CYBER DEFENSE MAGAZINE

eMAGAZINE

JULY 2023

In This Edition

Before You Deploy Advanced Tech, Consider the Hidden Cyberthreats

Healthcare Under Siege

The Role of AI in Cybersecurity

...and much more...

MORE INSIDE!

CONTENTS

Welcome to CDM's July 2023 Issue ---------- 7

Before You Deploy Advanced Tech, Consider the Hidden Cyberthreats ---------- 18

By Jennifer Varner, Director Security Solutions Sales - North America, Verizon Business

Healthcare Under Siege ---------- 22

By Ty Greenhalgh, Industry Principal, Healthcare, Claroty

The Role of AI in Cybersecurity ---------- 27

By Alysia Silberg, CEO, Street Global

The Best of Both Worlds Made Possible with A Hybrid SOC ---------- 30

By Chase Richardson, Principal Lead Consultant, Bridewell

AI In Cybersecurity – Risks and Rewards ---------- 34

By Aimei Wei, Co-Founder and CTO, Stellar Cyber

Cyber: Dealing with a Data Breach ---------- 37

By Rishi Baviskar, Global Head of Cyber Risk Consulting at Allianz Global Corporate & Specialty (AGCS) and Michael Daum, Global Head of Cyber Claims at AGCS

From AI-driven Defense to Dark Web Threat Intelligence ---------- 42

By Annabelle Klosterman, Cybersecurity Reporter, Cyber Defense Magazine

Has MFA Had Its Day? ---------- 49

By Ori Arbel, CTO, CYREBRO

Boost Your Business Security: How Cyber Insurance Shields You from Cyber Threats ---------- 52

By Simon Pascoe, Director, FD Beck Insurance Brokers

Bridging the Widening Gap in Cybersecurity Talent: Addressing the Urgent Need for Skilled Professionals ---------- 57

By Travis Doe, Marketing Executive, Secure IT Consult

A Passwordless Future ---------- 64

By Sam Rehman, SVP, Chief Information Security Officer, at EPAM Systems, Inc.

Blockchain Technology: Strengthening Cybersecurity and Protecting Against Password Leaks and Data Breaches ---------- 68

By Thomas Carter, CEO, True I/O

Adaptive DDoS Attacks Get More Sophisticated: How to Beat Attackers' New Ground Game ---------- *72*

By Gary Sockrider, Director, Security Solutions, NETSCOUT

Analyzing Four Diverse Attack Techniques Used by XeGroup ---------- *75*

By Brett Raybould - EMEA Solutions Architect, Menlo Security

How Ai Can Be Used as A Tool to Help Monitor for Cybercrimes and Keep Kids Safe From Cyberbullying And Scams ---------- *79*

By Ron Kerbs, CEO of Kidas

What to Consider When Choosing Cybersecurity Insurance Coverage ---------- *82*

By Richard Clarke, Chief Insurance Officer, Colonial Surety Company

TikTok Ban: The Death Knell for Free Access to the Web? ---------- *86*

By Sebastian Schaub, CEO, hide.me

Three Ways to Protect the Data Powering Summer Vacations ---------- *88*

By Amit Shaked, CEO and Co-Founder, Laminar

Triple Tactics ---------- *92*

By Andy Mills, VP EMEA, Cequence Security

Criminals are Bypassing Authentication with Stolen Session Cookies ---------- *98*

By Trevor Hilligoss, Director of Security Research, SpyCloud

Cyber Attacks on Municipalities ---------- *102*

By Veronika (Nikki) Jack, Student Majoring in Information Technology-Cybersecurity, George Mason University

Six Tips to Ensure a Strong Patch Management Strategy ---------- *105*

By Ashley Leonard, CEO and Founder, Syxsense

Overcoming Challenges in Cyber Defense Business Naming in The Age of AI ---------- *108*

By Darpan Munjal, CEO and Founder, Squadhelp.com

Why IT Governance and Mitigating Risk is a Critical Part of Cyber Defense ---------- *112*

By Vincent Tran, CISSP, Co-Founder and Chief Operating Officer, Liongard

Gartner's Calling for a Human-Centric Approach to Cybersecurity - Here's How to Implement It ---------- *115*

By Roy Zur, CEO, ThriveDX Enterprise

How Continuous Authentication Is Changing the Game for BYOD And Contracted Employees ---------- *118*

By Jasson Casey, Chief Technology Officer, Beyond Identity

How The Growing Adoption of Cloud Is Giving Rise to New Security Challenges ---------- *121*

By Joseph Carson, Chief Security Scientist & Advisory CISO, Delinea

Simplifying your Approach to the Zero Trust Journey ---------- *126*

By Chris Cullerot, Director of Technology and Innovation, iTech AG

No Cloud, No Problems: Why Dynamic DNS Reigns Supreme Over Cloud Applications -------- *129*

By Dan Durrer, Founder & CEO, No-IP

Promoting Safety Across Your Digital Supply Chain ---------- *133*

By Guy Golan, CEO at Performanta

Recruiting and Retaining Women Talent in Cyber Amidst the Cyber Shortage ---------- *136*

By Oriana Vogel, Chief Human Resources Officer, Trustwave

4 Reasons Why Not to Use Whatsapp for Secure Communications ---------- *139*

By Nicole Allen, Senior Marketing Executive at Salt Communications

How To Ensure Information Security of An Organization Basing on Business Requirements *144*

By Sergio Bertoni, The Leading Analyst at SearchInform

The Power of Policy: The Best Weapon in Your Defensive Arsenal Isn't New Tech ---------- *149*

By Craig Burland,CISO of Inversion6

The Basics of Digital Forensics ---------- *152*

By Milica D. Djekic

Why Power Matters in Cyber Protection ---------- *156*

By James Martin, Global Connectivity Product Manager, Eaton

With Increased Cybersecurity Awareness, Why Does Phishing Still Work? ---------- *159*

By Zac Amos, Features Editor, ReHack

@MILIEFSKY

From the

Publisher…

Dear Friends,

Reviewing current trends at Cyber Defense Magazine, as well as the broader perspective of Cyber Defense Media Group, we continue to see a growing interest in the implications of privacy concerns and artificial intelligence. Our authors and readers both reflect a broadening of interests beyond the technical side of cyber security.

At the same time, the core of our audience and editorial focus continues to be in the realm of CISOs and other professionals in our industry. This presents both a challenge and an opportunity. In response, we have opted to take the broader approach, as reflected in the selection and publication of numerous articles appealing to the interests of our growing readership.

With the rapid development of applications based on artificial intelligence, such as privacy, identity theft and fraud, and consumer protections, we trust that we have found a middle course with benefits for both our increased readership and advertisers.

We continue to see a race between developers and regulators, private sector and government functions, and the hopes and fears of our society in understanding how these rapid developments will benefit or harm all of us.

As publisher, it's important to be mindful of the mission and contribution we have undertaken, to provide the most professional and up-to-date forum for keeping our readers informed of challenges and responses in today's cyber world. With the support of our contributors and readers, we continue to pursue our role as the premier publication in cybersecurity.

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@cyberdefensemagazine.com

ADVERTISING

Marketing Team

marketing@cyberdefensemagazine.com

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

http://www.cyberdefensemagazine.com

PUBLISHER

Gary S. Miliefsky, CISSP®

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

11 YEARS OF EXCELLENCE!

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

CYBERDEFENSEMEDIAGROUP.COM
MAGAZINE TV RADIO AWARDS
PROFESSIONALS VENTURES WEBINARS
CYBERDEFENSECONFERENCES

Welcome to CDM's July 2023 Issue

From the Editor-in-Chief

As we enter the second half of the calendar year, from the Editor's desk it's clear that events continue to accelerate. Accordingly, the challenges for cybersecurity continue to grow. As a result, we see this reflected in the focus of the articles we receive and publish.

Artificial Intelligence (AI) continues to be an area of particular interest and concern. From worries about job replacement to privacy to weaponization and politicization of this rapidly-developing phenomenon, both our readers and contributors face daily challenges to relate to and digest the potential implications of AI.

At the same time, the march of cyber threats and responses continues unabated in the world of cybersecurity professionals. While we must address the future of AI, there is no room for anyone to become complacent in assuring that all the everyday measures are completed to prevent cyber breaches.

