mindset to remain ahead. Trusted industry partners can help agencies by providing scalable solutions and innovative approaches to realize the spirit of the cyber EO and guard against future attacks.

About the Author

Brittany Johnston is the Research Director for MeriTalk, where she develops and manages integrated market research programs for government’s top technology partners. With nearly 15 years of experience in survey design, data analysis, and insight development, Brittany helps Federal executives and their partners explore new technologies, uncover market opportunities and challenges, and identify strategic recommendations for improving the outcomes of government IT. Brittany can be reached online at bjohnston@meritalk.com, LinkedIn, and at our company website https://www.meritalk.com/.

Cyber Risk Management: The Right Approach Is a Business-Oriented Approach

By Michael Maggio, CEO & Chief Product Officer of Reciprocity

As rates of cyberattacks continue to increase – and organizations continue to grapple with how effectively they are protecting themselves – companies need to find better ways to safeguard every level of the business. Many are waiting for the next great technology solution to save the day. However, they're going to be waiting a very long time – as the problem isn't a technical one. It's a business issue. And the crux of the matter is that cybersecurity failures are often due to decision making failures, not technology failures.

While organizations have thrown money at the problem for years, the issue is that regardless of how large the investment, cybersecurity incidents are still happening and will continue to happen. History has shown that you can't outspend or outsource your way out of the situation (regardless of how much you might try).

The right approach is a business-oriented approach – one that balances an organization's risk appetite with prioritized investments to achieve a desired business outcome.

Putting your business priorities and outcomes at the center of your cybersecurity efforts should be at the heart of a strategic approach to IT and cyber risk management. By creating and managing programs that unify compliance, risk, vendor assessments, and other requirements around business objectives, you can gain the continuous, real-time insight and reporting you need to have data-driven business conversations that will help avoid and mitigate risk and prioritize the investments that optimize security.

As companies continue to struggle to effectively protect themselves, the imbalance between rising threats and low confidence is putting pressure on Security and InfoSec teams to clearly communicate risk in a way that enables leaders to make informed decisions that weigh risk tolerance, as well as cost and value, which are at the heart of every business decision. Understanding the implications of various options is what enables informed and effective decision making. An organization's cybersecurity investments shouldn't be any different.

Organizations should look to cyber risk management solutions that provide a unified, real-time view of risk and compliance that is framed around business priorities. This will provide the contextual insight needed to easily and clearly communicate with key stakeholders to make smart, strategic decisions that will protect the enterprise, systems and data – while earning the trust of customers, partners and employees.

Avoiding and managing risk in the context of business priorities and desired outcomes is imperative for facilitating productive business conversations with business leaders and executives so they understand the cyber implications of strategic decisions.

In a compliance program, controls are simply pass-fail. When the organization is "in compliance," it has met the minimum requirements under its obligations. But being able to say "we're compliant" is not the same as understanding to what extent implemented controls have effectively reduced the underlying risks. Compliance programs can be the foundation for establishing effective risk management with just a little more focus.

As compliance demands expand and become more complex, it becomes more difficult for companies to prioritize where to invest resources to respond to growing requirements. A better information security program moves on from "check-the-box compliance" to thinking more about risk and business context. This includes how compliance activities impact the broader organization and its strategic direction and goals.

No organization will ever have 'perfect' security. Businesses will always need to balance cybersecurity risks and investments against business value and outcomes. So, the goal should be to build a sustainable program that balances the needs to protect with the needs to run the business.

About the Author

Michael Maggio is the CEO and Chief Product Officer of Reciprocity. He is a serial entrepreneur and intrepreneur with a passion for building product teams. Leveraging leading-edge software stacks and complex data, he enhances existing solutions, creates new products, implements creative revenue models, optimizes operations and delights customers. Over his 30+ year career he has built startup companies from scratch to IPO in the automated testing and security spaces, reinvigorated enterprise product portfolios in F500 companies, such as CA Technologies and FIS, and has delivered cutting-edge products in mobile and location-aware markets. Michael has an MS in Computer Science from the University of Maryland and a BA/BS in Mathematics and Computer Science from Stonehill College

Michael can be reached online on LinkedIn and at our company website http://www.reciprocity.com/

Collective Resilience in an Era of Data Traps, Digital Borders, and Techtonic Geopolitical Shifts

By Andrea Little Limbago, SVP Research & Analysis, Interos

The technological explosion of the last few decades has not been accompanied by a similar modernization of global digital policies and standards. Discussions of a dynamic threat environment dominant security discussions with acknowledgement that the digital regulatory environment has more or less remained stagnant. However, thanks to a shifting geopolitical environment and renewed framing of data as a fundamental source of power, a sea change is underway.

Borders do exist on the internet, as ongoing regulatory shifts determine how data is protected or accessed and varies significantly from one country to the next. These opposing forces of data protection and government-mandated data access are reshaping data risks depending on an organization's global footprint, including its extended supply chain. Second, industrial policy is back in style, as geopolitical shifts and concerns over untrustworthy technologies are leading to a range of prohibitions regarding what technologies are restricted or allowed within an organization's tech stack – and that of their supply chain.

As digital transformation continues to upend business processes, these regulatory shifts further add to the complexity. The natural inclination may be to turn inward during such global transformations, but that would be a mistake. No single organization can build resilience against these dynamic shifts alone. Instead, collective resilience can help organizations better navigate the new normal of data traps, digital borders, and technology exclusions.

The Rise of Data Traps

In describing 'data traps', British Intelligence Chief Richard Moore warned, "If you allow another country to gain access to really critical data about your society, over time that will erode your sovereignty, you no longer have control over that data." This risk not only is true for governments but for the private sector, including the data risks introduced through their supply chain ecosystem.

For the most part, unauthorized data access by some form of a 'malicious actor' is the fundamental data risk. But what happens when the access is authorized through legal mandate? In a growing number of countries, there are legal requirements for data access in return for a physical presence and access to that market. Digital authoritarians – governments who deploy a range of digital tactics for information and data control – increasingly pursue legal paths toward data collection and access. Under the auspices of national security, government-mandated data access is the latest tool in the toolbox for many (largely authoritarian) governments who are legalizing government access to data upon request. Unlike the trend among many democracies that have a transparent judicial process for data requests, many new laws lack the judicial review and oversight.

China's Personal Information Protection Law (PIPL) and Data Security Law combine to enforce strict guidelines about data storage and data flows, but do not preclude data access by the government. Cambodia's data surveillance legislation permits monitoring on internet activity, intercepting and censoring digital communications, and collecting, retaining, and sharing personal data. And although Kazakhstan has failed at least three times in its implementation of a required government digital certificate that would allow the government to intercept all HTTPS traffic, Mauritius is now contemplating the same strategy, illustrating the spread of these programs into democracies as well. The era of borderless data is over and is giving rise to data traps abroad.

Technology Exclusions & Technospheres of Influence

Since Russia's invasion of Ukraine, the United States has sanctioned over 600 Russian companies, while security firm Kaspersky was added to the FCC's list of software they say poses a national security threat. This comes on the heels of the unprecedented wave of over 350 Chinese companies U.S. sanctioned between 2019-2020, the majority of which are tech companies. The United States is not alone in this renewed implementation of industrial policy. Across the globe, there is a geopolitically-driven bifurcation between trusted and untrusted technologies that is creating divergent technospheres of influence which present significant implications for cybersecurity and digital transformation.

The mandated exclusion of Huawei is perhaps the most prominent example of governments prohibiting a major technology supplier. Australia first excluded Huawei and ZTE in 2018, while many other countries have banned or introduced obstacles since then, including Sweden, France, Estonia, and most recently Canada in May 2022. In the United States, Huawei is one of five Chinese companies (along with Dahua, Hikvision, ZTE, and Hytera) and their affiliates that are prohibited under Section 889 of National Defense Authorization Act (2019) from being in the tech stacks and supply chains. In response, China has its own 'Unreliable Entity List'. And while governments continue to introduce regulatory shifts on 5G, the

competition over 6G is well underway, illustrating the tight coupling of technology, national security, and an increasingly splintering regulatory environment along geopolitical fault lines.

Of course, digital transformation during a time of growing technological divides is not only complicated but expensive. According to one assessment, it will cost US small carriers $1.8 billion to 'rip and replace' existing Huawei and ZTE equipment from their networks. A German estimate predicts an even larger cost, closer to $3.5 billion for their largest telecom provider. Acknowledging these significant costs – especially for small and medium businesses – the FCC approved a $1.9B replacement plan in 2021. However, in February 2022, this estimate ballooned to $5.6B in requests through the Secure and Trusted Communications Networks Reimbursement Program.

Given these significant costs for compliance, hyperconnectivity across supply chains, and divergent technospheres, no single organization can fully ensure its own resilience and security. Instead, there must be a shift in mindset toward a collective response among partners and like-minded organizations during such disruptions and uncertainty.

Toward Collective Resilience

Collective resilience captures this notion of strengthening defenses across an organization's entire supply chain ecosystem by pursuing strength in unity and providing collaboration and support to elevate the most insecure links within highly interdependent systems. At a strategic level, there has been a decisive movement toward collective resilience following Russia's invasion of Ukraine. There has been unprecedented and swift collaboration in the cyber domain among governments, the private sector, and the security industry. The Cybersecurity & Infrastructure Security Agency's (CISA) Shields Up campaign is remarkable in the speed and depth of extensive public/private sector collaboration and collaboration with allies.

This kind of collaboration must extend and persist beyond Shields Up and account for the digital regulatory sea changes underway. Given the one-two regulatory punch of growing global data access risks due to data sovereignty policies as well as technology-focused sanctions, there are significant advantages from defensive collaboration on the path toward trusted networks and secure supply chains. These benefits are only compounded when layering in the widespread geopolitical shifts underway. From incident response planning to information sharing to collaborative red teaming, there is no shortage of areas where joint planning and collaboration can strengthen an organization's entire supply chain ecosystem.

The perimeter has long been dead; now it's time to redefine security through collective resilience. The security strategies of the past are insufficient for the new normal and the geopolitical competition over technology and data. As CISA explained, protecting the nation's infrastructure requires a collective, coordinated effort. Whether it is avoiding data traps abroad or complying with technology exclusions at home, organizations are only as resilient and secure as the weakest link in their supply chain and it will require a collective effort among like-minded partners to navigate the ongoing transformations of the new normal.

About the Author

Andrea Little Limbago is a computational social scientist specializing in the intersection of technology, national security, and information security. As the SVP of Research and Analysis at Interos, Andrea leads the company's research and methodology regarding global supply chain risk, with a focus on globalization, cybersecurity, and geopolitics. Andrea is a Co-Program Director for the Emerging Tech and Cybersecurity Program at the National Security Institute at George Mason, an industry advisory board member for the data science program at George Washington University, a non-resident fellow at the Atlantic Council's GeoTech Center, and a board member for the Washington, DC chapter of Women in Security and Privacy (WISP). She has taught conflict studies and political economy in academia, was a technical lead in the Department of Defense, and has worked at several cybersecurity startups integrating social science fundamentals into analyses and models on attacker trends, human-computer interaction, digital authoritarianism, security and privacy regulations, and security culture. Andrea earned a PhD in Political Science from the University of Colorado at Boulder and a BA from Bowdoin College. Andrea can be reached online at @limbagoa and at our company website http://www.interos.ai.

Content Anarchy: The Lurking Security Risk in A Digital-First World

By Ellen Benaim, Chief Information Security Officer, Templafy

More than two years since the onset of the pandemic, remote and hybrid workplaces are here to stay. Research late last year from Gallup found that nearly half of full-time employees in the U.S. (45%) were still working from home to some degree, and there's no sign of hybrid work going away any time soon.

The hybrid work trend has further accelerated a pre-pandemic business movement towards a digital-first environment, also known as the "digital HQ." Now, businesses are rethinking everything from the way they structure internal communications to how they define business content. Today's definition of content encompasses traditional marketing materials like sales decks and social media copy, but it has also expanded to include business assets like legal contracts and metadata.

Recently, Templafy surveyed more than 600 full-time workers across the U.S. to better understand how the growth of content impacts the modern business. The research revealed that content creation is a massive part of today's typical work – on average, employees spend fifteen hours a week creating content. That's almost two full days.

As the amount of content used to conduct business on a day-to-day basis has grown exponentially – now any action with a digital record is new content – businesses are struggling to keep up. Many lack a strong content infrastructure to manage these workflows, allowing content to create risk – everything from security breaches to financial loss – instead of positive outcomes for a business. When this is how a business operates they're unknowingly submitting themselves to "content anarchy" and the only way to solve this is to implement technology tools to manage and govern workflows starting at the point of creation. And this is particularly important in documents, because they so often represent the health and

well-being of a business. Let's take a deeper look at how these risks manifest across a business and the potential solutions to solve for them today.

Manual classification leaves room for human error

Nearly every employee handles classified or proprietary information from time to time – in fact, 94% of our report respondents agreed with this statement. But in a digital business environment, where we've seen an uptick in asynchronous communication, the risk of accidentally sharing sensitive content within documents is higher than ever before.

Nearly two-thirds of survey respondents said their company lacked secure, system-wide alignment when it comes to content. Many companies still lack the technology needed to ensure privacy and security procedures are upheld, and instead depend on written processes and individual employees to properly classify and safeguard sensitive documents. Even worse, Templafy's study found that over half of respondents said their company had mistakenly shared sensitive documents with unauthorized parties. In today's hyperconnected world, where security and privacy are paramount, these types of mistakes not only open the door to lost business and revenue, but also damage to brand reputation and the risk of consumer complaints and fines from regulating bodies.

Regulatory requirements are evolving, content infrastructure must too

Industries like financial services, legal, healthcare and insurance have long been beholden to strict and ever-changing regulatory and compliance requirements. But in today's environment, every business must scrupulously attend to regulation requirements, including those in education, technology, and even retail, since the majority of business is conducted online and more user data is housed in the cloud than ever before.

For example, new privacy legislation in the United States like California's CCPA requires any company dealing with personally identifiable information to properly safeguard customer data. That's new territory for many companies, and demands they think about how this data is being used in business documents in order to ensure it is compliant. However, complying with these new regulations is next to impossible with the current tools being used to govern company content.

Unfortunately, there are major legal and financial consequences for companies that do not comply with regulatory requirements, and employees recognize this: 88% of respondents agree that security requirements are increasing and upholding them has never been more important than it is today. Yet until businesses evolve their content infrastructure systems to safeguard their content, they'll struggle to stay on top of ever-changing regulatory requirements.

The meta risk of metadata

With the proliferation of content over the past few years, businesses have also seen a proliferation in metadata. Metadata is increasingly important in helping businesses organize and secure content, yet nearly two-thirds (58%) of respondents in leadership roles admit they lack comprehensive knowledge on what metadata is or why it is important to business document management and creation.

Metadata is information that helps describe and classify content, and it plays an important role in driving business outcomes and reducing financial and brand risk. Enterprises can even use metadata to prove they're complying with the latest security regulations. A document governance system is essential to managing metadata, and without one, businesses are vulnerable to classification mistakes. In fact, three in five survey respondents agreed that a lack of control when it comes to metadata and classification poses a significant financial risk to the business.

Control and good use of metadata can help streamline workflows and ensure permission levels for sensitive content are upheld. Conversely, Templafy's survey found that poor metadata practices risk significant legal ramifications (67%); damage to reputation (66%); loss of customer trust (62%); and significant business risk (60%). Executives and technology leaders must not overlook metadata when developing their security and compliance strategies.

Templafy's research shows that managing content anarchy is paramount to protecting a business and benefitting the bottom line. Enterprises must implement content enablement solutions which will streamline content creation, govern documents and manage metadata, removing the brand and security responsibility from individual employees. Enterprises that invest in content infrastructure will see a return in the form of revenue, productivity, brand reputation and security. Those that do not may be left picking up the pieces.

About Ellen Benaim

Ellen Benaim is the Chief Information Security Officer at Templafy, the next gen document generation platform. As CISO, Ellen has developed Templafy's security-first approach and oversees company-wide information security and governance programs to ensure the organization follows all necessary protocols. This enables Templafy to provide the best, most secure platform to its customers as it aligns workforces and enables employees to create on-brand, compliant and high-performing business content faster.

Ellen started her career as technical support at Templafy, quickly attained the role of Information Security Officer due to her merit, and was promoted to Chief Information Security Officer in March of 2020. She holds a Bachelor of Science in Business Information Systems from University College Cork. Ellen can be reached online at linkedin.com/in/ellenbenaim/ and at https://www.templafy.com/

Crisis Point

How the skills shortage is threatening cyber security

By Jamal Elmellas, COO, Focus-on-Security

Finding sufficient talent has been a real problem in the cybersecurity sector for many years but, with demand growing on average 14 percent each year, the sector is fast approaching crisis point. The shortages are now becoming so acute that there's a real risk they could jeopardise the ability to maintain adequate cyber defences in a situation that is only expected to get worse.

The sector requires 17,500 new entrants per annum yet, according to the DCMS 'Understanding the Cyber Security Recruitment Pool' report, only 7,500 are entering the profession. Of these, just over half are graduates (4,000) with the remainder made up of those that have upskilled, changed career or come through apprenticeships, revealing an annual shortfall of 10,000 and growing.

It's a problem further exacerbated by a brain drain in the form of the Great Resignation, which has seen an exodus of workers following the pandemic. Stress and burnout are common complaints due to issues such as alert fatigue, with the Voice of the SOC Analyst report revealing that 71 percent feel stressed and 60 percent intend to resign over the course of the next year. That's on top of those 4-7,000 who usually leave the profession to retire naturally.

Under resourced, over exposed

What this means in real terms is that there will be less hands at the pumps and a dearth of expertise, leaving organisations under-resourced and over exposed. Consequently, when an incident does occur, it's likely that it will prove harder to mitigate. In fact, a report from the World Economic Forum found that

the majority said they would “find it challenging to respond to a cybersecurity incident owing to the shortage of skills within their team”.

There’s already evidence that this lack of people power is eroding cyber defences. The Cybersecurity Skills Gap Global Research Report found 80 percent of the organisations it surveyed worldwide had suffered one or more breaches that could be attributed to a lack of cybersecurity skills and 67 percent agreed that the shortage of qualified cybersecurity candidates was creating additional risk.

The report also looked at where those skills shortages were and found cloud security and security operations (ie SOC management, threat protection, endpoint security) and network security were the areas hardest to recruit for, suggesting these may well be the hardest hit. Interestingly, these are also the areas where we’ve seen the greatest automation over recent years, so could this provide an answer? Automation has the power to make a real and tangible difference in cybersecurity and in the SOC Analyst survey, 66 percent said between 50-100 percent of their workload could be automated and would welcome this particularly of repetitive manual tasks such as threat monitoring, triaging and reporting.

Robots to the rescue

Automation is also leading the charge in other areas, buoyed by the cloud. We’re seeing continuous monitoring solutions emerge, for example, in the form of Cloud Security Posture Management (CSPM) and also Continuous Automated Red Teaming (CART) for security testing and compliance. But the expectation is these tools will free up professionals and help them to specialise further, so that they’ll supplement manual resource rather than replace it, doing little to solve the skills crisis.

The reality is that there really is no substitute for human intuition and oversight when it comes to security, so as a sector we now need to think long and hard about how we will continue to ensure we have sufficient resources within the marketplace. Fighting over the same pool of talent from conventional routes such as universities is not sustainable and nor can we continue to favour technical skills and experience over tenacity and a willingness to learn.

It would seem we’re now at a tipping point in this regard, with the ISACA ‘State of the Cybersecurity Workforce’ survey revealing that, while experience, credentials and hands-on training were top factors in recruitment, other skills, from communication to critical thinking and problem solving, are now also being considered.

That said, a worrying trend is the expansive job remit. This is seeing many look for a ‘cyber unicorn’ who can deliver on multiple fronts leading to unrealistic job descriptions. For example, there have been reports of job adverts for CISOs requesting penetration testing experience. Consequently, some job posts are going unfilled for over six months not only due to the skills shortage but due to these unrealistic expectations.

Recruitment and retention

A far more effective strategy is to refine the recruitment drive according to the market, seek to adapt the employment package to meet candidate needs, and to prioritise staff retention. We've already covered the changing skillsets and the need to think beyond certifications and experience, but what are candidates looking for and how can we improve retention?

Funnily enough, the answer to both those questions is the same because, salary aside, the top reason for changing jobs given by candidates is career progression. It's a topic seldom dealt with at interview and often neglected during employment reviews, as evidenced in the ISSA survey that found 82% were dissatisfied because there was insufficient capacity within their role to develop their skills.

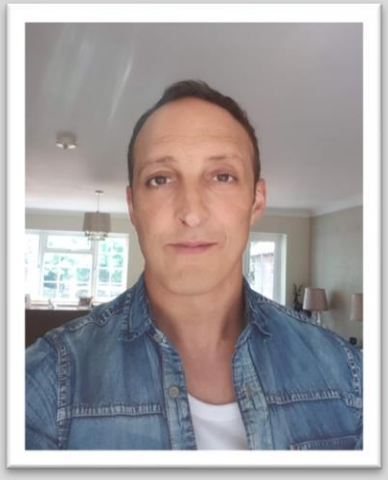
It's also one of the areas the security sector really struggles with, which is why the Cyber Pathways initiative, currently being thrashed out by the UK Cyber Security Council, is to be welcomed. The framework aims to align particular skillsets with job roles to provide employees with clear career objectives but it will also allow organisations to create career development programs and make it much easier to progress through the ranks. The pathways are currently being developed following a consultation earlier this year but expectations are these will be in place by 2025.

In the meantime, employers will need to adopt a more expansive approach and to widen their remit so that they can harness raw talent. It's worth remembering that many of the industry veterans we have today started out in other sectors. They're self-starters who often taught themselves and were able to climb the ladder due to their zeal and determination. It's that willingness to learn and natural aptitude that employers need to once again tap into to both fill the skills gap and protect their defences.

About the Author

Jamal Elmellas is Chief Operating Officer for Focus-on-Security, the cyber security recruitment agency, where he oversees selection and recruitment services. He previously founded and was CTO of a successful security consultancy where he delivered secure ICT services for government and private sector organisations. Jamal has almost 20 years' experience in the field and is an ex CLAS consultant, Cisco and Checkpoint certified practitioner. Jamal can be reached at and at the company website

First Name can be reached online at Jamal.Elmellas@focus-on-security.org and at our company website https://focus-on-security.org



Cyber Insurance: a fast-changing landscape

Focus on the evolving cyber insurance market in Europe for businesses, and the key factors that companies looking to buy cyber cover need to be aware of to make sure they secure the best deal

By Alta Signa Branch Manager Ingo Trede

It has become increasingly difficult for companies to find affordable cyber insurance in recent months, as the willingness of insurers to provide capacity for this market shrinks in the face of increased risk, and intense scrutiny from governments and regulators paired with heightened uncertainty

Considering the scale of global inter-connectivity and on-going digitalisation, it's not surprising that the number of opportunities and new methods of attacks opening up to cyber criminals is increasing. But even with the emergence of new techniques and approaches - such as the recent shift in attention towards pure destruction attacks - ransomware as a threat still remains a key concern.

This concern is so great that cyber attacks and data loss have been ranked as the most likely risk for a business in the global Directors Liability 2022 survey; and with the escalating war in Ukraine, such risks are unlikely to disappear off the top of peoples' radars anytime soon.

Along with fears of state-sponsored cyber attacks on European supply chains, there are also growing concerns that Russian sanctions could in fact be creating fertile ground for attackers. The recent attack, for example, on Oil India's field headquarters by the REvil hacker group, allegedly by Russian special

forces, which saw computers locked out in a large-scale ransomware event - may be a hint as to how the cyber war frontier is developing.

Political focus

Although European governments are becoming more active in combating cybercrime – such as the shut-down of Hydra Market, one of the largest darknet market-places where ransomware and related services were traded – legal boundaries around the cybercrime scene are still largely ambiguous.

A growing number of US States and countries around the globe are discussing the prohibition of ransomware payments; as it stands, when it comes to cyber insurance, a ransomware payment itself is not deemed illegal, unless the payment is made to a sanctioned country, person, or group.

This approach has implications on both the current and future state of cyber insurance, particularly as cyber risk is expected to become more political. Attacks on state agencies – such as that seen in Finland for example – to the attempted disruption of financial systems, as seen in Ukraine, are instances of such political motives. Similar situations have also been witnessed in Israel, where websites hosting liberal news agencies were taken down in an attack.

The targeting of industrial control systems – such as that undertaken by Russia's "sandworm" group on the Ukrainian electrical grid – and non-monetary driven attacks are also on the rise. This type of malicious software "bomb" is based on so-called "wiper" malware, and rather than holding files to ransom, the intent of the attack is to delete all files on an infected device and simply cause maximum dammage and interruption.

Insurance Industry response

This constant uptake of new tactics by cyber criminals means insurers have to constantly learn, understand and adapt to the changing cyber landscape - a move which ultimately makes way for new and updated regulations. The European Council Network and Information Security 2 (NIS2) Directive, which will require more types of companies to take stronger cybersecurity measures, is one such example of progressive governance in this field.

With cybercrime on the rise, quality cyber insurance is in demand across Europe; however, risk appetite is not, and some insurers have even stopped writing this line of business in certain market segments. The insurability of future attacks is also being brought into question, with ratings agency Moodys recently suggesting that if future attacks were to cause "widespread business interruption and economic disruption", they could "represent an uninsurable event".

The consequential paradox arises through hefty rate increases from the insurers to build reserves enabling them to sustain expected substantial losses that meet stringent budgets being even tightened due to the recessionary pressure.

The most effective and value-adding cyber policies are underwritten in line with core areas of the NIST cybersecurity framework. For those insurers who are in this marketplace, attention is being drawn towards wordings, exclusions and definitions, particularly in relation to the new non-monetary forms of attacks and the potential cumulative threat of spreading vendor attacks resulting in multiple insureds being affected as happened in the solarwind scenario. Policies try to control for capacity limits while requiring high risk mitigation measures,

Such cyber security includes – but is not limited to – ones that focus on detection, containment of a suffered attack, and the restorative abilities of systems. Clients should also have endpoint and server detections and response capabilities in place, restrictions on access and administration controls, as well as two factor authentication for accessing key systems and hardware, not to mention continuous testing and vulnerability scanning.

In short, insurers expect their clients to take the job of protecting themselves seriously. Companies without basic risk mitigation controls in place are likely to increasingly find that they are unable to secure insurance.

Finding the right coverage

As cyber security threats evolve, demand for expert insight and advice on coverage options will continue to increase, as will the type and availability of cyber insurance on offer. Cyber attacks represent a serious and growing operational and reputational risk to companies in Europe, and those corporations looking to secure effective cyber insurance in 2022 and beyond will need to understand their exposure to these risks and take active steps to improve their risk profile, working hand in hand with their insurance partner.

About the Author

Ingo Trede, Branch Manager at Alta Signa. Ingo started his career at Houston Casualty Company Global in Barcelona as a Financial Lines Underwriter at the German, Austrian & Swiss and Eastern European Desk. His main responsibilities were the development of the Swiss and Eastern European markets for both commercial and financial institutions accounts. His insurance product expertise includes all Financial Lines and Cyber for Financial Institutions. He further gained insights into Transaction Risk, Contingency and K&R Insurance through cross-selling initiatives in his former role at a leading specialty insurer. Ingo graduated from HEC Lausanne, Switzerland, in Economics (MSc) and further holds an LL.M. in Insurance law from University of Hamburg. He is fluent in French, Spanish, (Swiss-)German and English.

Ingo can be reached online at itrede@altasigna.com and at our company website https://www.altasigna.com/

EVERYONE is Part of the Security Team and Solution

By Jim Nitterauer, Director of Information Security, Graylog

Often, companies approach cybersecurity as a technology problem, forgetting that people and processes are also part of defending against threats. It's important to remember that those technologies exist to make people's lives easier and that people must be an essential part of security.

Effective cybersecurity requires purposeful collaboration across all departments, from senior leadership to individual contributors. Getting everyone on board with security requires setting goals that engage employees regularly, keeping leadership up to date, and demonstrating value back to the organization.

New Challenges in a New Landscape

Security - and security teams - are increasingly important to all organizations.

Today, customers want digital experiences, but they also expect organizations to limit data collection. Customers have higher security and privacy expectations today, especially as data breaches and ransomware attacks are often in the news.

This directly leads to the second challenge companies find themselves facing. In response to these news headlines, more governments are passing privacy legislation. While the General Data Protection Regulation (GDPR) is no longer new, we can't underestimate its impact on the regulatory landscape. In November 2020, Californians voted to update the California Consumer Privacy Act (CCPA), renaming it the California Privacy Rights Act (CPRA), which included several new, stricter requirements. The CPRA

is notable because it gives customers the ability to sue in civil court. In 2022, at least four more states - Virginia, Colorado, Utah, and Connecticut - will likely implement new privacy laws as well.

Finally, cybercrimes are financially lucrative and easier to commit than a bank robbery. Cybercriminals can make a lot of money stealing and selling data or holding it for ransom, especially with easy to deploy Ransomware-as-a-Service (RaaS) business models.

Situational Awareness - The Building Block of Teamwork

The key to creating a collaborative approach to security is going beyond the annual security awareness training. Security leaders need to surpass the compliance checkbox and continually remind people to think about security in their daily activities.

People get busy. They get focused on their work. They stop thinking about security. This makes sense, but it also creates problems.

The key is building a mindset of situational awareness. It's recognizing surroundings and changing activities accordingly. People pay less attention to their wallets when walking in an empty field than in a crowded city. Digital situational awareness is the same thing. In cybersecurity, situational awareness is about understanding what normal tasks look like and what daily workflows look like so people can recognize events outside of that normal. When people are working on a computer, reading emails, talking on the phone, and interacting with other people, they need to be just a little bit mistrusting and be able to analyze interactions that seem suspicious.

Best Practices for Building Collaborative Cybersecurity

As with everything else in cybersecurity, saying that something needs to happen is a lot easier than making it happen. However, security leaders can build this teamwork mentality by engaging everyone across the organization.

Get Everyone Involved

The first step to creating a collaborative security program is talking to people. Posing these two simple questions to everyone across technology and line of business can give security leaders insight they didn't have before:

- What are the risks that you see that the company's not addressing?
- What would you recommend we do to fix that problem?

The first question can provide visibility into new risks. People in different roles see risk differently. New perspectives can shine a light on risks that the security or IT team may not have seen or understood.

The second question helps reduce risk by getting people involved to buy into the implementation and maintenance of the control. When people feel ownership over creating processes, they're more likely to follow them, whether it's change management, code commits, QA reviews on the development team, or user access to marketing websites.

Communicate Responsibilities

Clearly communicating responsibilities to people is fundamental. People need to know the definition of their responsibility from:

- An operational perspective
- An ownership perspective
- A compliance perspective
- A security perspective

Mature companies often have these roles and responsibilities clearly defined. It's important that organizations create these definitions as soon as possible because waiting until the company "gets big enough to need it" leads to technical debt. In a small company, it's easier to implement because there are fewer people, then it can iterate as it grows by evolving the roles, definitions, and responsibilities.

Identify Critical Teams and Start There

Identifying a critical team is a good starting point for security leaders who feel overwhelmed. For example, a development company might find its DevOps team and processes are the most critical.

Now, it can:

- Create well-defined roles
- Establish segregation of duties
- Explain responsibilities from operational and compliance perspectives

Engage in Routine Self-Assessment

After implementing controls, it's important to make sure they're operating effectively. This usually means implementing routine self-assessments to make sure people are following processes. It also usually includes some form of documentation to prove compliance.

For example, monitoring user access can prove control enforcement after implementing segregation of duties within the DevOps team. Monitoring user access can show holes in processes and potential points of improvement. Having documentation proves that the controls are operating effectively for the compliance team.

Find Security Ambassadors

You can find security ambassadors on any team – both at the technical and line of business levels – to participate in the security program and spread situational awareness within their team. They feel a sense of ownership and care about security.

This is another area where companies often forget that security is about people, not just technology. Not all controls are technical. Security ambassadors can help identify risks and implement controls within their teams. Then, the IT or security team can use technology to document whether the controls are working.

Access management is a perfect example of this. Managers are the ones who best understand their employees' needs and should define who can access what. The definitions and decisions aren't technical. The technical aspect is in the setting and monitoring of the access. Many smaller companies use their centralized log management to monitor user access, changes to data, and data exfiltration, all of which prove whether or not the access controls are working.

Security is a Team Sport

Getting everyone on board with security starts by getting the buy-in from technical and non-technical staff. Security starts with people because they're the ones who use technology. Technology should exist to support them.

For many IT teams, security tools can feel overwhelming. They're complex and time-consuming. Most teams can't use all the features and functionalities that would allow them to manage security more effectively.

However, they do know how to use and optimize monitoring and visibility tools and how to share information from them. Finding the right technology that enables people rather than hinders them is the way to communicate successfully so that everyone within the organization understands their role and participates effectively.

About the Author

Jim Nitterauer is the Director Information Security at Graylog. He holds the CISSP and CISM certifications in addition to a Bachelor of Science degree with a major in biology from Ursinus College and a Master of Science degree with a major in microbiology from the University of Alabama. He is well-versed in ethical hacking and penetration testing techniques and has been involved in technology for more than 25 years. He stays connected with the InfoSec and ethical hacker community and is well-known by his peers. In addition to his work at Graylog, he devotes his time to advancing IT security awareness and investigating novel ways to implement affordable security.

Jim can be reached online on Twitter @Jnitterauer, LinkedIn and at our company website http://www.graylog.com

The Future of Cybersecurity in SaaS

By Sean Malone, Chief Information Security Officer, Demandbase

Security for Software-as-a-Service (SaaS) solutions has been a priority since the inception of this technology, but it's become even more essential over time. As the number of platforms has increased, so has the volume of data that SaaS companies gather, store, and use. At the same time, it's recently been found that 40% of all SaaS assets are unmanaged, leaving companies and their customers at significant risk of security incidents and data breaches.

With this in mind, SaaS organizations can no longer take a status quo approach to cybersecurity. It's time to modernize and improve. Here's a look at how, and what the future of cybersecurity in SaaS needs to look like to ensure the protection of consumers, companies, and ever-increasing volumes of sensitive data.

The Current State of Security in SaaS

Today, cybersecurity in this segment of the tech industry is highly variable. Some SaaS companies handle their security programs extremely well, while just as many (if not more) struggle to do so. Most SaaS platforms are built on Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS), operating with a shared responsibility model. This means that there are components of the security responsibilities that the IaaS or PaaS cloud provider operates, and then there are components that the company building a SaaS product on top of that cloud environment is expected to operate. This setup can be challenging, as there are many competing priorities, particularly for early stage and hyper growth SaaS companies.

The Catalysts for Change

Even when SaaS companies are aware of their responsibilities and the need to tighten up their security, it can be hard to carve out the time, energy, and resources to make that happen. For many, it's downright overwhelming. Because of this, they might kick the can down the road and wait to make meaningful changes until it's too late.

In addition to the security concerns, this frequently presents a compliance risk for privacy regulations as well. Typically, companies that struggle to protect their infrastructure and manage the security of their data will also struggle with meeting customers' privacy expectations for that data. Both B2B and B2C organizations are feeling the squeeze of selling to customers who are increasingly concerned about the security and privacy of their data. As consumers continue to demand more from companies, companies will have to improve their cybersecurity and data management in order to earn — and keep — customer trust.

How to Implement Forward-Looking Quality Management

As SaaS organizations look to prudently manage the security and privacy of their platforms, there are some key points to keep in mind. First, building on top of cloud platforms as if they're just another data center is not an effective strategy. Even with containerized software, treating a cluster of servers as if it were a cluster of servers in an on-premise data center results in brittle environments that are difficult to secure and manage. This approach requires more manual changes, and fails to take advantage of the agility and resiliency offered by cloud-native architectures. More importantly, though, it increases the likelihood of making critical mistakes in that environment. This is because, more so than with on-premise tech, you're typically only one configuration change away from creating a significant security issue. Instead, here's a look at how the savviest SaaS companies handle quality management now - and in the future:

Automating deployment of cloud architecture through infrastructure as code (IaC).

This has multiple security benefits, but one of the primary benefits is that it lets you scan the architecture definitions, just like you scan any other code prior to deployment. So you can identify issues before anything touches a production environment. This also enables the next key item, which is…

Drastically minimizing manual changes in production environments.

It's critical you roll out changes through IaC through a version-controlled, peer-reviewed software repository as part of a standard development practice. And beyond this, seek to eliminate human access to production environments altogether. As humans, we tend to make mistakes when implementing changes manually, so if you create an entire discipline around automated testing, peer review and version-controlled repositories when it comes to infrastructure management, you'll have more securable (and more stable) environments.

Working closely with product teams and engineering teams.

The final key to top-tier quality management of the future is to collaborate with product and engineering teams to integrate security requirements into the normal research and development processes. Your ability to secure the environment will depend on a great relationship with these teams.

Key Milestones & Metrics

If you're wondering how to measure forward progress toward handling cybersecurity as the future will require, here are some questions you can consider and metrics you can measure:

To what extent are security requirements fully baked into product requirements?

To what extent does the product team proactively reach out to the security team to think about security early in the process?

What percentage of infrastructure is deployed as IaC?

What percentage of both infrastructure and application code is automatically scanned for security issues before going into production?

When issues are identified, how long do they take to resolve?

These are all areas to be reviewed and quantified, when possible, in order to gauge improvement. And, you can put metrics around these at individual engineering team levels. This helps you evaluate the security performance of an individual engineering team, and then aggregate that to engineering departments. You could even gamify security, by making it a friendly competition and using these metrics as a way to raise the bar on engineering security across the entire organization.

Great Security Depends on Great Engineering

Above all, one of the main tenets of product security is that it is either strengthened or weakened by the quality of engineering practices — and this is not going to change anytime soon. If anything, as we move into the future, SaaS organizations' security will only be as good as their operational practices and architectures can support. So, by driving quality expectations throughout the entire research and development organization, you can create more securable platforms.

This requires robust, resilient architectures, IaC that reduces manual access, knowing where your data is and how it's used, and thorough documentation around all of it. Great engineering practices may not technically fall under the umbrella of cybersecurity, per se, but they enable a security team to embed security controls in an efficient manner. They also can make you less dependent on manual changes by humans, which we know are where the lion's share of security breaches originate.

What is the Future of Cyber Security in SaaS?

As SaaS platforms continue to be created, elevated, and relied upon, the data they capture and store will also grow. It's every SaaS company's responsibility to not only implement the minimum requirements, but to look ahead to what future expectations will be and start planning to exceed them now. This will help organizations ensure that they can earn customer trust and loyalty, and that our data-rich world will stay secure for all.

About the Author

Sean Malone is the Chief Information Security Officer at Demandbase. In his role, he is responsible for the information security and IT functions. Prior to joining Demandbase, Malone led information security, delivery, product, and R&D for VisibleRisk, which was acquired by BitSight Technologies. Prior to that, he was Head of Cyber Defense for Amazon Prime Video, and previously spent ten years in offensive information security, performing red team engagements and cyber defense consulting for major financial institutions, casinos, gold mines, social media platforms, and similar high-value targets. Malone holds an MS in Information Security & Assurance, as well as the CISSP, CISM, CISA, CCISO, AWS Solutions Architect, and AWS Security Specialty certifications. He's active in the security community, including presenting research at Black Hat, DEF CON, and other conferences. He has a patent pending for his work on assessing security programs and quantifying cyber risk.

Sean can be reached online at https://www.linkedin.com/in/seantmalone/ and at our company website https://www.demandbase.com/.

GDPR: Four Years After Its Enactment, Where Do We Stand?

By Kevin Kelly is the VP and GM, Global Compliance Solutions, Skillsoft

More than 15 years ago, the expression “data is the new oil” was popularized and it seemed to signal the start of a corporate race defined by facts, figures, demographics, and psychographics.

In the period since businesses and business categories have been predicated on the collection and use of personal data.

Needless to say, data privacy is a complex issue for most organizations, and it has been made even more complicated by legislation such as GDPR. Four years later, GDPR compliance is something that many organizations continue to struggle with for a variety of reasons. In fact, just looking at the GDPR enforcement tracker, we continue to see related fines and penalties – ranging from a few thousand to hundreds of millions of dollars – being issued on a weekly basis.

So, where do we stand now that a few years have passed since GDPR went into effect? Let’s explore.

Data As a Fundamental Right

In speaking with business leaders whose responsibilities include data privacy and complying with GDPR, I have learned that companies are finding ways to apply the law in a practical way.

In the global marketplace, not all data is treated equally. In Europe, data privacy has become a fundamental right for the individual. While the collection of personal data from digital trackers in the Eurozone is automatically opted out, in the U.S. it is automatically opted in.

Needless to say, in the U.S., when it comes to the process of data collection, there seems to be a disconnect about how this intersects with data ethics. However, high profile issues related to this and specifically about GDPR compliance have many with governing responsibility revisiting their understanding of the overall issue.

Regardless of where you come from or the geographic footprint for which you are responsible, GDPR compliance can be a costly and confusing commitment. Let's review the basics.

What Is GDPR?

GDPR is a set of rules created to secure the personal information of EU citizens. GDPR is applicable to organizations with more than 250 employees that handle personal data in the process of trading goods and services within the EU.

One of its goals is to bring data protection protocols up to speed with new and unprecedented ways in which information is now used. GDPR also looks to empower individuals (or "data subjects") by giving them the right to challenge how, what, when, and why data is held about them. Data subjects have the right to access any information a company holds on them, and the right to know why and how that data is being processed, how long it's stored, and who gets to see it.

The enforcement deadline for full GDPR compliance was May 25, 2018. Since then, GDPR has prompted significant improvements in the governance, monitoring, awareness, and strategic decision-making regarding the use of consumer data. Not only that, but GDPR legislation has pushed the topic of data privacy to the forefront.

Why Do We Need GDPR?

GDPR obliges organizations around the world to take data protection more seriously than ever before, primarily because their reputation now relies on it – and because the penalties are crippling. One of the ideas behind GDPR was to assure consumers that their data would not fall into the wrong hands. Consumer data and privacy is now considered a top priority by leading companies.

The simple truth is that data privacy legislation provides organizations with a genuine opportunity to reconsider their data strategy and governance.

GDPR has brought some cost savings and improved efficiencies by forcing companies to address archives of data and ask whether the information collected is necessary or fit for purpose. Data maintenance has therefore become a more active process that is managed regularly.

GDPR has also encouraged organizations to assess the efficacy of their networks. Many have had to migrate over to improved infrastructure – enabling them to better align with the latest and emerging generations of technology as old hardware is replaced with more capable (and secure) devices. While initially expensive, this has been offset through an improved user- experience for employees that promotes greater levels of engagement and productivity.

At an even higher level, GDPR has empowered the public by improving trust in the emerging digital economy. By streamlining data protection across the EU (and effectively the world), goods and services now flow more freely. Confidence between organizations and the public has increased.

What Are GDPR Compliance Requirements In The U.S.?

Even if an organization is not physically located within the EU, it must still comply with GDPR if they handle personal data that is identifiable to a resident that is located within the EU. GDPR reaches into companies based in the U.S. because it is designed to protect the personal data of individuals.

The vast majority of companies whose business relies on consumers' personal data conduct themselves in a respectable and responsible manner. For these organizations, simple changes to data privacy regulations should not change the forecast for success.

Multinationals may choose to separate their U.S. and European business operations to take a more focused approach to GDPR compliance. In fact, the data privacy laws enacted by the state of California (California Consumer Privacy Act, CCPA from 2018) should have prepared any compliance officer to the issue of data privacy and put in motion structural changes within their business to adhere to this legislation.

GDPR Best Practices

GDPR has seven fundamental principles to ensure an individual's rights and security of sensitive personal information is used for illegitimate purposes. Organizations must think about each of these principles regularly to ensure compliance:

1. Accountability: Are you doing everything you can to comply with GDPR principles?

2. Accuracy: Is the data you've collected on individuals both accurate and up to date?

3. Data Minimization: Have you only collected data that is necessary to perform the task the information is intended for?

4. Integrity and Confidentiality: How do you always assure the security and privacy of personal information?

5. Lawfulness, Fairness, and Transparency: Is all the personal information in your possession processed lawfully?

6. Purpose Limitation: Does all the personal information you've collected have a lawful and legitimate purpose?

7. Storage Limitation: How long do you hold on to personal information?

The sheer volume of data for regulators to monitor is overwhelming, so it would be reasonable to expect them to concentrate their efforts on only a small number of organizations that have raised a red flag in some way. Most organizations are not really evaluated or scrutinized; they are simply continuing to build their own paths toward compliance.

What GDPR Help Is Available?

Fortunately for companies that want to train employees to comply with regulations such as the GDPR, there is no shortage of tools and resources. Compliance training courses help employees understand their responsibilities in mitigating the risks surrounding GDPR to help organizations acknowledge and adhere to best practices.

Microsoft recently noted that there are more than 200 updates issued by 750 regulatory bodies around the world every day. With that, identifying a compliance training partner that rigorously updates content via a team of experts to assure training is up-to-date and accurate is essential to executing and maintaining a successful program.

About the Author

Kevin Kelly is the VP and GM, Global Compliance Solutions, Skillsoft. He leads Skillsoft's Global Compliance Go-To-Market initiatives, including Legal Compliance, HR Compliance, Corporate Ethics, Cybersecurity and Data Privacy, and Workplace Safety. Kevin has more than 20 years of experience delivering business transformation in the compliance, legal, digital, and SaaS markets.

Kevin can be reached via LinkedIn at https://www.linkedin.com/in/kevinjkelly1/ and at our company website https://www.skillsoft.com/

Global Shipping Industry Faces Wave of Cyber Threats

By Capt. Rahul Khanna

Commercial insurer Allianz Global Corporate & Specialty just released its latest Safety & Shipping Review, an annual analysis of shipping losses and accidents worldwide. The international shipping industry is responsible for the carriage of around 90% of world trade, so vessel safety is critical to the global economy.

The 2022 report reveals that the maritime sector continued its long-term positive safety trend over the past year with 54 total losses of vessels reported globally, compared with 65 a year earlier. This represents a 57% decline over 10 years (127 in 2012); while during the early 1990s the global fleet was losing 200+ vessels a year. The 2021 loss total is made more impressive by the fact that there are an estimated 130,000 ships in the global fleet today, compared with some 80,000 30 years ago. Such progress reflects the increased focus on safety measures over time through training and safety programs, improved ship design, technology and regulation.

However, the industry is not without its challenges. Russia's invasion of Ukraine, costly issues involving larger vessels, crew and port congestion and managing decarbonization targets, means there is no room for complacency.

Another growing challenge facing the shipping industry is cyber security. The digital era may be opening up new possibilities for the maritime industry but its growing reliance on computer and software and increasing interconnectivity within the sector, is also making it highly vulnerable to cyber-attacks. All four of the largest shipping companies, Maersk, Cosco, MSC (and CMA CGM), have been victims of cyber-attacks in recent years. Port operators have also been affected. Even the United Nations' global shipping regulator, the International Maritime Organization was recently targeted by a cyber-attack, forcing some of its services offline. In particular, ransomware has become a global problem.

According to a recent industry survey just under half (44%) of maritime professionals reported that their organization has been the subject of a cyber-attack in the last three years. Of these, 3% agreed to pay a ransom, which averaged at around $3mn. It also found 32% of organizations do not conduct regular cyber security training while 38% do not have a cyber response plan.

To date, most cyber incidents in the shipping industry have been shore-based, such as ransomware and malware attacks against shipping companies' and ports' database systems. But with the growing connectivity of shipping, the fact that geopolitical conflict is increasingly being played out in cyber space – recent years have seen a growing number of GPS spoofing incidents, particularly in the Middle East and China, which can cause vessels to believe they are in a different position than they actually are – and with the concept of autonomous shipping, there is little doubt that cyber risk will become a more important exposure that will require much more detailed risk assessment going forward.

At the same time, the crippling ransomware attack against the 9,000km long Colonial oil pipeline in the US in May 2021 has raised concerns that critical maritime infrastructure, could be increasingly targeted in future. The attack resulted in the pipeline's systems, which connect some 30 oil refineries and nearly 300 fuel distribution terminals, being forced offline, resulting in petrol shortages across the eastern US.

As geopolitical risks rise, so does the prospect of malicious digital disruption. Security agencies have warned of a heightened cyber risk due to the conflict in Ukraine. NATO warned vessels in the Black Sea faced the threat of GPS jamming, Automatic Identification System (AIS) spoofing (prior to the Ukraine invasion there had already been a number of these incidents, reported in the Middle East and China), communications jamming and electronic interference. The US Cybersecurity and Infrastructure Security Agency also warned the maritime transportation sector could be a target for foreign adversaries.

There is concern that shipping assets and ports could become collateral damage if the conflict in Ukraine results in an increase in cyber activity.

Marine insurers have been warning for years about the cyber risk to shipping. From a hull perspective, the worst-case scenario is a terrorist attack or a nation state group targeting shipping in a bid to inflict damage or major disruption to trade, such as blocking a major shipping route or port. While this would seem a remote possibility, it is a scenario we need to understand and monitor. Although an accident, the recent blockage of the Suez Canal by the ultra-large vessel Ever Given is an eye-opener on many fronts as it shows the disruption a momentary loss of propulsion or steering failure on a vessel navigating a narrow waterway can cause.

The good news is that the shipping community has grown more alert to cyber risk over the past couple of years, in particular in the wake of the 2017 NotPetya malware attack that crippled ports, terminals and cargo handling operations. However, reporting of incidents is still uncommon as owners fear reputational risk and delays from investigations. Meanwhile, cyber security regulation for ships and ports has been increasing. In January 2021, the International Maritime Organization's (IMO) Resolution MSC.428(98) came into effect, requiring cyber risks to be addressed in safety management systems. The EU's Network and Information Systems Directive also extends to ports and shipping. This is a step in the right direction but the problem at the moment is quite extensive. Despite these measures we have seen a sharp rise in attacks.

Increased awareness of – and regulation around – cyber risk is translating into an uptake of cyber insurance by shipping companies, although mostly for shore-based operations to date. Typically, marine hull insurance policies exclude coverage against cyber-attack or any loss arising from a malicious act involving the use of a computer system, given the potential loss accumulation issues from such scenarios. Instead, shippers have to purchase standalone cyber insurance coverage, but to date the readiness of many in the sector to buy a marine hull specific cyber cover has been limited.

However, the threat to vessels is growing as more and more ships are linked to onshore systems for navigation and performance management. Smart ships are coming, and we would expect demand for insurance to develop accordingly. What we may see in the future is a potential increase in demand for a combination of onshore/offshore coverage and this is something we will need to discuss and observe with our clients and brokers to see how far this can be taken by marine hull insurance and how far it can be taken by a broader scope of cover in a combined policy.

Fortunately, there are also a growing number of resources available to help mariners learn about common vulnerabilities. Just one example is the internationally-recognized United States Maritime Resource Center, which assists the industry in cyber awareness, safety and security through evidence-based research. Then there are an increasing number of cyber security guidelines which can be followed, such as those from the IMO, but also from other important organizations such as BIMCO, CLIA, Intercargo and Intertanko.

There are also standard practices that can be implemented to reduce cyber risk, such as defining personnel roles and responsibilities for cyber risk management and identifying the systems, assets and data that, when disrupted, pose risks to ship operations. Ship-owners also need to implement risk control processes and contingency planning, developing and implementing activities necessary to quickly detect a cyber event. Identifying measures to back up and restore cyber systems impacted by a cyber event is obviously crucial.

Of course, these are challenging times for the shipping industry. However, IT security should not be put on the backburner. It is vital that investment in cyber risk education and security is not neglected at this time, despite economic pressures, as this risk has the potential to have catastrophic consequences, given the right confluence of events.

To read the full Allianz Safety & Shipping Review 2022, please visit https://www.agcs.allianz.com/news-and-insights/reports/shipping-safety.html

About the Author

Rahul is the Global Head of Marine Risk Consulting at Allianz Global Corporate & Specialty (AGCS), one of the largest insurance companies in the world. Based in London, he leads a global team of marine risk consultants who support the marine underwriting function in Marine risk selection and loss prevention at Allianz.

Rahul is a qualified master mariner who has spent 14 years at sea sailing on oil tankers and bulk carriers and moved ashore after sailing as a captain for 2 years.

Rahul joined Allianz in 2011 as a senior risk consultant and took over as Global Head of Marine risk consulting in 2014. In his current role he focuses on risk consulting strategy for the global marine business of AGCS.

Rahul can be reached online at @CaptRahulKhanna and at our company website https://www.agcs.allianz.com/.

How Bad Actors Are Learning to Hack Humans in Phishing Attacks

Phishing Attacks Continue to Grow Because Cyber Criminals Have Learned Which Psychological Buttons To Push

By Franco De Bonis, Marketing Director, VISUA

The last report issued by the APWG (Anti-Phishing Working Group) made for grim reading. In it, they reported that 316,747 phishing attacks were detected in Dec 2021; the highest monthly number in their reporting history and more than double the number of phishing attacks compared to early 2020. This figure was so troubling that we decided to do a historical deep-dive and compare the data over a number of years. You can see our full analysis here, but in short, one of the most troubling trends is the continued growth in brand spoofing, which reached an incredible peak of 715 separate brands and organizations being spoofed as of September 2021; a more than 200% increase since January 2108. Meanwhile, they have been busy spinning out phishing web pages, which are the key mechanism used to have victims give up their credentials and other personal details, or to download malicious files. In fact, this activity saw a more than 400% increase over the same period.

So it seems that bad actors are reducing the number of themes or subjects used in email attacks while targeting more brands and using more web pages to 'convert' recipients into victims. But why have they latched onto this specific attack methodology? The simple answer is because it works! It also helps that it's really quick and easy. Bad actors are not lazy by any means. Actually, they have shown themselves to be immensely resourceful, but the old adage of 'work smarter not harder' most definitely applies here.

A study by UC Berkeley over a decade ago showed that well-designed fake sites were able to fool more than 90% of participants. With so much work having gone into staff training, one would hope that this number would have decreased significantly, and in a recent study by Canada's Terranova Security, the

number does seem to have reduced, but still remains at an alarming 20% of recipients being fooled into clicking a malicious link in a fake email or website. This means that of every ten recipients of a phishing email in an organization, two will take action that could lead to a compromise of the company systems or data. Further, according to Deloitte, 91% of all cyberattacks begin as a phishing email.

It's clear, therefore, that bad actors understand that this is a numbers game. Many experts and pundits across the cybersecurity sector have uttered variations of the phrase 'we have to stop phishing emails reaching every single person while they only need to fool one!' This highlights that bad actors are using human nature and emotional factors to hack what is currently a technology-oriented protection system. They are exploiting four key elements in everyone's life; trust, lifestyle, urgency and confidence.

Trust:

Companies work really hard and spend a lot of money to build trusting relationships with their customers. Bad actors exploit this by very closely imitating the communications of these companies. Often they will use pixel-perfect copies of existing communications, manipulated to achieve their goals. But they also work off the trust we have in individuals. An example of this is when you receive a link to an online document from a 'colleague', which when clicked asks you to login to your Google or Microsoft account. But this login form/page is fake, so when you login they now have your credentials. The really smart scammers will even forward on your own credentials to the real service, effectively logging you in for real, so you never even know that you've been phished!

Lifestyle:

Our lives are busier and more hectic than ever. We are in a multi-screen era, often on our phones while watching TV and switching between tasks all the time. We struggle to balance work and family life and this all creates stress and a FOMO (Fear of Missing Out) and FOF (Fear of Failure). Add to that our constant access to email and the web through our smartphones and you have a recipe for potential disaster as people look to action a request when they're tired or frazzled..

Urgency:

Bad actors use this frenetic pace of life against us by adding a sense of urgency to communications. "Your account will be suspended if you don't confirm your account details", "Your shipment will be returned if you don't confirm your credit card details". Just two examples where urgency can help overcome doubt when we're busy and/or stressed; because nobody has time to fix a lapsed account or track down a missing parcel!

Confidence (see Over-Confidence):

It is most definitely true that anti-spam and anti-phishing systems have done a great job in reducing the levels of malicious content we receive and training has helped to educate. But that can work against us. If you don't get a lot of phishing emails you may be over-confident about the capabilities of the technology protecting you. Likewise, if you have had training on how to spot a phishing email, you may be overconfident about your ability to know if an email or web page is fake or genuine. So when one does slip through, you may well be more trusting about its authenticity than you should be.

High-Tech Solution To A Low-Tech Problem

By combining these factors with relatively simple techniques, bad actors are seeing great results that achieve their goals. But the anti-phishing industry is focused on AI that targets programmatic attack vectors. Even here bad actors have learned new ways to hide. Not only do they make use of logos and other graphical themes used by companies, but they hide text and forms as graphics too. They also use javascript to obfuscate key text strings with random letters, so 'Login' looks like 'Lhkgdgowyailgqtagpibvzmen' (I've coloured the actual letters for ease) until it's rendered in a browser.

So, how do you deal with a relatively low-tech problem like brand spoofing that uses graphics as a weapon? You need to use Computer Vision (Visual-AI) to look at the email or web page, not as code, but as the user sees it - as a fully rendered page. To do this the email/page needs to be captured as a flattened jpg and then processed through the computer vision engine. This is a key step because all the tricks used by bad actors are not effective post-render, so you see what they want the victims to see.

Processing of this image is then carried out using a combination of techniques:

Visual Search: looks at the overall image and compares it to previously 'known good' and 'known bad' examples, which can give a quick confirmation of a phishing attack using a previously used design/layout.

Logo Detection: looks for brands that are often spoofed, this can lead to priority processing if it meets a potential threat profile.

Text Detection: analyzes the text looking for trigger words that could indicate a threat, like 'username', 'password', 'credit card', etc.

Object Detection: looks for key elements like buttons and forms, which in combination with text and logo detection increases the potential threat level.

The important thing to remember is that this approach does not replace the current programmatic methods to detect attacks, but works in concert with them to provide additional signals which can lead to more accurate determinations. There's an interesting video on this subject here.

Ultimately, based on the volumes of phishing emails highlighted at the beginning of this article, the industry approach to controlling the flow and severity of phishing attacks is much like the old Chinese proverb of moving a mountain - one shovel-full at a time. Using many tools and solving the small issues

one at a time may seem insignificant in the scheme of things, but as bad actors adapt and even simplify their approach to ramp up volumes, every 1% reduction in the number of phishing emails that make it through equates to thousands of emails blocked and pages blacklisted, which can have a critical impact on the number of compromises that succeed.

About the Author

Franco De Bonis is the Director of Marketing at VISUA, a massively scaling company in the world's fastest-growing future-tech sector – AI.

Franco was always fascinated with technology, which led to a career marketing technology and SaaS products, and a PostGrad and Masters in Digital Marketing. Franco also set up a digital marketing agency in 2007, which grew quickly and was acquired by a national marketing chain in 2013.

Franco joined VISUA (originally LogoGrab) in September 2019. It's a company with a vision to address the growing challenge of providing insights and intelligence from visual media using a 'People-First' methodology. It has grown, really big, really fast, with minimal outside investment. The VISUA brand was launched in 2020 to reflect the much broader range of solutions it now delivers to leading companies in the fields of brand monitoring, protection, and authentication.

If you want to discuss Visual-AI you can contact Franco at franco@visua.com or on LinkedIn. Find out more about Visual-AI (Computer Vision) at https://visua.com

How To Design and Build Longer Lasting Drones

Overcoming the limitations inherent in drone technology

By Shaun Passley, Founder, Zenadrone

Drones work. From search and rescue operations in Ukraine, to COVID-19 vaccine drops in India, to tracking bison in protected landscapes across Colorado, drones have proven in recent years to be an indispensable tool for a wide range of organizations. Still, like all technologies, there is room for improvement.

It's easy to buy the hype that says the sky's the limit regarding the potential applications for drones, but it doesn't take long to realize their limitations. For drones to achieve all the things that the industry's manufacturers are promising, they will need to evolve into a tool that is more efficient and longer-lasting.

Identifying the barriers to achieving longer-lasting drones

Battery power is the lifeblood for drones. Thus, producing longer-lasting drones means increasing the amount of battery power they can store. Barring any unforeseen breakthrough in battery technology, this remains an issue that is best addressed by simply adding more batteries. Unfortunately, that path leads to the other major barrier to achieving longer lasting drones: Reducing their weight.

Decreasing the weight of a drone is the easiest way to extend battery life. With less weight to lift, drones draw less power from batteries. However, decreasing weight often means using materials that are less stable, which decreases the overall lifespan of a drone.

Achieving the proper balance between weight and power is one of the key challenges for drone manufacturers. Nonetheless, finding solutions to this challenge is critical not just for sustaining the current state of the industry, but also for allowing the drone industry to expand.

Developing drones that fly longer

Creating drones that can fly for longer periods of time is crucial; not merely for extending the range of work that contemporary drones are performing, but also for expanding the areas in which future evolutions of drones will work. For new industries to take advantage of the utility drones can provide, drones must be properly developed and equipped to carry new and larger payloads.

Drone used in search and rescue operations provide an excellent example of this. For example, drones being used for search and rescue in Ukraine provide users with two-way audio. Whereas most other drones only carry tools for capturing photos and video, these drones must also come equipped with microphones and speakers, allowing pilots to hear what is happening in the drone's vicinity or talk to people the drone encounters.

In addition, using drones in new industries means they will need to be prepared to encounter new, and often, unpredictable, flight conditions. When flight conditions become unpredictable, so does the drone's battery usage. Again; extending battery time becomes a critical factor.

The use of Beyond Visual Line of Sight (BVLOS) drones is yet another area in which longer battery life is essential. While current regulations have limited the use of such drones, manufacturers are counting on BVLOS drones to manifest the drone delivery programs that Amazon and other companies have.

Increasing performance with new technology

When it comes to building a better drone battery, the development of hydrogen fuel cells for drone use has been heralded as a major innovation. When used with drones, these cells allow for flight times to be extended to two hours while also lowering the recharging time of batteries to as little as ten minutes. Unfortunately, these cells also cost thousands of dollars, which equates to a dramatic increase in drones ' costs.

Increased costs are also an issue when it comes to engineering lighter drones that still retain necessary stability. Using carbon fiber-reinforced composites increases costs while lowering weight. More affordable options for materials sacrifice durability, and shorten the life of drones.

Another option for increasing performance is implementing intelligent features that prolong the life of the drone and increase its effectiveness. These include obstacle avoidance technology, sensing systems, and failsafe protection. When coupled with advanced pilot training that reduces crashes and increases efficiencies in flight, this technology can lead to drones that fly longer, last longer, and provide greater returns on investment.

About the Author

Dr. Shaun Passley is the Founder of Zenadrone. He holds numerous master's degrees from DePaul University, Benedictine University, and Northwestern University and has a PhD in Business Administration. In addition to founding ZenaTech, he is also Chairman & CEO of Epazz, Inc. – an enterprise-wide cloud software company — and the manufacturing company Ameritek Ventures – a manufacturing company. ZenaDrone is an entirely bootstrapped venture that is aiming to help the agri sector in Ireland close its emerging labor gap through automation. Shaun can be reached online at shaun@epazz.net and at our company website https://www.zenadrone.com/

How To Increase User and Executive Participation In Security Awareness Training Programs

By Theo Zafirakos, CISO, Terranova Security

The universal participation of an organization's employees in security awareness training programs is fundamental to improving its long-term security. Building a security-aware culture is the first step to cultivating the participation for security awareness training programs. The challenge for many companies is that if the training materials are not easily digestible, engaging, and entertaining, then participation tends to be low.

In security awareness training, anything below 90% participation is considered to increase risk for the organization. This means, knowing how to target employees, including senior leaderships, and executives, is crucial to teaching them the skills and information they need to protect the organization.

Identifying Your Target Audience

Relevancy is key to having engaging security awareness content. There's no shortcut to producing relevant training materials; the only way is to take time to identify your target audience and the cyber threats they're exposed to daily. Most organizations' target audiences can be broken down into several key groups:

- Executives – Executives and Leadership team need to be aware of security risks to understand the importance of supporting and funding security awareness initiatives.
- Managers – Managers' security awareness is critical to ensure they take responsibility for acting as ambassadors and security role models.

- Individual Contributors– Contributors are your first line of defense against cyber-attacks, so it's paramount that they adopt best practices and behaviors needed to stay safe online.
- IT Security Team – Your ITS team will help guide your information security best practices and manage the network, systems, and application vulnerabilities in your environment.

Recommended Topics Per Audience

Training topics depend on the security risks specific to an organization's environment. There are, however, a few go-to topics that apply to all organizations:

1. Executives

Consider covering topics like priority risks facing your organization, secure use of mobile technology, safe handling of sensitive information, common attacks and scams targeting executives, and security and awareness compliance obligations.

2. Managers

All executive topics plus an overview of information security and governance, your IT security environment, proposed security awareness program, and IT security controls.

3. End-users

Aim to increase knowledge of security threats with topics such as information security and privacy, security essentials (like password creation, email use, malware), internet usage essentials (social media, safe browsing, cloud computing), typical phishing and social engineering techniques, cyber-attacks, and data handling.

4. IT Staff

Raising awareness of security best practices related to the networks, systems, and application vulnerabilities in your environment, consider network security overview, application security overview, common network and application attacks, system development life cycle, secure coding, cryptography, and key management.

Building Effective Awareness Training Materials for Your Audience

Once targets have been identified, you need a strategy and implement engaging training materials. The first step in the process is to create educational topics relevant to the individual and audience with their day-to-day activities.

For example, if your end-users are sales or account representatives who send lots of emails, incorporating training materials on phishing threats and phishing simulations will provide them with helpful guidance to detect phishing scams.

The most important thing is to focus on building engaging and interactive materials. In practice, that means:

- Create bite-sized microlearning modules that employees can easily digest
- Use plain language the audience can understand
- Communicate with your audience in their native language
- Incorporate gamification and interactive exercises like phishing simulations

The importance of Executive Participation

A significant mistake an organization can make when building its security awareness training programs is not to prioritize executive participation. This oversight can have a real negative impact, as not only are executives valuable champions of cyber security investment and cultural change, but they are also end-users who are the target of cyber threats themselves.

C-suite executives are often the target of cyber criminals through credential harvesting campaigns as they hold valuable data nefarious actors are looking for. If they fall victim to these attacks, the damage to an organization can be immense; therefore, it's essential to ensure that everyone in the organization is involved in the training program.

To See Success, Know Your Audience

There are no shortcuts to creating engaging security awareness training programs and increasing participation. The best way to build the proper program is to tailor the learnings to your audience. Knowing who your audiences are and the threats they face on a day-to-day basis will allow you to provide them with relevant learning opportunities. With this knowledge you can cultivate a security-aware culture within your organizations and build cyber heroes who will know how to protect themselves from cyber threats.

About the Author

Theo Zafirakos is CISO of Terranova Security. He is responsible for all areas of information security for the creation and management of strategy, programs, governance, information risk assessments, and compliance for Terranova Security. Terranova Security is the global leader in Cybersecurity Awareness, with 10M+ Trained Cyber Heroes in 200+ Countries and 40+ Languages. He leads Terranova's Professional Services team that helps our clients implement and execute information security awareness programs with measurable results. Programs that assist users in recognizing the events that require a specific action know what the appropriate action is and are motivated to take that action. Theo can be reached online at LinkedIn and at the company website http://www.terranovasecurity.com

How Zero Trust and Secure Identities Can Help You Prevent Ransomware Attacks

By Danna Bethlehem, Director Identity and Access Management (IAM), Thales

With ransomware attacks on the rise in a big way, security has become a hot topic worldwide. These attacks put organizations that don't have sufficient security measures at risk of significant data breaches. As hacks become much more sophisticated, the costs of recovering from a ransomware attack are tremendous and continue to rise.

According to cybersecurity ventures, the cost of ransomware attacks is predicted to reach over $265 billion by the end of 2031. As no industry is safe from ransomware attacks, organizations should implement effective security measures to avoid being the next victim.

Ransomware gangs shift to a RaaS model

Ransomware gangs are shifting to a raas (ransomware as a service) model and leveraging stolen or compromised identities found on the dark web. This business model of operators and affiliates gives criminals a platform for showcasing their skills and collaborating with others. Ransomware operators, therefore, do not need complex skills to access networks; they can offer their malicious techniques as easy-to-use products in the form of a franchise or an affiliate program model.

The relative ease of launching a raas attack across the web has fostered the security agencies of the us, uk, and australia to issue a joint alert warning business that:

- Raas has become increasingly professionalized, with business models and processes now well established.
- The business model complicates attribution because there are complex networks of developers, affiliates, and freelancers.
- Ransomware groups share victim information, diversifying the threat to targeted organizations.

Access-as-a-service (aka initial access brokers

a common way for criminals to gain access to an organization's network is by relying on access-as-a-service groups, aka initial access brokers (iab).

Ransomware operators depend on iabs to reduce the need for extended reconnaissance or the time to find a method for entry. Initial access brokers provide ransomware attackers with an easy way into corporate networks, paving the way for the actual damaging attacks. The access-as-a-service marketplace is the source of the disconnect between an initial corporate breach and the subsequent attacks that follow days or even months after. As a result, security professionals argue that criminals no longer break into networks or systems; they instead simply log in.

Strengthen resilience against RaaS attacks

Organizations can take several steps to increasing their resilience against raas attacks, including:

- Deploy multi-factor authentication for all your applications and systems, for all your users
- Encrypt all your data-at-rest
- Keep all operating systems and software up to date.
- Secure and monitor rdps and make sure they are not exposed to the internet
- Implement a user training program and phishing exercises
- Require all accounts with password logins to have strong, unique passwords.
- Protect cloud storage by backing up to multiple locations.
- Segment networks
- Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a network-monitoring tool.

Secure identities are the foundation of a zero-trust policy

The boundaries of digital enterprises cannot be confined within four walls. Identity has emerged as the frontier to defend and protect businesses against a multitude of threats, including ransomware gangs. Identity is also one of the foundational pillars of zero trust architecture, with nist and the omb memorandum highlighting the importance of securing digital identities to prevent data breaches and ransomware attacks.

In this regard, two essential practices for establishing a zero trust policy include access control and network micro-segmentation.

Access control is based on verifying and authorizing identities to access the right resources. Authentication gives us information about who the identity is, while authorization grants access for the

verified identity to specific resources, apps, and data. Authentication and authorization are core elements of a zero trust policy.

On the other hand, network micro-segmentation helps reduce the threat surface by creating smaller, segregated trust zones. Based on the principle of least privilege, users need to prove their authenticity to be able to access each trust zone. Micro-segmentation reduces the potential attack surface, hinders lateral movement between networks and systems, and ultimately limits the impact of a successful breach.

The ability to verify a user's legitimate identity with multi-factor authentication, whether they are accessing a micro-segmented trust zone, or a service directly, forms the basis of solid security practices ensuring the identity requesting access to a resource is trusted.

Mfa is a key requirement for a zero trust architecture

"mfa is one of the most important cybersecurity practices to reduce the risk of intrusions—according to industry research, users who enable mfa are up to 99 percent less likely to have an account compromised," reads a CISA advisory.

By presenting two different factors of authentication, mfa builds confidence that your identity cannot be easily compromised and places extra obstacles in the criminal's path towards breaking into the corporate networks. Hence, mfa has become a strict requirement for implementing a zero trust architecture. "agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent," states president biden's executive order on improving the nation's cybersecurity.

However, it is important to select an mfa solution that offers the following features:

A choice of authentication methods, including phishing resistant methods such as fido and pki-based mfa, in accordance with the requirements mandated by the office of management and budget.

Flexibility and scalability to cater to diverse business needs and user authentication journeys

Low implementation and running costs

As each day passes, cybercriminals continue to develop more sophisticated ways of obtaining confidential and sensitive data that they can exploit. The world of cybersecurity must stay one step ahead with technologies and practices to secure digital identities and ensure that organizations can prevent ransomware attacks.

About the author

Danna Bethlehem, director identity and access management (iam), thales. Danna bethlehem is passionate about product marketing, positioning, messaging, content strategy, competitive analysis, feature prioritization, and external communications for global cyber security solutions.

She loves being at the heart of promoting technology solutions that impact our lives but enjoys hiking in the desert on her time off - even through sandstorms!

Danna bethlehem can be reached online at https://www.linkedin.com/in/danna-bethlehem-coronel-7a3355b/ and at our company website https://cpl.thalesgroup.com/ bethlehem is passionate about product marketing, positioning, messaging, content strategy, competitive analysis, feature prioritization, and external communications for global cyber security solutions.

She loves being at the heart of promoting technology solutions that impact our lives but enjoys hiking in the desert on her time off - even through sandstorms!

Integrated Risk Modeling

Better Intel for Managing Risk

By Andrew Beagley, Chief Risk Officer, OptimEyes.ai

An Integrated Risk Modeling & Reporting SaaS platform allows companies to measure, monitor, quantify, and report on many types of risks side-by-side and on-demand. Risks related to cybersecurity, data privacy, regulatory compliance, operational effectiveness, supply chain resilience, and more.

This creates a timely, contextualized, enterprise-wide view of the organization's unique risk profile. This eliminates the informational and operational silos common in enterprise risk management and empowers risk managers, executives, and board members to compare one vulnerability to another and understand the biggest threats facing their organizations.

The Integrated Risk Modeling & Reporting platform also links these business risks to the company's strategic objectives and risk tolerance, so comparisons and decisions — about where to allocate resources and how to pivot as new risks emerge — are informed by this critical context.

Once a company aggregates and centralizes its risk data in a single platform, it can leverage the information in a variety of ways — assessing the need for cyber insurance, for example, or ensuring compliance with the myriad data privacy regulations enacted in jurisdictions around the world.

A Customized, Personalized Perspective

Each company populates its platform with up-to-date internal data and information reflecting its specific circumstances. This bespoke “inside-out” view precisely conveys the organization’s risk profile and benchmarks to inform priority setting, decision making, and operational responses to emerging, evolving risks.

Financial Impact is Quantified

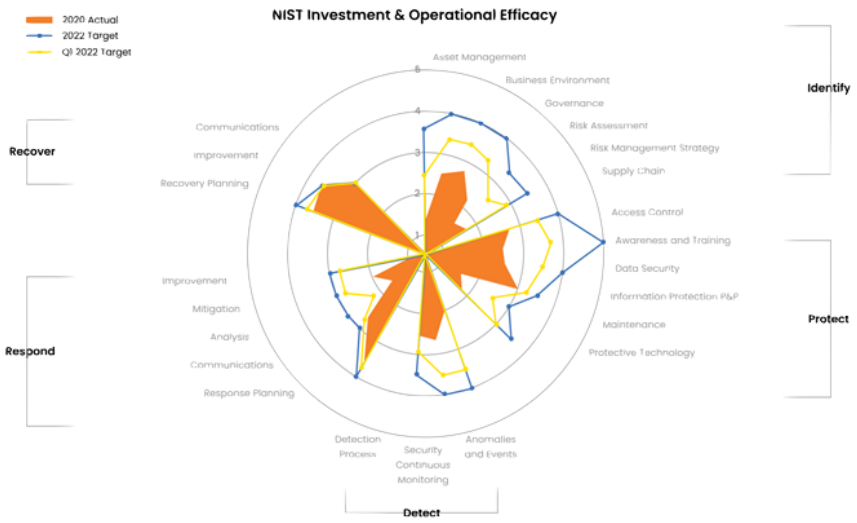
IDRM goes beyond traditional risk score methodology to calculate and predict the financial impact, remediation cost, and annual loss expectancy of each factor of risk across the enterprise. When risks are quantified, decision-makers can immediately compare the severity of one challenge to another, set priorities, and create data-driven remediation plans.

Industry-Specific Risk Benchmarking

Traditional benchmarks available today, unfortunately, typically provide only high-level guidance due to the generic framework applied. On the other hand, within an Integrated Risk Modeling & Reporting platform data can be adjusted to take account of industry type, company size, risk appetite, data assets, and other factors. This provides a company-specific industry benchmark to assess a company’s specific threat exposure and overall risk management program performance.

Best-in-class “outside-in” risk benchmarking maps three coordinates:

- The enterprise’s own risk profile and risk scores based on its unique data.
- Broad industry average risk scores.
- A narrower band of benchmark data reflecting the enterprise’s specific peer group.



Dashboard Reporting for the Executive, Management, and Operational Teams

The OptimEyes.ai platform collects and analyzes data, translates it into business intelligence, and presents it visually in intuitive dashboards — customizable for each level of the organization. This enables the C-Suite, functional leadership, and operations to drill into the information that they need to do their jobs and to communicate with each other more effectively as decisions are made.

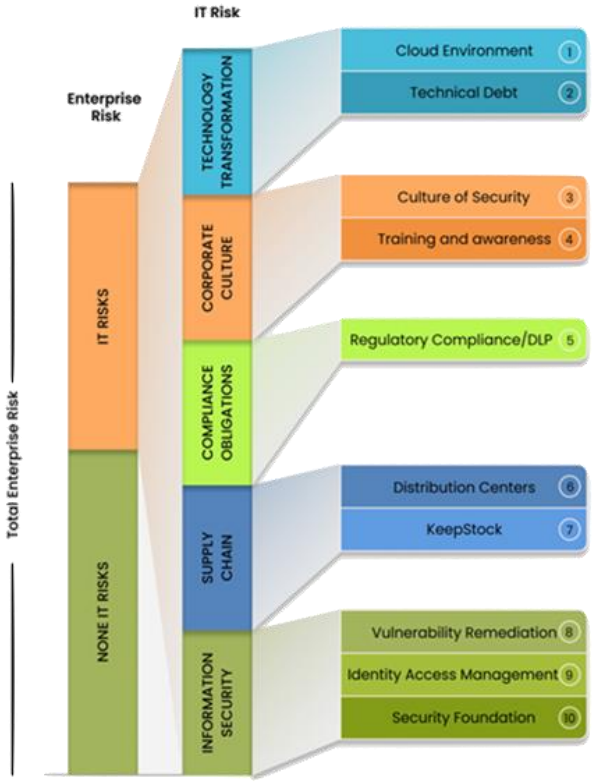
Risk Scenario Planning

Artificial intelligence and machine learning makes OptimEyes' solution a reliable, predictive process that enables enterprises to compare threats — looking at best and worst-case scenarios — and decide where to invest in risk mitigation.

Rapid Platform Customization and Deployment

When you buy a suit, you start with the same product as the next person and then make any necessary alterations. The length of the sleeves, the hem, perhaps the waistline. A bit of tailoring to make it bespoke and ensure it's a perfect fit for you. You don't wear it home off the rack and you don't design a new suit from scratch. It's 90% ready, and you and the tailor do the rest to make it yours.

That's the OptimEyes' approach to enterprise risk modeling. It starts with a template and default settings that reflect best practices, experience, and common preferences. Then it adjusts to reflect the company's industry, unique set of risks, the weight it gives to specific vulnerabilities, and its objectives, business priorities, and risk appetite. This customization enriches the platform, enabling the generation of risk quantification and exposure analytics that are accurate and specific for the organization.



Conclusion

Gartner defines Integrated Risk Management (IRM) as a "set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks. Under the Gartner definition, IRM has certain attributes: strategy, assessment, response, communication & reporting, monitoring, and technology.

Integrated Risk Modeling & Reporting overlaps, supports, and informs IRM as the risks confronting large companies continue to expand, change, accelerate, and grow more complex. Ransomware attacks, regulatory demands, technological disruption, disparate state and national data privacy laws, geopolitical tensions threatening vulnerable supply chains — these are just a few of the challenges organizations face day after day.

As risks emerge and evolve, however, companies often lack the information and context needed to assess the situation effectively, compare one threat against another, gauge the implications, set priorities, and make informed decisions. They need their enterprise-wide risk profile presented clearly, in real-time, to enable informed, consistent decision-making – at the board, managerial, and operational levels.

About the Author

Andrew Beagley, Chief Risk Officer of OptimEyes.ai. Andrew is a highly experienced Chief Risk & Compliance Officer focused on developing cyber, data privacy and compliance risk model solutions. Using AI and machine learning, Andrew helps organizations quantify and benchmark their risk to enable smarter business decision-making.

Based in New York and London, he has worked for corporate and regulatory organizations across multiple industries; supervised global teams; and managed significant regulatory relationships. He is an award-winning film maker, bringing to life complex corporate compliance and ethics issues on the big screen

Andrew online at andrewb@optimeyes.ai and at our company website http://www.optimeyes.ai

Leading a Revolution to Provide Secure CCTV Cameras

By Mitch Muro, Product Marketing Manager, Check Point Software Technologies

When building IoT devices, it is important to understand that an IoT device (by default) is rarely secure. This is due to the simple fact that these devices are often designed to increase productivity and provide immediate value to its customers, leaving security as an afterthought (or completely out of the equation). It is unsafe to assume that skipping the step of implementing security is no big deal because "no one will want to attack a smart doorbell." On the contrary, evidence has proven to us time and time again, that cybercriminals will attack **wherever** the most lucrative rewards can be found. And when it comes to unsecure connected devices and networks, they serve as entry points for a cybercriminal to infiltrate a network and steal sensitive data, information, and even shut down operations. It Is extremely important now, more than ever, to secure these devices out of the box.

In this article, I wanted to focus on the CCTV/IP Camera market. CNBC projected that one billion surveillance cameras were active in 2021 so it is safe to assume that with the growth of IoT worldwide, the number of those devices are much larger now in 2022. CCTV plays a crucial role in keeping both people and organizations safe, everywhere from transport hubs to retail, banks, and critical infrastructure. According to cctv.co.uk, there are about 691,000 CCTV cameras active in London alone. As surveillance video is increasingly IoT connected, they become prime targets for cybercriminals for various reasons. Innovative companies, like Check Point Software, offer an embedded runtime protection solution that provides built-in security against attacks such as access control, memory corruption, shell injection,

import table hijacking, control flow hijacking, and more with 100% firmware coverage, including third party components, without compromising the device's performance.

Modern CCTV cameras are essentially functioning as small computers that run operating systems, applications, and have various networks and radio frequency (RF) interfaces. As such, they are also susceptible to hacking attacks. One of the biggest issues is that end-users will often keep the default usernames and passwords, essentially leaving the door open for hackers. Even with a strong password, traditional CCTV cameras are not supplied with adequate on-board security. But why even hack a CCTV camera? Well, the answer is simple. Criminals may wish to gain access to the camera's controls, to turn it off, point it in a different direction, and manipulate images and associated information or just to watch the activity covered by the camera. In addition, as a network device, once hacked, it can be used to gain access to sensitive resources on the corporate network via lateral movement, where cybercriminals can then exploit vulnerabilities and deploy botnets or crypto miners.

So, what can businesses do to protect themselves from these types of vulnerabilities? Companies like Check Point Software Technologies, a leading provider of cyber security solutions globally, and international CCTV market leader Provision-ISR (Israel) take these issues head on. The partnership combines Check Point's Quantum IoT Protect Nano Agent solution being embedded in Provision-ISR's CCTV cameras for on-device runtime protection against zero-day attacks. The solution brings an entirely new level of cybersecurity to the video surveillance market.