As always, we are delighted to receive both solicited and unsolicited proposals for articles. Please remember to submit all articles on the Cyber Defense Magazine writer's kit template, which incorporates the major terms and conditions of publication. We make every effort to close out acceptance of articles by the 15th of each month for publication in the following month's edition.

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@cyberdefensemagazine.com


SPONSORS

RSAConference™2024

San Francisco | MAY 06-09 | Moscone Center

Stronger Together

See for yourself why we are **Stronger Together.**

RSA Conference 2024 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From MAY 06-09 , you'll get the chance to:

- See what the future holds in expert-led Track Sessions covering the hottest topics and emerging trends.
- Expand your knowledge and be inspired by forward-thinking Keynotes.
- Demo the latest products to find real-world solutions from over 600 companies.
- Enhance your career through valuable networking opportunities.

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

FOLLOW US

CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

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

GET YOUR FREE eBook

Get https://cionsystems.com/

DAKOTA STATE UNIVERSITY

CYBER 27 INITIATIVE

< mission_BestCyberAnywhere />

The Cyber 27 Initiative is what's next for Dakota State University. Over the next five years, we're building new labs, forming new partnerships and pushing the limits of what a STEM university can do.

It's not just what's next for DSU.
It's the next chapter for cyber everywhere.

DSUcyber27.com

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

UNKNOWN
CYBER

"70% of Malware Infections Go Undetected by Antivirus..."

Not by us. We detect the unknowns.

www.unknowncyber.com

2001  2023

ALLEGIS CYBER CAPITAL

The first dedicated cybersecurity venture firm in the world.

AN INTEGRATED GLOBAL, STAGE-AGNOSTIC CYBERSECURITY INVESTMENT PLATFORM SPANNING SEED THROUGH GROWTH.

For 20 years, AllegisCyber Capital has offered a proven investment platform that actively engages with the most promising entrepreneurs in cyber and delivers the market access, team building, and operating experience essential to their success.

BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER

Signifyd | SAFEGUARD CYBER | ELISITY | panaseer | Synack

SkyHive | cyber GRX | DRAGOS | CONCEAL | varmour

ALLEGISCYBER CAPITAL

www.allegiscyber.com


DATATRIBE
CYBER STARTUP FOUNDRY
Forging dominant companies from nation-state domain expertise
CAPITAL | RESOURCES | GUIDANCE | SUCCESS
HOME TO THE WORLD'S FASTEST GROWING CYBERSECURITY AND DATA SCIENCE COMPANIES
quickcode
DRAGOS
ENVEIL
INERTIALSENSE
PREVAILION
the cyberwire
Ntrinsec
SIXMAP
STRIDER
CONTRAFORCE
BLACKCLOAK
SightGain
JOIN THE TRIBE
DATATRIBE.COM

CYDERES

We will focus on your cybersecurity, so you can focus on your business.

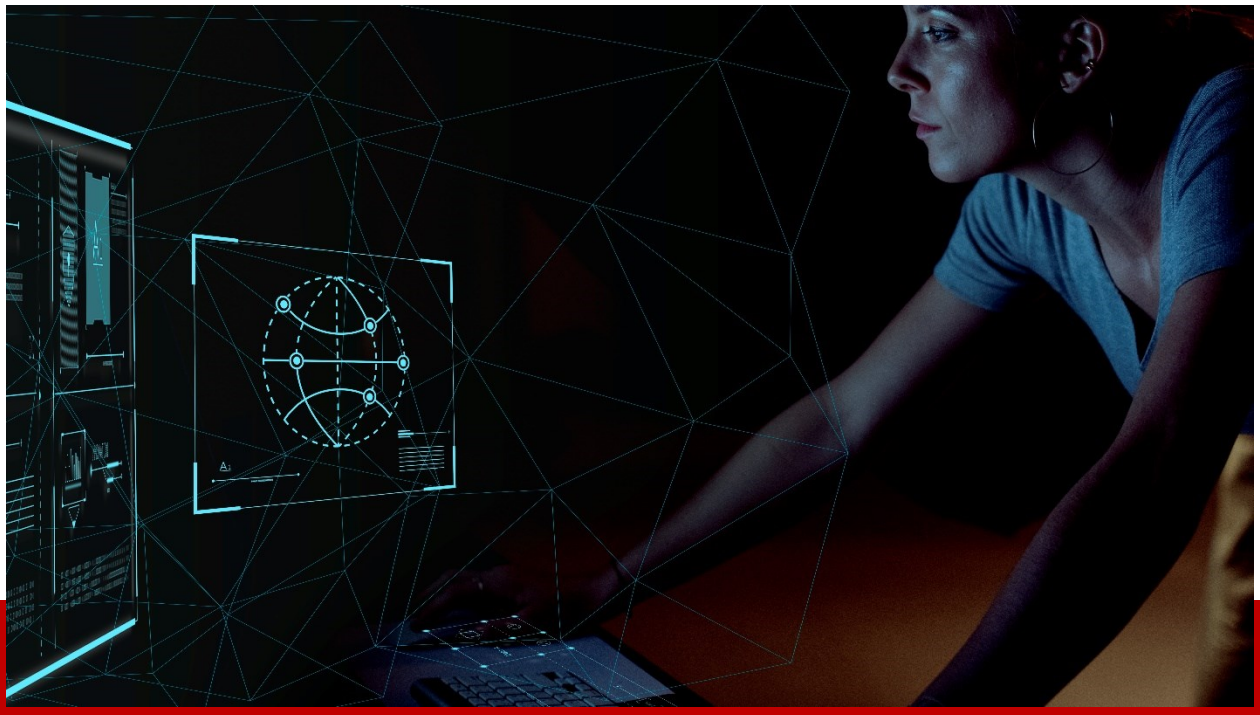
We have the right mix of people, processes, and technology to build your robust security program and respond successfully to any threat that comes your way.

Cyber **De**fense
& **Res**ponse.

It's what we do.

cyderes.com


ARTICLES



Before You Deploy Advanced Tech, Consider the Hidden Cyberthreats

By Jennifer Varner, Director Security Solutions Sales - North America, Verizon Business

Every year, emerging technologies come to market, offering new opportunities to connect with employees and customers in previously unimaginable ways. However, these advances can come at a price for businesses as they may unlock new avenues for hackers to exploit.

Staying ahead of the latest technologies is paramount for today's technology leaders, and so is protecting sensitive information by understanding the latest cybersecurity threats and countermeasures. Adoption of new technology across the enterprise can drive incredible innovation but can be fraught with unknown risks, especially in today's complex threat environment.

Cybercrime is on the rise as technology makes forays into every corner of the working world, with ransomware used in almost 24 percent of malware breaches over the past year, according to Verizon's 2022 Data Breach Investigations Report (DBIR). Our annual report examines thousands of data breaches across industries, providing a detailed analysis of current cybersecurity threats and emerging trends.

Overall, the report showed 40 percent of ransomware incidents used desktop-sharing software and 35 percent involved email. Ransomware attacks have hit companies on two fronts: causing both a loss of access to their data, as well as a need to publicly report a data breach – given the actors have also taken a copy of the organization's data. Notably, ransomware attacks are four times more likely to come from external threats than from inside the company, and four out of every five breaches are attributed to organized crime.

Despite this fertile ground for bad actors to exploit these new technologies, the need for innovation never stops. To help avoid costly and potentially devastating problems down the road, here are several newer technologies that IT decision-makers need to understand and the ways they can bolster their organizations safety measures.

Improving security of 5G devices

When it comes to network deployment, the arrival of 5G wireless technologies marks a new era of network connectivity and ushers in what many are calling the Fourth Industrial Revolution. The transition from 3G and 4G to 5G is already providing dramatic increases in both bandwidth and upload and download speeds, together with extraordinary decreases in latency.

But 5G-enabled applications and business processes may pose security risks if they are deployed without appropriate security scrutiny and oversight. For example, a poorly secured database or misconfigured application remains a risk even if the connection to it is significantly faster.