With all of this in mind, the problem becomes very clear – internet connected devices (like surveillance cameras) are growing rapidly year over year but are often rushed to market with security left behind as an after-thought. This leaves an open door for cyber criminals to infiltrate with malicious intent. Business should remain resilient and proactive to ensure their business' products/solutions are safe from threats by following security best practices and partnering with experienced and leading security vendors. I will leave you with a few best practices that you can take action on immediately to take a step in the right direction:

Cyber Security Best Practices & Safety Tips

1. Remain resilient in updating passwords/credentials for your internet connected devices and DO NOT leave in place the default device password
2. Uncover security risks in any your internet connected device firmwares via free security risk assessments – Check Point offers a free service here: IoT Firmware Risk Assessment
3. Take advantage of on-device runtime protection solutions to protect yourselves from zero-day attacks
4. Define and enforce policies on a per device basis for ongoing network access
5. To learn more, head here for additional resources and information: IoT Device Security for Manufacturers

About the Author

Mitch Muro, Product Marketing Manager, Check Point Software Technologies. Since joining Check Point Software Technologies in 2020, Mitch Muro leads product marketing activities, strategies, and vision for Check Point's Quantum IoT and SMB product offerings. Mitch brings a decade of experience in cybersecurity marketing – including payments, e-commerce, networking, IoT, cybersecurity, and cloud solutions. Mitch also possesses expertise in converting customers and business needs into innovative and valuable product material to generate business opportunities and customer value. Prior to joining Check Point, Mitch spent time at Actiance and Broadcom where he led the development, business, and go-to-market execution of innovative new products for e-commerce security solutions and data archiving.

Mitch can be reached at our company website: www.checkpoint.com

Levelling The Battlefield with Cyber as An Asymmetric Leverage

By Goh Eng Choon, President for Cyber, ST Engineering

From sabotaging, stealing and destroying valuable enterprise data to crippling critical information infrastructure as the precursor to a conventional war, cyber-attacks are harbingers of chaos to both nations and businesses.

But the dynamics in cyber warfare are different. Classical military theory often calls for a numerical superiority ratio of 3:1 to win a battle with good probability and acceptable risks. In cyber warfare, this rule is overturned as smaller actors have an asymmetric advantage.

Small but deadly

While cyber attacks may not result in high human casualties or physical destruction, we have witnessed their devastating effects – disrupting lives and crippling everything from satellite communications to energy-generating wind turbines.

Take cyber espionage as an example. At the corporate level, companies have been caught stealing information in deliberate attempts to erode the competitive edge of their competitors. At the national level, top secret military intelligence and aviation technologies have been leaked.

In an increasingly digital world, the convergence of digital networks and systems has resulted in a global spike in cyber-attacks. In 2021 alone, governments worldwide saw an 18.9-fold increase in ransomware attacks, while healthcare institutions faced a 7.6-fold increase in similar breaches.

The asymmetric nature of such attacks means that it only takes a small team of very talented people with the know-how to cause catastrophic disruption. Given their power to wreak massive economic and social damage, cyber-attacks could well be the new weapons of mass destruction in this digital age.

The Invisible Enemy

The threat is ever present. Some cooperatives may be passive, biding their time to steal information, while others are destructive and have the capabilities to cripple the operations of countries and organisations.

Cyber warfare, unlike physical combat and gunfights, can also be hard to spot. Stealth attacks make detection a challenge as we fight without full visibility and situational awareness. A lot of times, it can be difficult to trace or understand the extensiveness of the threat or damage. By the time companies or countries intervene, it can sometimes be too late.

As more interconnected systems come under perpetual attacks, the lines between peacetime and wartime cybersecurity are increasingly blurred. With no formal declaration of war – not to mention the difficulties of identifying the adversary – it is hard for countries to determine their defence readiness condition (DEFCON) state and ascertain when a skirmish becomes a full-fledged war.

No organisation should be a sitting duck, reacting only when the damage is done. All should maintain a proactive stance to mitigate and respond to such attacks. While investing in cyber defence is increasingly a priority among big corporate entities, many small and medium-sized enterprises (SMEs) still regard cybersecurity measures as cost drivers and tend to put them on the backburner. No surprise, then, that SMEs are the top targets of cyber criminals – they are three times more likely to be attacked than their larger peers.

A United Front

Given the volatile nature of cyber threats, every individual, organisation and country is crucial to keeping the cyber ecosystem secure. Here are three key areas to look into:

First, it is important to inculcate good cyber hygiene as everyone plays a role in cybersecurity. Sharing ways to stay cyber safe helps sharpen vigilance and ensure best practices – from exercising caution in the sharing of sensitive information to using certified cybersecurity products to better protect data.

Second, an organisation-wide mindset change is needed. Leaders must not regard cybersecurity as an afterthought or implement measures merely as a response to government legislation. Instead, cybersecurity should be seen as an enabler by providing greater value to its consumers.

Third, cyber diplomacy should be fostered among countries and industries. In this highly interconnected digital world, we would collectively benefit by building closer ties and being more open to sharing information. Many attackers are already sharing information and if organisations work in silos, they will

be on the losing end. It is therefore important to create a safe platform where organisations and nations can come together to share their experiences and expertise in combating cyber threats.

Arming to disarm threats

Protecting cyberspace should not just be the leaders' job. Instead, guarding against asymmetric cyber attacks is the responsibility of everyone in an organisation.

To begin, organisations should work within a cyber-secure network. For instance, in this era of increased remote working, sensitive data in transit and at rest should always be strongly encrypted from one end to another. This way, even if it falls into the wrong hands, hackers will not be able to make sense of the data as it will take them many years to decrypt the information.

Encrypted information in transit must also be secured. Critical networks should be segregated from other networks to create additional layers of defence. Connecting to workplaces and high-security clearance sites through virtual private networks is one way to achieve this segregation. For sites which require an even higher level of security, cross-domain solutions allow for highly secured unidirectional communication and isolated networks across sites.

Defending critical infrastructures from cyber attacks takes more than just antivirus software. Having an advanced cybersecurity operations centre to monitor these systems and networks will enhance the detection and response capabilities so that threats can be blocked and eliminated in a timely manner.

Ultimately, building cybersecurity capabilities in people is paramount to levelling up an organisation's capabilities. We need to shift our paradigm from passive defence to active defence and from reactive to predictive to be able to guard against and prevent attacks. Cyber defenders must start moving away from conventional task-based cybersecurity analysis to adopt a holistic, pre-emptive and proactive approach that is enabled by automation, cyber threat intelligence, and comprehensive threat awareness. This allows cybersecurity defenders to detect anomalies, anticipate hackers' moves, and provide actionable insights for C-Suites and analysts to make informed decisions to combat cyber attacks. At the end of the day, we need to secure what matters and people will still be the last line of defence to ensure a safe cyber future.

About the Author

Goh Eng Choon is the President of the Cyber Business Area at ST Engineering, a global technology, defence and engineering group with a diverse portfolio of businesses across the aerospace, smart city, defence and public security segments. He is also an appointed member of the Cybersecurity Advisory Group, a panel of eminent cybersecurity experts whose expertise may be tapped for cybersecurity issues or cyber threats that confront Singapore.

Eng Choon can be reached at our company website https://www.stengg.com/

Microsoft Support Diagnostic Tool Vulnerability: What to Learn from It and How to Stay Safe

By Dirk Schrader, Resident CISO (EMEA) and VP of Security Research, Netwrix

A new vulnerability in the Microsoft Office universe has been recently discovered. Let's examine some details about it. How Microsoft Support Diagnostic Tool (MSDT) and other tools can be turned against organizations? What IT teams can do to prevent something bad from happening?

What is going on?

Freshly discovered CVE-2022-30190 vulnerability in MS Office provides attackers with a new way of hijacking organizations' IT environments through endpoints. This exploit is likely to work on most Windows / MS Office installations, if they aren't patched yet.

The attacker crafts a MS Word document that contains the malware code, sends it to someone's business email address and uses common social engineering techniques to lure the recipient into opening it. Remember Log4Shell vulnerability discovered in December 2021, where the issue was about an uncontrolled way of executing a function in a function combined with the ability to call for external resources. This 0-day, initially named 'Follina', works in a similar way.

Word has a feature called 'remote template' which is misused to get a HTML file from a distant location. Once received, this HTML file uses a functionality in MSDT to execute an embedded payload, using Powershell script or other tools available on the target.

Windows built-in security tools are likely not to catch this activity.Standard hardening benchmarks don't cover it either. Built-in defensive mechanism like Defender or common restrictions for the use of macros will not block this attack as well.

The exploit seems to be out in the wild for more than a month now, with various modifications as to what should be executed on the targeted system.

What is affected?

Microsoft lists 41 different product versions, from Windows 7 to Windows 11 and from Server 2008 to Server 2022. Known and proven as affected are Office, Office 2016, Office 2021 and Office 2022, regardless of the version of Windows they are running on. Patches have already been issued.

The bigger picture

Both this MSDT vulnerability and Log4Shell are trying to use documented functions against the victim, relying on the aspect that these are executed within the trusted space. APT groups will look for more of these 'function in an function' vulnerabilities. In the weeks after CVE-2022-30190 was published, some additional ways of exploiting similar functionality made the round.

Within the coming weeks, attackers will likely check for ways to weaponize this attack vector and use it in spear phishing campaigns. Cyber crooks will apparently combine this attack vector with other recent techniques (like one discovered in Japan) as well as with privilege escalation techniques to elevate from the current user's context. Keeping in mind the possibility of this 'combined' tactic, IT pros should make sure that systems are closely monitored to detect breach activity.

What to do to ensure security?

For CVE-2022-30190, initial findings indicated that deleting a certain registry key will stop this exploit from working, but benchmarks like those from CIS and DIA STIG seem to not cover the needed setting as part of the hardening process. In the meantime, installing the patch should be on the priority list, if not done yet.

To detect suspicious activity related to this kind of attack vector, IT teams need to closely monitor changes within their organizations' systems, especially in system folders, and timely spot unwanted processes or services started.

In Windows-based environments, another measure that can help prevent these types of attack is establishing a set of Windows group policies and PAM 2.0 measures that will lock down your systems so that the vector is prevented from executing that function in function or the user is confined and restricted in the privileges assigned.

About the Author

Dirk Schrader is Resident CISO (EMEA) and VP of Security Research at Netwrix. A 25-year veteran in IT security with certifications as CISSP (ISC²) and CISM (ISACA), he works to advance cyber resilience as a modern approach to tackling cyber threats. Dirk has worked on cybersecurity projects around the globe, starting in technical and support roles at the beginning of his career and then moving into sales, marketing and product management positions at both large multinational corporations and small startups. He has published numerous articles about the need to address change and vulnerability management to achieve cyber resilience.

Dirk can be reached on Twitter @DirkSchrader_ at www.netwrix.com

Mitigate Risk by Securing Third Party Software And Environments

Software Security Requires Ongoing Vigilance Against New and Evolving Vulnerabilities

By Tim Kenney, Chief Operating Officer, SOOS

Businesses Need Software and Today's Software is Built with Open Source.

Modern businesses need specialized software to run their organizations. Today, more than 90% of new software is built on open source components called packages. Developers have access to an almost limitless array of open source packages to build their products, which has been transformational for the industry. Nearly every organization has adopted open source development; even the largest like Google, Microsoft and IBM. It makes development faster, easier and economical. The software needs of a business can get large: accounting, payroll, database management, asset management, communication systems, websites, payments, and sales management to name only a subset few. Some verticals require specialty software that interface with devices (IoT) and those devices contain software. You and your clients need these systems up and running to deliver your products and services.

Attack Vectors May Be Lurking Inside Your Software

Unfortunately, each of these systems represents a security risk to an organization. Often, within the open source components used to build custom software, vulnerabilities are lurking. This is the downside of modern development. Ransomware attacks, fraudulent financial transactions, and leaked confidential personal data all represent a reputational and financial risk for your business. Bad actors are waiting for

mistakes, by your business, or by your vendors. Many businesses have focused on hardening their networks against attack and securing their users from phishing attacks and password hacking. While these are good practices, they skip what has been a repeated root cause of some of the largest attacks, vulnerabilities in the software that businesses run or the software that runs on devices, unwittingly leaving their systems and data at risk

The consequences of these hidden vulnerabilities can be very expensive. Equifax has said the data breach that started with an unpatched open source module has cost the company nearly 2 billion dollars since hackers gained access to their servers in mid July 2017. Developers had used Apache Struts open source package. A vulnerability for this package was patched in the open source library on March 7, 2017, but developers at Equifax didn't apply the patch for months, inadvertently leaving them open to an attack.

Unpatched systems represent a problem for even the largest software companies. In 2021, Facebook had 533 million user data compromised and Linkedin had 500 million user profiles compromised due to open source vulnerabilities. Recently, a very serious vulnerability was found in the Log4J package, a utility many software packages use for logging. Apple's Icloud service was vulnerable as was Microsoft's Minecraft. But the problem isn't limited to just software running on servers or PCS, it impacts devices too. Another vulnerability, NAME:WRECK, is believed to be in more than 100M devices. Many companies have stepped forward with advisories including companies like Siemens, GE and Lockheed Martin. These are all high-profile examples, but incidents like this are happening at companies of all sizes, across the country, every day.

Check during development & keep checking

The risks are significant, but not insurmountable. The good news is that open source packages mean more people working with them and vulnerabilities are found quickly and reported. When a vulnerability is found in these packages it is shared via some public databases like National Vulnerabilities Database (NVD), the Common Vulnerabilities and Exposures (CVE) or others like GitHub Issues usually with accompanying fix information. New vulnerabilities can be posted at any time. What was safe yesterday might not be safe today. The vulnerabilities can be as severe as letting a bad actor take complete control of your system, capable of installing their own software for future use. There are automated tools for developers to make certain they are using packages that are secure. These tools are called Software Composition Analysis Tools (SCA). These tools can generate a Software Bill of Materials (SBOM) which contains all the components and may also contain the known vulnerabilities.

Additionally, care needs to be taken with another type of vulnerability, typo-squatting. Typosquatting is when a malicious actor tries to place an open source package in a repository that is similar to a popular package but has vulnerabilities. Maybe a version number is changed or a single letter. These packages can run just like the legitimate package. Some SCA tools can highlight these potential vulnerabilities.

Developers can make mistakes in their own code that may not be caught by your quality assurance team. These mistakes / bugs can lead to security issues and they can be easy to overlook. Simply not checking a single input field can lead to a flaw that exposes a database through a vulnerability known as SQL

injection. Browser based applications are susceptible to another common form of attack known as cross site scripting where a website uses the input from the user within the output it generates at a later time without checking it. APIs are also susceptible to these attacks. These types of attacks can be reduced by running modern Dynamic Application Security Testing (DAST). OWASP Zap is an open source version of such a tool.

There are additional tools for developer security during the build practice such as Interactive Application Security Testing (IAST), Static Application Security Testing (SAST) and Runtime Application Self Protection (RASP). These are tools your developers should be interested in but you wouldn't be able to run without access to the underlying source code.

For IT professionals and software engineers, SCA and DAST should be considered a minimum security measure for software systems prior to bringing any software live. Additionally, these tests should be redone on a periodic basis as new vulnerabilities are discovered at any time. It's a continuous process. If you can get the software bill of materials from your vendors, whether for software or devices, you can and should perform an open source vulnerability test on those components and versions. You should always request this, to hold your vendors accountable. Similarly, it would be best practice to run a DAST test against your delivered software and against any IoT devices that have an API or internal Web endpoint so you can be aware of vulnerabilities.

In summary: build securely, verify, deliver, test, and continue to test periodically to mitigate risk.

About the Author

Tim Kenney, Chief Operating Officer, SOOS. Tim Kenney is on a mission to democratize software security. As President and COO of SOOS, Tim and his team are dedicated to ensuring all developers have the tools they need to identify and remediate code vulnerabilities, making software safer for everyone. Prior to leading SOOS, Tim was President and CTO of MyWebGrocer, a pioneer in the online grocery and big data space. He also has deep roots in healthcare tech, as a former VP of R&D at GE Healthcare Information Systems and at IDX. He is a lifelong Vermonter and frequently shares his expertise with the Vermont State Government in a wide range of areas and has been a board member of Vermont Information Technology Leaders. Find him online at Twitter: @soostech, www.SOOS.io, https://www.linkedin.com/in/tim-kenney-vt/

New Research Reveals Network Attacks at Highest Point Over the Last Three Years

By Corey Nachreiner, Chief Security Officer, WatchGuard Technologies

Cybersecurity threats continue to grow every year, with hackers consistently staying one step ahead through increasingly sophisticated, targeted attacks. Compounding that, for many organizations the shift to a hybrid workforce has dramatically increased the attack surface, offering more ways than ever for the bad guys to get in. To provide some insight into the threat landscape, each quarter WatchGuard Technologies' Threat Lab releases an Internet Security Report (ISR) based on threat intelligence and security expertise, outlining the top malware trends and network security threats over the previous three months.

Our most recent report, which looks at Q4 2021, revealed a record number of evasive malware attacks for the quarter, with a 33% increase in advanced threats, as well as the largest total network intrusion detections of any quarter over the past three years. So, let's take a look at some of the key takeaways from this year's report:

Total network attack detections continue to climb, highlighting the complexity of network security – The trajectory of network intrusion detections continued its upward climb with the largest total detections of any quarter in the last three years. This also represented a 39% increase quarter over quarter. This may be due to the continued targeting of old vulnerabilities as well as the growth in organizations' networks; as new devices come online and old vulnerabilities remain unpatched, network security is becoming more complex.

Malware threats were detected in EMEA at a much higher rate than other regions in the world – Europe, the Middle East and Africa were also the regions most targeted by malware threats in Q4. In fact, EMEA saw malware detections per Firebox (49%) at near or above double the rate as other regions of the world (AMER 23% and APAC 29%).

78% of malware delivered via encrypted connections is evasive – Overall, 67% of malware detections arrived over an encrypted connection, and within those malware detections, 78% were zero day malware threats that evade basic detections. This continues a trend seen in previous quarters. These threats can often be stopped at the perimeter by setting firewalls to decrypt and scan incoming traffic – a step that, unfortunately, many organizations fail to take.

A new leader in Office exploit malware emerges – Q4 saw a significant incidence of malware targeting Office documents, similar to findings from Q3. CVE-2018-0802 remains on the top 10 malware list, landing at number 5 this quarter, up one spot from last quarter, and remains on the most widespread malware list. Researchers suspect this may have replaced CVE-2017-11882 as the top Office exploit.

Emotet comes back with a vengeance – Two new malware domains were added this quarter to the list of top malware domains detected by WatchGuard. One of these domains, Skyprobar[.]info, has been linked to Emotet, the banking trojan that has evolved into a C2 and distribution infrastructure malware for other payloads. After diminishing due in part to direct disruption by US law enforcement, the Emotet malware saw a resurgence in Q4 2021.

In Q4 the Threat Lab saw the highest level of zero day threats the team has ever recorded, as well as an attack surface reaching well outside the network perimeter to home networks, mobile phones, smart devices, and more. This clearly demonstrates that attackers are getting more sophisticated and threats are becoming more damaging. To address this, organizations must implement a truly unified approach to security that is able to adjust quickly and efficiently in the face of emerging threats. By wrapping security services into a simple, “single pane of glass” strategy, organizations and casual Internet users alike can stay a step ahead of threat actors and significantly lower the chance of an attack.

About the Author

Corey Nachreiner is the Chief Security Officer at WatchGuard Technologies. A front-line cybersecurity expert for nearly two decades, Corey regularly contributes to security publications and speaks internationally at leading industry trade shows like RSA. He has written thousands of security alerts and educational articles and is the primary contributor to the Secplicity Community, which provides daily videos and content on the latest security threats, news and best practices. A Certified Information Systems Security Professional (CISSP), Corey enjoys "modding" any technical gizmo he can get his hands on and considers himself a hacker in the old sense of the word. Corey can be reached at https://www.watchguard.com.

Omnibus Spending Bill Highlights Need for Protecting Critical Infrastructure

By Tony D'Angelo, Vice President of Public Sector, Lookout

With international tensions continuing to rise, the Biden administration signed a $1.5 trillion omnibus spending bill in March that includes funding to bolster cybersecurity resources for U.S. critical infrastructure and billions of dollars for ongoing aid to the Ukrainian government.

This effort — combined, in part, with portions of a previous supplemental funding request — highlights a strengthening of cyber defenses in response to a crisis and points to specific sectors where operations are both critical and likely targets of potential serious cyberattacks, such as technology supply chain networks, electrical grids and large federal agencies that provide a wealth of essential citizen-facing services.

Since the beginning of the conflict in Ukraine, there have been fears that the cyber threats initially directed at Ukrainian government bodies and infrastructure could easily be targeted at other nations, especially in retaliation for ongoing sanctions from Western countries.

As seen with previous cyber threats, such as the 2017 NotPetya ransomware outbreak, targeted zero-day attacks could rapidly spread to other networks and cripple critical services.

While those institutions can serve as targets during a crisis, it's important for private and public sector leaders to implement lasting modernization efforts that strengthen the nation's cyber resilience with additional cyber spending.

U.S. seeks to safeguard the supply chains of dual use technologies

As part of the funding package, the Department of Commerce will increase the enforcement efforts of its Bureau of Industry and Security to help ensure strong export control technologies that have both civilian and military purposes, also known as dual-use technologies.

The department will also seek to analyze various potential chokepoints related to "U.S. supply vulnerabilities; technological infrastructure and information sharing platforms with allies and partners, as well as responses to chokepoints in the U.S. supply chain that could be used against U.S. interests," according to the initial budget request.

The manufacturing sector has been and will continue to be a prime target for cyberattacks within the supply chain, especially as they increasingly rely on cloud apps and mobile devices for their operations. According to research from Lookout, mobile phishing attacks spiked 118% in 2021 compared to 2020. This means attackers are recognizing these devices as a major attack vector to compromise an organization.

To ensure work-from-anywhere workers stay productive while safeguarding against these threats, organizations need to embrace zero trust architectures.

Funding to secure electrical grids in Ukraine and at home

Part of the omnibus bill provides funding for the Department of Energy to assist Ukraine in integrating its electrical grid with the European Network of Transmission System Operators for Electricity (ENTSO-E) to provide more stable electrical performance.

Along with this, it calls for the DOE to utilize its National Laboratory system to aid in "modeling and analytics, cybersecurity, synchronization and other assistance prior to an integration with ENTSO-E," according to the initial budget request.

This omnibus bill comes at a critical time for the energy sector, following 2021's Colonial Pipeline attack that impacted U.S. gas prices and could help defend critical power grids in a contested cyber environment.

There is also seeing an increase in cyberattacks targeted at the industry. As the 2021 Lookout Energy Industry Threat Report outlined, mobile phishing attacks on energy sector employees were up 161% compared to 2020. The energy sector also faces a mobile app threat exposure rate nearly double the average of all other industries combined, according to the same study.

As the conflict in eastern Europe continues, agencies will likely see a rise in cyberattacks such as phishing and ransomware.

Cyber-attacks in Ukraine could spread more broadly

The 2017 NotPetya ransomware attacks, while initially directed at Ukrainian businesses, soon spread to impact as many as 65 other nations, serving as what the White House called in 2018 the "most destructive and costly cyber-attack in history."

To prevent a similar event from occurring, the omnibus bill also includes national defense components and provisions related to the Treasury Department.

As the Treasury Department continues to enforce ongoing sanctions against the Russian government, its leaders and various oligarchs, funding from the omnibus aims to fortify the department from targeted cyberattacks.

Because of the heightened cyber threat posture of recent events, it's critical for federal agencies to take steps to safeguard their networks and help implement zero-trust plans to mitigate potential attacks.

Cyber resilience is critical

With this budget package, the federal government seeks to secure global supply chains and support Ukraine's technology infrastructure with new funding.

Already under increasing cyberthreats, critical infrastructure sectors remain susceptible to attacks as a result of the war in Ukraine. And with historical precedence of targeted attacks on Ukrainian networks spilling over to other countries, this spending bill will help secure essential operations both home and abroad. It will also reinforce cybersecurity postures that support the nation's digital transformation in the long run.

About the Author

Tony D'Angelo is the Vice President, Public Sector at Lookout. He leads the Americas Public Sector team, bringing more than 30 years of experience in the IT industry. Prior to joining Lookout, Tony held various sales leadership roles at Proofpoint, Polycom, Brocade and Nortel. Originally from New York, Tony received his Bachelor of Science in mechanical engineering from the University at Buffalo and has spent his entire professional career in Washington, D.C. Having joined Lookout in 2019 to lead the Americas commercial enterprise team, he now heads the combined federal-SLED business unit.

Tony can be reached online at https://www.linkedin.com/in/tony-d-angelo-2017867/ and at Lookout's company website https://www.lookout.com/.

Poor Identity Management Amplifies Ransomware

By David Mahdi, Chief Strategy Officer and CISO Advisor, Sectigo

While ransomware *is* malware, security leaders must go beyond legacy anti-malware approaches to mitigate risk. Ransomware is a data-centric threat; that is, ransomware preys on corporate data. Cunning and successful ransomware attacks hijack user access with an aim to encrypt sensitive files, stealing data. So, if ransomware is all about the data and the hijacking of user access to get to the data, then the more data a user can access, the more attractive target the user is for the attacker.

Ransomware is a multi-faceted cybersecurity issue, and best practice dictates using email security and antivirus, in addition to other tools to fend it off. Indeed, while these are good best practices, IT leaders need to undergo a crucial perspective change when it comes to ransomware and understand it isn't solely a traditional malware problem. Bad actors want access to data, and they gain access by compromising user accounts, or in other words, by compromising the identity layer of an organization. Without considering the importance of identity and data access, organizations will remain vulnerable to attack.

Yet, organizations and security leaders can't simply lock down identity and data access to prevent ransomware. Typically, IT departments tend to over privilege users to avoid interrupting business. While this approach generally helps day-to-day operations, it's also precisely what allows bad actors who breach the perimeter to run amok throughout the environment. If a highly privileged user and their associated accounts have a lot of access, when compromised, the amount of damage could be catastrophic. Focusing on identity and data security in terms of right-sized access will significantly reduce the attack surface for many threats, including ransomware.

With that in mind, enterprises must focus on establishing and maintaining trust for every single identity in their environment, both human and machine (software, bots, devices, applications, etc.). Otherwise known as identity-first security, the aim is to mitigate the damage from identity and data-centric attacks, such as ransomware.

Right-Sized Access and The Least Privilege Principal

Once trust is established with a digital identity, security leaders must then think about right-sized access. That is what that identity (or user) needs access to in order to fulfill its role requirements. Simply put, the path forward would be to leverage a "least privileged" approach.

Of course, ransomware attacks can still occur even with a least privilege or right-sized access approach. As such, behavior monitoring that focuses on identities and data is critical. By constantly gauging normal, anomalous, and malicious behavior, security leaders can achieve a better balance of security and business agility. The goal is to ensure that users and machines have the access they need, but that there is a safety net if a security issue occurs (I.e. insider attack, ransomware, or other threats).

Establishing Digital Trust for Digital Identities

Enterprises need a clear method of verifying and establishing digital trust for all (thousands or hundreds of thousands) types of identities, ensuring only valid and trusted users and machines can log into networks.

One proven way to establish digital trust in identities is by leveraging public key infrastructure (PKI) digital certificates. This technology has been around for decades and remains the most secure way to provide authentication and continuously prove identity, especially as the volume of both human and machine identities continues to rise. Certificates, issued by Certificate Authorities (CAs), provide validation that the user or machine is trusted and secure. PKI uses cryptographic keys to authenticate identities and is much more reliable than passwords or other traditional forms of authentication. When it comes to fending off ransomware, using PKI-based identities can and should act as the baseline for digital identities. Rooting digital identities in digital certificates, for humans and machines, ensures that identity-first security has a strong foundation.

Gartner, which first coined the concept of identity-first security in 2021, describes the approach as putting "identity at the center of security design." This way of thinking is a major step forward in cybersecurity because it replaces the legacy and dated approach of the walled fortresses pre-pandemic that left organizations feeling secure behind firewalls.

Connecting Identity-First Security to Data Security

While there are several best practices to employ from an overall identity-first security perspective, let's focus on data security. Data can take many forms, structured (databases), unstructured (I.e. files) or semi-structured. Regardless of the data type, knowledge about the data, its risk, sensitivity levels, and therefore classification should be established. Understanding the risk and classification levels of data should then be aligned to the overall identity-first security strategy. Ultimately, it will help security leaders understand what kind of data their users and machines have access to. Leveraging data access governance (DAG) tools are one approach to help close the data-access gap. However, DAG tools are

only as good as the trust in identities that they leverage to control corporate data. As such, security leaders must start with establishing trust in digital identities, as we discussed above.

Identity-first Security Is the Most Important Line of Defense for Ransomware Attacks

It's impossible to stop all cyberattacks, regardless of how much time, money, or labor enterprises pour into security. However, establishing digital trust for every identity – both human and machine – in company environment and ensuring right-sized access can limit the damage done by the attackers who break through.

Going forward when we think about ransomware, we need to recognize that at its core it is an identity and data access issue. Ransomware wants access to data, and it will typically compromise accounts/user identities to gain access to that data. So, rather than worrying about just malware detection, security and business leaders looking to improve their chances of coming out of a ransomware attack unscathed should establish strong identity-first and data security strategies. This includes knowing where all the sensitive data resides, and monitoring user and machine access to that data in order to mitigate ransomware and other cunning cybersecurity attacks.

About the Author

David Mahdi is the Chief Strategy Officer and CISO Advisor of Sectigo. In his role, David leads the company's overall strategy, direction, and M&A efforts to expand its leadership in the digital trust space. With 20+ years of experience in IT security, most recently serving as Vice President and Analyst in Security and Privacy at Gartner, David has helped large organizations tackle digital transformation projects in the digital trust, identity, cryptography, and cybersecurity spaces.

David can be reached online at (David.mahdi@sectigo.com, @davemahdi, linkedin.com/in/dmahdi.) and at our company website: https://sectigo.com/

Protect Small Businesses from Ransomware

By Prem Khatri, Vice President of Operations, Chetu, Inc.

Ransomware attacks are crippling businesses, government organizations, and educational institutions. And, these attacks are making the news.

In fact, the Sinclair Broadcast Group, a company that owns TV news stations, was hit by a ransomware attack in October 2021, according to Reuters. The wire service noted that some of Sinclair's servers and workstations had been encrypted by the malware.

In April of this year, the Costa Rican government was hit by a major ransomware attack that affected multiple government agencies, according to the Associated Press.

Even educational institutions have become targets of cyberattacks. On May 2, 2022, Kellogg Community College (KCC), a Michigan-based community college, issued a written statement saying that the college would close all five of its campuses and cancel classes as part of an effort to resolve a ransomware problem. KCC's website shows that the campuses are now open and classes have resumed.

Small businesses might not be as lucky, though. They might lack the resources needed to recover from ransomware, a type of malware that encrypts digital files, blocking access to them until an expensive ransom is paid. So, cybersecurity professionals should focus on providing software solutions that can be used to protect *these* businesses.

AdvisorSmith recently underscored the need for that protection. In November 2021, the company published the results of a survey showing that 41.8 percent of small businesses had been victims of a cyberattack in the past year.

Endpoint Security

These businesses must use endpoint security to guard against attacks. This type of security is used to secure a business network by protecting devices such as laptops, tablets, mobile phones, and digital printers from cyberattacks. Each of those devices serves as an endpoint, which is an entry point to a network.

Endpoint security software can analyze, detect, block, and contain cyberattacks. Two types of endpoint software are used by businesses to perform those tasks: endpoint protection platforms (EPP) and endpoint detection and response (EDR) software.

Layered Protection

EPP software typically uses a database of malware signatures for detection. These signatures are the identifying digital characteristics of malicious files and programs.

An EPP platform might not be enough to stop those files and programs, though. A different approach is needed.

In the research paper, *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*, the Cybersecurity and Infrastructure Security Agency (CISA) recommends a layered approach to security known as Defense in Depth. In the paper, CISA notes that this approach involves applying multiple layers of defense. The idea of this strategy is that if one layer of defense fails, another layer can be used to thwart cyber criminals.

One way to add layers of defense is to use endpoint detection and response (EDR), which was defined by Gartner.com analyst Anton Chuvakin as a set of tools for detection and incident response. EDR software can be used to detect malware that has made it past preliminary defenses. This software uses behavioral analysis to detect and respond to attacks.

Fileless Malware

One emerging threat that is particularly difficult to detect is fileless malware, which doesn't write files to a hard drive but exists in a computer's RAM instead. This type of malware infects trusted software applications that have already been installed on a computer and uses processes from the computer operating system to launch attacks.

Endpoint detection and response (EDR) software can use continuous monitoring techniques to detect fileless malware, according to Ben Canner, a writer and analyst for SolutionsReview.com, an enterprise software news website.

One particularly insidious version of this malware is fileless *ransomware*. In an article on TrendMicro.com, Karen Victor describes one such instance of fileless ransomware: Netwalker. In the article, Victor says

that the Netwalker ransomware attack is conducted through reflective dynamic-link library (DLL) injection. She also notes that this technique allows a DLL to be injected in a way that bypasses the windows loader. That way, she adds, the DLL isn't loaded as part of a process and can evade DLL monitoring tools.

A DLL is a program module containing code used by multiple programs that run on the Windows operating system.

Protection for Small Businesses

Ultimately, small businesses need access to advanced endpoint protection tools that can stop fileless ransomware and file-based ransomware. Such tools should be supplied as part of affordable solutions. After all, small businesses have extremely limited budgets but, as a whole, employ a lot of people.

Software proprietors and off-the-shelf software companies should work closely with these businesses to ensure that advanced endpoint software such as EDR software can be deployed quickly.

About the Author

Prem Khatri is the Vice President of Operations for Chetu, Inc., a global, custom software development company, where he oversees all development projects and technical operations. His primary responsibilities are to lead, track and manage technical teams that create custom software solutions. His background includes software development using C++, Java, and Microsoft technologies. Since joining Chetu in 2008, he has helped the company become an award-winning global presence in the customized software development field. Prior to joining Chetu, Prem worked for Tata Consultancy Services, as well as Blue Star Infotech, and is a graduate of both the University of Mumbai and Savitribai Phule Pune University. Prem is a certified Project Management Professional (PMP). He can be reached online at our company website, www.chetu.com.

Q&A With Mickey Bresman, CEO Of Identity Security Pioneer, Semperis

By Mickey Bresman,CEO of identity security pioneer, Semperis

Why should IT security pros focus on Active Directory?

Active Directory —AD—is the heart of most organizations' infrastructures. If AD is compromised, so are business operations. It's the #1 infrastructure target of ransomware attacks because if attackers can manipulate or take down AD, they can manipulate or take down anything, anywhere in your IT environment.

But although it is the backbone of most organizations' identity systems, AD has been largely unchanged for two decades. It was developed before the cloud, mainstream adoption of virtualization, before the spread of IoT devices, and before the rise of remote work and mobile devices. The biggest need for AD recovery at that time was in response to natural disasters or power outages—not cyberattacks. Security perimeters were based on physical infrastructure.

Now days, most organizations—especially larger organizations with AD implementations going back to the early 2000s —struggle to effectively secure this vital part of their infrastructure. For many years, admins were warned "not to mess with AD." So, misconfigurations and outdated entries have crept in over time. New threats and new ways to exploit vulnerabilities are emerging constantly. Many companies now have hybrid environments, mixing on-premises AD with Azure AD or other IDPs, which have different requirements and vulnerabilities. And organizations might be dealing with an AD implementation that involves thousands of users, servers, and devices over multiple years. Securing AD is no easy task, but it's absolutely vital.

What are security teams missing, and why?

Most organizations have very little insight into the nooks and crannies of Active Directory. AD is difficult to clean up over time, and attackers know and exploit this fact. AD admins are consumed with simply managing the identity service. In a large organization, they might get tens of thousands of changes per day. They don't have time to proactively evaluate AD security or keep track of security indicators—warning signs of exposure or compromise. The basis for many of these vulnerabilities are outdated configurations, misconfigurations, and other risky settings that need to be cleaned up but are difficult to find.

AD admins often rely on security logs, but many attacks bypass logging. The attackers are adept at covering their tracks. So, failing to catch indicators of exposure or compromise isn't the result of a lack of knowledge; it's simply the result of the sheer amount of information and, often, a lack of automation and reliable notification.

On top of that, many early assumptions about AD no longer hold true. Some of the best practices that many admins learned years ago are now out of date. For example, in the early days of AD, the domain was understood to be the security boundary. As a result, many companies implemented multiple domains. Now, it has been proven that domains are not a security boundary; forests are, but restructuring AD is a complex and risky project. Even more recent recommendations, like Red Forest, are now being decommissioned.

What's at stake if organizations are breached?

Semperis' recommendation—and that of pretty much any security expert as well as the U.S. FBI and other government agencies—is that organizations should not pay ransom. Aside from the fact that there's no guarantee that attackers will honor their word to return data or unlock systems, your funds are going to be used for nefarious purposes. Financial losses include the cost of downtime, costs related to potential data loss and loss of reputation or intellectual property, and the cost of the resources you'll need to recover Active Directory. Unfortunately, unless you have a good and tested recovery plan that can be trusted in a time of a disaster, you are left with few options.

Beyond that, cyberattackers are now targeting industries that used to be off limits—like healthcare—so preventing or quickly recovering from an attack can literally be a matter of life or death. And as the recent news of a proposed $1 million fine for the Colonial Pipeline attack illustrates, organizations could also be subject to hefty regulatory fines and penalties for failure to properly secure their environments.

Why are Active Directory assessments vital?

Most organizations don't realize how vulnerable their Active Directory implementation is. Running a comprehensive assessment enables you to create a baseline and then monitor improvements against it.

This is why we created a free tool for the community, Purple Knight, a security assessment tool that provides valuable insight into your AD security posture. The standalone tool queries your AD environment

and performs a comprehensive set of tests against many aspects of your AD security posture, including AD delegation, account security, infrastructure security, Group Policy security, and Kerberos security. Purple Knight runs on a domain joined computer in the forest you want to evaluate or uses "Run As" credentials to a trusted forest. The tool looks at AD from the perspective of an attacker, so it has no dependency on any other product, doesn't require an installation, and doesn't require any special privileges to run.

What do assessments reveal?

In the year since we released Purple Knight, more than 5,000 organizations around the world have used it to assess Active Directory. That's a great sign that organizations are becoming more aware of the importance of AD security.

We recently conducted a survey of Purple Knight users. Across the 1,000 organizations that participated, the average score—on a scale of 0 to 100, where 100 means that no indicators of exposure were found—was just 68. That's barely passing.

The tool also provides category-specific scores across five categories: account security, Group Policy, Kerberos security, AD delegation, and AD infrastructure. We found that account security scored lowest. This category score reflects challenges in password management, permissions drift from nested groups or other groups that need to be cleaned up, and other risky settings. We also found that organizations in the transportation, retail, and healthcare industries had the lowest scores, so that's a sign that organizations in those industries can benefit by taking a hard look at AD security.

What should organizations do with assessment results?

Whatever tool you use to assess Active Directory, your next step is to prioritize your efforts to harden the most vulnerable areas. This is especially important for industries that offer critical services or that are prime targets for attackers, or if the assessment shows vulnerabilities that are particularly popular with attackers. The Purple Knight user report provides initial recommendations and a list of prioritized steps to take.

Organizations can also use assessments to identify gaps that might exist in their AD in advance of a merger—of companies or domains. Closing those gaps in advance can make AD management much less painful after the merger occurs.

In conclusion, what's the biggest misconception about Active Directory security?

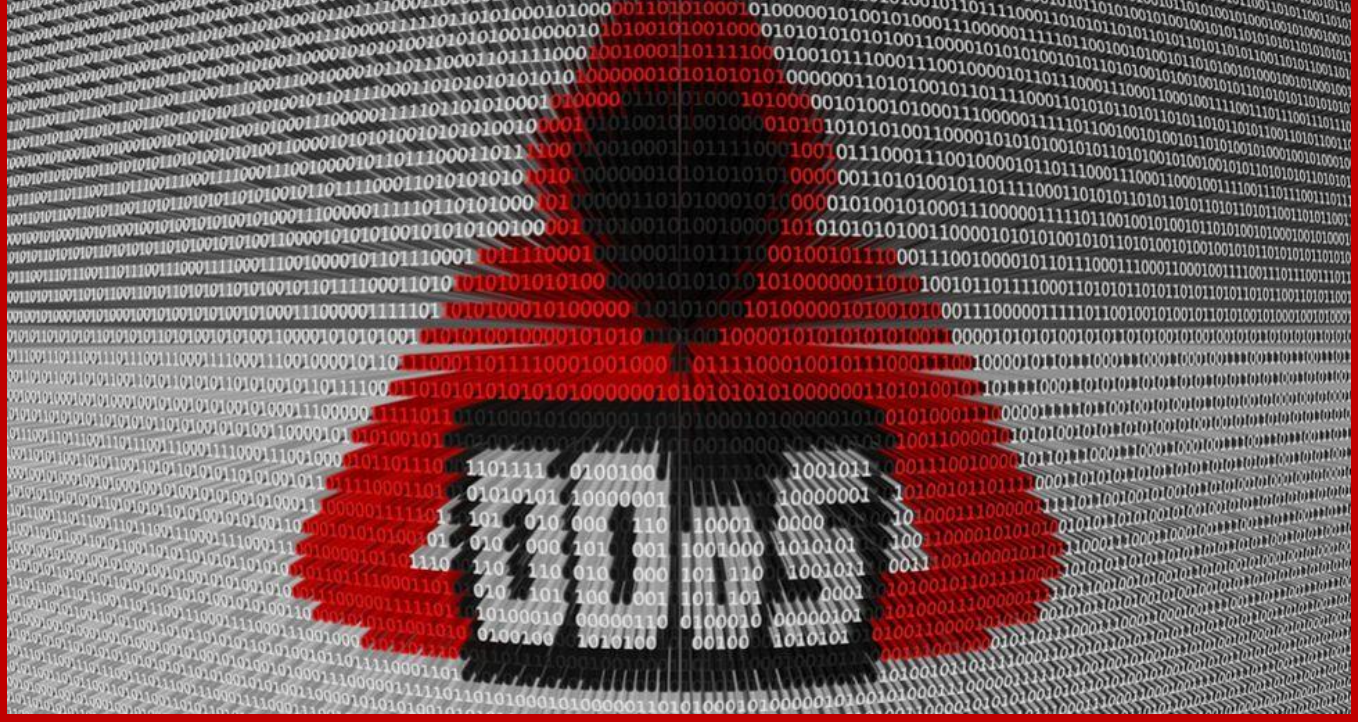
I think the biggest misconception is that so many organizations are used to having AD around—so just like with air, they don't think about it until something goes wrong. They might have endpoint or other types of security products in place, so they don't think they need an Active Directory – specific solution. Or they have an incident response plan, but it hasn't been updated to account for changes in technology. Or

they're using a solution that addresses one part of the AD attack lifecycle but doesn't provide comprehensive security for the entire attack kill chain. With AD playing such a crucial part in your organizational security and operation, I'd recommend running an assessment to confirm you are covered on all bases. After all, when it comes to protecting AD against cyberattacks, there's no such thing as "too secure."

About the Author

Mickey Bresman is the CEO and Co-Founder of Semperis and leads the company's overall strategic vision and implementation. A long-time enterprise software expert, Mickey began his technical career in the Navy computing technical unit over a decade ago. Prior to co-founding Semperis, Mickey was the CTO of a Microsoft gold partner integration company, YouCC Technologies, successfully growing the company's overall performance year over year. Mickey holds a BA in Technical Management and a Minor in Electronic Engineering.

Mickey Bresman can be reached at https://www.linkedin.com/in/%E2%9A%99-mickey-bresman-1574923/ and at http://www.semperis.com



Raising the Alarm on DDoS Attacks

By Ivan Shefrin, Executive Director for Managed Security Services at Comcast Business

Many organizations underappreciate the risk of distributed denial-of-service (DDoS) attacks, which remain a significant threat to the availability of networks, systems, and application infrastructure. Recent events shown just how costly DDoS attacks can be.

DDoS attacks compromise the availability of network, server, and application resources to render them unavailable for legitimate users. Criminals and nation states can launch severe DDoS attacks using millions of compromised botnet computers simultaneously. Botnets help ensure attacker anonymity because malicious traffic originates from what would otherwise be a legitimate IP address. DDoS attacks are hard to defend against because they often look like legitimate traffic and firewalls can run out of capacity. Defending against DDoS attacks upstream of your perimeter is a best practice to maintain Internet availability.

Threat actors constantly innovate to exploit new attack vectors, to avoid detection, and to hide their tracks. Defenders must continually evolve their countermeasures to stay safe from financial and reputational damage. With good reason, business and public sector stakeholders currently focus on defending against malware and zero-day vulnerabilities. However, because DDoS attacks are much less expensive and easier to launch than ransomware but can still cause a complete outage lasting for days, they are a significant residual risk. With the right partner, defending yourself against DDoS attacks is relatively straightforward. The first step is to determine if your organization is at risk and how much a complete outage would cost you.

The state of DDoS attacks

2021 was a record year for global DDoS attacks – at 9.84 million, it represents a 14% increase from two years prior. But this number is likely much higher, as some corporations have extensive internal resources to withstand attacks without noticeable disruption, and most typically don't report publicly on attacks against their networks, applications, and infrastructure. This trend may change with new cybersecurity regulations.

Buoyed by the COVID-19 pandemic and the quick transition to remote work environments, Comcast Business threat research shows DDoS attacks have evolved into a lucrative business and, unfortunately, are here to stay.

Why are DDoS attacks so prevalent?

While threats like ransomware can take months to develop, DDoS attacks are very sudden. A large one can result in a complete business outage just as effectively as ransomware. That's why we've seen them increase by over 125% in the last couple of years.

There are several reasons why DDoS attacks have greatly increased in popularity. For one, these attacks are incredibly cheap and easy to create, and the attacker does not need to have any technical knowledge. All the attacker needs to know is the target IP address or range of IP addresses they want to attack.

Secondly, it is more difficult to defend against DDoS attacks that target multiple layers. In fact, multi-vector attacks involving layers 3, 4, and 7 combined rose 47% in 2021.

Multi-vector DDoS attacks aren't new, but our research shows criminals increasingly using repeat short-duration vectors, often part of multi-vector attacks, as a misdirection tactic to distract IT teams while exploiting other network vulnerabilities to steal data, activate malware, or install viruses. Short duration attacks are more difficult to detect, and you have less time to respond.

For instance, DDoS attacks using L7 application services are designed to masquerade as legitimate traffic to avoid detection. This makes multi-vector DDoS attacks harder for victims to defend against.

Lastly, the volume of DDoS attacks is driven by the economics of botnets. These large networks of compromised computers and IoT devices across the internet can be used for a variety of malicious cyber activities, including DDoS attacks, e-commerce click fraud, ransomware, and crypto mining to name a few. Additionally, it is very easy to repurpose botnets across different types of attack vectors.

This has led to the creation of a botnet black marketplace across the criminal underground. Essentially, botnets have become a fungible asset for organized crime. As the price of crypto currencies drops, we expect to see a corresponding drop in botnet crypto mining.

Finding weak spots in your cybersecurity plan

With threat actors constantly changing tactics, techniques, and procedures (TTP), organizations must stay equally vigilant to protect their infrastructure from bad actors determined to cause financial or reputational damage. This includes assessing your risks and assets to find DDoS vulnerabilities.

Bad actors often combine strategies for maximum impact against easy, unprotected targets. They may launch repeated short burst attacks to distract or consume the resources of an IT organization. And, while the organization is at capacity defending itself, aggressors may use several small-volume attacks to map out network vulnerabilities for follow-up data breaches. We increasingly see ransomware attacks launched against business customers in combination with DDoS. After all, attackers can leverage the same botnets for both purposes.

Even if you are a small business and think you are at a lower risk, you could be in the supply chain for a larger organization that's a target. Before ignoring the risk of a DDoS attack, ask yourself if your organization can shoulder the costs of reputational damage or lost opportunity and if you'll be able to recover from the financial damage.

Considerations for mitigating DDoS attacks

DDoS attacks can bring even large enterprise networks to their knees, prevent businesses from reaching customers, cause financial and reputational damage, and even force businesses to close their doors. Yet, they can also be difficult to recognize. Often, business owners may just assume that their network is down, when in reality the server is under attack. Lengthy dwell times to determine the root cause mean organizations lose even more revenue during a DDoS-related outage.

The best way organizations can effectively protect themselves against DDoS attacks is by using a fully managed DDoS mitigation service provider that can block malicious traffic at the provider's network edge before it ever reaches the target. These services provide real-time detection to minimize damage and typically mitigate attacks within seconds.

Regardless of whether an organization wants to mitigate the residual risk of DDoS attacks, there are steps everyone should take to assist with detection. Implementing an advanced firewall rate-limiting policy at least gives IT an early warning and better log details about whether a DDoS attack is underway. In addition, many DDoS mitigation service providers also offer emergency options that IT organizations can use in a pinch after an attack takes place.

It is vital that businesses of all sizes take active steps in DDoS attack prevention and mitigation to help maintain network availability. Investing in the right security tools and services can provide an extra layer of defense to prevent DDoS attacks from taking over your business.

About the Author

Ivan Shefrin is the executive director of Managed Security Services for Comcast Business. He is a hands-on cybersecurity leader with 25-years of experience partnering with enterprise and communication service providers to anticipate and capitalize on disruptive technology trends, transform IT architectures, and generate security value using data analytics, machine learning and automated threat response. He is responsible for Comcast Business DDoS mitigation, managed detection and response, and endpoint protection services.

Ivan can be reached online at business.comcast.com/enterprise.

Russia's Invasion of Ukraine Lays Ground for a New Era of Cyberwarfare

Russia is known to be the world's leading hacking superpower for a reason. The country has an infamous history of executing high impact cyberattacks, often aimed at one of the most critical functions of any nation: its infrastructure.

We've seen this play out against Ukraine, even before the current geopolitical uprisings.

By Alon Nachmany, Field CISO of AppViewX

In 2015, Russia sabotaged Ukraine's power grid that caused a massive blackout and affected nearly 80,000 customers. The country issued another attack the very next year in Kyiv that left about one-fifth of its citizens powerless. And two years after that, Russian state-sponsored actors unleashed one of Ukraine's biggest supply-chain attacks via the NotPetya virus—a destructive malware that affected several electric utility companies in the region. Worldwide fallout ensued, disrupting operations across many different industries and causing more than 10 billion USD in damages. Since then, independent Russian hackers have also been linked to several insidious global Operational Technology (OT) security breaches.

Fast forward to 2022, and Russia has used similar tactics as an alternative battlefield to its war on Ukraine. From more than 3,000 DDoS attacks unleashed on Ukrainian government websites, to other more small-scale but harmful, Russian-based attacks reported in other western countries to those that condemned its actions – the impact has again amounted to global proportions.

In the wake of escalated cyber threats, U.S. President Joe Biden alerted companies and government entities to the surge of activity aimed at the U.S. and called for "hardening cyber defenses immediately" – a battle cry that has echoed in a variety of ways from numerous U.S. government agencies, industry organizations, and experts. The FBI specifically warned U.S. energy organizations to closely inspect their network traffic after discovering increased network scanning activity from multiple Russian-based IP addresses, and security experts urged critical infrastructure organizations to be on "high alert" when Russian hackers scanned five U.S. energy companies.

While POTUS preemptively warned Russia that if it launched an attack on any critical infrastructure within the U.S., the country would be "prepared to respond"—amidst looming threats like the latest BlackCat malware—is U.S. infrastructure realistically prepared for such offenses?

The sorry state of current OT security

OT is a combination of hardware and software used to monitor and control industrial equipment in critical infrastructures, such as power plants, water treatment systems, transportation, and gas pipelines. It includes, among others, PLCs (Programmable Logic Controllers), SCADA (supervisory control and data acquisition) systems, DCS (distributed control systems), and lighting controls. Within these are special systems used to control physical devices such as pumps, valves, electricity meters, and light poles that need to operate around the clock.

Previous attacks on these OT systems were not as common as they are today. Before the days of digital transformation -- and due to the highly critical nature of their operations -- OT systems were completely air-gapped and therefore impenetrable, limiting threat actors to exploit IT networks. This also allowed for weaker security on these systems. But as more critical infrastructure organizations transition to digital models for stronger efficiency, OT systems are now connected to IT networks and the cloud. The IT-OT integration has connected the once isolated OT network to the internet, exposing all of the OT systems to the attack surface.

Unfortunately, our critical infrastructure isn't as prepared as it should be, and the implications are not fully realized. Many agencies and companies are often underfunded and reliant on incredibly outdated technology, meaning the security of OT technologies is also dated. With the typical lifespan of OT systems around ten years, agencies hardly plan for patches or upgrades, leaving vulnerabilities continuously unaddressed.

For example, in some water treatment facilities, pump controllers do not require passwords for access or don't use encryption for communications. This means that if there is a password, an attacker just needs to stay online long enough to hear a password and then use it to enter the network.

There's also the issue of technology mismanagement due to third-party vendors or partners. For example, there are ports connected to other organizations that do not have accurate information about their cable connections. So, when a partner suffers a ransomware attack, no one knows which cable to unplug.

Since organizations have predominantly focused on securing IT systems, many cybersecurity professionals lack the skill to work with OT technology. In addition, OT system operators are neither informed of the security risks nor trained on cybersecurity. As “availability” is a top priority in an OT environment, operators always put the continuous operation of OT systems above the integrity and confidentiality of data -- a combustible combination of circumstances.

What could happen if the critical infrastructures were attacked?

In May 2021, a ransomware attack took down the mighty Colonial Pipeline that supplies diesel, gasoline, heating oil, and jet fuel to 19 states across the U.S. The attack has since been attributed to a Russian ransomware gang called the DarkSide. During the days of the attack, the pipeline shut down its industrial control systems for about a week, causing fuel panic-buying, supply shortage, and price hikes. Had the pipeline been shut down for longer, the cascading effects could have been devastating. Eventually, first responders would have run out of fuel and been unable to respond to emergencies, causing mayhem in many major cities.

In another dangerous incident in February last year, hackers broke into the systems of a Florida city’s water treatment plant with the intent of poisoning the water supply. They attempted to increase the level of sodium hydroxide (commonly known as Lye) in the water supply to make it poisonous for consumption. While the attack was thwarted in time, it did threaten the safety of local customers.

The Electrical Grid is another critical infrastructure that powers the nation’s economy and safety. Any disruption in the power sector would have a debilitating effect on the nation’s security, economy, and public safety. Once hackers infiltrate a power plant's network, they can quietly lurk inside for several months, learning the systems before orchestrating an attack. They could also alter critical data, change settings, disable security functions, or even upgrading firmware to help facilitate the attack. We all remember the infamous Northeast blackout of 2003 that affected more than 50 million people across eight states and parts of Canada. The power outage lasted more than a day and resulted in incidents of reckless looting and torching and claimed the lives of 11 people.

Don’t plan to repent at the eleventh hour, prepare for war today

Although experts believe that Russia is exercising restraint in launching a full-scale cyber assault, developments are continuing to unfold and it’s only a matter of time before the lid is fully blown off.

President Biden’s 2023 federal budget plan budget proposal clearly underlined the urgent need to shore up defenses against this. Critical infrastructures such as power, water, gas, and health are a nation’s lifeline and must be protected at all costs. Given that these are prime targets for malicious actors, organizations operating these critical infrastructures must focus on taking a defense-in-depth approach by implementing Zero-Trust security controls at every level.

To accomplish this, it is important they invest in technology that helps:

1. Achieve end-to-end visibility of all the assets in the IT and OT networks
2. Takes control of all assets to provide right access to the right resources at the right time
3. Continuously monitor assets for anomalous behavior

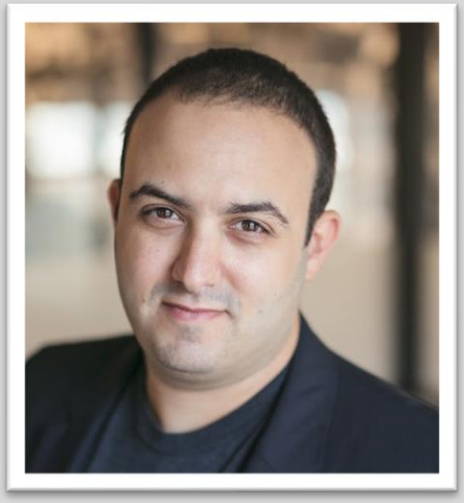
To that end, organizations must treat identity as the new perimeter and reinforce identity and access management, an effective OT security solution.

It is essential to understand that it is not enough to only verify user identities; machines, too, must be verified before allowing network access. Every OT system connected to the internet, such as the PLC must be secured with digital certificates and keys. It must be authenticated before every communication and be constantly monitored. This includes implementing strong encryption standards for all machine-to-machine communications. In addition, machine identities should be managed efficiently, so they do not serve as weak links in the system.

Leaders should also plan to upgrade outdated software and hardware systems that no longer support modern security controls. Without adequate security, they would be highly vulnerable to cyberattacks. Strong security policies must be enforced across the organization to prevent security gaps and improve OT compliance.

It's not an exaggeration to say that cyberattacks may affect the functioning of life as we know it. These threats are a big deal and cyber postures across all operations can no longer be an afterthought. The best way forward is to shield up, follow cyber-hygiene, and always stay vigilant.

About the Author



Alon Nachmany is a cybersecurity expert currently working with Fortune 500 enterprises in helping them achieve their security goals at AppViewX. His experience in leadership roles across industries from small start-ups to established enterprises has enabled him to secure some of the most cutting-edge innovations in the world of technology.

In the past Alon has served as the Director of IT and Information Security for WeWork and the CISO for National Securities Corporation, uniquely positioning him to understand and address the mounting security challenges of the modern-day enterprise. His feet are firmly planted on the ground, his eyes are turned to the skies, but he spends most of his days in cyberspace.

Alon Nachmany can be found on LinkedIn

Scared Of Your Own Shadow IT? Addressing The Top Security Concern Around SaaS Adoption

By Uri Haramati, co-founder and CEO, Torii

The pandemic struck, and organizations were forced to embrace remote work and cloud applications. Software-as-a-Service (SaaS) apps like Zoom and Slack kept us connected, while others like Asana and Monday kept us organized. But today, businesses are reevaluating the future of work in digital HQs, and IT leaders are sharply focused on security and Shadow IT.

According to Torii's 2022 SaaS Visibility and Impact Report, 69% of tech executives reported that Shadow IT—unsanctioned technology used by employees without the IT department's knowledge—is a top concern related to SaaS adoption.

Why Shadow IT is increasing (and why it's here to stay)

It's not just the physical workplace that's decentralized. SaaS stacks and tech decisions have followed suit, driving Shadow IT adoption to a new level.

To quickly build the digital workplace with SaaS apps, organizations were willing to bend some rules—55% of organizations made exceptions to their security protocols for SaaS applications. Why? The vast majority (80%) say those applications were adopted outside IT's purview.

While 36% of tech executives reported that line of business (LOB) managers are driving the adoption of unsanctioned apps, individual employees are even more likely to experiment and implement new applications autonomously.

The reality is, if employees think their company's existing tools are insufficient to do their jobs, they'll find their own solutions. Any employee with a corporate email, three minutes to fill out a trial form, and a credit card, has instant access to thousands of applications, each with the ability to integrate with business-critical apps.

Businesses need to also consider that digital natives are taking over as the majority in the workforce. They've lived with and used cloud technology for most of their lives, and their comfortability with tech will likely continue to drive Shadow IT growth.

For the sake of innovation, experimentation, creativity and efficiency, these apps could be a major win for employees and the business overall. But where cybersecurity's concerned, shadow IT apps pose a threat if they're unmonitored.

Why shadow IT poses threats

Cybersecurity breaches are extremely costly. As we've all seen, they can cripple companies. In a time where many business leaders are trying to minimize cost, maximize ROI, and ensure business continuity, keeping security tight is mission critical.

IT leaders with Shadow IT in their blind spot are rightfully spooked. Sensitive data —which cybercriminals would be thrilled to get their hands on—flows in and out of those unsanctioned apps. And if those apps have configuration errors, weak login credentials or unauthorized users, your data is at even greater risk.

And Shadow IT's threat doesn't end with an employee's tenure. The SaaS Visibility and Impact Report found that offboarding people from applications was the second greatest concern, right behind Shadow IT. If employees leave a company or consultants complete their engagements and aren't immediately offboarded from all SaaS apps–including those procured by Shadow IT–, they can still access sensitive corporate data and information, without anyone's knowledge.

Full offboarding can only be done when you know what apps you have and who has access to them in real-time.

But with the ever-present specter of Shadow IT, how can organizations truly protect against breaches? How can they act on what they can't see? The answer is in SaaS management.

How SaaS management platforms illuminate and secure Shadow IT

Visibility is your greatest defense against security threats posed by Shadow IT, and that's where SaaS management platforms (SMPs) shine.

SMPs that are designed to automatically discover all sanctioned and unsanctioned applications on your employees' laptops in real-time, give IT security teams a single orchestration point for visibility, control and risk management. Knowing all the cloud apps in use or licensed within your company means that you can take steps to turn unsanctioned Shadow apps into known, sanctioned and secure apps.

SMPs can also make the offboarding process more secure. When integrated with HR systems, an SMP can automate deprovisioning when it detects changes in employment. In other words, if an employee is on their way out, the SMP can automatically remove their access to all sanctioned and unsanctioned apps, and the sensitive data they contain. They also provide audit trails that give visibility into who had access to what apps and when, in the event of breaches.

The Shadow IT name itself implies there are inherent threats—monsters lurking in the unseen cloud app world. But when properly monitored and secured, Shadow IT can also represent value. If business leaders or individual employees find and adopt tools that power greater efficiency, keep them engaged and that they enjoy using, why not support that? With an SMP, businesses don't have to fight autonomous decisions and experimentation with SaaS apps.

Rather than take a fingers-crossed-that-nothing-bad-happens approach, or a locked-down approach where rigid guardrails block employees from using company credentials to adopt apps unless explicitly authorized, businesses can use an SMP to put checks and balances in place so threats can't hide in the shadows.

About the Author

Uri Haramati is Co-Founder and CEO of Torii, whose automated SaaS management platform helps modern IT drive businesses forward by making the best use of SaaS. A serial entrepreneur, Uri has founded several successful startups including Life on Air, the parent company behind popular apps such as Meerkat and Houseparty. He also started Skedook, an event discovery app. Uri is passionate about innovating technology that solves complex challenges and creates new opportunities. Uri can be found on LinkedIn and at our company website: https://www.toriihq.com/

Smart IoT Security Starts with a Secure Network

How to safeguard your IoT implementation to reap the benefits without the risk

By Matthew Margetts, Sales & Marketing Director, Smarter Technologies

From mobile phones to smart grids and supply chain management, the Internet of Things (IoT) has become entrenched as an essential part of our daily lives. All these items send and receive data over an IoT network, inducing variety and volume of data in the shared space. Notwithstanding the advantages of the IoT, it also presents a range of potential security risks; risks that many traditional IT security models are unable to cope with.

In our increasingly digital world, where smart sensors can detect information from the physical world, perform specified instructions, and relay the data to other systems, the amount of generated data is constantly growing, creating new challenges in terms of scalability and security. Cyber-attacks are also a very real threat, since IoT devices open the way for hackers to penetrate connected vehicles, critical infrastructure, businesses and even people's homes.

According to research commissioned by Opengear, network engineers and CIOs agree that cybersecurity issues represent the most significant risk for organizations that fail to put networks at the heart of digital-transformation plans. The study found that 53% of network engineers and 52% of CIOs rank cybersecurity among the list of their biggest risks. When it comes to the digital transformation of networking, 70% of network engineers say security is the most important focus area, and 31% say network security is their biggest networking priority. Their concerns are justified, fueled by an escalating number of cyberattacks. CIOs reported a 61% increase in cybersecurity attacks and breaches from 2020-21 compared to the preceding two years.

With security front of mind when it comes to any networking decision, how can today's CIOs and network engineers find the most secure solutions for their IoT network rollouts?

Here are some security best practices to follow:

Securing IoT networks with a zero trust approach

With a zero trust model, devices and users are not automatically trusted. This prevents unknown entities are prevented from gaining access to a particular network. Rather, the system constantly checks and re-checks each user and user permissions when they try to access any data. Zero trust principles should be implemented at both a device level and an IoT network level to protect against vulnerabilities that may arise from IoT device manufacturer hacks.

End-to-end encryption

End-to-end encryption (E2EE) implementation prevents third parties from accessing data while it's transferred from one end system or device to another, which is crucial for an IoT network. All data should be encrypted from the point it is generated to wherever it is transmitted. When E2EE is in place, data is encrypted on the sender's system or device, and only the intended recipient can decrypt it. Data is thus secured against tampering from hackers, internet service providers, application service providers, or any other entities or services. Crucially, end-to-end encryption works in conjunction with the zero trust principle. This means that even if an “eavesdropper” were to access a network pipeline, E2EE ensures confidentiality.

Choosing RFID over GPS

When choosing a data network for IoT implementation, RFID and GPS (or a combination of the two) are common data transfer methods. Both RFID technology and GPS enabled devices face both back-end and front-end security threats, with back-end communication happening over the internet protocol. Generally speaking, back-end security protocols are well developed and less vulnerable to security threats than the front end. When comparing RFID and GPS, GPS front-end communication is more vulnerable to security threats than RFID technology. Because the front-end communication goes through multiple nodes, a typical GPS front-end communication is more vulnerable to spoofing, which is when a hacker creates a false impression about the location of the device.

An end-to-end Internet of Things (IoT) low-power radio network solution like Smarter Technologies’ Orion Data Network incorporates end-to-end encryption and zero trust network infrastructure. It also has the benefit of being a private network, which means more control over traffic, confirmed capacity, and an inherent level of security.

The interconnection of all devices will result in increased automation in nearly all fields, which will lead to increases in efficiency, accuracy, and economic benefit, as well as a reduction in human intervention. The possibilities are endless, but ultimately, to reap the full benefits of the IoT, organisations need to prioritise network and device security at all levels.

About the Author

Mattthew Margetts is Director of Sales & Marketing at Smarter Technologies. His background includes working for blue-chip companies such as AppNexus, AOL/ Verizon, and Microsoft in the UK, Far East and Australia.

Matthew can be reached online at https://www.linkedin.com/in/matthew-margetts-36b5181/ and at our company website: www.smartertechnologies.com

VIP3R: Dissecting A New Venomous Spearphishing Campaign

By Tom McVey, Solution Architect at Menlo Security.

Social engineering attacks are among the most prevalent and dangerous threats facing organizations globally today.

One study shows that 83% of organizations experienced a successful email-based phishing attack in 2021, which saw a user being tricked into risky action, such as clicking a bad link, downloading malware, providing credentials, or even executing a wire transfer. Cisco's 2021 Cybersecurity threat trends report concurs, suggesting that at least one person clicks on a phishing link in around 86% of organizations, the firm also linking nine in 10 data breaches to phishing attacks.

For many firms, the human is the weakest link in their cybersecurity defenses – and threat actors know it, continuing to launch phishing campaigns in various forms at scale year after year. They take advantage of our inherent cognitive biases, tricking us into entering our credentials. When you combine that bias with the tactics used by attackers, it makes these attacks very successful.

Many attackers opt for a 'spray-and-pray' approach, looking to spread their net far and wide to reach as great a number of potential victims as possible. However, others pursue a more dangerous approach in the form of spearphishing, launching highly tailored attacks that meticulously target specific organizations or individuals in an attempt to achieve greater success.

It is the latter that our team in Menlo Labs recently identified after discovering an open directory full of usernames and passwords.

Upon analyzing the contents of the web server, we found that a single spearphishing campaign had successfully compromised the credentials of 164 users at various companies using 147 unique lures, targeting organizations from cybersecurity companies to financial services – and everything inbetween.

While analyzing the kit, we spotted a unique string: “DH4 VIP3R L337”. Having not seen this previously, we decided to dig a little deeper.

A unique way of validating victim credentials

In analyzing the attack sequence, we found that the attackers would begin by sending a customized HTML attachment payload to its target victims. Should they fail to detect its malicious intent and open the attachment, they would be presented with a phishing page impersonating a service that they would typically use.

Why did the attackers opt to use a HTML attachment? While most secure email gateways (SEG) have default blocks for certain file types, HTML attachments are exempt from these defenses. This is because many large financial firms send encrypted emails that require you to first register and create an account to securely view the message, and these encrypted emails are usually in the form of HTML attachments.

Once the victim submitted their credentials, validation and verification of the password happens on the server side and a response is sent accordingly. This part of the process would be achieved using the PHPMailer library, sending an email with the victim’s username and password directly to an email address controlled by the attacker.

If the email failed (i.e., the verification of the password fails), an error message in the form of a “json response” would be sent back to the user via the browser, who would then be redirected to the legitimate website of the lure. However, if the email was sent and password verification was successful, then the client would be to a pdf hosted on Microsoft OneDrive.

In this way, the attacker created a unique way of validating the credentials submitted by the victim.

The Menlo Labs team has concluded that it is likely that these HTML attachments are being created automatically using a payload generator kit. Having spent significant time looking for it, we have been ultimately unable to locate it at present. Therefore, until we uncover any further information, we’ll be tracking it as “VIP3R_L33T Generator”.

Combatting progressive phishing threats

Credential phishing continues to the most common form of attack that we see our customers facing. Across geographies, industry verticals, and different sized organizations... everyone is affected.

More than one fifth of the attacks that we see on our platform are credential phishing attacks, with 7% of not being detected by legacy URL reputation engines. This evasion of legacy URL reputation evasion techniques (dubbed LURE by the Menlo Labs team) can be attributed to one of the four evasive techniques found in Highly Evasive Adaptive Threats (HEAT).

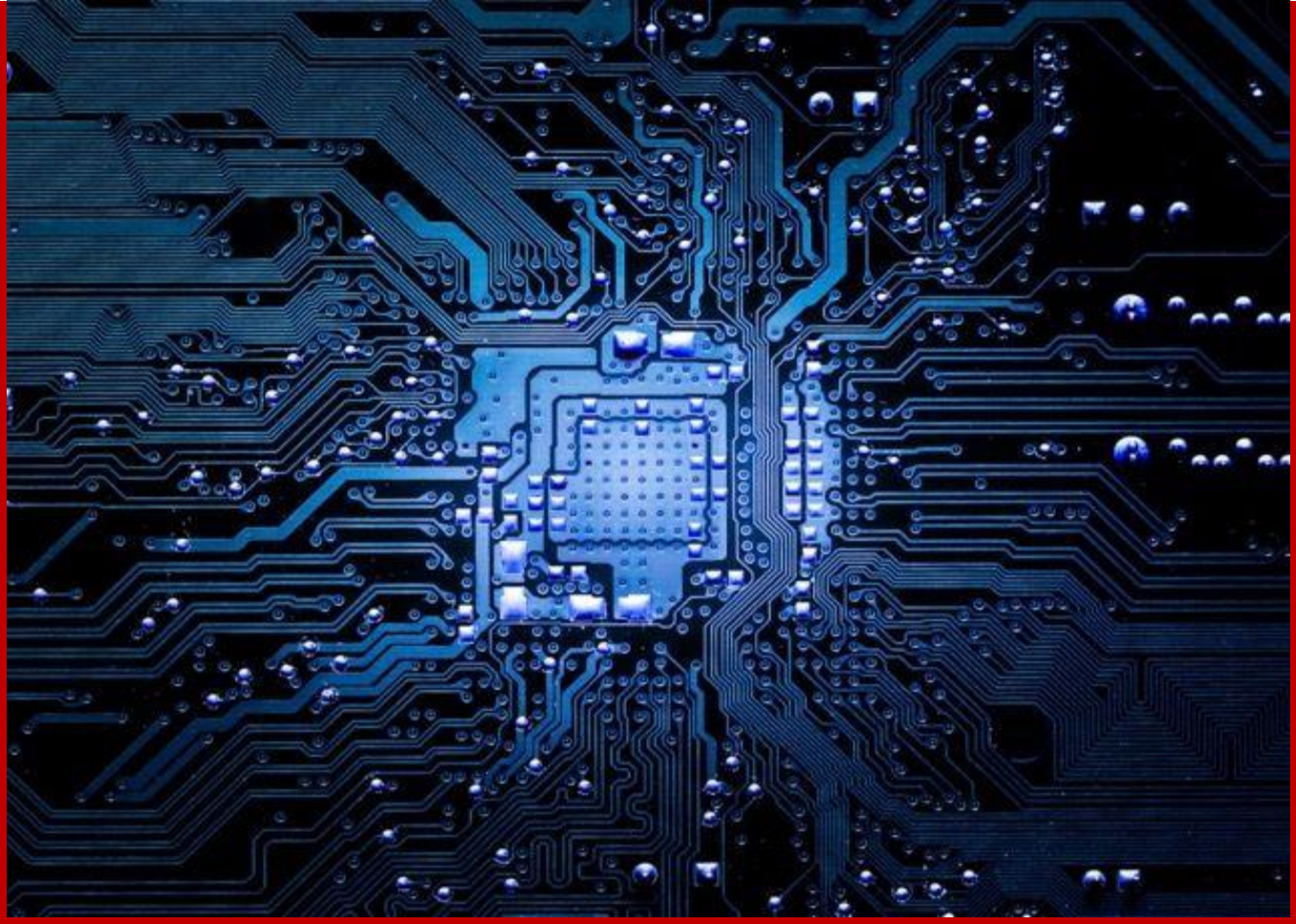
Critically, we have seen a distinct uptick in HEAT attacks.

After analyzing more than half a million malicious URLs, the team determined that 69% of them leveraged HEAT tactics. Further, it observed a 224% increase in HEAT attacks in the second half of 2021.

To protect against phishing, organizations should always look to improving cybersecurity awareness first through training and education initiatives. To mitigate the threat of evasive threats, however, modern businesses will need to go further and step out of their comfort zones, taking a Zero Trust approach to security and adopting the Secure Access Service Edge (SASE) framework.

About the Author

Tom is a Solution Architect at Menlo Security for the EMEA region. He works closely with customers to meet their technical requirements and architects web and email isolation deployments for organisations across different industries. Prior to Menlo Security, Tom previously worked for LogRhythm and Varonis.



Software-Defined Radio for Incident Response

By Brendon McHugh, FAE & Technical Writer, Per Vices

Wireless technology has become ubiquitous in people's lives and will continue to expand with Industry 4.0, smart cities, smart grids, and a whole plethora of internet of things (IoT) devices. As wireless standards continually evolve to accommodate changing user and device requirements, many issues are also becoming apparent, including the need to mitigate spectral challenges and issues related to cyber security, as well as appropriate responses to these incidents. In order for this, a flexible, reconfigurable, and programmable framework is required. A software-defined radio (SDR) is a radio communication system that is up to such a challenge.

In this article, we discuss the various threat incidents to machine-to-machine (M2M) and human-to-machine communications (HMC)/human-machine interfaces (HMI) in industrial and critical infrastructure–so-called industrial internet of things (IIoT). This includes cyberattacks such as sniffing, spoofing, replay attacks, and various others, which can threaten the various wireless devices in these settings. Other incidents occur in the electromagnetic (EMS) itself, including jamming, co-channel interference, and various other spectral issues. SDRs are capable of monitoring, detecting, and protecting wireless communication as well as being able to locate the origin of interference and alert of any communications failures.

Basic overview of M2M/HMC/IIoT Communications

In recent years, research on wireless systems that link with other devices has grown rapidly in an effort to replace traditionally wired systems while expanding the use of wireless technology. One such example is the Industrial Internet of Things (IIoT), used in areas like manufacturing, energy, transportation, agriculture, and more; essentially a wireless system of automation, learning, and sensor technology working together in order to provide smooth collaboration between critical systems. M2M IIoT technologies are being used by industrial and manufacturing organizations as they become more flexible in capabilities while increasing productivity. Implementing M2M solutions can yield benefits in terms of time and cost savings, operational efficiency gains, and optimized performance from key remote plants or other assets, whether it's maintaining machines and plants installed across the globe from a central point, scanning data from distant outstations and mobile applications, or controlling plant-wide processes.

Unlike in the past, when factories required personnel to actively check the operation of each system, today's manufacturing organizations are all focused on M2M and HMC/HMI combined with the Industrial Internet of Things (IIoT). Advanced sensors and actuators are used in M2M technologies to monitor a machine's overall status and performance. The technology automatically conveys vibrations, temperature, pressure fluctuations, and other signals of mechanical failure to other linked devices, helping personnel to discover and handle issues sooner. Companies can deliver all preventative maintenance chores to protect the equipment's longevity and ensure effective functioning since M2M-linked devices can notice warning signals and report problems practically instantaneously. Furthermore, these technologies aid in improving machine performance and productivity.

Often, microcontrollers are used to control input and output (from sensors, actuators, etc) as they communicate through cellular, Wi-Fi, and various other IEEE 802.1 standards. 5G and Time-sensitive networking (TSN) are also becoming more popular as mobility becomes more important for IIoT devices. Moreover, satellite communications for GPS/GNSS receivers embedded in transportation systems used in IIoT are becoming a requirement.

While various security features do exist in these standards, there is still high susceptibility to cyber and EMS threats, both intentional and unintentional, and so, examining, monitoring, and safeguarding IIoT devices is becoming increasingly critical.

Cyber and RF Attack Vectors

As discussed, a number of methods, technologies, and protocols for sending data or voice wirelessly between people, M2M, and/or HMC/HMI exist. However, these systems are susceptible to various cyber and RF threats. Commonly referred to as attack vectors, vulnerabilities of complex wireless systems such as those used in IIoT, are conducted through attacking hardware (radio frontend (RFE), time boards, sub-system microcontrollers/PLCs, etc.) and software/firmware used in devices (APIs, Ethernet cards/NICs, FPGA, ASICs, CPUs, Servers, etc.) as shown in Figure 1.

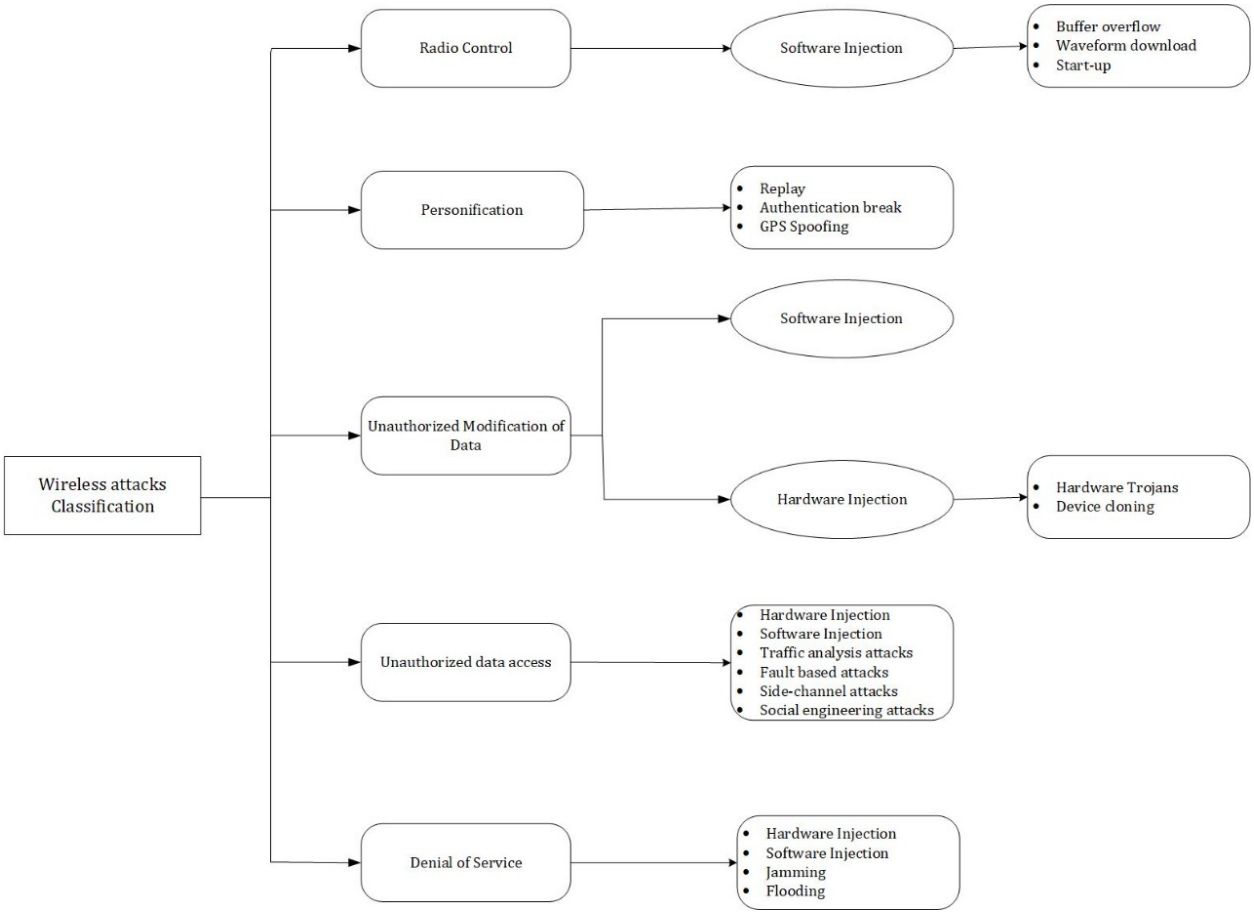


Figure 1: Cyber threats and RF attacks classification

While numerous methods exist for ensuring networks are secured from cyber threats, via device identification and access control, authentication encryption, distributed denial of service (DDoS) protection, and firewalls, it's becoming increasingly important to fend off RF-related attacks and spectral issues as the RF spectrum becomes increasingly congested.

RF EMS threats, issues, and incidents are numerous in IIoT settings. For example, numerous technologies in IIoT operate in the 2.4 GHz band, causing co-channel overlapped operation and hence facing severe cross-technology co-channel CCI. Another example is intentional jamming, such as a denial-of-service (DoS) attack where transmission capabilities are blocked from either the receiving or the emitting end. Such attacks affect the availability of information/data flow from IIoT devices. Of course, numerous other RF attacks are possible, including spoofing, replay attacks, and eavesdropping, to name a few.

SDRs for M2M/HMC

SDRs are also becoming more common for use in IIoT settings as they can be used as a gateway for connecting numerous wireless devices using various wireless protocols, and their associated tuning

frequencies, modulation schemes, and so on. Such interoperability is made possible by an SDR's reconfigurable and flexible nature.