Businesses eager to implement 5G-enabled technologies like Internet of Things (IoT) or autonomous network-connected devices to improve the customer experience or increase operational efficiency should consider if the firmware of these devices can be exploited.

Unpatched device firmware is a common weak point that could lead to network incursions by cybercriminals. If your security program lacks a robust process to review and approve new technologies or devices before they are connected to the network, expect blind spots. Don't let your company's "attack surface" go unchecked in a rush to take advantage of 5G. And don't let innovation outpace security oversight.

Remember to lock down the blockchain

Blockchain is a distributed database or public ledger used to record digital transactions, which are linked and secured using cryptography. It's ideal for many security applications, including managing digital identities, protecting the configuration of key IT systems and ensuring secure supply chains.

While the transactions cannot be altered retroactively, having confidence that the machines that power and protect your business are configured correctly is a necessity. Unauthorized and undetected changes to settings in any number of blockchain systems can lead to data theft, fraud

and unsanctioned wire transfers – and to greater exposure to email-based malware, viruses and phishing campaigns.

A new approach to a key element of blockchain cybersecurity is called machine state integrity, or MSI. This technique captures concise “state” information and continuously monitors machines in an organization’s environment to accurately identify, analyze and flag changes to those systems.

Blockchain-inspired security solutions can have a significant positive impact on an organization’s security posture, but the technology itself has a reputation for being complex and abstract. When a security vendor proposes a solution based on blockchain, it’s a good idea to focus on the measurable, practical security benefits and results of the solution. Don't get caught up in the details behind the tool.

Smarter security for AI and ML applications

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly becoming the driving force behind several new advanced cybersecurity tools that Chief Information Security Officers (CISOs) and their teams may be advocating to adopt. For example, ML automates many facets of threat hunting, a critical but time-consuming security activity designed to find bad actors who have compromised corporate IT systems.

Traditional threat hunting, conducted by humans, can often result in a large number of false positives. This “noise” distracts from focusing on the real, hidden threats. ML-driven threat hunting systems may reduce time to detection from 200-plus days on average to just a few hours. And the faster a hacker can be found, the less damage they can inflict. AI-driven security solutions can enable organizations to accelerate and, in many cases, automate their response to cyber incidents.

Embrace the future with modern security

No matter what advanced technology your organization is looking to deploy, you can’t embrace the future if your security architecture is stuck in the past. These innovative technologies are transforming organizations, helping them to increase a range of key performance indicators.

To be successful with any new technology, it’s essential that organizations understand the risks and the company’s posture so that the correct cybersecurity measures can be implemented. It’s been long said that an ounce of prevention is worth a pound of cure, and that’s especially true for organizations seeking to deploy advanced new technologies in today’s sophisticated threat environment.

About the Author

Jennifer Varner is the Director Security Solutions Sales - North America at Verizon Business. She leads Verizon's Security Sales Organization for Global Enterprise and Mid-Market in the Americas and is focused on helping customers improve security postures and reduce risk through the power of Verizon's secure network portfolio which includes Network-as-a-Service and Private 5G technologies, Integrated and Managed Security Solutions, and a best-in-class Cybersecurity Consulting practice. Jennifer can be reached online at https://www.linkedin.com/in/jennifer-varner/ and at www.verizon.com/business.

Healthcare Under Siege

The Critical Threat of Cloud and IoMT Vulnerabilities

By Ty Greenhalgh, Industry Principal, Healthcare, Claroty

The healthcare sector is grappling with a perfect storm of challenges: economic uncertainty, staff shortages, COVID-related backlogs, and scarce public funding. Now, cyberattacks are escalating the crisis, with threats to both finances and patient care.

Cyberattacks targeting healthcare organisations surged by 45% last year, while the average cost of a breach rose by over 40% since 2020. With 2023 predictions pointing to healthcare as a prime target for cybercriminals, the stakes have never been higher.

The rapid expansion of the digital landscape, particularly the Internet of Medical Things (IoMT), leaves healthcare networks vulnerable. Devices like remote monitoring systems and digital insulin pumps can unwittingly provide entry points for attackers.

Worse still, interconnected medical systems risk widespread disruption when breached, affecting vital services and patient care. Ransomware attacks such as those on Medstar Washington Hospital and André-Mignot teaching hospital in Paris highlight this grave reality.

As Dr. Christian Dameff, Medical Director of Cybersecurity at UC San Diego Health, aptly puts it, "we are at a point where bits and bytes are meeting flesh and blood." Now, more than ever, it's crucial for security teams to secure healthcare's digital landscape, protecting both the industry and the patients it serves.

The growing risk of vulnerabilities in cyber-physical systems

The convergence of cyber-physical systems and IoMT devices is transforming healthcare services in a positive direction, by enabling real-time monitoring and analysis of patient data, and creating more effective opportunities for personalised treatments. Such technologies are also enhancing healthcare efficiency by automating processes, reducing human error, and facilitating remote healthcare services. All of these factors are significantly improving healthcare accessibility and cost-effectiveness.

At the same time however, this convergence is also creating a ticking time bomb of security risks. As medical systems become highly integrated into the cloud and remote servers, there is a growing risk of potential cyberattacks disrupting critical patient care facilities. The fallout from potential incidents like ransomware can lead to devastating consequences, including delayed treatments, misdiagnoses, and even loss of life. Patients, already facing the physical and emotional toll of their medical conditions, now find themselves as unwitting pawns in a high-stakes game of digital warfare.

So what's leading to these increased vulnerabilities in healthcare systems? One of the major reasons is the use of outdated operating systems and devices, many of which are no longer supported by vendors with essential security updates. For example, numerous NHS GPs in the UK continue to rely on a decade-old version of Windows OS, leaving them exposed to unpatched vulnerabilities that can be exploited by malicious actors.

Adding fuel to the fire, many healthcare institutions still depend on legacy medical devices that cannot support the latest software updates or security features. These vulnerabilities are compounded by the fact that IoMT devices often aren't developed with proactive security in mind. Weak default passwords, lack of encryption, and an absence of two-factor authentication are just a few examples of where IoMT are failing. Such failings leave the door wide open for attackers to access healthcare networks, compromise patient data, and hinder physicians' abilities to provide care.

Moreover, there's a glaring deficiency in the regulatory landscape, with insufficient focus on cybersecurity. While the MHRA is responsible for conducting conformity assessments of medical devices, their primary concern is operational feasibility rather than cybersecurity exposure. This means manufacturers may not be testing devices for vulnerabilities in line with current standards.

Vulnerability disclosures are significantly increasing

Security has continued to be a significant challenge across the Extended Internet of Things (XIoT). This umbrella term encompasses all connected devices, from consumer gadgets to industrial and medical control systems. Recent research by Claroty discovered a 6% rise in vulnerabilities affecting XIoT devices from 2021 to 2022.

More importantly, we have seen over 150 IoMT vulnerabilities disclosed in the past two years, demonstrating that medical networks are increasingly becoming an important part of vulnerability assessment practices.

All of these factors point toward the fact that there is a growing awareness of XIoT security issues. Device manufacturers, end users, and the security industry are focusing more on finding these vulnerabilities and closing them before they can be exploited.

The most positive takeaway is that vendor disclosure rates have increased unprecedentedly since 2020. For the first time in our research, the number of vendor self-disclosures of XIoT vulnerabilities has

surpassed those of third-party security companies' research teams and independent researchers. This is a very positive indication that vendors are becoming more vigilant with their security assessment efforts, investing more effectively in cyber-physical systems security, and improving their product-security programs altogether.

If vendors continue to maintain such acute vigilance going forward, security teams will be in a much better place to address and patch healthcare vulnerabilities before they are exploited by threat actors.

Nevertheless, despite this increasing rate of disclosures, it's important to remember that vulnerable devices are still pervasive. Physicality is the biggest issue when managing and securing these devices. Healthcare organisations can quickly lose track of their IoT assets, particularly in sensors where a very high volume of devices will be distributed across a site.

Additionally, many connected devices still have design issues that make them more prone to vulnerabilities and more challenging to manage. For example, a device might have a complex user interface, making it more likely to be misconfigured and poorly secured. In other cases, a device might need to be physically opened up for patches and maintenance – a big problem when there are hundreds of units to manage.

Even for organisations making a concerted effort to keep their XIoT estate secure, it's very easy to miss a few devices. A single vulnerability is often all it takes to enable a breach.

Applying proactive security to healthcare

While the number of vulnerability discoveries has increased, the threat is being taken more seriously. Governmental bodies, including the UK and EU, are working on laws to regulate XIoT security more closely, pushing for more secure designs and faster action in addressing vulnerabilities.

As the industry continues to develop, we should naturally see a greater focus on security from XIoT device vendors, particularly in high-risk areas like healthcare. Developers and manufacturers are responsible for ensuring their products can be easily managed and supplied with regular updates.

From the manufacturers, there needs to be a greater emphasis on following standard cybersecurity practices laid out by key regulatory bodies. Standards such as the IMDRF (International Medical Device Regulators Forum) guidance provides foundational security principles and best practices for ensuring the cybersecurity of medical devices throughout their total product life cycle (TPLC). Healthcare organisations should also ensure they're only acquiring products and systems that meet these regulatory principles.

In the meantime, organisations implementing any XIoT into their operations must do their due diligence. This means taking the time to fully evaluate products and ensure they address security basics such as vulnerability patching.

For existing XIoT implementations, critical infrastructure organisations must ensure complete visibility of every device connected to their network, from the smallest vital sensor to the biggest MRI machine or Industrial Control System (ICS). Automated asset discovery tools can help to identify connections and make this task more manageable. With all devices identified, it is then crucial to implement a regular cadence for applying security updates.

Healthcare organisations should also consider implementing network hygiene measures that limit the possibility of a connected device being discovered and exploited. Among the various options available, network segmentation is highly effective and our research revealed it to be the most successful security approach in addressing critical vulnerabilities. Essentially, this involves dividing the network into virtual zones, making it challenging for attackers to penetrate the main network from a vulnerable XIoT device.

Given the ruthless nature of cybercriminals who are willing to endanger people's lives for financial gain, the healthcare sector must prioritize the security of their XIoT estate, as connected devices often offer an easy path for attacks and a means of causing major disruption.

About the Author

Ty Greenhalgh has been dedicated to the Healthcare Information Technology and Information Management industry for over 30 years. He is an ISC2 certified Healthcare Information Security and Privacy Practitioner (HCISPP) and Cybersecurity Officer. His experience has leveraged advanced disruptive technology solutions to assist healthcare organizations in overcoming seemingly insurmountable challenges. Ty is an active member in several groups and associations; Healthcare and Public Health Sector Coordinating Counsel's Joint Cybersecurity Workgroup, the National Initiative for Cybersecurity Education (NICE) Workforce Development Workgroup, the North Carolina Health Information and Communications Alliance (NCHICA) Biomedical Taskforce.

Company website: https://claroty.com/

The Role of AI in Cybersecurity

By Alysia Silberg, CEO, Street Global

As technology increasingly connects us, people, businesses, and governments are more concerned with Cybersecurity than ever before.

The development of Artificial Intelligence (AI) provides a unique opportunity for combatting digital threats. But it also creates new challenges. Therefore, it's essential to examine how AI intersects with Cybersecurity now and in the future.

AI is a computer science branch that focuses on building machines capable of performing tasks that typically require human intelligence. On the other hand, Cybersecurity aims to protect digital systems from attacks.

These related fields bring valuable insights to each other: AI can help detect cyber threats more quickly and efficiently, while Cybersecurity can train AI software using real-world data. Currently, AI is already being used in various ways in Cybersecurity. Some examples include automating threat detection and response systems or predicting network breaches based on historical patterns. This has resulted in more robust security infrastructures that flexibly respond to ever-changing threats.

However, integrating AI into existing security frameworks presents challenges, such as unpredictable false positives or overreliance on old data when dealing with new types of attacks.

Additionally, adversaries may use adversarial AI to circumvent digital defenses by spotting weaknesses an algorithm hasn't been trained against. Despite these existing challenges, there's still enormous potential for enhancing current cybersecurity standards through advances in AI research and development. For instance, future technologies might improve predictive capabilities or anomaly detection, so fewer attacks slip under the radar unnoticed.

An important consideration regarding artificial intelligence (AI) involves its use in Cybersecurity ethically. As technology advancements occur, so does the possibility of unethical practices by malevolent actors manipulating the system towards destructive purposes, which erode trust levels while breaching privacy boundaries.

Thus, establishing clear ethical principles for utilizing AI on cybersecurity matters helps preserve digital assets while elevating a company's reputation among consumers.

In addition to this step lies implementing government-enforced laws against using said technology wrongfully which goes a long way toward discouraging individuals or groups from attempting anything similar effectively.

Moreover, investing sufficiently in high-quality, diversified data sources remains vital, as accuracy relies directly on quality.

Furthermore, ensuring rigorous data audit protocols helps avoid biased or flawed systems altogether caused by inferior quality material.

The entire process guarantees more dependable results when combating evolving cyber threats with superior resiliency where necessary - always making adaptive responses contextually appropriate.

In summary, Artificial Intelligence's incorporation into Cybersecurity brings both hurdles and prospects that require careful assessment to enhance security measures without compromising other factors such as privacy or ethics.

Although introducing AI poses an opportunity for more robust digital defense mechanisms than before -- thanks to greater adaptability and efficiency -- adopting such systems requires utmost caution in navigating potential risks such as adversarial AI or ethical dilemmas. As a result of these ever-changing landscapes, implementation strategies require constant analysis for optimal results. Continually adapting to evolving scenarios is essential to attesting precisely during this digital age's evolution phase. Needless to say, continuous learning is the key to moving forward, empowering employees and equipping them with the tools they need to exploit the potential of AI securely while amplifying their productivity. Furthering cyber-safety efforts is paramount in better protecting people from attacks by hackers aided by innovations therein.

In conclusion, AI is a tool that amplifies, not replaces, human abilities - which remains at the crux of cybersecurity initiatives.

About the Author

Alysia Silberg, CEO and General Partner of the investment firm Street Global. Here are some additional information:

Alysia Silberg is a cross between a survivalist and an industrialist – someone who has had to innovate and use whatever resources are available because they had to, and someone who sees opportunities in the marketplace and capitalizes on those.

A math and science prodigy, she nurtured her entrepreneurial instincts while still in grade school, starting her first business, an import-export agency, at age 11. Alysia also grew up in poverty in South Africa where she experienced violence, abuse, and even a gunshot wound.

Today, Alysia is a leading venture capitalist in Silicon Valley, where she mentors tech startups and helps them go public. She is CEO & General Partner of the investment firm Street Global.

Alysia can be reached on Twitter and Instagram via @AlysiaSilberg, on LinkedIn here, and at her website https://www.readunemployable.com/.

The Best of Both Worlds Made Possible with A Hybrid SOC

By Chase Richardson, Principal Lead Consultant, Bridewell

The revolving door of cyber-attacks on major organizations continues to turn. Among the most significant of breaches over the last year was a ransomware attack on the Los Angeles Unified School District in September. Accounting for over 1,000 schools and approximately 600,000 enrolled students, hackers from the Russian-speaking ransomware gang Vice Society stole 500 gigabytes of personal data and demanded a ransom for its return. When the district refused to negotiate, thousands of social security numbers, student assessment records, driver's license numbers, positive Covid test results, and legal records were leaked online.

Furthermore, it later came to light that student psychological evaluations had also been published in their hundreds on the dark web, containing intimate details about medications, diagnoses, incidents of abuse, and past traumas. With the Los Angeles Unified School District coming under renewed fire for failing to acknowledge the existence of these records, this incident highlights a crucial gap in existing federal privacy laws – and the critical need for transparency at all levels of cybersecurity.

With extremely sensitive data at play, organizations can't stand still in the fight against evolving risks. As the nerve center for defenses against cyber dangers, security operations centers (SOCs) are essential to modern cybersecurity strategy. With 24/7 surveillance and responsiveness, shaped and supported by human expertise, a SOC helps to proactively hunt for risks, monitor and respond to real-time security incidents, and reduce the time taken to detect and respond to an attack.