A typical SDR system has an analog front-end and a digital back-end. The analog front-end handles the transmit (Tx) and receive (Rx) functions of a radio communication system. Signals are translated from one domain to another using analog-to-digital converters (ADCs) and digital-to-analog converters (DACs). Once in the digital domain, signals enter an FPGA with onboard DSP capabilities for modulation, demodulation, upconverting, downconverting, and data packetization over Ethernet optical links. It's also possible to implement various security features on the FPGA as part of the network stack, configure it for various modulation/demodulation schemes of radio protocols, etc.

An SDR can support a vast range of wireless technologies used in IIoT M2M, HMI, etc., and provides a compact, programmable, open-source, and full-duplex, solution for acting as a gateway to devices. Moreover, hardware designers can use the onboard FPGA to encode and decode the data for the various wireless standards, especially as open-source software/IP cores are becoming available. The FPGA also can also be used to encrypt or scramble the data to avoid transmitting in a way that is susceptible to RF attacks.

Examples of SDRs for M2M/HMC

With the deployment of 5G technologies and their use in IIoT, SDR technology is becoming critical, as these devices employ critical functions such as Network Function Virtualization (NFV). This not only enables a virtualized re-configurable environment of the SDR but also provides an opportunity to extend the overall network coverage, for instance, to mobile IIoT devices used in transportation networks, etc. For more global operations, such as international shipping and logistics, satellite communication with IIoT devices and gateways is also becoming critical. SDRs are also proving to be useful in this domain.

SDR technology has also become increasingly popular in the energy sector as it can aid with grid monitoring by allowing utilities and energy businesses to better monitor and regulate energy infrastructure or the electric grid for possible issues, as well as quickly adjust to changing conditions improving grid management efficiency and safety. It is widely utilized in the oil and gas industry for pipeline monitoring, asset tracking, and remote tank monitoring. SDR is also being utilized in renewable energy applications like wind farm monitoring and control, solar panel monitoring, and energy storage management.

How SDRs can Defend and Respond to Cyber/RF Threats and Incidents

Generally, today's network security threats are becoming very sophisticated, so advanced solutions are needed to keep networks safe. Software-based solutions that have been used to protect network infrastructure are no longer good enough. One way to close this performance gap is to use reconfigurable software controlling hardware; in other words, the SDR paradigm. An SDR-based IIoT system combines the parallelism of hardware and the flexibility of software to make a network security solution that can be used in many different ways.

M2M communication security is required to safeguard the system from all forms of threats and infiltration. This includes means to prevent denial-of-service (DoS) attacks, transmission eavesdropping, routing attacks, floods, and data center security and access control. Physical attacks include inserting legitimate authentication tokens into a manipulated device, modifying or changing software, and environmental/side-channel attacks. A DoS attack is one that attempts to bring a system or network to a halt, rendering it unreachable to its intended users. SDRs are capable of protecting against these since they are networked devices and can be used as a barrier by monitoring data being received/transmitted at the SDR gateway (via FPGA end-point security, etc.) before being passed over to other network components (cloud servers in data centers, other IIoT devices, etc.), as well as alert of any suspicious activities.

One important aspect to consider is the use of SDR in the IIoT communication stack such as to self-heal, autoconfigure, and adapt the radio based on various EMS environments. For instance, there is always a chance that data communications could be harmed by radio frequency (RF) interference, which is unwanted energy in the form of emissions, radiations, or inductions. RF interference can affect a wide range of wireless technologies, including Bluetooth, Wi-Fi, and GPS. On the other hand, jamming occurs between a transmitter and a receiver. The purpose of radiofrequency or communication jamming is to prevent receiving or decoding, by disabling the opponent's radio connection. To respond to these incidents, SDRs can reconfigure by various means, such as changing antenna directionality, changing center frequency, or using a redundant SDR gateway elsewhere in an IIoT network, thus mitigating RF spectral issues.

Other schemes for a secure SDR architecture incorporate an automatic calibration and certification unit (ACU), an radio security module (RSM), and a GNSS receiver for the position. The ACU is an SDR security threat mitigation method that monitors the output spectrum to enforce local rules. Such systems may set the necessary spectrum rules depending on the SDR's location and spectrum configuration files. The SDR monitors spectrum laws globally (for example, spectrum configuration files). Even a malicious waveform in the SDR node can be stopped by the ACU. These modules are downloaded and executed by the RSM. User and device authentication, event and access logging, encryption, port disabling, and smart password and network key management are also important to consider.

Current research is also being done on SDRs used to prevent issues related to co-channel interference. As mentioned, one common IIoT protocol is Zigbee, however, it suffers from co-channel interference with WiFi sharing the same band. At 2.4 GHz, ZigBee uses offset quadrature phase-shift keying (O-QPSK) and direct-sequence spread spectrum (DSSS). But, each WiFi orthogonal channel has four ZigBee channels (2 MHz each), and thus, buried or blind terminals, and variations in channel sensing/response time still cause co-channel interference. To prevent this, matching local noise variance (LNV) is estimated after the interferers appear, and the Log-likelihood ratios (LLRs) are scaled using Local noise variance LLR scaling (LNV-SC). Figure 2 depicts the full interference detection and LLR scaling process. Adding LLRs to SDR software simplifies implementation. In an article published in IEEE Transactions on Vehicular Technology, researchers from Oulu University in Finland and Kaiserslautern University in Germany demonstrated how SDR can successfully mitigate the effects of multiple co-channel ZigBee interferers. The researchers found that SDR-based interference reduction may considerably improve ZigBee network performance in both lab and field settings.

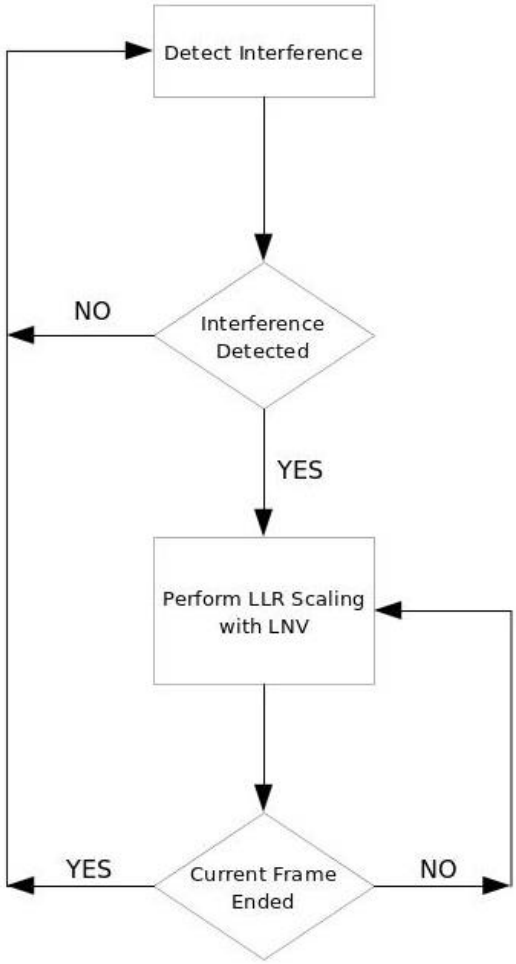


Figure 2: Flow chart of interference detection and LLR scaling (source: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1512-3)

Moreover, an SDR can act as a spectrum monitoring device in IIoT networks only on factory floors using the common 2.4 GHz band (Wi-Fi, ZigBee, Bluetooth, etc) is critical for minimizing various co-channel interferers. Spectrum monitoring is a spectrum management technique that entails tracking a section of the radio frequency spectrum and storing the data for further study. The SDR can locate and isolate interfering devices by monitoring the spectrum, allowing the network to continue to function normally. In addition to spectrum monitoring and its function in interference mitigation, SDRs can identify possible sources of interference, locate them, and take actions to minimize them by continuously scanning the spectrum. Therefore, it can assist keep the IIoT network free of interference and running at maximum efficiency.

Conclusion

As discussed, wireless networks are prone to a large number of cybersecurity and spectral threats that if not handled and responded to in a timely manner, may lead to compromise in confidential/proprietary data and disruption in the networks. SDR-based systems are able to create a flexible and high-performance network security solution and respond to wireless RF communications vulnerabilities. This security layer solution overcomes traditional security solutions' fundamental constraints and allows for real-time deployment of complicated protection functions. Because they are reconfigurable and enable high parallelism, FPGAs onboard SDRs are perfect for implementing this network security solution. With the ever-growing emergence of new wireless technologies, it is therefore imperative to adopt SDRs technology to ensure flexibility as well as security in IIoT M2M, HMC/HMI networks.

Per Vices has extensive experience developing and integrating highly secure SDRs for mission-critical applications, including that in industrial M2M communications, satellite communications, and other IoT applications. For more information, contact solutions@pervices.com

About the Author

Brendon McHugh is a Field Application Engineer and Technical Writer at Per Vices Corporation. Per Vices has extensive experience in developing, building, and integrating software defined radios for CEMA operations. Brendon is responsible for assisting current and prospective clients in configuring the right SDR solutions for their unique needs, and possesses a degree in Theoretical and Mathematical Physics from the University of Toronto.

Brendon can be reached online at mailto:solutions@pervices.com and at our company website https://www.pervices.com/

The 6 Biggest Financial Sector Cybersecurity Threats in 2022

By Veniamin Semionov, Director of Product Management, NAKIVO

The financial sector cybersecurity is always a concern because this industry branch is among the top targets for cyberattacks. And this is no accident. Intruding into the IT systems of banks or other financial institutions aims for illegal enrichment, espionage, geopolitical challenges, and terrorism. Lone actors and criminal groups initiate attacks to steal money from individual bank accounts. At the same time, rival states and ideological opponents can aim to gain classified data, cause disruptions in financial systems and provoke panic among citizens.

In the post-COVID era, digital transformation processes in industries are accelerating and evolving, opening new possibilities and bringing new dangers. The overwhelming expansion of online solutions means the exponential growth of risk factors and vulnerabilities, both inside and between the IT infrastructures.

Here are the six biggest threats to cybersecurity in the financial sector to be aware of in 2022.

State-Sponsored Attacks

An average user might think that a usual financial sector cyberattack initiator is a solo hacker or a criminal group. But governments can sponsor and coordinate such digital strikes too. The increasing frequency of state-affiliated cyberattacks resulted in the official definition of cyberspace as a warfare domain by

NATO in 2016. Attack initiators from abroad can aim to destabilize the financial and social situation in a target country by disrupting and paralyzing financial flows.

Ransomware

The risks for financial industry organizations have increased along with the global rise of ransomware threats. During the first half of 2021, a year-on-year growth of ransomware attacks on financial institutions reached 1,318%. Hackers regularly improve and develop their ransomware strains to stay ahead of protection solutions, so a ransomware breach is a matter of "when", not "if" for an organization.

As ransomware attacks on financial institutions continue, and complete prevention of ransomware infiltration in the organization's infrastructure is barely possible, concentrating on data protection is a wise decision. Regular backups are the most reliable way to protect critical data from loss. Contemporary solutions like NAKIVO software enable you to set automatic backup workflows, store backup data in air-gapped locations and apply immutability. Immutable backups are protected from alteration or deletion during the chosen period, and usable for recovery even if ransomware tries to reach your backup repositories during the attack.

Unencrypted Data

Although sensitive data encryption seems obvious for financial organizations, not every bank encrypts data by default. Unencrypted data is a problem for smaller banks that don't always have enough funds to invest in cybersecurity. Criminals can use unencrypted data right after retrieval, which means more danger for clients and partners of every financial organization falling victim to a data breach.

Third-Party Software Vulnerabilities

An IT infrastructure of an average organization is never isolated. Organizations integrate third-party solutions to support the required level of online presence, speed and productivity of internal and external workflows without overly investing in proprietary software. Still, such a forced reliance on multiple partners in a supply chain increases the instability of IT systems.

Every piece of third-party software integrated into an organization's environment brings not only functional benefits, but also vulnerabilities that bad actors can exploit. For example, malware can go through unnoticed backdoors, resulting in sensitive data theft, corruption or deletion. The timely third-party vulnerability discovery and neutralization are possible only with the regular assessment and monitoring of the whole IT infrastructure of an organization, including digital supply chains and integrated solutions.

Social Engineering

Social engineering defines a broad range of attacks having interpersonal interactions at their core. For example, a hacker can pretend to be an outsourcer, an IT specialist contacting bank staff members via email and asking them to urgently provide personal account login credentials to help with the prevention of security breaches. The attack scenario and the intruder's role can change, but the purpose is always the same: to get the confidential data or make an authorized person act in favor of a bad actor.

Phishing attacks on financial institutions are a social engineering instrument. Senders can make their emails look official by pretending to be, for example, a CEO of a target bank. The content of a phishing email aims to trick a recipient, for instance, a bank staff member, and make them click a malicious link or open a virus-infected attachment. After the security of an organization is breached, a hacker can continue the attack inside the IT infrastructure.

Insider Threats

When speaking of cyber threats to banking industry organizations, the most frequent actors to blame are outsider hackers. However, dangers can also originate from the inside. Apart from social engineering outcomes, there are at least two more things for finance cybersecurity specialists to stay aware of: human errors and malicious insiders.

- **Human error.** Any team member can get tired, careless, or inattentive. An error when doing one's job is the consequence. A single tap on the wrong web banner as a result of distraction may be the reason for a disaster inside the organization's IT environment.

- **Malicious insiders** are more dangerous and less predictable because they aim to open or exploit a security breach purposely. This threat source can be a former employee who thinks they were unfairly fired, or a current employee acting in favor of third-party interests.

Conclusion

In 2022, the challenges of cybersecurity in the financial sector have evolved together with industry developments. Among other threats, the six most significant are:

- State-sponsored attacks
- Ransomware
- Unencrypted data
- Third-party software vulnerabilities
- Social engineering
- Insider threats

Keep those six points in mind when building a reliable protection system for the IT environment of your financial organization.

.

About the Author

Veniamin is a Director of Product Management at NAKIVO. He obtained his Master's degree in Software Engineering from the National Aviation University, which is located in Kyiv, Ukraine. Veniamin is responsible for driving the implementation of features and functionality for NAKIVO Backup & Replication. Before his position as a director of product management at NAKIVO, Veniamin worked as a QA Engineer at Quest Software. Veniamin has 10 years of experience in product management, working with virtualization and cloud technology.

The Artificial Intelligence Tug-of-War: Adversaries vs. Defenders

By Corey Nachreiner, CSO at WatchGuard Technologies

Artificial intelligence (AI) is playing an increasingly important role in cybersecurity. A recent Pulse Survey shows that 68% of senior executives say they are using tools that use AI technologies, and among those who are not yet using AI, 67% are considering adopting it. Going forward AI will be essential for cybersecurity in organizations given the number of benefits it can offer security teams. These include increased threat detection speed, predictive capabilities, error reduction, behavioral analytics and more. AI can also help reduce zero-day vulnerabilities where AI automates the discovery and patching of flaws.

AI in cybersecurity enables a system to process and interpret information more quickly and accurately, and in turn, use and adapt that knowledge. It has substantially improved information management processes and allowed companies to gain time – a critical component of the threat detection and remediation process. Additionally, today's ML/AI is good at automating basic procedural security tasks. Often this can result in taking noisy security alerts, and removing the obvious false positives, or events that may not be serious, and only leaving the important things that humans need to validate.

But as the defenders grow more and more sophisticated in their use of AI, so are the adversaries. For example, attackers use it to automate the discovery and learning about targets. When ML is applied to social networks, it can help identify the most prolific users with the most reach, etc., and it can then help automate learning what those individual users care about. This type of automated investigation of public profiles can help attackers use AI to craft messages that will more likely appeal to that target. In short, AI can automate the research into human targets that was traditionally done manually, enabling hackers to quickly collect enough information about the targets to deliver very specific phishing messages.

In fact, recent research on this subject presented at Black Hat demonstrated that a typical, widespread phishing attempt will see about a 5% success rate. Layer on machine learning which uses knowledge about the targets to make the phishing attempts more accurate and believable, and hackers will see about a 30% success rate. This is nearly as much as they see in a highly specified, targeted spear-phishing attempt.

Another example is with self-driving cars. A car using ML algorithms to make decisions could see a stop sign that has a sticker intentionally placed on it by a bad actor as perhaps a 45-mph sign. Imagine the disaster there!

With AI/ML being used more and more by both the good guys and the bad guys, it's become a true cat and mouse game. As quickly as a defender finds a flaw, an attacker exploits it. And with ML this happens at line speed. But there is work being done to address this. For example, at DEFCON 24 DARPA created the Cyber Grand Challenge which placed machine versus machine in order to develop automatic defense systems that can discover, prove, and correct software flaws in real-time.

Outside of that, to address this the first place to start for companies is security awareness training. Teach employees how to recognize phishing and spear-phishing attempts. Understanding the problem is a big step in addressing it. Additionally, employ threat intelligence that sinkholes bad links, so even if they are clicked on, they get quarantined and don't cause harm. While this tug-of-war will likely go on indefinitely, we can continue to take steps to help the good side gain a little more muscle.

About the Author

Corey Nachreiner is the CSO of WatchGuard Technologies. A front-line cybersecurity expert for nearly two decades, Corey regularly contributes to security publications and speaks internationally at leading industry trade shows like RSA. He has written thousands of security alerts and educational articles and is the primary contributor to the Secplicity Community, which provides daily videos and content on the latest security threats, news and best practices. A Certified Information Systems Security Professional (CISSP), Corey enjoys "modding" any technical gizmo he can get his hands on and considers himself a hacker in the old sense of the word.

Corey can be reached online at https://www.linkedin.com/in/corey-nachreiner-a710ba1/ and at our company website https://www.watchguard.com/

The Balance of Power: One Disturbance Could Ignite The First Cyber World War

By Guy Golan, Founder and CEO of Performanta

The Russian invasion of Ukraine has led to the awful re-emergence of war on the European continent. This time round however, we've witnessed a significant development: the ongoing conflict has a cyber facet at its very core. And one wrong move could have cataclysmic repercussions.

The fate of the wider tensions between nations is in the hands of a few key players. Global powers – namely the United States, China and Russia – have had access to each other's national critical grids for years. However, there has been an agreement between these states that prevents them from going beyond the realms of what they already have access to – an unspoken balance of power. As the developments in Ukraine continue, we're seeing a strain on this agreement, and therefore a threat to this Détente of the modern day.

A building pressure

Cyber-attacks on critical infrastructure are nothing new to the cyber community. However, this is the first time in history where a mutual understanding between powers could spill out into a fully-fledged cyber world war. The cyber element is an incoming aspect of modern warfare, and this is something that is only going to play more of a significant role in years and decades to come.

We are just one major act of aggression away from triggering a devastating series of events. An attack on one party's critical infrastructure will cause further retaliation and greater damage. But equally, an attempt to remove the others' control and take back their systems could force the hands of parties

involved. Relieving one pressure could result in a larger pressure elsewhere. Maintaining the 'balance of power is therefore of fundamental importance to avoid global devastation.

It is important to note that Russia, in effect, have less to lose. Critical infrastructure in Russia is less advanced as many rural areas still depend on wells. In this sense, Russia is in a stronger position to disrupt this equilibrium as its impact on the western nations would be far more severe than that on itself. However, it must not be presumed this is an inevitable step for Russia to take. The main cause of this precarious position is down to external factors, including the role the IT Army plays.

A heroic act in a troubling climate

Made up of over 300,000 independent cyber experts, the IT Army will play a major role in how this situation escalates or de-escalates between Russia and the West. This new variable, lacking any real accountability, has the potential to completely usurp the balance of power between these states. Successful attacks from the IT Army on Russian resources will most likely put strain on the relationship between Russia and the west – there is no political advantage for Russia to hit back at the IT Army due to their nomadic foundations.

The IT Army is admirably supporting Ukraine but, in doing so, a new pressure point has been added. Whilst independent from any global power or alliance, if its activities are viewed as the opposite, then there is a risk of an aggressive response from Russia as the balance of power comes under threat of disruption. One foot over the line could be enough to tip the balance, and the escalation would be immediate.

A valuable stalemate

All sides of the balance of power know that crossing the line could result in physical catastrophe that would endanger millions of lives, such as long-term damage to critical infrastructure or even nuclear fallout. However, neither side wants this to happen, so the stalemate continues, and the risk of this situation changing is low. But for the first time, this balance has come under genuine threat.

Where cybersecurity was previously kept in the shadows, a discreet use of aggression between governments, organisations, and countries, has now broken through the surface and into the public domain. The emergence of the IT Army and the pressure point this has created has caused havoc to this balance of power between nation states. The shift has, and will continue to, change the way that cyber is viewed and utilised moving forwards, for all of us – especially in times of war.

About the Author

Guy is the Founder and CEO of Performanta. Appointed as CEO in 2011, Guy leads the culture, vision, strategy, and global expansion for the group, pioneering modern cyber security solutions to organizations worldwide.

With over 17 years experience in the cyber security industry, including 6 years as Managing Director at NGS LTD, Guy joined as Managing Director of Technologies in 2010. Guy focuses on building sustainable and mutually beneficial relationships with both customers and partners, giving him a deep understanding of the ever-evolving dynamic needs of the information security landscape.

Guy can be reached online at https://www.linkedin.com/in/guygopurple/ and at our company website: https://www.performanta.com

The Cost of a Siloed Response: How a Lack of Collaboration is Becoming Security's Biggest Vulnerability

By Neil Ellis, CIO and CISO at CafeX Communications

Disparate Solutions Are Costing Your Organization

Breaches from the past year have made clear that current approaches to Cyber Incident Management need drastic reassessment. The average total cost of a breach rose by 10%, with lost business, compromised information, and time to resolution being central determinants to the severity of the breach. Despite differences in type, size, industry, and sector, breached organizations shared a siloed and unadaptive approach to managing risk and responding to incidents. However, there were organizations that managed incidents with quick, effective, and comprehensive responses.

The success of their approach can be identified in three conclusions:

1. **Incident Management is cross functional** and needs to connect the right people to the right information in order to make the best possible decisions.
2. **Incident Management is multifaceted and multi formed**, and should bring in stakeholders across the organization according to their roles and expertise.
3. **Cyber risk is increasingly dynamic and enduring**, and requires solutions to automate baseline requirements, such as application integrations, knowledge management, and information sharing, so that SOC teams can focus on strategy, rather than the manual, error-prone tasks of their response.

SOCs lack solutions that allow them to visualize and collaborate on their response end to end. Collaboration solutions maximize the value of existing technology investments with embedded integrations that allow teams to act on information from one view, in real time. With a unified view and an adaptable way to structure responses, collaboration solutions help SOCs coordinate their people, tasks, and applications to improve decision making and streamline the overall process.

Incident Management is Cross-functional

Historically, security teams have been solely responsible for handling incidents. Despite security's expertise, compartmentalizing the response to them alone fails to address the complexity of the breach. This approach siloes information, leaving out necessary perspectives and knowledge from the rest of the organization.

The organizations that came out on top of breaches were the ones that recognized incident management as a cross-functional effort. Incident Management needs to be threaded throughout the organization so that the right people are tasked with the right assignments and

informed with the right information in order to make the best decisions possible. With clearer procedures for how events are managed within the organization, tasks can be assigned with expertise, and collaboration can be managed efficiently.

Where collaboration can help:

- Create detailed logbooks of any event, which teams can use real-time to inform the actual response, and down the line in the process improvement stage. CISOs can view how their teams performed, assessing their activity to identify the strongest candidates for each role, and their competency to deliver on its responsibilities.
- Prepare response plans targeted to specific events. With workflow automation, connect tasks with relevant information, applications and other tasks to streamline the response.

The Response is Multifaceted and Multi-formed

Historically, the majority of approaches to Incident Management were in having a small team that worked off of a relatively generalized response plan, but recent breaches have shown the shortcomings of this type of approach. Incident Management is much more effective when the response is communicated across multiple stakeholders and developed with their involvement.

Where collaboration can help:

- Assemble internal and external stakeholders by connecting through chat, voice, and video to align on status and priorities.
- Notify the team with updates and task assignments so that the response maintains accuracy and control.
- Access to key documents from multiple information sources with embedded integrations and powerful search capabilities.

Risk is Increasingly Dynamic and Enduring

Incidents are not one-off or temporary threats. They are ongoing developments to the circumstances of the organization and its environment. While the nature of a breach is unpredictable, the probability that it occurs is not. The organizations that got in front of breaches invested in solutions that streamlined and automated the structural elements of their response, such as application integrations, knowledge management, and information sharing, so that their response teams could focus on strategy rather than manual, error-prone tasks.

Where collaboration can help:

- Provide teams with a quick way to meet, gather information and respond to the incident.
- Organize past and incoming information that can be visualized and designated to specific tasks, role assignments, and stages of the response.
- Record all response activity to provide insight in real time, and post-incident for process improvement, auditing, and reporting.

The Success of Incident Management is in Collaboration

Existing solutions are not fit to manage incidents, which have become increasingly complex, diverse, and interconnected. CISOs can maximize the value of existing technology investments, and even more, improve their response, by investing in a collaboration solution to unify their response. Solutions like Challo track chat, video, and voice communications alongside incoming information so that SOCs can improve decision making and the overall quality of a response.

About the Author

Neil Ellis is the CIO and CISO at CafeX Communications, which has developed Challo, a process optimization platform with an emerging presence in designing, automating, and accelerating organizations' Incident Response. Neil's 30-year background in security and compliance has driven the successful development of CafeX Communications' solution for Incident Management. He can be reached over LinkedIn at https://www.linkedin.com/in/neil-ellis/, and through the company website at http://cafex.com/.

The Future of Attack Surface Management: How to Prepare

By David Monnier, Team Cymru Fellow

To stay ahead of threat actors, organizations must monitor their attack surfaces continuously, maintain accurate and updated asset inventories, and judge which vulnerabilities to patch for the most significant risk reduction.

At Team Cymru, we have spent decades developing solutions to help organizations better understand adversaries by mapping their infrastructure; it's now time for us to equip our customers with the adversary view of their own.

We are providing the home-field advantage to proactively defend their critical data and infrastructure. This article looks at our vision of the future of attack surface management (ASM) and the tools needed to understand and manage cyber risk.

What the Future of ASM looks like

Each hour that passes after threat actors breach your defenses allows them to extract more and more valuable data and learn how you respond to certain types of attacks. A delayed response can cost your organization millions when it comes to cyberattacks. But speed alone is not enough.

ASM begins with a deep understanding of threats and vulnerabilities; this is where Team Cymru is truly unrivaled with another Pure Signal Orbit stablemate. Our Pure Signal™ Recon platform gathers signals from across the globe and has been the recognized leader in this space for many years. It provides security teams visibility far beyond their internal infrastructure and provides the ability to trace threats more than a dozen hops to their source.

After IPs associated with confirmed malicious activities are added to a dynamic IP Reputation feed to create a network-level blocklist, the information is automatically fed to the insight engine of our Pure Signal™ Orbit—a recently launched solution. This sequence allows Orbit to autonomously identify known and unknown customer assets, remote connectivity, and third-party and fourth-party vendor assets that are impacted by current threats anywhere across the globe.

By continually monitoring these assets to determine the presence of vulnerabilities or threats, Orbit can provide a fulsome and holistic risk score, so C-suite and security teams benefit simultaneously from strategic and tactical views. Leaders can prioritize remediation efforts and drive risk-based decisions from their enhanced vantage points. This is the future of ASM, and we call it ASM v2.0.

It is estimated that the external attack surface for more than two-thirds of organizations has expanded in the past year. It is critical to gain an awareness of internal and external vulnerabilities as quickly as possible. With ASM v2.0, teams can gain a holistic view of their attack surface and detect supply chain threats and dangers posed by business partners.

For business leaders considering a merger or acquisition, ASM v2.0 capabilities become even more critical to reduce the financial exposure of ingesting an already compromised organization. No longer wait for months to get a static report that was out of date the moment it was sent to you, do it now, do it tomorrow, and do it every day until that deal completes. Every moment is another opportunity for an attacker to compromise your target acquisition and cause more pain. On the flip side, a weak security status is grounds for negotiation in your favor—another few million here saved in the cost of breach avoidance, another few more beating them down on sale price.

Leaders need to know that the other organization is not inadvertently hiding threats or vulnerabilities to make essential risk-based decisions.

Because there's no time wasted trying to take the information provided by one tool and apply it to a second, third or fourth, we have integrated the features of our ASM v2.0 solution, Pure Signal™ Orbit, into a single platform. This integrated approach drives speed and accuracy as all critical data, threats, and risks are available in a single place.

Additionally, a pricing advantage is realized by buying one tool instead of four disparate solutions. The need to manage a single tool also provides savings in administrative costs.

The ASM v2.0 approach of integrating legacy ASM, vulnerability management, and threat intelligence is a better solution. It brings best-in-class threat intelligence and never before seen visibility of your expanding attack surface into a combined solution.

What to ask yourself to prepare for ASM v2.0

For budget planning, it is essential to ask yourself if the licensing model of an ASM v2.0 solution works for your organization. You will need to consider leadership's expectations about the future growth of your organization.

By most standards, ASM is still immature, but it is evolving rapidly. EASM solutions are at the top of management investment priorities for 2022.

Competitive solutions vary in breadth and depth. To further complicate buying decisions, offerings can be standalone solutions or part of an integrated platform.

ASM is a set of processes for discovering, identifying, managing, and monitoring external IT assets. Solutions to aid teams in implementing these processes are commonly referred to as EASM (external attack management) solutions.

Less than a third of organizations have a formal external attack surface management solution. Most still rely on manual processes and spreadsheets to implement ASM processes. Using these manual processes can take more than 80 hours for an organization to update its attack surface inventory alone.

Another vital thing to consider is the stability of the EASM vendor. EASM is a volatile space, so the longevity and track record of the various vendors should weigh heavy in purchasing decisions. Assumptions about the capabilities of each solution are based chiefly on marketing claims, so look for a vendor with a history of meeting customer expectations.

The Future is Bright — For Those Who Evolve

The future is coming faster than we think, and being prepared to evolve as emerging threats present to your environment is critical. Research has demonstrated that most companies do not entirely understand their attack surface. Upwards of 70% of organizations have been compromised because of an unknown, unmanaged, or mismanaged visible asset.

Transitioning from legacy ASM processes to an ASM v2.0 EASM solution reduces your organization's risk of being left behind in addressing cyber threats.

Integrating threat intelligence, vulnerability scanning, and attack surface management will be essential to ensure a bright future for your organization. Now is the time to extend your view of your attack surface beyond your company or cloud provider's walls.

About the Author

David Monnier is a Team Cymru Fellow who has 30+ yrs experience in cyber intelligence and has presented keynote insights more than 100 times in over 30 countries.

David Monnier was invited to join Team Cymru in 2007. Prior to Team Cymru, he served in the US Marine Corps as a Non-Commissioned Officer, then went to work at the Indiana University. There, he drove innovation in a high-performance computing center, helping to build some of the most powerful computational systems of their day. He then transitioned to cybersecurity, serving as Lead Network Security Engineer at the university and later helped to launch the Research and Education Networking ISAC.

At Team Cymru, he has been systems engineer, a member of the Community Services Outreach Team, and a security analyst. David led efforts to standardize and secure the firm's threat intelligence infrastructure, and he served as Team Lead of Engineering, establishing foundational processes that the firm relies on today.

After building out the firm's Client Success Team, he recently moved back to the Outreach team to focus once again on community services, such as assisting CSIRT teams around the globe and fostering collaboration and data sharing within the community to make the Internet a safer place.

With over 30 years of experience in a wide range of technologies, David brings a wealth of knowledge and understanding to threat analysis, system hardening, network defense, incident response and policy. He is widely recognized among veteran industry practitioners as a thought leader and resource. As such, David has presented around the globe to trust groups and at events for network operators and security analysts.

David can be reached online at LinkedIn and Twitter. Our company website https://team-cymru.com/

The Growing Importance of VPNs

By Izzy Murphy, Reporter, TechRound

There are many advantages which come from using a VPN, such as being able to bypass geo-blockers, access information or data remotely and above all, increased security online. Consequently, the use of a VPN is becoming more and more popular with hybrid working meaning more people are accessing sensitive content from their own homes than ever before. Here are the key benefits of using a VPN and why they are growing in importance and popularity:

Increased Security and Accessibility for Companies Offering 'Work from Home' Policies

Using a VPN massively increases online security. VPNs reroute an internet connection through an alternate server, meaning that a user's IP address will not be available online. All data transmitted from a device should be encrypted through the use of the VPN, meaning that attackers will not be able to decode it.

Having high security levels online is crucial for any individual or organisation accessing the internet. If the connection is not secure, attackers can steal personal information and use it to access online accounts. This can lead to people being locked out of their own email or bank accounts, and struggling to regain access as the attacker has taken full control.

Additionally, organisations should also have high levels of security, especially if they are storing customer or employee data. It is especially important if the information stored by the company is highly sensitive or personal and could provide attackers with information which was not designed to be shared.

There is also a kill switch enabled with most VPNs which will cut the users connection to the internet if the VPN stops working. This ensures that users will never be left vulnerable online, and will restore the connection once everything is secure and the website is safe to use. The kill switch will be turned on automatically by the VPN provider and should only be activated for the time taken to fix any technical issues, meaning that users should only have their internet access restricted for a short time.

VPNs can provide individuals with the ability to access content from a specific region where it would not usually be available. For example, most companies or organisations have restrictions in place so that sensitive files can only be accessed from specific locations or devices.

This is not ideal in the modern day, as many employees now choose to work remotely, meaning they may work from personal devices or be connected to networks not affiliated with their company. VPN logins can be provided to each individual employee within an organisation, allowing them to access content which would usually be restricted. Organisations often use this system to allow employees to work worldwide and collaborate internationally, increasing productivity and accessibility.

Organisations who allow their employees to login through a VPN simultaneously increase their security. This is because only individuals affiliated with the organisation should be provided with access to the VPN, meaning that files and documents should not be available to access by the general public.

Bypassing Geo-Blockers to Stream Online

Some VPNs can provide users with the ability to bypass geo-blockers. Geo-blockers are in place to prevent users accessing content or streaming services from specific regions. Geo-blockers may be in place due to licensing restrictions or issues with legality in specific countries. Sites such as Netflix or BBC iPlayer may be prohibited in other European countries besides the United Kingdom, or have alternative streaming options available.

A VPN can provide a user with a different address to make it seem like they are not attempting to access content from a prohibited location. This is also beneficial for employees who need to access company content remotely and cannot do so through their usual VPN provider.

In spite of this, it is important not to use VPNs to bypass geo-blockers which will enable users to access illegal content. Some blockers will be in place to ensure that pirated content cannot be accessed by the general public, and these should not be overcome. In addition to this, some countries will have legal restrictions in place to prevent users from using VPNs. Using a VPN to conceal data within these regions is not advised as there may be legal action taken against users rerouting connections through a VPN server.

The Chance to Reduce Costs

Additionally, using a VPN can reduce a company's staffing costs. Information technology professionals are usually employed to oversee the day to day running of a site and detect any problems which could potentially arise. With a VPN, this is already taken care of, and the provider may also be able to fix an issue before a member of staff has even been alerted.

This means that companies will not be required to pay additional employees, but can instead pay for a VPN to cover the cost. VPNs allow the service provider to take control of performance checks, general upkeep and security measures, ensuring that there are no technological issues that need to be resolved. If there are problems associated with a website or application, the company will then be able to resolve it without the need for additional staff.

Preventing Censorship and the Spread of False Information in Ukraine

VPNs can also be useful for Ukrainians during this time as accessing sensitive information and the internet is compromised in many cases. People in Ukraine right now deserve access to reliable information about what is going on both in their country and worldwide.

It has been reported that Russia has tampered with the infrastructure in Ukraine, meaning there is a chance for them to begin censoring news. Using a VPN can help internet users within Ukraine to appear as though they are accessing the internet from a different location, and consequently provide them access to major news outlets.

In addition to this, using a VPN can provide not only Ukrainians but any user with increased security. Using a VPN successfully secures web traffic through the creation of an encrypted connection between a device and server which is controlled by the VPN company. It prevents an individual from being able to monitor a user's connection and checking which sites or information are accessed online. It also hides a user's IP address and makes it harder to trace online activities back to a device.

About the Author

Izzy Murphy is a Marketing Executive and Reporter for TechRound. Izzy can be reached online at isabelmurphy48@gmail.com and at her company website https://techround.co.uk/.

The Impact of Mobile Networks on the War in Ukraine

Securing mobile networks while expanding their utility to both civilian and military users has been an important factor in Ukraine's defence against the Russian invasion. The denial of direct access to much of the country's mobile network infrastructure to invaders has proven instrumental in shaping a battlefield on which the cyber terrain and the physical territory itself have intersected to a degree unprecedented in the history of warfare.

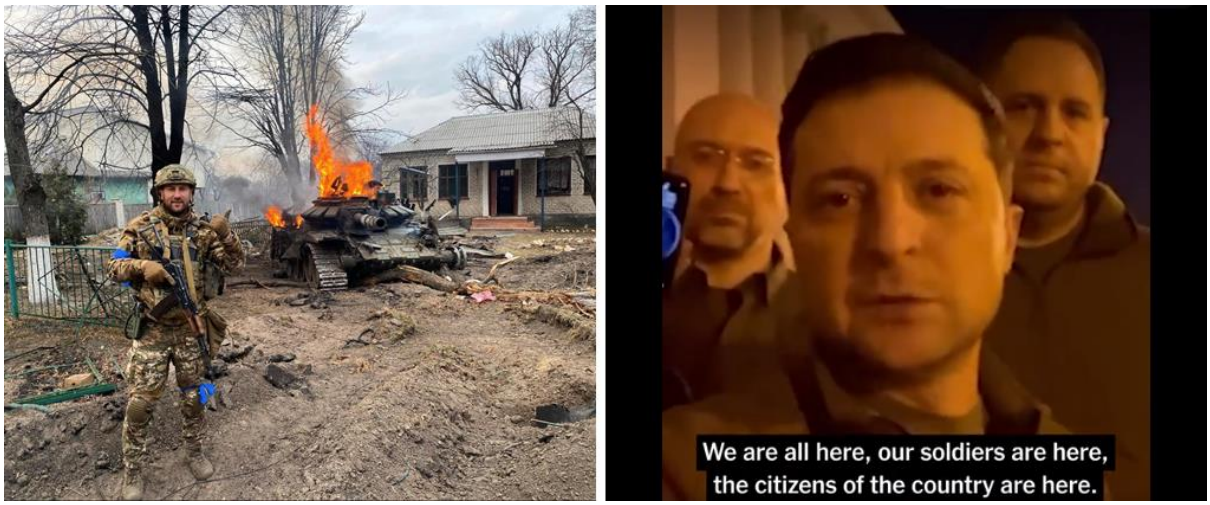
By Rowland Corr, Director of National Security Intelligence at ENEA AdaptiveMobile Security

The Russian invasion of Ukraine has seen an unprecedented involvement of mobile telecom networks in warfighting - especially in how they have been defended, maintained, and utilized in offensive and defensive efforts. The utility of mobile telecoms networks on the battlefield and their role in the wider conflict has profound implications for what we might expect in the future of the war in Ukraine as well as for approaches to mobile telecommunications security as the lynchpin of a country's cyber defences.

Morale and the international response

Beyond its critical role in supporting an essential service to the Ukrainian people, functional mobile networks enabling citizens to speak, text, and message each other at home and abroad has been key to supporting morale and enabling access to the internet for vital information resources and services. Examples showing the positive impact on the morale of Ukrainian defenders abound. These range from the practical: such as the thousands of images of destroyed Russian military vehicles being uploaded using mobile phones, to the inspirational: such as President Zelenskyy's Telegram message, recorded on his phone, on the day after the invasion confirming he was alive and well. Crucially moreover, the social media post was clearly intended to directly confront Russian disinformation that Zelenskiy had fled

the country as he asserts “We’re all here defending our independence, our country, and it will stay this way” against the backdrop of the famous ‘House with Chimeras’, an important symbol of Kyiv itself. These lead not only to greater morale within the country, but - along with the immutably tragic images of the impact of the invasion on the Ukrainian civilian population and infrastructure – have arguably catalysed consensus across many countries regarding international aid for Ukraine, and galvanized international resolve to impose sweeping sanctions on Russia.



Left: Ukrainian soldier posing beside destroyed tank. Right: President Zelenskyy video in Kyiv recorded on February 25th. Source: Twitter, Telegram

The impact on the Russian invasion forces

It is interesting to note that, unlike Ukraine, Georgia did not block inbound Russian mobile phone roamers when the country was invaded by Russia in August 2008. It would later be reported that Russian forces had used the Georgian mobile networks for communications seemingly as a workaround for deficiencies in deployed military radio capabilities. Today in Ukraine, invading Russian forces, again apparently facing radio issues, have once again had to resort to accessing the invaded country's mobile networks. However, due to the Russian and Belarusian inbound roamer blocking implemented by Ukraine’s regulator and network operators, the only way the networks may be utilized directly by invading forces is by using devices with Ukrainian or other non-Russian SIM cards. Reports have surfaced of ‘clean Ukrainian SIMs’ being available for Chechen commanders, and presumably other members of the Russian armed forces and, in addition, some (likely a small number of) seized Ukrainian SIMs may indeed be in use.