Today, traditional security monitoring and notification approaches to threat prevention are not sufficient. Threat detection and response capabilities are needed drastically minimize the impact of cyber-attacks and ensure organizations are better prepared to deal with future security threats. The SOC is the engine that allows this to happen.

Searching for the right SOC model

There are a number of available SOC models, so it can be a little overwhelming at first. Many organizations are likely to be drawn towards in-house management for full control over their operations. An in-house SOC can also be customized to meet very specific needs and requirements, enabling the organization to tailor policies, procedures, and security controls to their unique risk profile.

However, several issues arise from a fully in-house approach. For example, as IT estates spread and perimeters expand, so does the number of tools needed to cover the cloud and all possible vulnerabilities. Each of these tools must be expertly configured, supported, and monitored 24/7, to the highest standards. To add to the challenge, many organizations currently have tools that are poorly integrated, or have overlaps or dangerous gaps in coverage that could leave them exposed.

Then there is the issue of cybersecurity skills shortages – a problem that continues to plague the industry across the country. Of those that do make up the workforce, it's estimated that 62% of professionals in the U.S. have less than four years of experience. Stretched teams therefore have little time to deal with the numerous alerts that come in, with almost no opportunity to respond, let alone monitor in the first place. A large quantity of false positives may also create excessive noise that needs to be sifted through and will lead to inaccurate reporting.

At the other end of the scale is a fully outsourced service. On the surface, this seems to be the obvious alternative and provides access to much-needed external expertise. A managed security services provider (MSSP) will typically provide an end-to-end threat detection and response service, helping in-house IT teams to understand potential risks. They usually have a wider range of threat intelligence platforms to inform detection capabilities and can access open-source intelligence from across the web. A fully outsourced SOC can also be easily scaled up or down based on the organization's changing needs and budgets.

However, the main downside to a comprehensive outsourcing strategy is that MSSPs often lack a full understanding of the environment and context of the business. This can lead to communication challenges with the organization's internal IT teams, which then makes it difficult

to mount a coordinated response to security incidents. Remoteness from an organization's operations can also result in difficulties integrating with their existing IT infrastructure, causing delays, false alarms, additional costs, or even friction and indifference.

The hype around hybrid

To find that perfect middle ground, a hybrid SOC model can bring out the advantages posed by in-house and outsourced variants, while eradicating the drawbacks. The hybrid SOC makes the most of the knowledge and skills of professionals already within the business alongside the expertise of the MSSP. A key focus is on collaboration between the two teams and how improvements can be made. It might be that the MSSP takes responsibility for threat intelligence, security engineering or managed architecture. However, flexibility is important to adapt to changing business needs.

There are many examples of successful hybrid SOC models. Manchester Airport Group (MAG), the largest UK-owned airport operator, launched a hybrid SOC pilot scheme in partnership with Microsoft in 2021, in order to improve its visibility and protection against ever-evolving cyber threats targeting the aviation sector. This approach increased real-time monitoring on devices and servers from 5,000 to 80,000 events per second, supporting faster, more comprehensive, and accurate threat detection and response. By leveraging a hybrid model to safely transition from an outsourced to in-house SOC setup, MAG was provided with the confidence and expertise to fully upskill team members, resulting in significant cost savings on training and a greatly enhanced security posture.

Crucially, a hybrid SOC gives a business autonomy over its cyber threat response while still allowing staff to drive projects and internal improvements. An MSSP in this setup can take the lead on the high value incidents, but also develop the skills of in-house personnel where capabilities are lacking. Security orchestration, automation and response (SOAR) tools can be better utilized for investigation and action. Developers are also able to build custom API-based integrations to enable even greater efficiencies beyond SOAR setups.

However, regardless of the nature of the SOC they opt for, every organization should be prioritizing ongoing education and training for SOC personnel. Effective threat detection and response relies on security teams being knowledgeable, up-to-date, and coordinated at all times, working together seamlessly to investigate and tackle an ever-widening range of security incidents. To ensure a collaborative and agile response to threats, organizations must provide regular, multilayered cybersecurity education to all SOC personnel, complete with hands-on opportunities to practice their skills in real-world situations. This training will ensure that SOC teams keep pace with the latest threats and technologies, so that they can be relied on to protect their organization's assets 24/7.

Flexibility under a combined approach

Ransomware and other growing threat vectors are understandably causing concern among organizations. A SOC model is necessary to defend against increasingly sophisticated cyber-attacks, but the type deployed can prove to be the difference between success and failure. Rather than go all in on outsourced or in-house variants, a hybrid model eradicates recruitment headaches, provides relevant expertise, and keeps the business up-to-speed on the latest trends and threats. By incorporating this, organizations can drive much-needed improvements in their cybersecurity posture – and ultimately, ensure their security operations are maximizing the benefits of both worlds.

About the Author

Chase Richardson is a Principal Lead Consultant at Bridewell. Chase lives in Houston, TX where he leads US Operations at Bridewell, a global Cybersecurity consulting firm. He joined Bridewell last year to open its first US office. Prior to Bridewell, Chase was a founding member of another Cybersecurity consulting firm in Houston where he helped grow the business from 5 to 50 employees over 4 years, specializing in Cybersecurity Risk, Governance, and Compliance, Offensive Penetration Testing, Security Operations and Data Privacy. Chase has an MBA from Emory University and is a Certified Information Systems Security Professional (CISSP) and Certified Information Privacy Professional (CIPP/US).

Chase can be reached online at LinkedIn and at our company website https://www.bridewell.com/us.

AI In Cybersecurity – Risks and Rewards

By Aimei Wei, Co-Founder and CTO, Stellar Cyber

The global cybersecurity workforce grew to a record 4.7 million people in 2022, according to an (ISC)2 2022 workforce study, but the same study found that the sector still needs 3.4 million more security professionals – an increase of over 26% from 2021's numbers. This workforce shortage, combined with the ever-rising frequency and complexity of cyberattacks, means that organizations face greater risks than ever before.

Since AI is the hottest labor-saving technology in at least a generation, it makes sense to look at its ability to reduce manual efforts with cybersecurity detection and response platforms while improving detection accuracy. What are the benefits? What are the potential risks?

The Good News about AI

Cybersecurity detection and response is a heavily data-intensive process. Generally speaking, AI should be able to help organizations improve their security postures by detecting and responding to threats more quickly and accurately than with traditional methods, because it can analyze more data more quickly than humans can. Moreover, an AI-driven cybersecurity platform can report detections as context-based incidents with specific pointers about how to address them, making it much easier and faster to investigate and remediate attacks. With the latest development in LLM, an AI-driven cybersecurity platform can potentially allow users to interact with the platform using natural language. This greatly eases the cybersecurity analyst shortage by enabling the use of lower-skilled security analysts who may be more readily available as well as less expensive.

Here are some specific advantages to using an AI-driven cybersecurity platform:

Improved Detection and Response – AI-based cybersecurity platforms can quickly analyze massive amounts of data, enabling faster detection of threats and more timely responses to them. Machine learning (ML) algorithms can learn from past attacks and detect anomalies in real time, reducing hacker dwell time in a network and thereby reducing the chances of a successful attack.

Automated Threat Detection and Prevention – AI-powered cybersecurity platforms can automate threat detection and response, allowing security teams to focus on more complex tasks. For example, AI can detect and respond to commodity attacks such as phishing emails, malware, and others automatically, leaving analysts relatively free to dive into more complex human operated attacks.

Advanced User and Entity Behavior Analytics (UEBA) – AI can analyze user behavior patterns and detect anomalous behavior that could indicate a threat. UEBA uses ML algorithms to detect and respond to suspicious user activity in real time, using a baseline understanding of what constitutes normal user behavior.

Easy to use/access – Recent advancement in the LLM can be leveraged to present the security product in a much more user-friendly way, making it easier for people to get their questions answered, actions carried out using natural language.

Predictive Analytics – Predictive analytics can help organizations prepare for future threats and develop proactive cybersecurity strategies. AI can identify patterns and trends in cyber threats, enabling organizations to predict and prevent future attacks.

AI Risks

However, the use of AI in cybersecurity platforms also presents its own set of challenges and risks.

Lack of Understanding – Many organizations lack an understanding of how AI works, which can make it difficult to implement effectively. Organizations must invest in the necessary education and training to understand how AI can be used to improve their security postures.