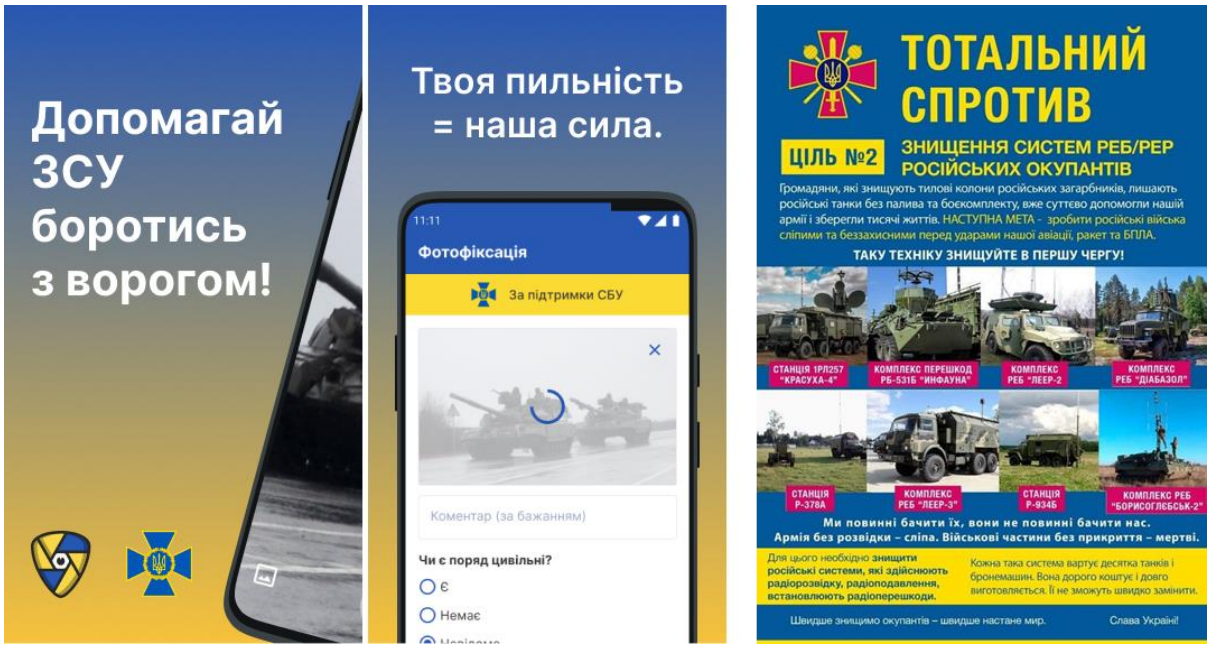
Ukraine’s denial of direct access to much of the country’s mobile network infrastructure to invaders has proven to be an important factor shaping a battlefield on which the cyber terrain and the physical territory itself have intersected to a degree unprecedented in the history of warfare.

In seeking to utilize Ukraine's mobile networks to support military command and control, Russian forces have been prone to interception of communications at multiple points once their use has been identified. Reporting has directly linked this very vulnerability to the loss by Russia of at least 2 generals. Moreover, where the use by invaders of foreign SIMs is discovered, their location can also be identified using the mobile network. This has even been put to use in combating Russian propaganda declaring that the Chechen leader Ramzan Kadyrov had entered Ukraine himself and was with Chechen forces threatening Kyiv. In response to this, Ukrayinska Pravda reported that they had been able to determine that Kadyrov was in fact located in Russia.

The remarkable revelations of the use by Russian forces of SIMBox equipment for call relaying appear to reflect Russia's move to circumvent Ukraine's blocking of Russian and Belarusian SIM registration. While the use of SIMBoxes can also help Russian forces to avoid interception of communications as calls made inside the country are more difficult to identify, it is a model ill-suited for deployment at scale to support reliable command and control, not to mention being a far cry from secure communications. This means that even as Russian forces have sought to adapt to a digital battlefield shaped early-on by Ukraine's swift defensive action, the utility of Ukrainian mobile networks to the Russian war effort has remained substantially suppressed as the war has continued.

The execution of the war

Mobile devices have shown an extraordinary range of uses within the war, from providing a statement of record of locations and damage, to reportedly being used to help guide drones in conjunction with other communication systems. One of the most innovative uses of the mobile networks we have seen has been their direct integration to defensive action by Ukraine against Russian forces. Specifically, multiple channels have been established through which the positions of Russian forces can be reported in real-time. These include a telegram channels and even mobile apps such as Bachu (now available on iOS as well as Android) which enable such reporting even where the internet is not available.



Left/Centre: Bachu App to report enemy movements, Right: Russian EW Systems to report/destroy

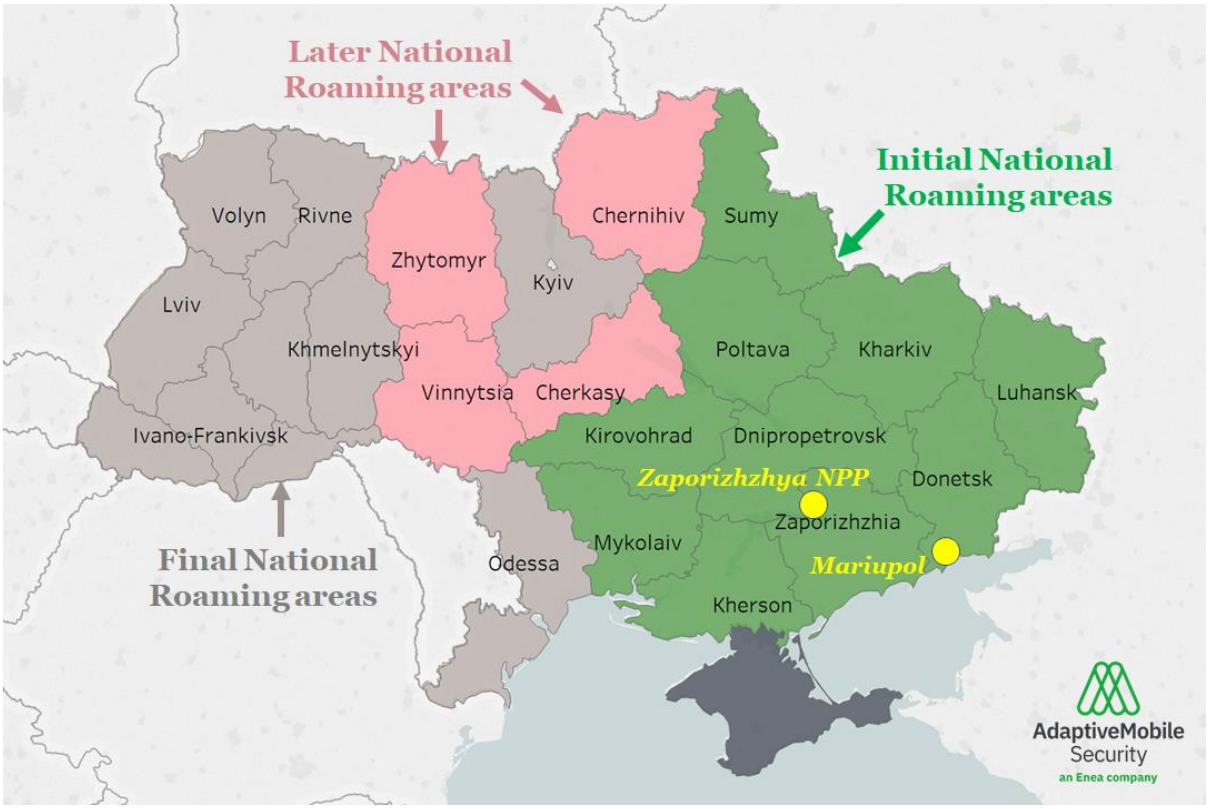
This capability is supported by the expanded national roaming implemented by Ukrainian operators at the onset of the invasion from basic SMS and voice to also allowing a degree of mobile internet access. This enabling of an effectual crowd-sourced kill-chain (i.e. targeting chain) – supported and guided by the Ukrainian Ministry of Defence pushing out visual charts to enable identification of Russian Electronic Warfare systems – is illustrative of how, in the face of Russia's total hybrid warfare, Ukraine has been able to mount hybrid defence underpinned in every respect by mobile network functionality.

Preparation for the Fight

It must be kept in mind that many of these measures taken by Ukraine could not have been executed overnight. They reflect the culmination of months, and in some cases years, of planning and preparation. To give some examples:

- The idea of expanded "national roaming" had been suggested before within Ukraine as an option to overcome issues both in Crimea and Donbass in 2014 due to some of the Ukrainian mobile operators having their equipment interfered with, although it was not implemented then. Even before that time however, Ukraine had put in the necessary legal underpinning for national roaming, something many countries worldwide have not yet done. A legal basis is not enough on its own of course, as to implement national roaming there needs to be a co-ordinated agreement on many topics about how it might work, not least on billing flows and capacity constraints, and then there is the question of technical ability to implement it. Its success, however, is hard to overstate. Within 5 days of being introduced, over 1.3 million people had used the service, with a notable example being the employees of the captured Zaporizhzhia nuclear power plant, as well as the residents of Mariupol, where at the end, regardless of their phone subscription, a single

remaining Kyivstar cell tower was able to be used by all Ukrainian subscribers within signal range.



Map of Ukrainian areas (oblasts) where National Roaming was announced to be enabled initially (Green), and then to enabled later (Pink). Note: actual roll-out may have differed. Data source: Ukrainian Telecom Regulator (NKRZI)

- A key decision was the aforementioned co-ordinated blocking of roaming for Belarusian and Russian mobile devices which was implemented at the very onset of the Russian invasion on 24th February. In our paper covering Hybrid Warfare we previously outlined tactics like this, where we stated: "*Defensive examples could include the prevention of all roaming updates from hostile mobile network sources or links,"*, but we also clearly state that plans need to be put in place prior to any hostile action to allow such decisions and actions to be taken due to the complexity of implementation. Ukrainian mobile operators clearly had such preparation completed and plans in place well in advance of the invasion, as illustrated in the speed with which such decisions were made, and measures adopted.

This last point is important due to the little-known nature of how mobile networks work. In the past, Russian-originated, potential state-level actors have used the SS7 (2G+3G) mobile interface for location tracking and interception of specific individuals.

Ukraine experienced just such SS7 location tracking and call interception at the start of the 2014 Donbass Invasion, at a time when Russian capabilities in this area were extensive. Indeed, the latest invasion has also seen Russia attempt to execute such attacks, as indicated by the head of Ukraine's Information Security and Cybersecurity Service in what she aptly describes as **"the world's first real cyberwar".** The blocking of inbound roaming means that, as well as Russian forces not being able to use their SIM cards, Ukrainian mobile operators can greatly reduce their 'attack surface' from Russian mobile SS7 and Diameter (4G) network sources. While Russia retains other means for the interception of communications along frontlines using Electronic Warfare (EW) platforms, by making these pre-planned network changes, Ukraine has reduced the risk of interior, country-wide attacks which could have targeted a much wider range of individuals, installations, and associated assets. Beyond the interception of communications, the threat posed by weaponized mobile network access by Russia ranges from signalling-enabled Denial-of-Service attacks as described in our Hybrid Warfare white paper, to real-time location identification supporting targeting for missile or artillery strikes by Russia. Essentially, Ukraine both increased defenders' ability to intercept the mobile communications of Russian troops (by forcing them to use non-Russian SIMs), while conversely reducing the potential for Russia to weaponize Ukrainian mobile critical communications infrastructure.

Some observers seeking to explain why Ukraine's mobile networks were still functioning after several weeks of war – i.e. why they had not been disabled or destroyed – have attributed this to the deliberate intent of Russian command. While the reliance of Russian forces on Ukrainian mobile networks has indeed been demonstrated, the problem with some of the commentary on the subject has been an implicit assumption that Ukraine has no agency in determining whether the country's networks would remain active. From our observations, we believe that the speed and scope of the decisions made by the Ukrainian mobile operators and the regulator, both before and since the invasion - as well as the incredible ongoing efforts by technical teams on the ground to sustain network functioning - demonstrate that Ukraine has fought very effectively to keep these networks alive day-in and day-out wherever outages have been caused by damage to infrastructure.

As we have seen, Ukraine's mobile networks are providing so much more than normal service – remarkable on its own given the circumstances – they are serving at a national and international level as a means to boost morale, deny Russia's efforts to weaponize the country's critical information infrastructure, and as a key 'force-multiplier' in stopping and attempting to turn the tide of the invasion.

Finally, it merits remarking on a recent development of concern which is the apparent deployment of both separatist and previously unseen mobile operators by Russia in newly controlled territory. The likely relationship between these services and Russian separatist operators is covered in the third part of our blog series on the Mobile Network Battlefield in Ukraine. In addition to offering Russia a means to support military command and control they could ultimately also enable Russia to control the information environment available to citizens in captured territories such as Kherson (not to mention enabling intelligence and surveillance). The appearance of these Russian-controlled networks thus presents a worrying portent of annexation of the Ukrainian territory involved and could indeed constitute the first structural step towards same by Russia.

About the Author

Rowland Corr is Director of National Security Intelligence at ENEA AdaptiveMobile Security, based in Dublin, Ireland.

Rowland can be reached on Twitter, LinkedIn, and and at the AdaptiveMobile Security website https://www.adaptivemobile.com/.

The Importance of Responsible E-Waste Disposal for Enterprise Cybersecurity

An Outline of the Importance of Proper E-Waste Disposal for Enterprise Best Practices in terms of both CSR and Cybersecurity

By Milica Vojnic, Senior Digital Marketing Executive, Wisetek

E-waste is a growing concern. In 2021 alone, it's estimated that more than 63 million tons of electronic waste was generated globally. When improperly disposed of, e-waste can release toxic chemicals into the atmosphere. Furthermore, irresponsible e-waste disposal is putting significant strain on the future availability of non-renewable precious metals. Every year, around $10 billion worth of platinum, gold, and palladium end up in a landfill.

However, responsible e-waste disposal isn't just about sustainability. For organizations worried about cybersecurity, data erasure is just as important as the physical destruction or recycling of hardware and electronic devices.

Enterprise E-Waste Explained

E-waste can include anything from everyday appliances to the plugs and cords that power them. In the United States, the average person produces around 46 pounds of e-waste every year. For businesses, e-waste statistics are far more staggering.

While the average consumer may replace one or two electronic devices annually, a typical business will actively replace every piece of hardware within an organization once every few years. This includes

laptops, desktops, servers, printers, and much more. Although businesses than ever before are committing to sustainable practices when disposing of e-waste, only a fraction of electronic waste is recycled.

E-waste is on the rise. By 2030, annual e-waste production is set to hit 82 million tons globally. Organizations need to take charge of responsible e-waste disposal to offset the environmental impact. However, it's not just about being sustainable. Proper disposal of electronic waste also makes sense for businesses looking to mitigate cybersecurity risks.

E-Waste and Cybersecurity Risks

Even when properly maintained, IT equipment and electronic assets naturally reach the end of their operational life. To maintain business-critical processes, these assets need to be replaced. Chances are, you'll invest considerable time and effort into protecting these new devices against cybersecurity threats. However, discarded devices will also need to be safeguarded to ensure valuable data isn't accessed by malicious third parties.

What Data Can Hackers Access?

If e-waste isn't properly disposed of, you're making life easy for hackers. If you've taken no steps to destroy data, even criminals with minimal hacking expertise can access information. Naturally, this poses a significant cybersecurity risk to any organization.

It's easy to overlook the extent of sensitive information contained on hardware. Many companies prioritize data erasure with things like flash drives and desktop computers, but seemingly innocuous devices like fax machines can also provide a treasure trove of information for hackers.

Even if you have robust e-waste protocols in place, there's no guarantee every piece of data has been destroyed permanently. Many companies assign data erasure tasks to internal teams. This is certainly cost-effective, but it's worth bearing in mind that a significant proportion of wiped hard drives can still contain retrievable data. Worryingly, a recent study suggests more than 10% of wiped drives may contain recoverable information.

Data Breach Statistics

If a hacker gets their hands on a device that hasn't been successfully wiped of sensitive information, you leave yourself vulnerable to data branches. According to the 2021 Data Breach Report compiled by the Identity Theft Resource Center, there were 1,862 data branches in 2021. This represents a significant increase from previous years. More concerning is that cybercriminals were shifting focus to high-value enterprise targets, rather than concentrating their efforts on individual victims.

Around a third of businesses experience some form of data breach each year. Although the vast majority of breaches are the result of email-based phishing scams, an increasing number are occurring because of e-waste that's been improperly disposed of. The financial implications of a data breach can be devastating to organizations. In 2021, average data breach costs hit $4.24 million. This is a marked increase from previous years and represents the highest average since records began.

It's not just the financial cost of data breaches that businesses need to worry about. Falling foul of a data breach is a clear indication you're not taking enterprise cybersecurity, which can be catastrophic for brand identity and reputation. Most businesses go above and beyond when investing in securing their hardware assets and internal networks. Furthermore, most organizations educate employees on anti-phishing practices during the onboarding process. However, these efforts are futile if you're not working to mitigate cybersecurity risks posed by substandard e-waste disposal.

E-Waste Disposal Best Practices

When disposing of e-waste, committing to sustainability and mitigating cybersecurity risks go hand in hand. The foundations of secure e-waste disposal ultimately hinge on clearly defined asset lifecycle management. With this in place, there's no chance of end-of-life assets slipping through the net before thorough data destruction has been performed.

When it comes to erasing data, simply wiping a hard drive isn't enough. To ensure that sensitive information can never be retrieved, certain components will need to be physically destroyed. Even then, there's a slight chance that recoverable information may remain. This is why employing the services of an IT Asset Disposition (ITAD) partner is recommended.

IT Asset Disposition Explained

IT Asset Disposition companies are becoming increasingly popular with companies eager to protect themselves from data branches and reduce the environmental impact generated from e-waste. As of 2021, the ITAD market was worth $5.8 billion in the United States alone. By 2026, the US market is expected to be worth more than $7.2 billion.

ITAD companies are the obvious choice for businesses without the resources to take charge of data destruction and device sanitization themselves. However, these companies provide far more than peace of mind. These providers are fully versed in best practices and ensure your business adheres to the latest data protection regulation legislation. If your enterprise is a global one, ITAD makes staying compliant simple in every territory you have business interests in.

If you're considering utilizing ITAD, look for providers that provide full oversight of data destruction procedures. Every step of the process should be itemized, while certification of data erasure should also be provided. ITAD providers should also be able to provide full evidence of certification in any area they operate in.

The other major benefit of ITAD partners is that they will usually ensure the hardware itself is responsibly recycled. Once data has been destroyed, your end-of-life assets will be delivered to compliant recycling facilities. This means precious metal resources can be reclaimed for future use, while toxic elements like mercury, lithium, and lead are prevented from polluting the environment.

Taking Charge of E-Waste Disposal

Rethinking your approach to e-waste disposal is essential if you want to maintain green credentials and ensure your enterprise is protected against cybersecurity threats. E-waste looks set to increase considerably over the next decade. As more devices are retired from service, the chance of you falling foul of cybersecurity risks also increases.

Too many companies focus solely on protecting existing infrastructure and in-use assets. While this is crucial, the disposal of end-of-life assets requires special attention. It all starts with asset lifecycle management. Once hardware reaches is ready to be retired, you need to ensure that rigorous data destruction procedures are adhered to. It's tempting to rely on in-house teams to handle data destruction, but investing in IT Asset Disposition is, without doubt, the best approach.

Conclusion

With data breaches on the rise and more e-waste being produced than ever before, the ITAD market is thriving. Certified ITAD companies will provide you with a guarantee that data has been successfully destroyed, while also ensuring your remain GDPR compliant in every territory you're operating in. By using an ITAD provider, you not only mitigate cybersecurity risks, but you're also ensuring that hardware is disposed of responsibly, causing minimal impact to the environment.

About the Author

Milica Vojnic is a Senior Digital Marketing Executive at Wisetek, who are global leaders in manufacturing, data sanitization, reuse, and IT asset disposition. Wisetek's goal is to provide world-class IT services that are world-class in terms of sustainability, security, and compliance. Vojnic specializes in advising businesses in avoiding Data Breaches through effective Data Destruction Services, include proper e-waste disposal. Vojnic is also the author of articles outlining these topics for a variety of online publications. Milica can be reached online at https://ie.linkedin.com/in/milicavojnic and at our company website https://wisetek.net//

The Numbers Are In: Identity-Based Attacks (Still) Reign Supreme in 2022

By Greg Notch, CISO, Expel

The list of challenges security professionals face will not let up, as new threats emerge on a weekly—even daily—basis. Security teams need to stay informed if they want to effectively protect themselves and their organizations, so they're constantly asking themselves a stream of questions: How are attackers behaving? Are certain attack types becoming more prevalent? What vulnerabilities are attackers exploiting, and how can organizations fight back?

Today's businesses can't afford to wait--they need information they can act on right away. That's why Expel recently released its first Quarterly Threat Report (QTR), highlighting cybersecurity trends from the first quarter of 2022 that provide insight into what organizations can expect as the year continues. It won't come as a shock to learn that identity-based attacks loom large and should be considered public enemy number one.

Attackers Continue to Exploit Poor Identity Security

Identity-based attacks accounted for 65% of all incidents observed by Expel during Q1, with business email compromise (BEC) and business application compromise (BAC) accounting for 63% on their own. The remaining 2% were identity-based attacks within cloud environments like Amazon Web Services (AWS) and Google Cloud Platform (GCP). This keeps with the broader trend: attackers are leveraging stolen credentials and other vulnerabilities to exploit poor identity security and gain access to networks. The 2022 Verizon Data Breach Investigations Report underscores these findings, noting that stolen credentials led to nearly 50% of all attacks in 2021—an increase of nearly 30% in the past five years alone.

BEC is particularly widespread. Of the incidents observed by Expel, 57% were BEC attempts in Microsoft Office 365 (O365), and 24% of customers reported experiencing at least one BEC attempt within O365. Expel findings showed that 2% of those attacks even managed to bypass multi-factor authentication (MFA) using OAuth applications. What's more, 7% of BAC attempts in Okta successfully satisfied MFA requirements by continuously sending Duo push notifications to the victim until they accepted—sometimes known as MFA fatigue or "prompt bombing." Security and IT teams need to be prepared to remove malicious OAuth applications and permissions in addition to resetting passwords and MFA tokens. As MFA becomes more common, attackers will also become more adept at bypassing it—which means defenders must be ready.

One interesting note was the uptick in BEC attempts during the week of Valentine's Day. It's not uncommon for phishing scammers and other attackers to attempt to tug the heartstrings of their victims to trick them into a risky click. The FBI issued warnings regarding the potential for BEC scams around the holidays, but it's notable that this extends beyond holidays like Christmas and Thanksgiving. Organizations should train their employees to be wary of the potential for BEC scams, year-round.

Ransomware Isn't Going Anywhere

It should come as little surprise that ransomware attacks persist in 2022, given the number of headlines already this year. Attackers are targeting hospitals, municipalities, tech companies, and anyone else they suspect might be worth the time and effort. During Q1, 5% of incidents observed by Expel were attributed to pre-ransomware activity where an attacker looked to gain a foothold within the network to launch an attack. If left undetected, those incidents could have led to potentially costly attacks.

This year, we have observed ransomware attackers shifting their tactics, with macro-enabled Word documents and Zipped JavaScript files serving as the initial attack vector in 82% of all pre-ransomware incidents. What's more, commodity malware and known malware families linked to pre-ransomware activity accounted for 26% of incidents. What does this mean? Using commodity malware, attackers can target organizations of all sizes with relatively little cost to themselves. It isn't just the big dogs that need to worry about ransomware anymore—small and mid-sized businesses should have strategies in place to defend themselves.

The big takeaway? Having a plan can make all the difference. Knowing what to do when an attacker is detected and keeping the time between initial detection and eventual remediation low are both critical components. That means knowing who to turn to—whether it's an in-house security leader or a managed security provider. The faster the security team can begin implementing recommendations, the less time the attacker has to gain a foothold and branch out from the initial point of entry. Organizations should track this data—if the time between detection and remediation is too long, they should consider serious changes to their security setup.

Using Current Data to Project Future Trends

Understanding the current cybersecurity landscape is critical, and organizations must have a plan in place to address today's most pressing threats. Annual threat reports, such as those produced by Expel and other security experts, can provide valuable insight into the way these threats evolve over time, while more frequent Quarterly Threat Reports can highlight new changes and trends as they emerge. BEC, ransomware, and other attack tactics are not new, but understanding the ways in which today's attackers are leveraging them can provide organizations with the knowledge they need to more effectively combat them.

About the Author

Greg Notch is the Chief Information Security Officer at Expel (CISO). As CISO (pronunciations may vary), he is responsible for ensuring the security of our systems, as well as keeping customers educated on the threat landscape and latest techniques for mitigating risk in their environments.

He's been doing the security and tech thing for over 20 years - helping companies large and small through all three dot-com booms to build high-performing engineering teams, and improve their technology, process, and security.

Before Expel, Greg spent 15 years as the CISO and Senior Vice President of Technology at the National Hockey League (NHL), where he led their information security program. He also led the league's technology strategy, digital transformation, and cloud initiatives.

Prior to the NHL, Greg worked on infrastructure, security, and software systems for Apple, Yahoo Search, eMusic, and several other NYC based tech startups.

The Rise of Crypto Regulations

How to Comply Now, and for the Future

By Ben Richmond, CEO and Founder of CUBE Global

As cryptocurrency is gradually explored as a mainstream option for payments – with Tesla, Starbucks and even Gucci offering customers payment options – it becomes increasingly striking that much of cryptocurrency continues to fall outside of the regulatory arena. Technology and innovation are moving at an incredible pace, unlike anything we've seen before, but financial regulation has struggled to keep up. As a result, as crypto providers, fintechs, and legacy financial institutions try to grapple with the patchy regulatory landscape, compliance remains complex and unclear.

This lack of regulation isn't for want of trying, however. In the last few months alone we've seen exciting developments from regulators across the globe. In particular, the Securities and Exchange Commission has made great strides in its journey to regulate crypto – doubling the size of its cyber unit in order to "be better equipped to police wrongdoing in the crypto markets while continuing to identify disclosure and controls issues with respect to cybersecurity."

We've also seen President Biden take the bold step of signing an Executive Order to ensure the responsible developments of digital assets – a move which was widely seen as bringing such assets into the mainstream of financial services. Or at least a step in that direction.

These are welcome steps toward creating a regulatory framework. But, given the news that the SEC has brought more than 80 enforcement actions related to "fraudulent and unregistered crypto asset offerings and platforms," some might say current regulatory activity is too slow.

This is especially true when you consider crypto for what it is – a borderless, global digital currency. Despite this, regulators the world over are operating in silos in their creation of cyber rules and regulations. This lack of cohesion makes current and future compliance even more complicated.

What's the current state of play?

While a watertight framework for crypto does not yet exist, we do see some regulators taking enforcement action under existing Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT) rules – as well as fraud. According to a report from Chainalysis, crypto crime hit a high of $14 billion in 2021, although this only represents a 0.15% share of the overall $15.8 trillion crypto transaction volume.

So crypto crime is on the rise, though remains comparatively low considered against legacy finance. This will be of little comfort to those who find themselves victim to such malpractices with little avenue for recourse or protection. The sheer volume of capital at play within the crypto market is often seen as reason enough for regulation.

The key to future regulation

Over the next few years, we will need to see regulations emerge. There are several factors for regulators to consider when forming new regulations:

1. They must protect consumers and financial stability
2. They should work cohesively across borders in order to be easily interpreted and actioned by compliance teams
3. They should be strict enough to ensure step 1, but not so strict as to prevent innovation, creativity or to push people to operate in secret.

This is no easy task for the regulators, and they will need to act swiftly, as innovation will not wait for them to catch up.

Managing future regulations for crypto

For many firms, the main challenge at present is anticipating regulatory change to come. Global regulators are issuing large volumes of speeches, consultations, press releases surrounding cryptocurrencies, but for many, it's difficult to keep up, and even harder to know what is important. Manual and legacy processes often lead to knowledge gaps – there's only so much a compliance team can manage, after all. As we begin to see real, hard-letter law and regulation for crypto, these outdated compliance processes will likely become more convoluted – and more prone to error.

Instead, fintechs, crypto providers and larger financial institutions should be fighting technology with technology and investing in compliance innovation that can keep up with regulatory change. RegTech is able to automate the end-end regulatory change journey. Using advanced technology and AI, RegTech is able to track regulatory change from inception, classify it, translate it, and consolidate all emerging regulation into a single regulatory inventory. Advanced RegTech – those that provide Automated Regulatory Intelligence – are not only able to automate the process but to essentially make sense of emerging regulation to suit your specific business profile.

This technology ensures that you're compliant, that you know what's coming around the corner, and that you can understand the context of regulatory change against your business operations.

Firms should not wait to implement new technology

One of the reasons we are where we are with crypto is that the regulators waited to act. It isn't clear why regulators are on the back foot – perhaps a lack of resources, uncertainty about the direction of travel, or wishful thinking that it would blow over. As we begin to see regulators starting to take action, firms may think that it's too soon to invest in compliance technology. This would be a mistake.

As we've seen with ESG, regulators are starting to pump investment and resource into emerging areas of regulation. Topics that were almost unheard of a few years ago are now seeing new regulatory expectation, and fast.

It is likely – as with ESG – that we will see crypto regulation published imminently from regulators. As global brands and businesses bring crypto into their everyday, regulators will be forced to act quickly. If firms are on the back foot with their compliance technology, they will only have further to travel when D-Day comes. Instead, they should be proactive in exploring compliance solutions that will intelligently automate their regulatory change management process. The time to act is now.

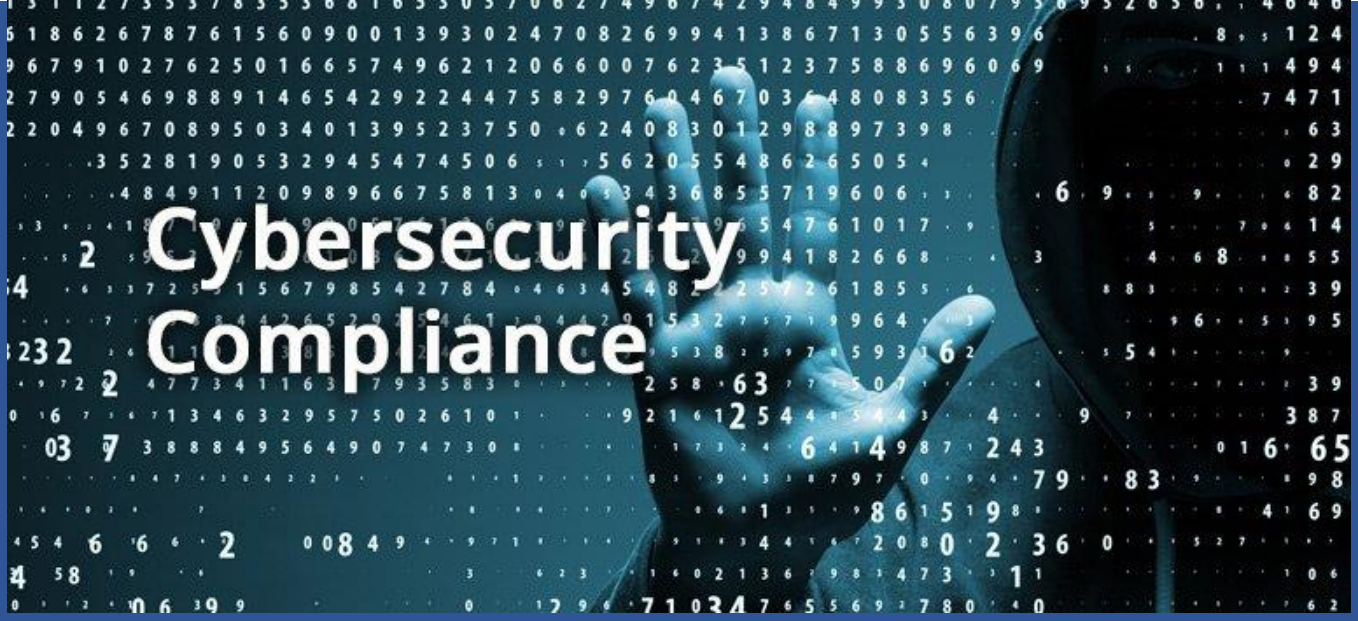
About the Author

Driven by a vision of the future of regulatory compliance, Ben founded CUBE in 2011. Once described as the 'world-beating Rockstar of RegTech', Ben is our results-driven CEO with a focus on progression and growth.

Ben started his career in technology at MISys and soon came to realize the untapped potential hidden within unstructured data. With this potential in mind, Ben set out to build business centered around harnessing unstructured data for the greater good within financial services. In 1998, he founded The Content Group, with a view to set global standards for content-related initiatives.

In 2008, in the midst of the global financial crisis, Ben was quick to see that the future of financial services was going to change. The industry had been brought to its knees due to lack of efficient controls. Ben saw that the future of finance was rooted in more rules, regulations and policies – unstructured data that would need to be harnessed and managed by financial institutions. With this vision in mind, Ben founded CUBE.

Ben can be reached online at Twitter, LinkedIn and at our company website https://www.cube.global/



The Role of Compliance in Cybersecurity

Cybersecurity compliance is essential as it contributes to cyberspace safety in meaningful ways.

By Anas Baig, Product Manager, Securiti

Cybersecurity is a complicated yet essential system - one that needs clearly defined rules, limits, regulations, and guidelines. A strict framework is essential for cybersecurity practices to function and fulfill their objectives of making cyberspace safe for the users, organizations, businesses, etc. These regulations make cyberspace resilient, dependable, and cohesive through compliance.

Some choose to see compliance requirements as an obligation. But for most industry experts, compliance is the key to staying ahead of the game, preventing destabilizing attacks, and having the upper hand when navigating cyberspace and providing your clients with the cybersecurity they deserve. Before we dive into a detailed look at the role of compliance, let us define what compliance means in cybersecurity.

What is compliance in cybersecurity?

Cybersecurity compliance is a risk management method rooted in administrational procedures. It is based on the pre-defined and collectively accepted security measures and controls for enhanced data confidentiality. Simply put, cybersecurity compliance creates a uniform, universal risk management approach that falls in line with the regulatory authorities and laws. Its primary purpose is to meet data management and protection requirements shared by those operating in cyberspace. The industry standards for cybersecurity are created through these compliance systems, which customers can use to assess the instrumental reliability of satisfactory service delivery.

Compliance guides organizations toward the best existing security practices and the protocols that minimize the chances of data breaches. When following the compliance procedures, organizations also get the action plan they can follow in case of a breach. This post-breach protocol communicates the consequences and then impacts the affected parties.

For example, IT security compliance helps the users maximize the system's reliability and resilience by aiding continued monitoring and assessment processes of devices and networks. Compliance also ensures coherence with regulatory cybersecurity compliance requirements. In short, compliance enables organizations to analyze existing risks, put in place a system to protect sensitive data, and an action plan to be set in motion in case of a breach.

Compliance takes all the hard work out of cybersecurity by offering a clear guide on how to breach-proof your organization and its cyber presence by incorporating the best security practices within the organization.

Why is compliance important for cybersecurity?

Compliance in cybersecurity is not just a pointless set of rules imposed by the regulatory bodies; they have an obvious purpose that benefits both sides, not just the regulator.

Compliance requirements make businesses and websites safer for clients and less vulnerable to attacks. Compliance also equips them with the tools to cope with breaches if an especially sophisticated attempt of attack succeeds. This also saves a lot of trouble for the regulator, but the benefits for the organization are evident.

Compliance is obligatory because too many organizations overlook the importance of cybersecurity and hence create more problems for themselves in the future. Compliance is an advantage over those who want to exploit the existing vulnerability within cyberspace.

Data breaches are common, and their consequences are frequently either downplayed or greatly overlooked by the businesses themselves. While the immediate dangers of data breaches are clear, companies have long-term consequences, including tainted brand reputation and a decline in trust from their clients. Coming back from a data breach scandal is anything but easy for businesses, especially as more and more people become familiar with the possible consequences of data breaches.

A Deloitte report has shown that 59% of clients think that a single data break would greatly affect their probability of preferring the organization. In comparison, 51% of clients would excuse the organization with a data breach if the organization rapidly resolves the issue. Even if the latter statement seems encouraging for those who do not see the real value of compliance in cyber security, all business owners should keep in mind that they should always prioritize defense before cyber security attacks. This is why we've seen such an uptick in using VPNs and antiviruses in organizations. If the data breach happens, the options for damage control are extremely limited, and the available options are usually suboptimal. Once the damage is done and the data breach has been confirmed, it's almost impossible to prevent third parties' abuse of said data.

How does compliance ensure cyber safety?

Compliance in the case of cybersecurity rests on a collection of rules and regulations that review the most crucial systems and protocols that collect, secure, and manage clients' sensitive data. Data protection laws and regulations are fundamental for building strong cyber defenses. Since these

regulations use the best industry practices, you are extremely unlikely to encounter an error within the system if you follow the rules. These guidelines help organizations with risk assessment, pointing out their weak spots, and providing guidance on fixing the issue within the cybersecurity framework.

Another point in favor of compliance is that data breaches are rarely isolated incidents. Usually, you will find a snowfall effect on cyberattacks. One data breach that may seem harmless at the beginning can easily turn into an all-out attack on a business that can completely change the trajectory of the mentioned business.

Another perk of following the regulatory requirements is avoiding penalties that come with data breaches. When it is clear that the lack of security measures from the organization is the reason for the breach, the organization will usually get fined. Organizations get fined regularly because their client information gets exposed through an internal or external breach. While these penalties serve as a costly lesson in cybersecurity, they also send the message to other organizations that compliance is essential for cybersecurity and that following the guidelines will benefit the organization in the long run.

About the Author

Anas Baig, working at Securiti as a Product Manager. I am a Computer Science graduate and did my Graduation from Iqra University. My interests include Information Security, Data Privacy & Security. Anas Baig can be reached online at (anas.baig@securiti.ai, https://twitter.com/anasbaigdm, https://www.linkedin.com/in/anas-baig/)

The Role of Endpoint Security and Management In Threat Detection

By Ashley Leonard, CEO & Founder, Syxsense

According to a recent Verizon DBIR, 70% of security breaches originate at the endpoint (servers, desktops, laptops, mobile devices and IoT devices). These attacks can happen through the operating system and application layers, as well as the firmware and BIOS levels. Compound that with the unpredictability of today's threat landscape in the wake of the pandemic, and the shift to remote and hybrid work models triggering a proliferation of endpoints, and companies are more vulnerable than ever to cyberattacks directed at the endpoints. Take the Colonial Pipeline incident where the largest fuel pipeline in the country was shut down due to a single, compromised password. Or the Log4j security vulnerability that was discovered to have affected potentially millions of endpoints. The ensuing scramble to remediate was widespread and urgent.

In this "new normal," post-Covid world, IT teams are now tasked with adapting to a large-scale, remote workforce, further challenging their ability to secure and manage endpoints ranging from PCs and smartphones to IoT-enabled printers and POS systems. Instead of one large headquarters, many companies are now comprised of multiple, smaller offices and home offices. With this, it's clear the office firewall is no longer able to effectively protect the enterprise. Furthermore, laptops and mobile devices have been hastily provided in the transition to remote work without sufficient security, and BYOD policies that reduce equipment costs but allow overlap between an employee's business and personal usage can unnecessarily expose companies to greater risk.

With more than 27 billion endpoint devices expected to be connected by 2025, and a 91% increase in cyber attacks on the enterprise in the first few months of the Covid pandemic alone, the problem is clear – endpoint security and management is crucial to mitigating today's cybersecurity vulnerabilities and threats.

These threats are detrimental to a company in many ways (reputation, customer loss, productivity loss, etc.), all of which roll up to the ultimate cost – financial loss. According to IBM's 2021 Cost of a Data Breach Report, the average cost of a data breach rose 10% from 2020 to 2021 – specifically $3.86 million to $4.24 million. And if we drill down into industries with strict compliance requirements, the numbers are worse. The average cost of a data breach in the healthcare industry is a whopping $9.23 million, and in the financial sector, its $5.72 million. These highly regulated industries face increased risk due to their responsibility for the protection of sensitive private data. Organizations in these industries that insufficiently safeguard data open themselves up to fines and legal proceedings in the wake of an attack as well.

So how can companies address this significant challenge of securing and managing endpoints? First of all, the perimeter of protection needs to expand beyond the conventional boundaries of an organization's offices or a network's on-premises location – it needs to extend to the individual endpoints each time they return to a network. More points of access mean more vulnerabilities. It's essential for any organization to know how many endpoints are in its network and have access to its data with a unified endpoint security system that discovers, scans, and logs devices in inventory any time a device is introduced to the network.

Additionally, it is critical for organizations to adopt consistent approaches to endpoint security, fully comprehending and addressing all risks associated with its endpoints. This involves vetting the security capabilities of new devices before they are introduced to the network and continuously monitoring device vulnerability levels to ensure they never become dangerously outdated and unprotected. One way for IT teams to achieve this without additional burden is with a unified security and endpoint management (USEM) system that automates critical security tasks for each individual device in a network.

Lastly, endpoint security hygiene is essential in effectively managing and securing an organization's endpoints. IT and security teams must retire and replace legacy hardware and software which tend to have unmanageable vulnerabilities. Devices with software or operating systems that are past their end-of-life oftentimes don't receive critical patch updates, leaving them exposed to cyberattacks, such as in the 2017 WannaCry ransomware attacks.