Lack of Trust – A related issue is reluctance to trust the results of AI-based detections, which, if severe enough, can limit or even eliminate any benefit from using the technology. Risk managers can improve their trust in AI by thoroughly understanding how AI arrives at its conclusions, and by ensuring that any baseline profiling for AI or ML is done with the organization's own data.

Complacency – In contrast to lack of trust, AI-powered cybersecurity platforms may generate a false sense of security that leads to complacency. Organizations should periodically cross-check AI-generated results to ensure that they're accurate.

Bias – An AI engine is only as good as the data used to train it. If the data used to train AI models is biased or incomplete, it can lead to inaccurate threat detection and response. Organizations must be aware of potential ethical issues surrounding the use of AI in cybersecurity and take steps to address bias and fairness in AI models.

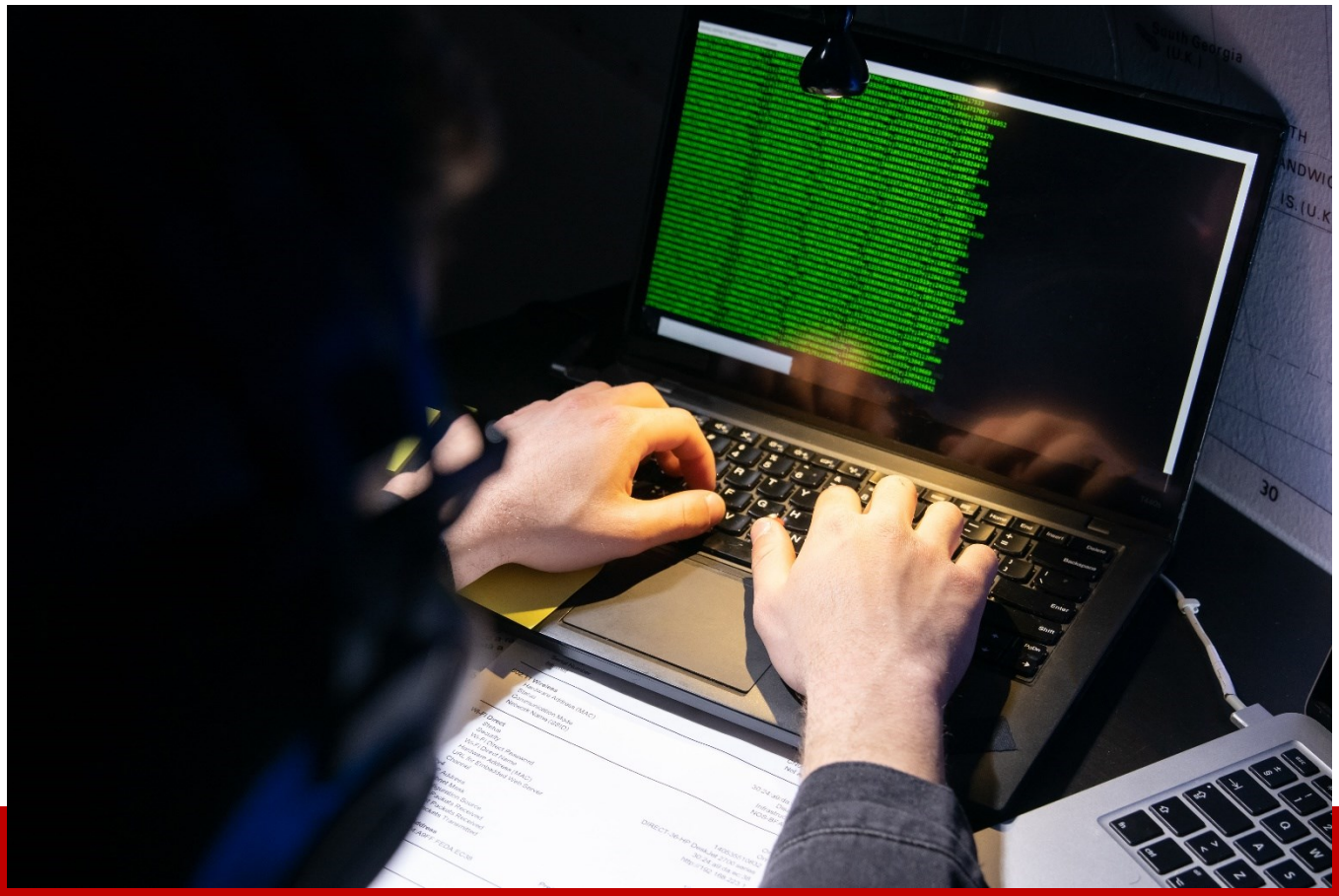
Cybersecurity Threats to AI Systems – AI systems can themselves be vulnerable to cyberattacks, and attackers may attempt to exploit vulnerabilities in AI models to evade detection. Given the potential for heightened attack damage, organizations must take steps to secure their AI systems.

AI has the potential to revolutionize the cybersecurity industry by improving threat detection and response, automating security operations, and enabling predictive analytics. However, organizations must be aware of the challenges and risks associated with using AI in cybersecurity platforms, too little or too much trust and potential bias. Despite these challenges, the benefits of using AI in cybersecurity are significant, and organizations that invest in AI-based cybersecurity platforms can improve their security postures, reduce the risk of successful cyberattacks, and save on analyst personnel costs.

About the Author

Aimei Wei has over 20 years of experience building successful products and leading teams in data networking and telecommunications. She has extensive working experience for early-stage startups (including Nuera, SS8 Networks and Kineto Wireless) and well-established companies like Nortel, Ciena and Cisco. Prior to founding Stellar Cyber, she was actively developing Software Defined Networks solutions at Cisco. Aimei enjoys building a product from its initial design to its final launch. Aimei has an M.S. in Computer Science from the Queen's University in Kingston, Canada and an Undergraduate degree in Computer Science from the Tsinghua University of China.

Aimei can be reached online at awei@stellarcyber.ai and at our company website https://stellarcyber.ai.



Cyber: Dealing with a Data Breach

Data breaches are one of the most significant cyber threats organizations face, but when they occur, many businesses do not respond in a manner that reassures their clients or the regulators. What can companies do to ensure their response is robust in the crucial aftermath of an incident?

By Rishi Baviskar, Global Head of Cyber Risk Consulting at Allianz Global Corporate & Specialty (AGCS) and Michael Daum, Global Head of Cyber Claims at AGCS

Following a cyber breach, there is a critical moment – perhaps only a few minutes or maybe an hour or two at most – when the decisions made will significantly influence the outcome. For this to be minimally damaging, there needs to be a thorough understanding of what is likely to happen and what is at stake.

A company must be meticulously prepared for a serious breach, with a cyber incident response organization and plan in place. This includes exercising critical scenarios in advance and having a trained team who clearly understand their roles and responsibilities.

Plans are important, but exercises are critical because even the best plans cannot replace a well-prepared team. Plans must be practiced to ascertain their effectiveness in a real-life incident.

The growing number of cyber incidents remains the most significant concern of companies for a second year in succession, according to the annual **Allianz Risk Barometer**. In the 2023 report, 34% of the responses from more than 2,700 experts around the world ranked cyber incidents as the greatest risk their companies face. In particular, we are seeing increasing cases of data breaches, either with ransomware attacks or stand-alone.

According to **Allianz Risk Barometer** respondents, a data breach is the exposure that concerns companies the most (53%). Data privacy and protection is a critical risk that is intensifying – IBM's The Cost of a Data Breach Report states the average cost from such incidents reached an all-time high in 2022 of $4.35mn and is expected to surpass $5mn in 2023.

Regulatory pressure ramps up

Regulators are getting tougher on companies with insufficient security measures to protect data. In 2019, British Airways received a £183mn ($222mn) fine from the UK's Information Commissioner's office (ICO) after data on 500,000 passengers were stolen. The fine was reduced in 2020 to £20mn on appeal.

Last year, two cases in the US sent a warning to directors and senior executives who fail to deal adequately with cyber breaches. In October, a former chief security officer of a mobility firm was found guilty of trying to cover up a cyber security incident. This is believed to be the first time a US company executive has been criminally prosecuted over a cyber breach. The executive faced a prison sentence of up to eight years for obstruction of justice and deliberate concealment of a felony.

Also in October, the Federal Trade Commission (FTC) announced action against the CEO of an online drink delivery business over security failures that led to a cyber breach exposing personal information on 2.5mn customers.

With regulators and prosecutors becoming more stringent, large companies are boosting investments in cyber security. Enhanced security is forcing hackers to seek victims in smaller and mid-sized companies, where weaker controls can make them easy targets.

When the unthinkable happens

Once a personal data breach occurs, the clock starts ticking. Under the European General Data Protection Regulation (GDPR), companies must report a breach within 72 hours of becoming aware of it. The ICO imposes the same timeframe in the UK.

In the US, it has been less clearcut with a patchwork of jurisdictions meaning, in some cases, data breaches could be reported within 60 days. However, last year President Biden signed new

federal data-breach reporting legislation. This could tighten the notice to report such incidents to the Department of Homeland Security to within 72 hours after one occurs.

The US FTC advises on the critical steps companies should take after discovering a data breach, as does the UK ICO. The EU provides guidelines for who needs to be notified and when, including other affected companies and individuals.

Mobilize the breach response team

However, within these steps, a flurry of complex actions must be taken. The most critical is to mobilize the cyber incident response plan. A cyber crisis is one of the toughest incidents to deal with. It is not like a natural disaster or when a factory burns down. If you are hit by an encryption and ransomware attack, you can suffer a business interruption that is global. Also, you are dealing with criminals and their specific behavior is hard to predict.

The application of double extortion has become widespread, which expands the dimensions of complexity further. Double extortion combines the encryption of data, systems, or back-ups with the threat to release sensitive data.

One of the most important things a company should do is secure expert assistance – both after and before a cyber attack.

It is increasingly difficult for companies to have the expertise necessary to handle a cyber crisis in-house. The shifting nature of the crime creates a dynamic threat environment that can be difficult to stay on top of. While many large and mid-sized companies are often well prepared for traditional risk scenarios, some have never properly thought through a cyber crisis management plan.

A significant breach would mean a company will want to call on their cyber security cover, so insurance contacts should be looped in as soon as possible. External experts can then provide specialist advice depending on the nature of the incident. AGCS has a global network of partners that offer assistance to insureds when a cyber incident occurs. These include incident response services such as IT forensic services, forensic accounting, public relations, crisis communications, response advice on cyber extortion, and breach coach or legal services. A breach coach is typically an attorney who specializes in data privacy and cyber security. Often companies are overwhelmed by the situation, and a breach coach can help steer them through the crisis in a structured manner to limit damage.

Clear communication is key

Each cyber attack is unique. One essential component a response team must oversee is a comprehensive communications plan that reaches all affected audiences – employees, customers, investors, business partners, and other stakeholders. Such a plan needs to anticipate questions people will ask.

Mishandling communications around a breach can contribute significantly to the reputational fallout around an incident, including a plummeting share price.

Norsk Hydro, one of the world's largest aluminum producers, suffered a cyber attack in March 2019 after ransomware encrypted files stored on all systems. Hackers demanded bitcoins to unlock the data. Yet, despite the severity of the breach, the share price of Norsk Hydro rose in the following weeks as the company battled to rectify the damage.

Norsk Hydro refused to pay. What was appreciated by the market was the transparency and openness of the company because it contrasted starkly with the secretive responses of many companies after being hacked. Trust was maintained, and the share price increased in response to the incident.

Crisis communications checklist

As well as your legal reporting requirements, timely and transparent communication with stakeholders after a breach is essential if you want to limit damage to your business activities and reputation.

A crisis communications plan should be part of your cyber incident response plan, comprising a list of contacts, urgent tasks and appointed people to oversee them – including a senior communications spokesperson – with pre-prepared statements drafted (and tested) for several scenarios.

Here's a checklist of what to consider when compiling a cyber crisis communications plan:

Who do you need to inform? As well as relevant authorities, this could be your customers, shareholders, employees, external contacts, the public, media, your lawyers, professional organization, insurer. Establish various communications streams to help steer target groups towards regular updates.

What is the purpose of the communication? It could be to provide reassurance, information on remedial measures, an apology, or a statement to pre-empt inaccurate coverage elsewhere.

How can you allay customers' fears? Show victims of the breach empathy and a readiness to offer solutions. When you are able to, communicate mitigation steps you are taking and keep customers informed. Give them guidelines on how they would have been accessed by the breach and what action they can take to protect themselves, such as password changes or checking emails for malware.

How can you reassure employees? Communicate quickly on multiple channels to put their minds at rest and arm them with the actionable information they need. Keep them updated. Similarly, provide any details that might be needed by your suppliers, consultants, investors, and staff representatives or unions.

How should you communicate with business partners? Time is of the essence to allow them to take action to protect themselves. This could involve regular calls and updates so partners can ask questions or delve into details. Consider dedicating named staff to critical business partners to ensure they are kept fully informed.

What are the best platforms or channels? Consider the regional, national or international press, trade journals/websites, email, social media, printed letters, webcasts.

Who should the communication come from? It could be the CEO, the chief information officer, chairman, head of IT, or customer services director.

What kind of language should you use? Keep the tone of your notifications friendly, non-alarmist and factual; decide how many languages you need to communicate in.

What will you do if your digital channels are unavailable? Consider keeping pre-prepared materials in cloud-based back-ups or even hard copies of statements.

About the Author

Michael Daum is Global Head of Cyber Claims at Allianz Global Corporate & Specialty (AGCS). Based in Munich, he was previously Deputy Practice Leader and Senior Underwriter for Cyber at AGCS.

Rishi Baviskar is Global Cyber Experts Leader, Risk Consulting at Allianz Global Corporate & Specialty. Baviskar has experience working within the IT field for large oil, gas, automotive and pharmaceutical companies. In his previous roles, he has worked across all levels of process development, ranging from onsite engineer to the design and implementation of cyber security policies.

Rishi and Michael can be reached online at Rishi.Baviskar@agcs.allianz.com and Michael.Daumand@agcs.allianz.com and at our company website www.agcs.allianz.com.

From AI-driven Defense to Dark Web Threat Intelligence

How RSA Conference's Cybersecurity Innovators are Advancing Defense-in-Depth

By Annabelle Klosterman, Cybersecurity Reporter, Cyber Defense Magazine

The world of cybersecurity is constantly evolving, with new threats emerging every day and innovative solutions emerging to combat them. At the recent RSA Conference, a gathering of leading experts and companies in the field, I had the pleasure of interviewing over 25 cybersecurity organizations. They showcased their groundbreaking approaches to defend against cyberattacks. From AI-driven defense mechanisms to harnessing dark web threat intelligence, these innovators are spearheading advancements in the realm of defense-in-depth.

In this article, I'll delve into the highlights from 15 of these conversations, exploring how these cybersecurity companies are revolutionizing the industry and paving the way for a more secure digital landscape. Throughout this, I had the goal of uncovering the cutting-edge technologies and strategies from some of the innovators at the RSA Conference, shedding light on the future of cybersecurity defense.

AI-Powered Defense for the Digital Battlefield - DarkTrace, Justin Fier

DarkTrace, a prominent player in the cybersecurity landscape, takes the top spot in our exploration of RSA Conference's cybersecurity innovators. With their AI-driven defense mechanisms, DarkTrace has revolutionized the way organizations combat cyber threats. Leveraging machine learning and advanced analytics, DarkTrace's technology enables in-progress cyber-attack interruption within seconds, addressing a wide range of threats, including ransomware, email phishing, and attacks on cloud environments and critical infrastructure. Their focus on anomaly detection and the human element sets them apart in the industry, emphasizing the need to detect the unknown and fortify cybersecurity postures.

Quantifying Cyber Risk: Utilizing a Cybersecurity Optimization Platform - CYE, Ira Winkler

In the realm of cybersecurity, understanding and quantifying risk are crucial for effective defense strategies. CYE, led by cybersecurity expert Ira Winkler, has emerged as a frontrunner in this domain. Their cybersecurity optimization platform empowers businesses to assess, quantify, and mitigate cyber risk, enabling security leaders to make informed decisions based on data rather than speculation. With a focus on cyber risk quantification, CYE's platform equips organizations with a mathematically-proven action plan, turning complex investment decisions into simplified equations.