Teams also need to ensure all endpoints are equally secured. A printer, often overlooked in a security posture, may not be a prime target, but can quickly become a gateway to a devastating attack. Take, for example, PrintNightmare, the zero-day Windows Print Spooler vulnerability which allowed attackers to run arbitrary code with SYSTEM privileges enabling them to install programs, view, change, or delete data, or create new accounts with full user rights. This was a "blended" threat that required not only a patch, but also configuration updates to be fully remediated. And don't forget about less obvious attacks such as logic bombs, MITM attacks and formjacking – since we're often so focused on the big ransomware/DDoS attacks and botnets. Patch management is another key factor when considering security hygiene. For example, organizations should enable automatic updates for the most critical security patches.

Implementing a unified security and endpoint management approach that discovers, scans and logs devices as well as automates critical security tasks for each device is key to an effective endpoint security posture. That's why at Syxsense we just launched Syxsense Enterprise, the world's first IT management and endpoint security solution that delivers real-time vulnerability monitoring and instant remediation for every endpoint across an organization's entire network environment.

I think Charles Kolodgy, principal at advisory firm Security Mindsets, summed it up best when he said, "As the market shifts to a hybrid workforce, the number of endpoints is growing exponentially, with corporate network connected mobile endpoints soaring. The need to manage and secure an increasing number of endpoints, including desktops, mobile phones and other devices, is becoming more apparent every day as sophisticated threats grow exponentially. Syxsense Enterprise is offering a solution that solves the need to both secure and manage a vast collection of endpoints. The key is the ability to scan for vulnerabilities and patch without losing business continuity."

About the Author

Ashley Leonard is the President and CEO of Syxsense. Leonard is a technology entrepreneur with 25 years of experience in enterprise software, sales, marketing, and operations; providing critical leadership during high-growth stages of well-known technology organizations. Ashley can be reached online at @SyxsenseIT and at the Syxsense company website https://www.syxsense.com.

The SEC Just Released Its 2022 Priorities - Is Your Firm Compliant?

By Jason Elmer, CEO at Drawbridge

As the calendar turns on a fresh fiscal year, the SEC Division of Examinations has published its list of 2022 priorities. Since 2013, releasing a list of examination priorities has been an annual tradition for the Division – a move designed to improve transparency among investors and registrants, flagging areas of increased risk to ensure firms can do all they can to protect themselves.

And in 2022, there's a great deal of risk.

The SEC's 2022 priorities

Some of the SEC's key priorities this year cover areas such as private funds, Environmental, Social and Governance (ESG) Investing, standards of conduct, and emerging technologies such as crypto-assets. For cybersecurity teams, it's the SEC's focus on information security and operational resiliency that demands immediate attention.

This year, the SEC Division of Examinations will be particularly focusing on broker-dealers', RIAs', and other registrants' measures to prevent interruptions to mission-critical services, as well as protecting investor information, records and assets.

The Division states it will also continue to review whether firms have taken 'appropriate measures' to safeguard customer accounts and prevent account intrusions by ensuring the correct steps are in place to verify an investor's identity. It will also examine whether firms are overseeing vendors and service providers, addressing malicious email activities, identifying red flags related to identity theft, and managing operational risk for those working from home. As such, the Division will be paying particular attention to compliance with Regulations S-P and S-ID, where applicable.

With the assaults on Colonial Pipeline, JBS Foods and CNA Financial, among others, 2021 was a lesson in just how much havoc a ransomware attack can wreak. And as the number of cyber-attacks show now sign of diminishing, the Division's 2022 priorities make it clear that firms must make operational resiliency and keeping customer data safe a core priority in 2022.

But it's not just about managing risk - it's also about recovery. The Division will also be reviewing business continuity and disaster recovery plans of registrants, paying particular attention to the impact of climate risk and 'substantial disruptions' to the flow of business operations.

Best practice for compliance

With security and compliance under the Division's watchful eye, firms must reexamine their security infrastructure and ensure they're meeting all compliance requirements – placing a particular focus on disaster recovery plans as flagged by the SEC.

Businesses must be realistic about the security risks they face and how to best mitigate them. They need to implement a clear recovery time objective and recovery point objective. They need to ensure that everyone knows their roles in the event of an incident and that there is a clear chain of command. And as the SEC noted, the shift to hybrid and remote working – which has stretched company networks and added extra endpoints - has made firms more vulnerable to cyber attack. As such, all security procedures must be adapted to reflect the changing landscape and ensure that even firms with a dispersed workforce will remain secure.

Real-time security

In today's fast paced environment, one of the most efficient ways to mitigate risk is through real-time monitoring of networks, third party providers,and endpoints, so malicious activity is flagged and addressed as soon as it arises. Point in time assessments simply do not cut it anymore - by the time malicious activity is detected, cybercriminals may have already stolen highly sensitive information and done irreparable damage.

Of course, it's not just devices that introduce vulnerability - it's the people who use them. Employees can be the weakest link in a company's security strategy, while also playing a major role in its cyber defense. Employee education is a crucial part of protecting against phishing attacks and account intrusions. With attacks designed to exploit people's ignorance and naivety, regular cybersecurity training to ensure all employees are security-savvy should be a priority across all departments.

Further, it would also be wise for firms to review their legacy systems and make necessary updates – keeping in mind that the infamous Colonial Pipeline attack was launched by breaching a legacy VPN, protected by a single password.

Risk may be at an all-time high in 2022, but that doesn't mean firms are powerless. By reviewing current security protocols, by putting new strategies in place, and by partnering with the right software provider, firms will be better placed to evaluate and meet regulatory obligations. After all, staying on top of security

and operational resiliency best practice is not just about matching the SEC's expectations, it's about providing the best protection and service to clients. Regardless of the Examination Priorities, this should always be the top priority for business.

About the Author

Jason Elmer brings more than 20 years of cybersecurity and IT infrastructure experience to his role at Drawbridge. As Founder and CEO, he is responsible for driving the firm's day-to-day operations, expanding its geographic and technology footprint, and leading the company for global growth and scale. His management background includes multiple executive leadership roles and extensive experience delivering business critical FinTech software and solutions that meet the specialized needs of hedge funds and private equity managers.

Previously, Jason served as a Managing Director at Duff & Phelps (now Kroll, LLC), where he founded and led the Cybersecurity Services team, working with alternative investment managers across the globe to help them ensure compliance with appropriate regulatory bodies while meeting investor demands. Prior to that, he was a Partner at Abacus Group with a focus on providing cybersecurity, hosted infrastructure and disaster recovery services for alternative investment firms. Throughout his career, Jason has been at the forefront of business, technology, and customer service innovation across multiple facets of the global financial services industry.

Jason holds a BS in finance from the Fordham University College of Business Administration and is an active member of the Young Presidents' Organization (YPO).

Jason can be reached online at http://www.drawbridgeco.com

The Top Cybersecurity Conferences for The Remainder Of 2022

By Nicole Allen, Senior Marketing Executive at Salt Communications

2022, and in person events are finally back! Attending cybersecurity conferences is a great opportunity to enhance your expertise and learn about new technologies and innovative ideas, whether you're a startup company or the Chief Information Security Officer of a large enterprise.

To keep informed on the most critical topics, interact with the security sector online or in person. 2022 has had some great events so far, so we've put up a list of the top cybersecurity conferences you should attend in the second half of 2022.

Gartner Security & Risk Management Summit
Website: Gartner Security
Date: 7-9 June
Location: National Harbor, Maryland

Through digitalisation and integrating new technical capabilities with the imperative to ensure safety across the technology lifecycle, Gartner Security and Risk Management will bring together cybersecurity specialists.

The Gartner Security & Risk Management Summit 2022 provides useful information on key strategic imperatives such as establishing an agile security programme, fostering a human-centric, security-conscious culture, devolving risk ownership, and establishing a new simplified cybersecurity mesh architecture. It will allow you to protect your company, defend against attackers, and provide business value.

As well as the above attendees have the opportunity to explore a holistic agenda that tackles the most pressing concerns of security and risk management executives. Each track focuses on a different aspect of delivering on what matters most to you and your company.

CYBERTECH Global
Website: CyberTech
Date: 13-14 June
Location: Grand Hyatt, Dubai

Since 2014, Cybertech has been the leading networking platform for the cyber business, hosting events all around the world. Cybertech will return to the Grand Hyatt in Dubai on June 13-14 2022 with 85K attendees, to take centre stage and explore our ever-changing world. Attendees at Cybertech have a unique opportunity to network, develop existing partnerships, and build new ones while learning about the newest technologies and solutions from the global cyber community.

The Cybertech Global UAE-Dubai conference and exhibition will include cutting-edge solutions from dozens of firms as well as top-tier speakers from around the world, including senior government officials, C-level executives, and industry trailblazers.

Hundreds of exhibiting companies and startups from around the world attend Cybertech global events, which provide excellent chances for startups to demonstrate their global and regional innovations in the Startup Pavilion alongside worldwide companies fulfilling today's global cyber demands. Cybertech also brings people together through thought-provoking conferences and exhibitions that feature renowned speakers and panellists who are the driving forces behind the most cutting-edge new cyber technology.

IDM UK
Website: IDM
Date: 15 June
Location: London

This distinguished and timely event will focus on the implementation of Enterprise-Wide Identity and Access Management across Commerce, Education, Economics, and Industry. As Europe's top identity and access management conference, IDM 2022 provides the ideal setting for participants to network, discuss, and innovate with the world's leading experts and organisations in developing and implementing IAM strategies that drive security innovation.
By attending IDM 2022, you will gain a deeper understanding of IAM as an enterprise security necessity, its function in the modern enterprise, and how to effectively use, perfect, and embed it in your organisation. You'll have the chance to hear from top industry speakers and listen to thought-provoking keynote addresses firsthand.

ISMG Fraud Summit
Website: ISMG
Date: 16 June
Location: Online

The Information Security Media Group (ISMG) is hosting the 2022 Fraud Summit, which is part of the organisation's virtual and hybrid summit event series. Security experts from Google Cloud, Visa, and the World Health Organization, among others, will speak at this year's event. Over the last nine years, ISMG, the leading media supplier to the cybersecurity industry, has demonstrated its dedication to education and networking by hosting a series of Fraud Summits. The annual Fraud Summit brings together executives and key decision-makers in an engaging educational atmosphere to meet and learn from one other's successes and issues in order to better battle fraud.
The Fraud Summit programme is designed to provide actionable knowledge that may be implemented right away in the office. Last year's speakers included Sameer Sait, Whole Foods' Amazon CISO, Claire Le Gal, Samant Nagpal, Mastercard's SVP of Fraud Intelligence, Strategy & Cyber Products, and others.

Infosecurity Europe
Website: Infosecurity Europe
Location: ExCel London

Infosecurity Europe brings together the best experts in the field. Bringing together industry peers to network, share, and ultimately grow stronger and more resilient together by delivering expertise and knowledge from the world's most renowned cybersecurity experts, connecting practitioners with suppliers to find true solutions, and bringing together industry peers to network, share, and ultimately grow stronger and more resilient together.

Infosecurity Europe is about learning from experts, networking with industry professionals, strengthening your cybersecurity skills, and finding solutions that will actually make a measurable impact within your organisation and complement your existing defences.

This event is where the industry's most pressing topics are debated, providing you with a strategy for dealing with current and emerging dangers. You'll also get special insights and know-how from experts who are engaged in the newest industry trends, so you can keep your security strategy one step ahead. There's no better event to attend if you want to gain new skills and make connections that can help you progress your career.

Black Hat 2022
Website: BlackHat
Date: 6-11 August
Location: Las Vegas

Black Hat USA, now in its 25th year, is proud to give a unique hybrid event experience, giving the cybersecurity community the option of how they want to participate. The first four days of Black Hat USA 2022 will be dedicated to training (August 6-11). The two-day main conference (August 10-11), which will include Briefings, Arsenal, Business Hall, and more, will be a hybrid event, with both an online and in-person component.

Black Hat is the world's most technical and relevant information security conference series. The latest in information security research, development, and trends were presented to delegates at Black Hat. The security community's needs drive these high-profile global Briefings and Trainings, which aim to bring together the brightest minds in the business. Black Hat motivates professionals at all levels of their careers by supporting growth and collaboration among academia, world-class researchers, and public and private sector executives.

Cyber Security Asia
Website: Cybersecurity Asia
Date: 15-16th August
Location: Kuala Lumpur, Malaysia

The Cyber Security Asia conference brings together specialists in the field of cyber security. This conference will celebrate women's achievements in cybersecurity and provide industry briefings on the country's cyber future.
Cybersecurity Asia allows attendees to discover the security use cases, business models and roadblocks that can support digital transformation, learn from international thought leaders and cyber risk experts and connect with global technologists to expand your network.

Infosec World
Website: Infosec World
Date: 26-28 September
Location: Lake Buena Vista, Florida
The "Business of Security" conference, now in its 28th year, brings together practitioners and executives for several days of top-notch teaching, networking, and more.

Expert insights, informative keynotes, and engaging breakout sessions instruct, engage, and connect the infosec community at this top cybersecurity conference for security practitioners and executives. This multi-day seminar equips attendees with the knowledge and skills they need to improve and safeguard their enterprises.

Cybersecurity & Cloud Expo
Website: Cybersecurity & Cloud Expo
Date: 20 September
Location: RAI Amsterdam

The sixth annual event of Europe's biggest enterprise technology exhibition and conference will be held on September 20-21, 2022. At the RAI in Amsterdam, this conference and expo will bring together major industries for two days of high-level content and thought leadership exchanges across seven co-located events.

7000 attendees are expected to congregate across Europe, including CTOs, Heads of Innovation and Technology, IT Directors, Telecom Providers, Developers, Start-Ups, OEMs, Government, Automotive, Operators, Technology Providers, Investors, VCs, and many more are anticipated to attend from throughout Europe. This show is not to be missed, with solution-based case studies, top-level content, live demos, and numerous networking possibilities.

Security500 Conference
Website: Security 500
Date: 14 November
Location: Washington DC

The 2022 Security 500 Conference will take place in Washington, DC on November 14th, 2022. This conference is intended to educate security executives, government officials, and industry leaders with critical information on how to improve their programmes while also allowing attendees to exchange their strategies and solutions with other security sector executives.
A keynote, engaging panel discussions, speaker presentations, and networking opportunities are all part of this unique conference.

With a pool of events pertaining to cybersecurity in 2022, you have a lot of possibilities to pick from. Attending industry events can help you gain new insights, see the newest in technology, and expand your cyber security knowledge.

If you require any additional assistance, please contact our experts for more information on this subject at info@saltcommunications.com or to sign up for a free trial of Salt Communications or to speak with a member of the Salt Communications team.

About Salt Communications

Salt Communications is a multi-award winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. Salt Communications offers 'Peace of Mind' for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. Salt Communications is headquartered in Belfast, N. Ireland, for more information visit Salt Communications.

About the Author

Nicole Allen, Senior Marketing Executive at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

Nicole can be reached online at (Linkedin, Twitter or by emailing nicole.allen@saltcommunications.com) and at our company website https://saltcommunications.com/

To Secure the Software Supply Chain, Start with a SBOM

Having a SBOM can reduce the "fog of war" and enable businesses to assess risk and impact faster as they will have a reference point. It would also expedite cleanup and make these unfortunate situations much more manageable.

By Michael Rogers, Director of Technical Advisory Services, MOXFIVE

A recent report from the Linux Foundation showcases the progress and adoption of software bill of materials (SBOM) tied to cybersecurity efforts. The report follows the U.S. Administration's Executive Order (EO) on Improving the Nation's Cybersecurity and the White House Open Source Security Summit earlier this year, highlighting the increasing importance of identifying software components and accelerating responses to newly discovered software vulnerabilities. The report found that 78% of organizations expect to produce or consume SBOMs this year, an increase from 66% in 2021.

As supply chain attacks grew by 300 percent in 2021, companies have been forced to come to terms with pervasive software libraries that might contain previously unknown (and easy-to-exploit) vulnerabilities. SolarWinds, Kaseya, and Log4j are just a few examples that provide a rude awakening of the challenges associated with the software supply chain. As organizations continue to scramble to protect themselves from the fallout, government officials are looking for ways to make future vulnerabilities less threatening.

The threat landscape is evolving, and dependence on external software suppliers is increasingly complex. The ultimate challenge is the ubiquity of a software component across cloud services, applications, and infrastructure that can make it incredibly difficult to deploy a patch quickly in the event a vulnerability is identified. Further, many organizations may not even know that their software contains the vulnerable component in the first place - and if they do not know, how can they remedy it? Keeping

an accurate record of your tech stack is one step towards addressing concerns around security in the software supply chain.

Rising Adoption of SBOMs

A SBOM is a list that organizations can reference to quickly understand what their exposure is based on the applications they use. The concept has been around for a long time, but has garnered more attention amid the Log4j fallout as government officials and industry executives grapple with the huge number of highly dangerous bugs that may be lurking deep inside software that's spread throughout the tech ecosystem.

While SBOMs would not have prevented Log4j, they could have made the cleanup far faster. They are particularly well-tailored to solve one of the biggest problems Log4j highlighted — that some bugs affect pieces of open-source software that are not only incredibly common but also frequently buried so deep in companies' digital systems that their IT and cyber staff do not even know they are there. As shown by the Linux Foundation report, producing SBOMs make it easier for developers to understand dependencies across components in an application, to monitor components for vulnerabilities, and to manage license compliance.

In the wake of last year's SolarWinds attack, President Biden issued an EO advocating mandatory SBOMs to increase software transparency in an effort to combat supply-chain attacks. These SBOMs are required to include all components, open-source and commercial, in an effort to help everyone in the software supply chain - from those who make, to those who buy and operate software.

Having a SBOM can reduce the "fog of war" and enable businesses to assess risk and impact faster as they will have a reference point. It would also expedite cleanup and make these unfortunate situations much more manageable. The Linux Foundation researchers also emphasized that industry consensus and government policy is helping to drive SBOM adoption and implementation, with 80% of organizations aware of the EO to improve cybersecurity and 76% considering changes as a direct result.

Catalyst for Change

It has become clear that cyber incidents are not only business crises: they can also become powerful catalysts for enhancing fundamental IT capabilities. As a growing universe of products and service providers compete for attention to be included in the plan, a clear starting point may not be evident. The next step as mentioned by CISA with SBOMs would be to enable businesses to automatically assess if they are vulnerable so that they can begin remediation and cut down the exposure time. This of course won't happen overnight but would be a great goal to strive for.

Today, SBOMs are not optional - they are essential to secure the software supply chain. Organizations that aren't already using a SBOM should take the lead from these government advisories and determine how a SBOM fits into their cybersecurity strategy, for the benefit of their organization and its customers.

About the Author

Michael is a Director of Technical Advisory Services at MOXFIVE. Heprovides strategic advisory services and solutions to large enterprises during and after impactful incidents. He holds a Masters Degree in Cyber Security and is accredited through SANS for the GCFA, GCIA, and GOSI certifications. He has a wide range of experience from building and managing global Security Operations Centers, Threat Hunting Teams, DevOps Teams, and Infrastructure Teams. Michael can be reached online at https://www.linkedin.com/in/mjrogers/ and at our company website https://www.moxfive.com/.

Top 3 Future Technologies to Look Out for In the Cybersecurity Market

By Saloni Walimbe, Senior content writer, Global Market Insights Inc.

Digitization has taken the world by storm as new technologies and developments pave their way through. With the world progressing on the digital fronts and adapting to the work from home and remote desktop work trends during the COVID-19 pandemic outbreak, it is no surprise that the incidences of cybercrimes have soared to new heights.

According to Internet Crime Complaint Center (IC3), the world observed a dynamic surge in cyberattack cases from 2016 to 2020. Comparing the statistics, the agency reported receiving nearly 791,790 complaints related to cyberthefts and losses in 2020, which was 69% more than that in 2019. Losses to businesses and individuals, during the same year, totaled to $4.2 billion, up by 20% from 2019.

Owing to such massive business losses, companies have now been shifting their interests in deploying inherent cybersecurity solutions and services to ensure proper work data security and safety on the digital platforms. Cybersecurity market is touted to account for a stellar growth in the coming years, driven by the notable developments and future technologies in the space.

According to Global Market Insights, Cyber Security Market will surpass USD 400 Billion by 2027 at 10% CAGR from 2021 to 2027.

Given below is a snapshot of the future technologies that are expected to shape the outlook of cybersecurity market beyond 2021:

- **Multi-factor authentication**

Gone are those days when just passwords were considered to be supreme in protecting the crucial data from being stolen. With technologies advancing today, it has become quite easy for people to carry out unethical activities and obtain access of other's information while trying to crack the password. This is where multi-factor authentication comes into picture. MFA is a verification method which calls in for the user to provide two or more authentication factors to gain access to a resource. It is different from single validation methods in a way that that it requires one or more additional verification factors, which reduces the possibility of a successful cyberattack.

Various multi-factor authentication industry players and other technology giants are striving to launch novel products in the business space of cyber security and password protection. Attesting the aforesaid, Google has reportedly announced working on the multi-factor authentication option on consumer accounts by default. The company aims to auto-enroll over 150 million users in the feature, by 2021 end.

- **AI and machine learning**

Artificial Intelligence (AI) and machine learning have become an integral part of information security, as these technologies are capable of quickly analyzing millions of data sets and tracing down a wide variety of cyber-attacks. Further, these technologies continually learn and improve, extracting data from past experience and present to pinpoint new variations of attacks that can occur at any point of the time.

Some of the advantages associated with the use of AI in cybersecurity include, breach risk prediction, detecting new threats, battling bots, and offering better endpoint protection. According to a Capgemini report, 69% of the enterprise executives firmly believe that AI is necessary to respond to cyberattacks, with 80% of the telecom companies relying on AI to help detect threats and thwart attacks.

- **Blockchain cybersecurity**

Blockchain technology is expected to offer potential cybersecurity benefits including alleviating the risks of cyberattacks. The technology has recently created immense hype as a cure for all current challenges related to cyber security.

Blockchain offers a strong and effective solution for securing networked ledgers. Blockchain technology is deemed to provide transactional and robust security than conventional, centralized computing services for secured networked ledgers. It can also be used to develop a standard security protocol and in securing private messaging by forming a unified API framework to facilitate cross-messenger communication capabilities.

Cybersecurity is at the tipping point today. Advancements in AI, ML, Big Data and other technologies, are accelerating its progress to a much larger extent. It is no doubt that cybersecurity is taking the world by storm, helping in reducing the number of cybercrimes. By creating a cybersecurity network that encourages diversity and value equality, the world can help to ensure that technology, innovation, and future, will be far better than today.

About the Author

Saloni Walimbe, an avid reader since childhood. Saloni Walimbe is currently following her passion for content creation by penning down insightful articles relating to global industry trends, business news and market research. With an MBA-Marketing qualification under her belt, she has spent two years as a content writer in the advertising field, before making a switch to the market research domain. Aside from her professional work, she is an ardent animal lover and enjoys movies, music, and books in her spare time.

Saloni can be reached online at (saloni.walimbe@gminsights.com) and at our company website https://www.gminsights.com

Top Legacy Active Directory Infrastructure Vulnerabilities and How Attackers See Them

By Tammy Mindel, Semperis Security Product Manager

Microsoft Active Directory (AD) has become a highly lucrative target for cyberattackers. That's no surprise, given the prevalence of the identity service in enterprise organizations (as of 2019, AD still held a 95 percent market share among Fortune 500 companies) and its security vulnerabilities. Attackers take advantage of weak AD configurations to identify attack paths, access privileged credentials, and deploy ransomware. Recent reports by 451 Research, Enterprise Management Associates (EMA), and Gartner highlighted the collective concern about AD security problems.

Many of the problems stem from the fact that AD has been in place since 2000, when cybersecurity was not a priority. Many organizations have legacy AD systems with components that haven't been used for years—but remain gateways for cyberattacks.

Cybercriminals know how and where to look for the bits and pieces AD has left behind over its many iterations. By exploiting the platform's identity management infrastructure, attackers can escalate their privileges. From there, the sky's the limit: They can deploy ransomware, steal data, or even take over the organization.

According to an EMA survey, in just the past two years, 50 percent of organizations have experienced an AD-specific attack, and more than 40 percent of these attacks were successful. Making matters worse, penetration testers can typically exploit an AD exposure roughly 80 percent of the time.

Reviewing legacy AD infrastructures for security weaknesses

Organizations can take action to prevent some of the common AD exploits. Following are practical guidelines for identifying and addressing security gaps in your AD infrastructure environment.

1. Maintain proper AD hygiene

Just as practicing good physical hygiene reduces your chance of getting sick, maintaining proper hygiene in your AD environment is crucial to combat cybercrime. If you configure the directory service securely and clean up misconfigurations, your system will be much less attractive to attackers.

First and foremost, continuously examine your AD installation in all its complexity to uncover potential exploits and attack vectors. Perform regular or even continuous vulnerability assessments. Apply basic cybersecurity best practices, such as deleting orphaned accounts, enforcing a tight access control policy, enforcing effective risk management, and removing legacy components.

That last action item, you'll soon learn, is arguably the most important.

2. Know that most major AD vulnerabilities have much in common

By studying frequently exploited AD security gaps, you will notice similarities. Consider the following vulnerabilities, three of the most common currently in the wild: PetitPotam, PrintNightmare, and SID History.

PetitPotam

This authentication coercion exploit was first published in July 2021. Attackers with domain access can authenticate using a vulnerable interface, such as Encrypting File System. They can then use a classic NT LAN Manager (NTLM) relay to further elevate their privileges.

Microsoft's recommended fix for PetitPotam is to disable NTLM authentication on all Active Directory Certificate Services systems, then enable Extended Protection for Authentication to help eliminate man-in-the-middle attacks.

PrintNightmare

PrintNightmare, as the name suggests, is a set of vulnerabilities that target the Windows Print Spooler service. Intended to store and queue remote print jobs, attackers within the network can use this service to perform DLL injection to printer drivers, then run them with system permissions. Any user can connect to the service and abuse it to gain access to the domain controller with system permissions.

As with PetitPotam, the recommended fix is simply to disable the Windows Print Spooler service on your domain controller.

SID History

Typically used only in migration scenarios, integration of new domains, or mergers, SID History is a user account object attribute that can yield thousands of records. Inevitably, some SID History fragments get left behind—fragments you might be reluctant to clean up because you're afraid of breaking access to older systems.

Addressing this vulnerability requires that you maintain visibility into security identifiers (SIDs), identify privileged SIDs, and scan for unauthorized changes.

What do these vulnerabilities have in common? First, they're easy targets. Second, they exploit legacy components. Third, they're easy to stop—the caveat being that you need to know where and how to look.

3. Know that attackers typically look for specific AD targets

When attackers target an AD environment, they're not usually using sophisticated methods. They're doing the digital equivalent of prowling a parking lot looking for an unlocked door or open window—the path of least resistance that will offer them the highest potential return.

Common targets include:

- **Legacy systems:** Older components are often underused, loosely monitored, and highly exploitable
- **SID misconfiguration:** Most commonly in the form of an orphaned privileged SID
- **Security policy issue:** Misconfigured Group Policy security is a common target

4. Use testing tools to uncover vulnerabilities

Tools that scan your AD environment for indicators of exposure and compromise—such as Purple Knight, a free AD security assessment tool built by the Semperis team of AD experts—can help you uncover and address common vulnerabilities. Although the ideal approach is to use a solution that continuously monitors your AD environment for exploits, using a standalone tool like Purple Knight on a regular basis (twice a month is the sweet spot) will raise your awareness of potential problems and give you a roadmap for remediation.

Securing AD is an ongoing process

As the mainstay of identity and access management for most organizations, AD will continue to be a core piece of the infrastructure security puzzle, even as assets shift to the cloud: AD is the foundation of the hybrid identity architecture commonly used today. Even though AD isn't going away anytime soon and has well-known security gaps, organizations can improve their overall security posture with frequent, systematic review of commonly exploited AD misconfigurations. AD remains a valuable tool. We just have to use it correctly and securely, as carelessness leaves the door open to adversaries.

About the Author

Tammy Mindel, Semperis Security Product Manager, has held customer and product-centric roles in the cybersecurity sector and has experience in application security, infrastructure/network security, incident response and forensics, and security best practices and standards.

Tammy Mindel can be reached at https://www.linkedin.com/in/tammy-mindel/ and at http://www.semperis.com

Web3, Good Hygiene, and the Need for End-to-End Security

By Professor Ronghui Gu, CEO, CertiK

Having a smart contract audit is a lot like washing your hands– do it only once, and be prepared for the consequences.

As the conversation around crypto security gets heated in response to a devastating year of losses to cybercrime – CertiK's recent report notes that "2022 is set to be the most expensive year for web3 on record"– it is vital to review some security best practices. Chief among them is the importance of thorough, and *regular* smart contract audits.

All too often, new blockchain projects treat their security checks as something to get out of the way before their launch, never to be thought of again. This haphazard attitude is seen clearest in projects that have only had a single smart contract audit. Projects that do this seem to think that audits are more for marketing purposes than actual security. While it is true that investors and users alike should steer clear of projects that haven't had any kind of smart contract audit, they should also make sure that the projects they invest in are taking an active, end-to-end approach to their security.

You may be wondering 'why should a project need regular audits at all? Shouldn't one cover the project in its entirety?'. This is a common (and expensive) misconception. While any good smart contract audit *should* provide a comprehensive evaluation of a project's underlying code, it cannot evaluate any changes or updates that occur after the audit has occurred, especially any time that a change is made to the underlying code.

Of course, any tech project that never updates will soon become redundant, and this is especially true in the fast-moving world of web3. Any good tech investor or user knows to avoid a project that refuses to update and develop, yet they regularly put their money in projects that never (or rarely) update their security. To return to the cleanliness metaphor, this is like shaking hands with someone after they say they haven't washed their hands in a year.

Take the Deus Finance exploit as an example, which saw an attacker drain close to $16 million USD in funds. While Deus did have their smart contracts audited, an attacker was able to target a new unaudited smart contract with a sophisticated flash loan attack. Though this attack, the hacker was able to change the price of Deus' DEI tokens and reap the benefits of this predictable price action. They did so by manipulating a lending pool that was used by the oracle - a node of code which interprets data - that dictated the price of the token.

Now, any smart contract worth its coin would warn you of the dangers of using an oracle that determines a price by using a trading pair as these can be easily manipulated. However, since the vulnerable smart contract was outside the scope of the initial audit, auditors were not given a chance to highlight the problem.

Deus should serve as a clear warning to projects that they must treat smart contract audits as an ongoing feature in their security framework and have them audited every time a significant change is made to the project. Yet, not all audits are equal. Time and again we see well-planned projects suffer from the flaws of bad auditing.

Take the recent FEG exploits as an example. The FEG (Feed Every Gorilla) hyper-deflationary governance meme token was recently hit by two flash loan attacks which collectively drained $3.2 million USD in funds from the protocol over the course of two days.

In each attack, the hacker (or hackers) targeted the same vulnerability in FEG's smart contract. CertiK's analysis of the exploit discovered that this was due to a flaw in the token's Swap-To-Swap function, which directly takes user input "path" as a trusted party without any sanitations. In simple terms, this flaw allowed the hacker to repeatedly call functions that allowed them to gain unlimited allowances and drain the contract of its assets.

Perhaps most frustratingly for FEG, this flaw should have been detected by a smart contract audit. Even though FEG did have their smart contracts audited, the auditors should have noticed that FEG's untrusted "path" parameter is passed to the protocol and approved for spending assets of the contract. Any good audit would then flag this as a major severity and advize the project to act and edit accordingly.

There is a lesson to be learned here for the crypto-security industry– that, as hackers continue to find new and ingenious ways to exploit projects, it is no longer enough for auditors to just update their checks in response to new attacks. Instead, they must constantly be updating their technology so that when a new attack happens they are prepared for it.

Both of these exploits highlight not only the need for rigorous and regular smart contract audits, but also the need for a proactive, consistent, end-to-end approach to web3 security. This amounts to a shift towards viewing security as something to be built and maintained rather than just a label to be bought and sold. This applies to the teams who need to be updating their project's security in tandem with their

technology, and also to auditing companies who need to be anticipating attacks, rather than just responding to them.

About the Author

Professor Ronghui Gu is the CEO of CertiK. He can be reached online at @guronghuieric or @Certik on Twitter, and at our company website http://www.certik.com/.

Why Cybersecurity Is Critical for ESG

Cyber-Awareness Can Help Companies Meet Esg Obligtions

By Sean McAlmont, CEO, NINJIO

One of the most important trends in the private sector—primarily among publicly traded companies, but increasingly among small and independent firms as well—is the analysis of business practices through the lens of environmental, social, and governance (ESG) issues. Beyond just the "bottom line," companies are being asked to open the aperture of success metrics to include how their everyday activities either positively or negatively impact life beyond their four walls. Consumers are becoming increasingly concerned about whether companies align with their best interests, while other key stakeholders (from investors to the leaders of communities where firms operate) want to see a greater emphasis on the public good.

Cybersecurity is a critical component of any company's ESG strategy, specifically in terms of product governance. From the protection of sensitive customer information to the adherence to laws and regulations around data privacy, a robust cybersecurity platform is indispensable to meeting basic ESG criteria. While many companies believe cybersecurity is all about IT teams, firewalls, and digital infrastructure, a well-trained workforce is actually a company's most significant cybersecurity asset. This is because the vast majority of cyberattacks rely on social engineering: the deception and manipulation of human beings to infiltrate an organization.

At a time when ESG is a major area of focus and reporting for the world's largest organizations and consumers are worried about how their personal data is being used, awareness with regard to various

attack vectors has never been more vital. What most people outside the security industry—executives included—often don't realize is that 85 percent of breaches involve a human element (according to Verizon's 2021 Data Breach Investigations Report). The good news: most attacks are preventable if employees are armed with the right information. This is why an effective security awareness training (SAT) program is a must-have for any company, large or small, that wants to report fewer (or zero) attacks on their organization's digital infrastructure.

A new era of consumer relationships

According to a 2022 Edelman report, 88 percent of institutional investors "subject ESG to the same scrutiny as operational and financial considerations." For most companies, how cybersecurity is implemented and prioritized is a core part of their overall governance as it directly impacts data security and privacy, continuity of service and technology, and the operational integrity of their networks and systems.

Beyond its broad range of governance implications, cybersecurity is particularly crucial at a time when consumers are extremely worried about how their personal data is being collected, stored, and used. According to Pew Research Center, 81 percent of Americans say the potential risks of companies collecting information about them outweigh the benefits, while another 79 percent say they are concerned about how companies use the data they collect. This is a powerful reminder that companies should have comprehensive and transparent data privacy and security policies, as well as an SAT program capable of keeping the company safe.

ESG reporting on initiatives related to cybersecurity not only builds trust with investors and provides a level of transparency for the public record, but it also ensures compliance with regard to consumer data protection. All you have to do is look at the headlines to see that companies face an unprecedented and constantly evolving cyberthreat landscape—from the increasing frequency and destructiveness of cyberattacks to the threat posed by state-sponsored cyberwarfare. Cybersecurity awareness among employees ensures human defenses against all these cyberattacks, which drastically reduces companies' vulnerability.

Taking responsibility for building a cyber-aware workforce

Social engineering can take countless forms, which is one of the reasons it has proven to be such a versatile tactic for infiltrating many different organizations. Cybercriminals use manipulative techniques such as email subject lines demanding "urgent" action, coercive messages threatening legal and professional consequences, or impersonations of government agents (especially law enforcement and the IRS). When companies don't have well-trained employees, they're especially susceptible to these deceptions, which poses a direct risk to their employees, customers, and other stakeholders who engage with them.

Over the past two years, there has been a huge influx of cyberscams due to the pandemic—a clear reminder that cybercriminals are always updating their social engineering strategies based on opportunities to exploit the vulnerable. For example, after the U.S. government announced that it would distribute free COVID-19 tests, cybercriminals set up dummy websites with domain names similar to legitimate resources like covidtests.gov. There are countless schemes: fake websites offering stimulus checks in exchange for sensitive payment information, emails promising miracle cures, fraudulent messages about updated COVID policies or compensation purporting to be from HR departments, and so on. According to Proofpoint, pandemic-related phishing attacks surged by 33 percent last summer.

Evolving tactics among cybercriminals and surging rates of successful attacks mean companies are more responsible than ever for protecting sensitive information and ensuring that their systems aren't compromised. A 2021 KPMG survey of CEOs found that they regard cybersecurity risk as their top threat to growth—a risk consumers and investors are taking more seriously by the day. Meanwhile, at a time when many companies are still relying on remote work—which presents an array of cybersecurity challenges, from the use of insecure home networks and IoT devices to the risks of using public WiFi—companies have to prioritize cybersecurity like never before.

Companies have never been under more pressure to pursue the public good along with profits, and maintaining the integrity of sensitive consumer data and essential digital services should be a key part of ESG efforts. This is why company leaders should make their SAT performance a critical indicator of how they're protecting their employees, customers, and stakeholders.

About the Author

Sean McAlmont is the CEO of NINJIO and one of the nation's leading education and training executives. He served as President of Career and Workforce Training at Stride, Inc., had a decade-long tenure at Lincoln Educational Services, where he was President and CEO, and also served as CEO of Neumont College of Computer Science, and President of Alta Colleges' Online Learning Division. His workforce and ed tech experience is supported by early student development roles at Stanford and Brigham Young Universities. He is a former NCAA and international athlete, and serves on the BorgWarner and Lee Enterprises boards of directors. He earned his doctoral degree in higher education, with distinction, from the University of Pennsylvania, a master's degree from the University of San Francisco, and his bachelor's degree from BYU. Sean can be reached online at (smcalmont@ninjio.com, @ShaunMcAlmont on Twitter, and on his LinkedIn page), as well as NINJIO's website: ninjio.com.

Why Secure Video Conferencing is Critical for EdTech and Business Video Learning

By Allen Drennan, Co-Founder & CTO, Lumicademy

The changing landscape of cybersecurity and the increased threat of cyberattacks are among the key issues facing today's technology leaders. Along with creating profound changes in the workforce, work from anywhere has also allowed new security concerns to emerge. During 2021, more sophisticated and destructive cyberattacks were widely reported, a trend which is expected to continue.

Gartner recently discussed some of the main factors exposing new attack surfaces, including changes in work and more widespread use of the public cloud. They cautioned, "These changes in the way we work, together with greater use of public cloud, highly connected supply chains and use of cyber-physical systems have exposed new and challenging attack "surfaces."

Along with vulnerable devices, connections and endpoints, video conferencing and video learning apps also represent a security risk. In the last two years, video conferencing software has expanded well beyond meetings. With the remote workforce, the majority of training, employee onboarding, and corporate education will continue to take place via video on a permanent basis. Remote learning is also a permanent option for higher education institutions. It's imperative for organizations to make secure video solutions a priority, by implementing a true security approach to threats, instead of applying a "Band-aid" easy fix.

Risks Involving Video Conferencing Persist

Many of the same risks reported with video conferencing software early in the pandemic remain a factor, but they've evolved to even larger and more widespread digital attack surface areas. The most problematic areas include weak encryption protocol; vulnerable endpoints and networks; and vulnerable devices including laptops, phones, tablets, and IoT.

Organizations continue to report threats and cyberattacks involving video conferencing. Many of these incidents are still making headlines two years after the pandemic began, including:

- Hijackings of live video conferencing sessions continue to make headlines. Malicious actors are still targeting private sector companies as well as local governments, schools and universities.
- Infiltration of private corporate meetings. Cybercriminals are seeking access to confidential information such as content or recordings, trade secrets, intellectual property or other sensitive data.
- Attacks attempting to gain access to data or personally identifiable information (PII).
- Infiltrating messaging or chat features to send malware.

Organizations of all sizes are at risk, from small business to global enterprises. All stakeholders need to understand and implement cybersecurity protocols and practices in order to minimize these risks.

Key Recommendations and Best Practices for Secure Video Learning

For video conferencing security to be most effective, organizations must establish and set clear policies and then communicate these policies to their employees and other users. Approaches such as Implement Zero Trust Architecture and Multi-factor Authentication should be established as part of any cybersecurity approach.

Organizations should implement and develop policies that start with some basic parameters that everyone should follow when using any type of video conferencing solution. Security levels should be set to match the organization, or even the individual meeting, conference, or training session.

Specific organizations, sectors or industries with more stringent security and privacy needs must implement more restrictive policies to meet requirements or guidelines. More advanced security levels include encryption key depth, cipher strength, transport layer security level 1.3, end-to-end encryption and control over the location and secure deployment of all server and service resources. Government agencies as well as organizations in healthcare, financial services, and education are only some of the areas where advanced security protocols apply.

Other basic videoconferencing security guidelines and recommendations include:

- Restrict or limit administrative access for certain features
- Require unique meeting IDs
- Require unique passwords
- Conduct roll call in all meetings
- Let meeting host identify attendees before entering meeting room
- Limit sharing of confidential documents over video or screensharing
- Limit ability to screen share
- Restrict ability to share meeting invitations

These guidelines are only effective if everyone is using them. Organizations are responsible for making sure that their employees, users, and teams are aware of the policies and understand how to properly use security protocols such as Zero Trust, MFA in all of their video and remote conference sessions.

About the Author

Allen Drennan, CEO, started Lumicademy in October of 2017, bringing together the team of senior engineers who created Nefsis, a cloud-based, video conferencing online service, which Frost and Sullivan cited as the first "conferencing service solution based on the technologies of cloud-computing, end-to-end parallel processing and multipoint video conferencing," to create the next generation of virtual classroom technology.

Engaging students and educators alike, Lumicademy provides the ability to interact in a live video meeting and view presentations with screen shares, document shares, annotations and whiteboards, all within a tablet or phone experience .Lumicademy offers a high quality video and audio user experience for most mobile devices with our GPU-centric mobile edition. Educators and learners can live chat with peers in up to 62 languages. Users enjoy the learning capabilities traditional 'video apps' cannot offer, with an unlimited amount of users joining in the mobile classroom experience.

At Lumicademy, we believe there's a better way to connect people online. Our goal is to unify the virtual classroom experience, providing a modular and customizable solution to education industries and corporate organizations. We're excited to bring the authenticity of face-to-face relationships in a virtually-driven world.

Allen can be reached online at https://www.linkedin.com/in/allen-drennan-0359a822/ and at our company website https://www.lumicademy.com/.

Why Automation Isn't Replacing Cybersecurity Pros Anytime Soon

By Mark Sasson, Managing Partner, Pinpoint Search Group

Human labor in verticals such as manufacturing has certainly been impacted by automation. For instance, 46 percent of existing factory jobs are projected to be replaced by automation by 2030. However, within the context of cybersecurity, and tech in general, automation is not an existential threat to human workers in the field. Instead, it is a welcome addition.

Of course, there's a place for automation in the enterprise, as it alleviates many of the challenges executives face on a daily basis. As it stands today, digital transformation and other modernization efforts are being stymied; for a variety of reasons, it's taking too much time to implement these initiatives. For instance, slow and laborious manual efforts are still being relied upon for important initiatives like cloud migrations and the implementation of new cybersecurity tools. Clearly, this is not an efficient way of doing things in today's day and age. Many of these efforts would be accelerated tremendously by automation.

Putting things into perspective, there are 2.5 quintillion (18 zeros) bytes of data being produced every day, according to Arvind Krishna, IBM's CEO. Even if there wasn't a labor shortage in just about every market today, there is no possible way humans can process all that data manually. It begs the question: What's the point of buying all this cool new tech if we can't implement it properly? Without enough skilled engineers to go around — and there are not enough — the most efficient solution without a doubt is automation.

As it relates to cybersecurity specifically, cyberattacks are increasing exponentially, both in frequency and sophistication. Combine that reality with the fact that there is a substantial gap between the need for and availability of cybersecurity talent, automation is essential. For already overworked cybersecurity teams, manually managing alerts, and engaging in repetitive tasks is exhausting an already overworked and burnt-out talent pool. Again, there is a need for automation.

But what many people forget is cybersecurity and tech in general are not entirely driven by engineering. A company can develop the best tech on earth, and there is a chance no one would ever know about it. For example, go-to-market (GTM) functions, such as sales, field engineering, marketing and customer success, play a critical role in the adoption of technology; however, many of the tools in these areas cannot be automated. They require humans behind the controls.

Successful GTM functions require human characteristics, such as strategy, nuance, and emotional intelligence. While automation may have replaced human interaction for basic tasks like scheduling and drip email campaigns, the purchase of six and seven-figure technology solutions is conducted by human beings.

For all these reasons and more, we are seeing automation enhance and increase the productivity of highly skilled cybersecurity professionals. Companies that did not have automation in place for cybersecurity programs spent an average of $6.7 million to recover from a breach, whereas those that did implement automation spent $2.9 million. And we still have a global “talent gap” of approximately 2.7 million, meaning that even with automation, more humans are needed to ensure the security of enterprise and government cyber domains.

While automation may end up replacing some jobs in cybersecurity at some point, it won’t be replacing all of them. For many cybersecurity professionals, automation is necessary but not a threat.

About the Author

Mark Sasson is the Managing Partner of Pinpoint Search Group. Pinpoint Search Group is a boutique search firm dedicated to filling vice president, director, and senior individual contributor searches for cybersecurity vendors. Pinpoint has represented top multinational cybersecurity vendors based in the U.S., U.K., Ireland, Israel and France selling to top commercial and public sector organizations.

Mark Sasson can be reached online at LinkedIn and Twitter and at Pinpoint’s company website https://pinpointsearchgroup.com

You Can't Prevent Every Attack, But You Can Mitigate the Damage

More than ever, attackers are leveraging compromised identities to carry out cyberattacks. Stopping them is a challenge—but limiting their impact doesn't have to be.

By Grady Summers, Executive Vice President of Product, SailPoint

A four-star general and a chef walk into the Pentagon. It sounds like the start of a joke, but it's not. Consider the differences between the two individuals, but also consider the similarities. Both work in the same building. Both are employed by the government. Both probably have a key card that grants them access to the building and dictates where they can go within it.

Of course, this is where the similarities end. The general has access to the more secure areas of the building containing sensitive materials and information pertinent to his or her job. On the other hand, the chef probably has access to parts of the building that the general would never think to go, such as kitchens, storage, or areas where food is served. The chef's access card isn't going to provide access to the war room, and there's a good chance the general's card won't grant access to every area where a chef might serve a meal for different teams. This is all perfectly logical—why risk the entire building being compromised because of one lost keycard?

Put in those terms, it seems obvious. So why do so many organizations fail to apply this same logic to their identity security? By granting users, devices, applications and other identities privileges well in excess of what they need to do their jobs, organizations are making it far too easy for attackers who compromise an identity. Unfortunately, compromising identities is something of a specialty for many of today's attackers—meaning that improving identity security must be a higher priority than ever for modern organizations.

The Danger of Poor Identity Security

Systems are growing ever more complex, and as that complexity increases visibility becomes more difficult. While many businesses had already been undergoing digital transformations, the past two years have accelerated the trend significantly—particularly as it applies to identity security. With remote work as the norm, new users and devices now need to access corporate networks from unfamiliar places every day. IT teams also need to grapple with securing the new applications that employees need to function remotely, such as Slack and Zoom. And of course, use of the cloud continues to expand, adding entirely new infrastructure and applications to the mix.

As the complexity of IT environments grows, so too does the potential threat surface. Users might need to access data across multiple servers, cloud environments, file sharing applications, and other locations. In an organization with hundreds or thousands of employees, determining access rights and privileges for each individual user can seem like an incredibly daunting task, especially when business operations are taken into account. And here's the real issue: no IT team wants to be seen as a roadblock to productivity. This is the core of the problem that leads to overprovisioning. It is easier to grant more access than necessary than it is to field access requests on a case-by-case basis. This makes it challenging to manually govern identities at scale.

Unfortunately, overprovisioning can have negative consequences. If our old friend the chef has a keycard that opens the door to the war room, anyone with access to that keycard could throw on an apron, grab a sandwich platter, and make off with top secret intelligence. In an enterprise IT environment, it's much the same. Should software developers have access to human resources files? Should the public relations team be able to approve purchase orders? When employees have outsized access levels, it opens the door to chaos. Anyone can be tricked into giving away their password—it happens every day. But compromising an administrative assistant's identity should not allow an intruder to access financial records or personal information. No individual identity should give an attacker the keys to the castle.

No "Set It and Forget It" for Identity Security

I was a CISO fifteen years ago when I first heard Mandiant CEO Kevin Mandia say that compromise was inevitable, and that smart companies should focus on preparation, detection, and response instead of assuming that prevention will work. Even though it's been 15 years—and "compromise is inevitable" is no longer even controversial—it seems like most of today's security tools focus primarily on stopping or preventing attacks, rather than mitigating their potential impact. Shifting the focus to mitigation represents a change in philosophy, but one that will have positive results for businesses. This isn't to say that preventative tools are not necessary—they absolutely are—but that they can be used most effectively in conjunction with tools that help lessen the impact of those attacks that slip through the cracks.

Given that 61% of breaches today involve credential data, that process starts with ensuring that individual identities have access only to the data and areas of the network they need access to. That means that if a marketing employee falls victim to a phishing email, some marketing data might be compromised—but the attacker won't be able to access payment information or personnel files.

While it is difficult to manage large numbers of identities manually, modern technology has—thankfully—made it easy. Today's organizations no longer need to individually provision access privileges for users and other identities. Artificial intelligence (AI) and machine learning (ML) have powered the growth of new automated tools capable of identifying patterns in behavior and understanding the degrees of access appropriate for different job functions. Modern solutions can even learn and adjust over time if they see repeated access requests from similar users, or notice that a certain type of access is almost never used. Identity security is not a "set it and forget it" solution. Needs and functions change over time, and a good identity security solution must change as well.

Contain the Blast Radius and Stay Out of the Headlines

A strong identity security solution establishes the right level of access for individual identities in a way that doesn't inhibit their ability to do their job. And really, why should it? The chef will probably never even know their keycard doesn't open the door to the war room—they have no reason to even try it. Likewise, the general has no reason to access wherever the chef is headed. Denying them access will not impact their performance in any way. There is no reason to give them access to areas that they will never need to do their respective jobs.

Automation has made it possible to apply this same principle at scale for today's organizations, establishing clear access parameters for different identities and ensuring that the damage caused by one compromised identity remains contained. While preventative tools are important, organizations must invest more resources into attack mitigation. Mandiant may have been early in its proclamation that breaches are inevitable—but it was true. But not every breach has to be a big one. Thanks to automation, today's identity tools can help organizations ensure that their next breach stays out of the headlines.

About the Author

Grady Summers has held technology and leadership positions for over 20 years and now serves as the Executive Vice President of Product at SailPoint. Grady will be responsible for driving SailPoint's technology roadmap and solution strategy, ensuring strong and consistent execution across SailPoint's identity portfolio. Most recently, Grady was the Executive Vice President of Products and Customer Success at FireEye. In his two roles before that, Grady was a Principal at Ernst and Young, helping to lead the firm's information security practice, and the Chief Information Security Officer (CISO) at General Electric, overseeing a massive global cybersecurity organization.

For more information, visit www.sailpoint.com.

Zero Trust Architecture: Adoption, Benefits, and Best Practices

What is Zero Trust security, and what are the benefits? Here's how to prevent data breaches by staying on top of security with Zero Trust architecture.

by Harish Akali, Chief Technology Officer, ColorTokens

'Trust Nothing, Verify Everything': Benefits and Best Practices of Zero Trust Architecture

No matter the industry or size, organizations have been embracing digital transformation at an astonishing pace. Necessarily, the cybersecurity industry is seeing a shift that many argue is long overdue. This is best described as a paradigm shift from reactive to proactive security that assumes the bad guys will get in. This is also the paradigm of Zero Trust architecture, which is built to stop the bad guys in their tracks from the inside out if need be.

Businesses today are essentially massively interconnected attack surfaces. Meanwhile, the maximization of telework and cloud computing are supersizing the number of attack vectors. Enterprise networks with traditional security have become a playground for bad actors, who rely on taking advantage of any processes, access, or traffic that are “trusted” to stay undetected. This is where Zero Trust architecture comes into play with its credo of “trust nothing; verify everything.”

Even President Joe Biden is among the proponents of Zero Trust architecture. As this wide embrace of Zero Trust is growing, security professionals want to know how they can make Zero Trust a reality for their enterprise. Many are coming to learn that Zero Trust is a journey, and understanding this journey is the first step down the path.

If you wish to dive deeper into the topic of Zero Trust, we've made a **FREE** copy of the first and only "The Definitive Guide to Zero Trust Security" available to all Cyber Defense Magazine readers.

First, you may be asking, 'What is Zero Trust security?'

Zero Trust security can be summed up with the phrase, "Trust nothing, verify everything." Resource access within a network is always limited by trust dimensions — and access is revoked if these parameters are ever unmet. It provides a 180-degree turn from traditional security models that provide implicit trust within the network.

For the most part, the principles of Zero Trust architecture can be broken down into the following components:

• ***Network traffic is untrusted***. This is true even if traffic originates internally. Inspection, authentication, and documentation are always necessary.

• ***Micro-segmentation is applied***. No user can roam freely throughout the infrastructure.

• ***Each entity is low trust***. An entity will gain only a specific level of trust.

• ***Zero Trust doesn't mean no trust***. Upon verification, entities are given appropriate, yet restricted, access that is limited to the function they must perform.

• ***Trust is dynamic***. Trust may be granted, but it isn't constant.

• ***Trust is impartial***. All users and entities will be assessed using the same criteria.

• ***Least privilege access always applies***. Trust is granted based on what's needed to perform the entity's intended functions.

When each of these principles comes together, IT teams can achieve long-term cyber resiliency.

The Benefits of Zero Trust Security

• ***Secure cloud migrations.***

IT teams gain the ability to visualize, monitor, and control network traffic with platforms like the Xtended ZeroTrust™ Platform — even those running in virtual machines and containers. If integrated with cloud management tools, Zero Trust also ensures that security policies move with workloads upon cloud migration.

• ***Increased visibility into lateral movements.***

Threats can go unnoticed as they move laterally across networks. With the granular visibility provided by end-to-end Zero Trust platforms, IT teams gain 360-degree visibility and control of their environments.

• ***Data breach prevention.***

By isolating high-value assets, IT teams can restrict access to all users, services, devices, and platforms other than those parties authorized as “need to know,” circumventing any widespread data breaches.

• ***Data breach resilience.***

Legacy systems are often wide open to the network and lack the isolation necessary to limit a breach. Zero Trust architecture platforms divide systems into micro-segments, building greater cyber resilience for companies.

• ***Massively reduced attack surface.***

Providing access to only those assets and workloads that users need creates smaller trust zones, reducing the attack surface and restricting unauthorized lateral movements should cybercriminals gain access.

• ***Greater compliance.***

Isolating high-value assets alone strengthens compliance, but Zero Trust security also prevents unauthorized access by internal and external parties, generates privacy-related regulation documentation, and establishes a wall between development and production within an organization.

• ***Limited scope of compliance audit.***

With segmentation being the initial step of Zero Trust security, companies limit the scope of a PCI-DSS audit by showing evidence of segmentation across the data center, cloud providers, and business locations.

• ***Mitigated risk from legacy systems.***

For example, many of our manufacturing clients operate with legacy, end-of-life systems that aren't replaceable or easy to upgrade for budget or business reasons. These outdated systems, however, are

unpatched with no support, setting the stage for cyberattacks. Securing these legacy systems quickly and for long-term resiliency is to prevent the movement of ransomware is possible with Zero Trust.

Basic Steps of Zero Trust Implementation

Zero Trust architecture isn't a "set-and-forget" solution to cybersecurity. As your organization begins preparing to implement Zero Trust security, it's important to keep in mind the following:

1. Map the environment.

Mapping the environment gives IT teams a clearer picture of the task ahead. With most companies containing many moving parts, start with one application or workload to get a grasp on the number of users, amount of traffic, required applications, and connections between all entities.

2. Define trust zones.

Trust zones are basically data assets that should be segmented, monitored, and protected as units, falling under a set of access policies. Automation can assist in identifying trust zones by looking at workloads in the same network segment, but always make sure to have human administrators verify that zones align with business practices.

3. Create security policies.

Security policies will dictate access not only to assets, but also between trust zones. Powerful policy engines will help by recommending policies, which will streamline the process.

4. Observe traffic between trust zones.

Schedule an observation period to capture the traffic patterns between established trust zones. You may find that certain parties need access to perform urgent tasks, and setting authentication boundaries between these zones could impact mission-critical activities. This is part of "building the muscle," which will get stronger over time.

5. Monitor and refine zones and policies.

Applications come and go. Workflows change. Team members are always on the move. Naturally, you'll need to track and adapt the policies that protect high-value assets. It's important to build in some flexibility and adaptability into Zero Trust architecture and the security tools used to enforce authentication.

For the ultimate breakdown of Zero Trust best practices and implementation, download a free copy of the first and only "Definitive Guide to Zero Trust Security."

Best Practices for Zero Trust Implementation:

With Zero Trust implementation being a new initiative, the chances are good that your organization will experience some growing pains with Zero Trust architecture. This isn't uncommon — nor should it serve as an excuse to abandon the new measures. In our experience, these tactics can often be of benefit:

1. Go zone by zone.

"Boiling the ocean" is never a good idea with Zero Trust architecture. Instead, enforce policies trust zone by trust zone. Perhaps start with your highest-value application and expand out from there.

2. Use orchestration for DevOps.

Integrating DevOps with cloud infrastructure tools can help protect data, applications, and workflows within cloud platforms when moved to Zero Trust architecture.

3. Update policies.

Zero Trust security is a dynamic environment. IT teams should be monitoring both policy violations and new connections that might require new policies. Update policies and enact new ones based on the findings. Again, the right policy engine can streamline this.

4. Extend Zero Trust to endpoints.

The same principles should be applied to all endpoints within an organization, including servers, laptops, PCs, and mobile devices. Traffic can help to identify where to direct IT attention. Only authorized processes should run at these endpoints, thereby reducing the risk of cyberthreats.

Zero Trust architecture should do more than stitch together security protocols. It can help an organization establish a set of rules and control to determine which entities can gain access to restricted locations and critical information within a company.

Selecting the Right Zero Trust Vendor

Not all Zero Trust vendors are created equal. In fact, some tout their products and services as “Zero Trust” without following through. This makes the selection process of a Zero Trust vendor suited to your organization more important than ever. Here are just a few of the criteria to keep in mind as you arrive at a decision:

• Platform approach.

A Zero Trust architecture should span the entire network, regardless of location. So naturally, point security tools cannot achieve unified context and control and will leave organizations with a fragmented Zero Trust posture. What’s needed is a single platform that provides end-to-end Zero Trust for workloads, users, endpoints, and applications. Such platforms like the eXtended ZeroTrust™ Platform can deliver Zero Trust at scale.

• Cloud delivery.

If your organization has already made the move to the cloud, look for a Zero Trust vendor that operates on cloud platforms. This ensures that the vendor and its security platform can scale with your operations.

• Scope of capabilities.

If a vendor doesn’t enable greater visibility and micro-segmentation cloud security, move on. You need the ability to monitor the network and divide data assets to limit and respond to cyberthreats.

• Breadth of protection.

Zero Trust zones are essential to *Z*ero Trust architecture and should offer control over a wide range of resources. Look for the capability to define user groups and create policies that control access to resources.

• Ease of implementation and management.

While Zero Trust vendors should always be on hand to offer support, the ideal choice will provide access to the security tools and resources to take internal control. Your IT team should have the capacity to classify user groups, create connection maps, adjust policies, and so on, without a call to the vendor.

• **Integration of other security tools**.

Zero Trust vendors should offer platforms that can share information with other security tools, including cloud service provider security; management and logging technologies; security information and event management systems; and orchestration and automation tools. Otherwise, the transition and enforcement won't be as smooth as you'd hoped.

• **Total cost of ownership**.

As with anything in business, it all comes down to budget. Narrowing the field of potential Zero Trust vendors should account for more than implementation costs. Factor in licensing and maintenance costs, as well as the cost for initial implementation and ongoing connection monitoring.

Above all else, it's important to factor in the savings you'll gain when your operations have all the proper controls in place to protect high-value assets, applications, and other resources. The wrong choice can affect you for years to come.

If you'd like to learn more about what ColorTokens' award-winning Zero Trust approach can do for your organization, please let us know. A member of our team would be more than happy to review your operations and develop a solution that's customized to your critical assets.

About the Author

Harish Akali is the Chief Technology Officer at ColorTokens Inc., a leading innovator in SaaS-based Zero Trust cybersecurity solutions. As a member of the ColorTokens leadership team, he uses his extensive knowledge of cybersecurity and enterprise software across multiple industries to drive innovation.

Zero-Trust Needs to be a Priority - For SaaS, Too

By Misha Seltzer, cofounder and CTO Atmosec

Call it a sign of the times; you can't trust anyone these days, even the most loyal members of your organization. As a result, enterprises have embraced the zero trust model of security - where all users connecting to a network are assumed to be untrustworthy, requiring vetting such as 2FA authentication.

But threats sometimes come from unexpected quarters, such as some of the most popular cloud-based applications, as evidenced by the increase in supply-chain attacks. Organizations tend to focus their security on malware transferred via email, as well as other exploits connected to users. The ubiquitous SaaS "trusted application platforms" need to be looked upon as potential security risks as well - and included in zero-trust policies. Indeed, some of the most "trusted" platforms and services - including Okta, Mailchimp, Heroku, TravisCI and Hubspot - have been hacked and/or subject to security breaches in recent weeks. Such incidents show that even major platforms – which presumably have extensive internal security - need to be included in zero-trust policies.

Platforms, like users, cannot be treated as "trusted." To protect against these threats, organizations need to set up systems that will examine all connections between users,SaaS platforms, and data, as well as evaluating and vetting the increasingly popular third-party apps used by employees.

Security flaws in these platforms could be weaponized by hackers who take advantage of them via third-party apps that connect to platforms. The SaaS platform itself may be usually safe, but security flaws - that even the platform isn't aware of - could enable bad actors to get a foothold on the platform, and from there to an organization's network, or the data stored on the SaaS platform itself. And because these SaaS third-party applications are widely used to enhance platform capabilities, both by employees in the office and those working remotely, stemming the threats presented by these connections can be a difficult challenge for security teams.

The problem for organizations - even those with zero-trust security policies - is that most cannot vet the connections within these trusted SaaS platforms. Hackers can thus take advantage of SaaS vulnerabilities to steal organization or personal employee data from the platform - and the security team won't know about it until it's too late. In fact, the security flaw may not even be that; it may be a "feature" of the SaaS platform, designed to help users be more productive - but such third-party apps that are often not vetted as well for security could provide hackers with the opportunity they need.

For example, researchers in 2020 discovered a bug that utilized a Request Smuggling exploit on the Slack SaaS platform, which would allow hackers to send rogue requests through an online application - perhaps a request to pass malware through to a client, or to siphon data off a connected cloud account. According to researchers, the vulnerability was discovered in an unnamed asset "that could be used to force users into open redirects, leading to a CL.TE-based hijack and the theft of secret user session cookies. These cookies could then be stolen, leading to the compromise of arbitrary Slack customer accounts and sessions."

It should be noted that the bug was actually designed to speed up user requests, and make the platform more efficient; but bad actors, as they often do, were able to hijack the feature for nefarious purposes. The Slack asset may or may not have been utilized by one of the many third-party applications on the Slack Marketplace, all of which utilize APIs and assets within the platform to provide assistance, shortcuts, and greater efficiency for Slack users; but it certainly could have been used in that way. The vulnerability was discovered by a bug bounty hunter before hackers could get hold of it - but there's no guarantee that others don't exist. And the same story could be told about other platforms - such as SalesForce, where researchers discovered that third-party applications that rely on the platform's OAuth protocol could open the door to bad actors.

The point is that there is no way for organization security teams to know about these potential problems in advance of their being discovered - possibly by hackers. The resolution of issues like these is in the hands of the SaaS platform that allows these third-party applications to utilize its resources, some of which may have security issues - but if any damage does ensue, it will be strictly the problem of the end-user victim. The task for security teams, then, is to ensure that their organization does not end up on that victim list - despite the fact that they would have no way of knowing about SaaS platform security flaws, or any way of doing anything about it, even if they did know.

Some organizations might try to impose a whitelist, allowing the use of only those SaaS platforms and third-party apps that have been thoroughly vetted. But that could be difficult to implement, especially if employees have a lot of assets and data invested in those platforms and applications - and yet another reason to implement zero-trust policies.

A better strategy might be to implement an automated system that will examine connections and logs for anomalies and other issues, utilizing techniques like AI, machine learning, neural networks, and other advanced data systems that will alert security teams of potential problems. If suspicious behavior is detected, teams can intervene to prevent or limit damage, ensuring that the organization's most important assets are protected.

Additional protections, also built on the zero-trust model, could include tighter policies for SaaS within the organization, including requiring frequent password changes, implementing 2FA, rotating APIs, and ensuring that SaaS accounts are closed when employees leave or take different jobs in the organization. Advanced data systems can help security teams keep up with changes as they occur, ensuring that all security risks are accounted for.

SaaS platforms have enhanced productivity for untold numbers of organizations - and have been essential to ensuring business success during the Covid and post-Covid periods, when many employees did (and continue to do) their work from home. The capabilities - and convenience - of SaaS platforms and their third-party apps will continue to be essential. Security teams that handle them correctly can ensure that organization employees remain productive - and safe.

About the Author

Misha Seltzer is the Co-Founder and CTO of Atmosec. He's driven by helping companies confidently secure the adoption, usage and management of any business application across their organization. Misha can be reached online on LinkedIn and at our company website https://www.atmosec.com/


EVENTS

CYBER DEFENSE CONFERENCES

THREE EVENTS IN ONE

Orlando, Florida, USA | October 27-28, 2022

One of the most exclusive, fun and educational CISO conferences of the year!

Limited to our selection of the top 100 CISOs in the world, amazing speakers and insider threat mitigation training by a world reknown expert - meets 100 top cyber defense companies in an intimate, high value two day summit

www.cyberdefenseconferences.com

REGISTER FOR FREE!

KCLIVE

The Future of Identity & Access Management

WED JUL 6

Do you want to understand what role decentralized identity / verifiable credentials / self-sovereign identity plays when it comes to customer identities? How will we transition from these to features like biometrics and going passwordless? How will we verify users in the future?

Come join our thought leaders and practitioners to discuss the Future of Identity & Access Management.

Get the keys to understand how to strengthen your identity proofing abilities, better mitigate remote work-force risk and provide your customers with a seamless digital experience.

Our top speakers

Leonardo Morales
Siemens AG

Neeme Vool
Swedbank

Paul Fisher
KuppingerCole Analysts AG

Christopher Schütze
KuppingerCole Analysts AG

kuppingercole.com/events/2022/07/future-identity-access-management

kuppingercole ANALYSTS

2nd Edition

CONNECTED AFRICA

Africa's premier Telecom Event

" Championing Connectivity in the Digital Era "

July 26th, 2022

Join Us In Cape Town

Organized and Conceptualized by

For More Information :

www.connected-africa.com

NFT EXPOVERSE

THE LARGEST MASS ADOPTION BLOCKCHAIN EVENT OF THE YEAR

This July

FRI 29 | SAT 30 | SUN 31

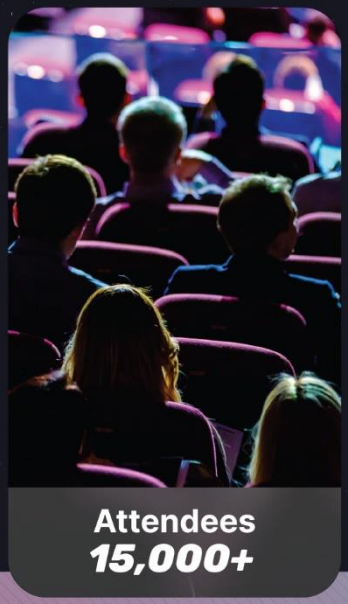
Los Angeles, CA
LA Convention Center

SCAN HERE!

Use code **CDEFENSEMAG** for **10% OFF** tickets!

nftexpoverse.com/get-tickets

Media Partners
100+



Attendees
15,000+

Speakers
150+

Vendors
400+

NFTEXPOVERSE.COM | +1-631-777-3455 | SALES@ZJEVENTS.COM | FOLLOW US!

CLOUD NEXT

The Shift of Cloud from Infra Solution to Business Strategy

August 05, 2022 | Bengaluru

Organised by NETNEX

WORLD FINANCIAL INNOVATION SERIES

16 - 17 AUG 2022

PHILIPPINES

HYBRID EVENT

Sofitel Philippine Plaza **Manila, Philippines**

PHILIPPINES' PREMIER FSI TECHNOLOGY & INNOVATION CONFERENCE

Organised by

TRADEPASS

IoT in Oil and Gas

8th Annual CONFERENCE

Hilton Americas - Houston, TX

https://iotinoilandgas.energyconferencenetwork.com/iot2022

+1 855-869-4260

info@energyconferencenetwork.com

SEPTEMBER 12-13 2022

Future Tech Event

UNDER THE PATRONAGE

سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and Information Technology

مسقط
العاصمة العربية الرقمية
Muscat Arab Digital Capital
2022

رؤية عُمان 2040
Moving Forward with Confidence

ENABLING OMAN'S VISION 2040

12 - 13 September 2022 | Oman Convention and Exhibition Centre | 9 am - 4 pm

HYBRID+ (In-Person and Online)

Future Tech is Sultanate of Oman's foremost B2B and B2G bespoke Technology Expo and Summit.

For Exhibiting Enquiries and Sponsorship Opportunities please contact:
Navneeth K, Director - Business Development
+968 9123 7892 | bdm@wpsummits.com
www.futuretechevent.com

ORGANISED BY

مسقط إكسبو
Muscat Expo

WPS
WHITE PAPER SUMMITS

FRANSEC

SECURING **FRANCE** FROM CYBER THREATS

13th - 14th September 2022

Paris, France

Join Free With Code: CDM-VIP

Join Us at the FranSec Summit on 13th - 14th September!

The 3rd annual **FranSec Summit** brings together **100+ IT security leaders** from across the **Retail, FMCG, Banking & Finance, Automotive, Utilities, Food & Beverage industries** for 2-days of insight building and expert knowledge exchange on **13th - 14th September.** Join us in **Paris, France** to hone your skills in areas including:

- *Digital transformation and cyber resilience*
- *The current cyber landscape and how to improve your security capabilities*
- *Working with third parties to improve your cyber security posture*
- *Reacting to an increasing attack surface*
- *Implementing risk-based security strategies*
- *The human factor in organisational cyber security*
- *And, more!*

CPD CERTIFIED
The CPD Certification Service

Speakers include CISOs, VPs, Heads of IT Security at: **La Banque Postale, Airbus, AXA, Interpol, Total, Suez,** and more...

Helene Bernardini
CISO
Groupe Lactalis

Xavier Boidart
Group CISO
Crédit Agricole

Maran Madiajagane
CISO
RAJA

Clara Le Gros
Deputy CISO/DPO
NATIXIS

Cristophe Civarella
Deputy CISO
Crédit Mutuel ARKEA

Stephane Boua
CISO
Groupe Les Echos Le Parisien

Michael Bonhomme
Group CISO / Head of IT Security
Baobab

Francis Bergey
Deputy CISO, Security Expert
eVoyageurs SNCF

Badi Ibrahim
Head of Hotels IT Security
Accor

Joy-Alexandra Denis
Deputy CISO
Arquus

This is a one-of-a-kind opportunity for cyber security leaders across France to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CDM-VIP** at: **france.cyberseries.io/register/**T&Cs apply.

BLOCKCHAIN in OIL & GAS

6th Annual

CONFERENCE

Hilton Americas - Houston, TX

https://blockchain-oilandgas.energyconferencenetwork.com/bcog2022/1614608

+1 855-869-4260

info@energyconferencenetwork.com

SEPTEMBER 14-15

2022

CYBER SECURITY & CLOUD CONGRESS

NORTH AMERICA

5-6 October 2022
Santa Clara
Convention Center

We're Back!
Join Us Live & In-Person

The Cyber Security & Cloud Expo will host two days of top-level content and thought leadership discussions around Cyber Security & Cloud, and the impact they are having on industries including government, energy, financial services, healthcare and more.

8 Conference Tracks

250+ Speakers

150+ Exhibitors

6 Co-Located Events

6,000+ Attendees

Speakers include:

Kavitha Venkataswamy
Senior Manager - Product Security, *Capital One*

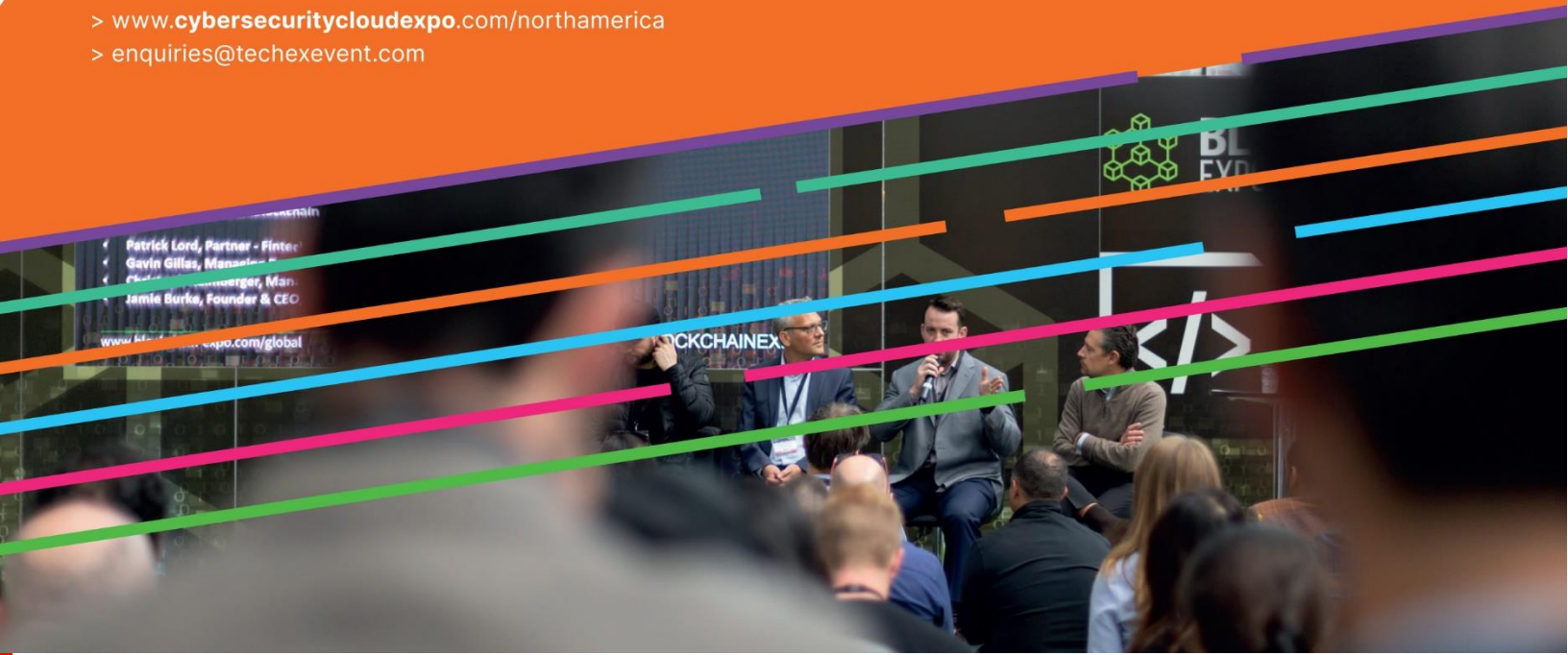
M.K Palmore
Official Member, *Forbes Technology Council*

Michael Fulton
Adjunct Faculty, *The Ohio State University*

Elizabeth Cartier
Director - Information Security, *Headspace Inc.*

Register now for free tickets!

> www.**cybersecuritycloudexpo**.com/northamerica
> enquiries@techexevent.com



LEVELLING UP UK CYBER SECURITY

We believe there is a knowledge gap between the expertise of the cyber community and UK business leaders.

We want to close that gap.

Contribute to the programme by visiting www.ukcyberweek.co.uk/call-for-papers.

OUR PARTNERS

IASME CONSORTIUM

Chartered Institute of Information Security

CREST

UK CYBERWEEK

3 ›› 4 NOVEMBER 2022

Business Design Centre | London

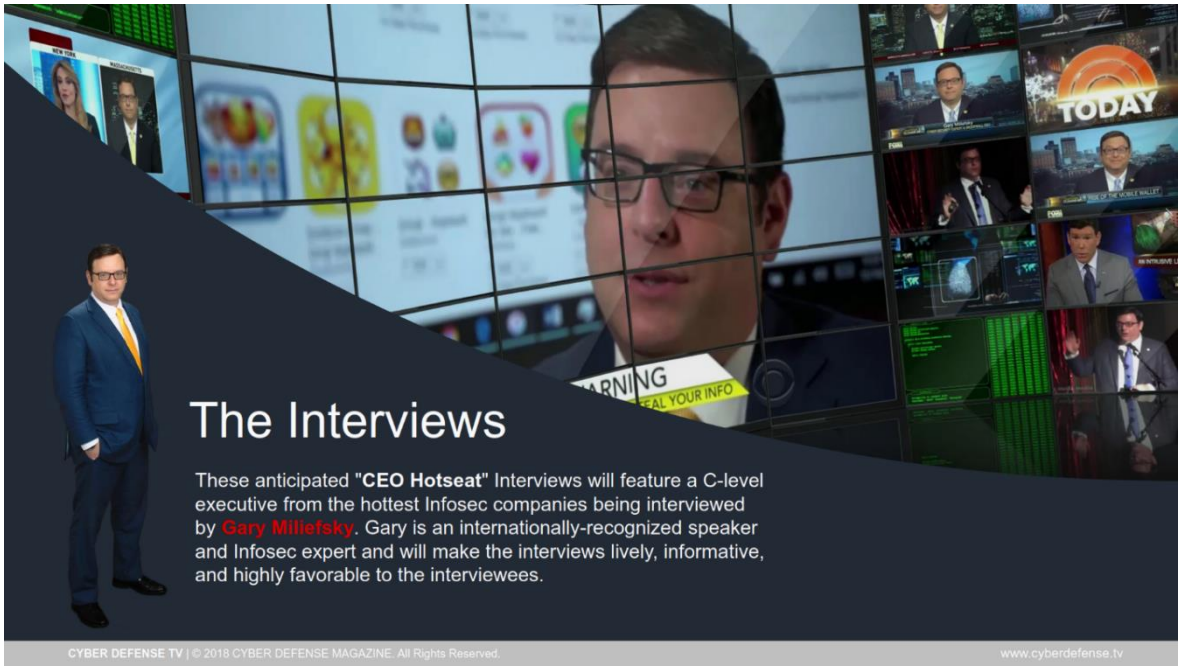
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

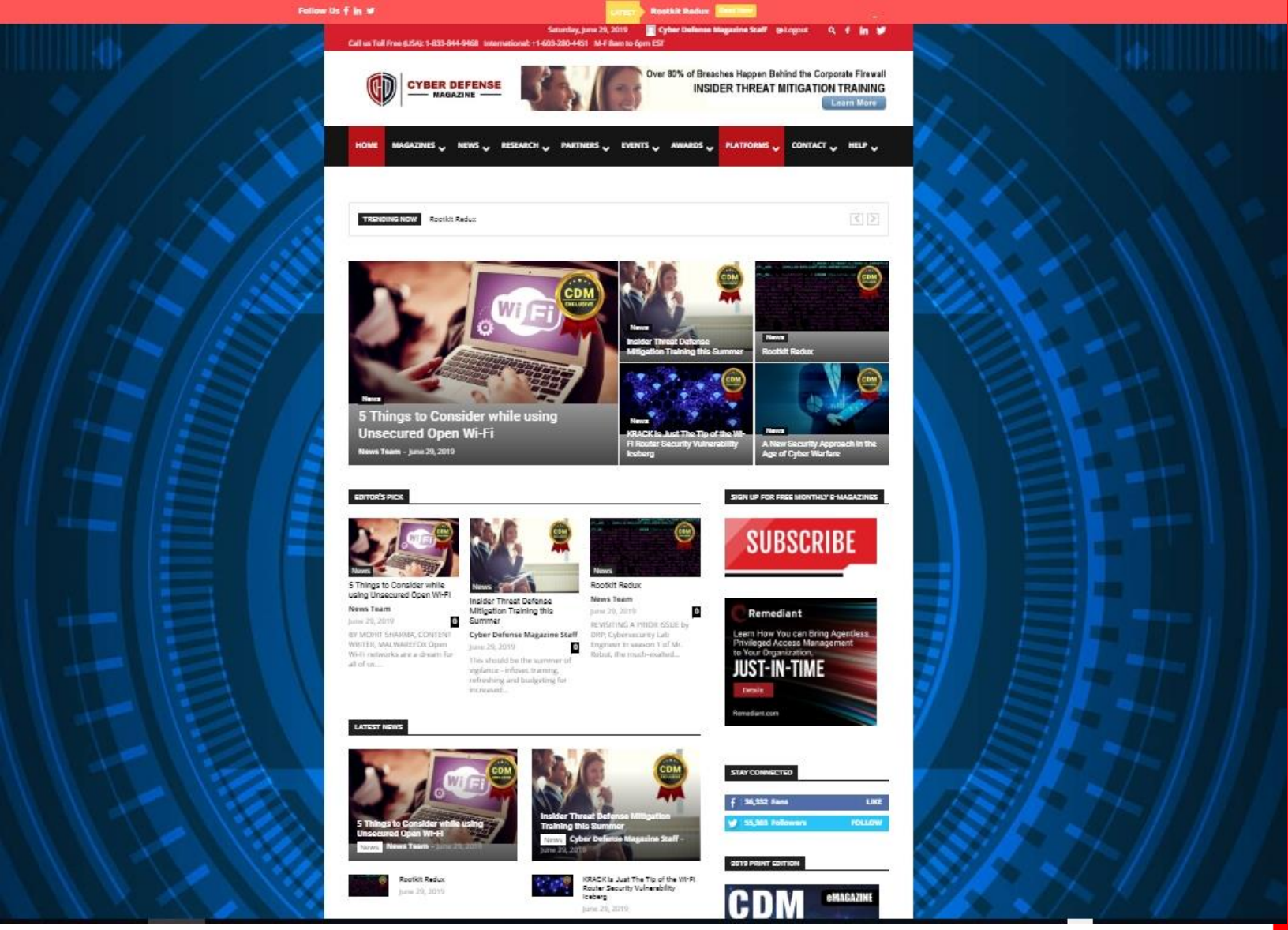
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 07/02/2022



Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

10 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites and our new B2C consumer magazine CyberSecurityMagazine.com. *Millions of monthly readers and new platforms coming…starting with www.cyberdefenseconferences.com this month…*

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert

ALWAYS FREE
NO STRINGS ATTACHED

Preventing Tomorrow's Malware

Today.

www.cythereal.com

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

*** with help from writers and friends all over the Globe.**