Passwordless Security: Advancements in Zero Trust Authentication - Beyond Identity,Patrick McBride

In the age of rampant credential-based breaches, traditional password-based authentication methods have proven vulnerable. Addressing this critical issue, Beyond Identity, led by cybersecurity expert Patrick McBride, has introduced a groundbreaking solution that eliminates passwords altogether. As a FIDO2 certified provider, Beyond Identity's enterprise-ready platform ensures user and device trust through their Universal Passkey Architecture. By offering secure and frictionless multi-factor authentication that continuously validates user identity and device security, Beyond Identity propels organizations towards a Zero Trust Security model.

Detecting Privilege Access Abuse: A Continuous Validation of Trust - Inside-Out Defense, Ravi Srivatsav

Inside-Out Defense brings a unique approach to cybersecurity with its software-as-a-service platform designed for Continuous Validation of Trust. Led by Ravi Srivatsav, their agentless privilege access abuse detection and remediation platform complements existing identity access management solutions. What sets Inside-Out Defense apart is its real-time detection and remediation capabilities, going beyond known behaviors to detect and address anomalous user

behaviors. With a comprehensive view of user privileges, their platform integrates seamlessly with other solutions, providing organizations with a holistic defense strategy.

Comprehensive Email Security: A Proactive Defense Against Modern Threats - Abnormal Security, Mike Britton

Email continues to be a prime target for cyber attacks, necessitating robust email security solutions. Abnormal Security, spearheaded by Mike Britton, provides total protection against a wide range of attacks, including phishing, malware, executive impersonation, and more. Their specialized focus on email security allows them to plug directly into the API, leveraging advanced techniques such as identity, context, and behavior analysis. By collaborating with third-party applications and ensuring minimal latency, Abnormal Security offers seamless protection without hindering email workflows.

Uncovering Data Risks: A User-Centric Data Protection Solutions - Next DLP, Connie Stack

Data protection is a critical priority for organizations dealing with valuable data and compliance requirements. Next DLP, led by Connie Stack, offers innovative data protection solutions designed to uncover risks, educate employees, and fulfill security and compliance needs. Their user-centric approach enables organizations to implement adaptive controls based on roles, behavior, and assigned privileges. With real-time context inspection and a flexible, cloud-native architecture powered by AI/ML, Next DLP is disrupting the legacy data loss prevention market.

Managing Cyber Risk Across the Supply Chain: Utilizing the Critical Function Framework - Exiger, Bob Kolasky

In today's interconnected business landscape, managing cyber risk across the supply chain is paramount. Exiger, under the leadership of Bob Kolasky, offers a unique perspective on cyber risk management with its critical function framework. By scrutinizing cyber risk at every stop along the supply chain, Exiger provides organizations with the tools to navigate risk and compliance challenges. Their software and tech-enabled solutions empower corporations, government agencies, and banks to proactively address risks related to third-parties, supply chains, and customers.

Securing the Cloud and Beyond: A Holistic Approach to Data Protection - Skyhigh Security, Anand Ramanathan

As organizations embrace cloud technologies and remote work, securing data across cloud, web, and networks becomes increasingly challenging. Skyhigh Security, led by Anand Ramanathan, offers comprehensive solutions to address these evolving security needs. Their expertise in cloud

security enables seamless collaboration and data protection across all applications, without compromising security. With a data-focused approach and frictionless implementation, Skyhigh Security helps organizations stay ahead of evolving threats.

Ensuring Mobile App and API Security: A Runtime Protection - Approv, George McGregor & Pearce Erensel

With the rise of mobile apps and API-based services, ensuring their security has become paramount. Approv, led by George McGregor and Pearce Erensel, provides a comprehensive runtime security solution for mobile apps and APIs. Their focus on mobile app and API security ensures that validation takes place directly with the application, safeguarding against security vulnerabilities. By keeping runtime secrets secure and protecting against threats, Approv empowers organizations, especially those in the fintech and healthcare sectors.

Unleashing the Power of Hardware and Software Collaboration: Xcitium and Intel Join Forces - Xcitium, Ken Levine + Intel, Carla Rodríguez

Carla Rodríguez, Annabelle Klosterman, Ken Levine

In the ever-evolving landscape of cybersecurity, collaboration between innovative companies is key to developing robust defense mechanisms. Xcitium, led by CEO Ken Levine, has forged a strategic partnership with Intel to combat the rising tide of ransomware and cyber-attacks. Leveraging Intel's Threat Detection Technology (TDT) and Xcitium's patented ZeroDwell Containment technology, this collaboration offers a layered approach to security. Xcitium's real-time detection-less software technologies, coupled with Intel's advanced CPU telemetry, provide unprecedented visibility and protection against undetectable threats.

Staying Ahead of Threats: An Innovative Approach to Proactive Threat Intelligence - HYAS, Dave Mitchell

In today's rapidly evolving threat landscape, organizations need to move beyond reactive measures and adopt proactive strategies. HYAS, led by CTO Dave Mitchel, offers an industry-leading protective DNS solution that detects, blocks, and protects organizations from emerging threats. By tagging infrastructure before it becomes malicious and collaborating with law enforcement agencies, HYAS ensures the swift takedown of threats. Their comprehensive approach, encompassing insight mapping, protection, and intelligence, empowers organizations to stay one step ahead.

Empowering Secure Digital Transformation: Some Cutting-Edge Solutions - Sangfor Technology, Guy Rosefelt

Cloud computing and network security have become paramount concerns for organizations in the digital age. Sangfor Technology, a leading global vendor of IT infrastructure solutions, has positioned itself at the forefront of this evolving landscape. With a comprehensive portfolio of products and services, including Hyper-Converged Infrastructure, Next-Generation Firewall, and Ransomware Protection, Sangfor Technology offers versatile solutions to address the diverse security needs of modern enterprises. Notably, their incorporation of a built-in ransomware honeypot and deception technology within their firewall sets them apart from the competition.

Navigating Cybersecurity Challenges: A Tailored Expertise and Solutions - Guidepoint Security, Mark Lance

In the ever-changing landscape of cybersecurity, organizations need reliable expertise and tailored solutions to navigate complex challenges. Guidepoint Security, led by Mark Lance, provides proven expertise and a range of services to help organizations make better cybersecurity decisions that minimize risk. With a focus on value-added reselling, professional services, cyber consulting, and managed services, Guidepoint Security offers comprehensive support. Their technical expertise, long-term relationships, and standardized approach set them apart.

Gaining the Upper Hand: An Unbiased View of Enterprise Security - Intrepres, Fred Wilmot

Understanding an enterprise's security posture is crucial for effective threat reduction. Intrepres Security, led by Fred Wilmot, provides an unbiased view of an organization's security posture, helping CISOs and security practitioners reduce threat exposure. By analyzing the dynamic relationship between defensive and adversarial capabilities, Intrepres Security prioritizes defensive actions and optimizes the security ecosystem. Their focus on attack surface management, vulnerability management, and adversarial simulation enables organizations to proactively identify and address weaknesses.

Unleashing Proactive Threat Intelligence: Deep and Dark Web Expertise - Cybersixgill, Delilah Schwartz

As cyber threats continue to evolve and expand, organizations require proactive threat intelligence to mitigate risks. Cybersixgill, led by Delilah Schwartz, offers cutting-edge solutions that capture, process, and alert teams to emerging threats on the clear, deep, and dark web. With the largest data lake on the market and an automation-driven approach, Cybersixgill provides end-to-end threat protection and access to its comprehensive database.

From speaking with the various innovators, it was clear how they are advancing defense-in-depth strategies. From AI-driven defense mechanisms to leveraging dark web threat intelligence, these companies are revolutionizing the industry. They are addressing critical cybersecurity challenges such as supply chain risk management, anomaly detection, risk quantification, passwordless authentication, continuous validation of trust, user-centric data protection, cloud and network security, mobile app and API security, hardware-software collaboration, proactive threat intelligence, among others.

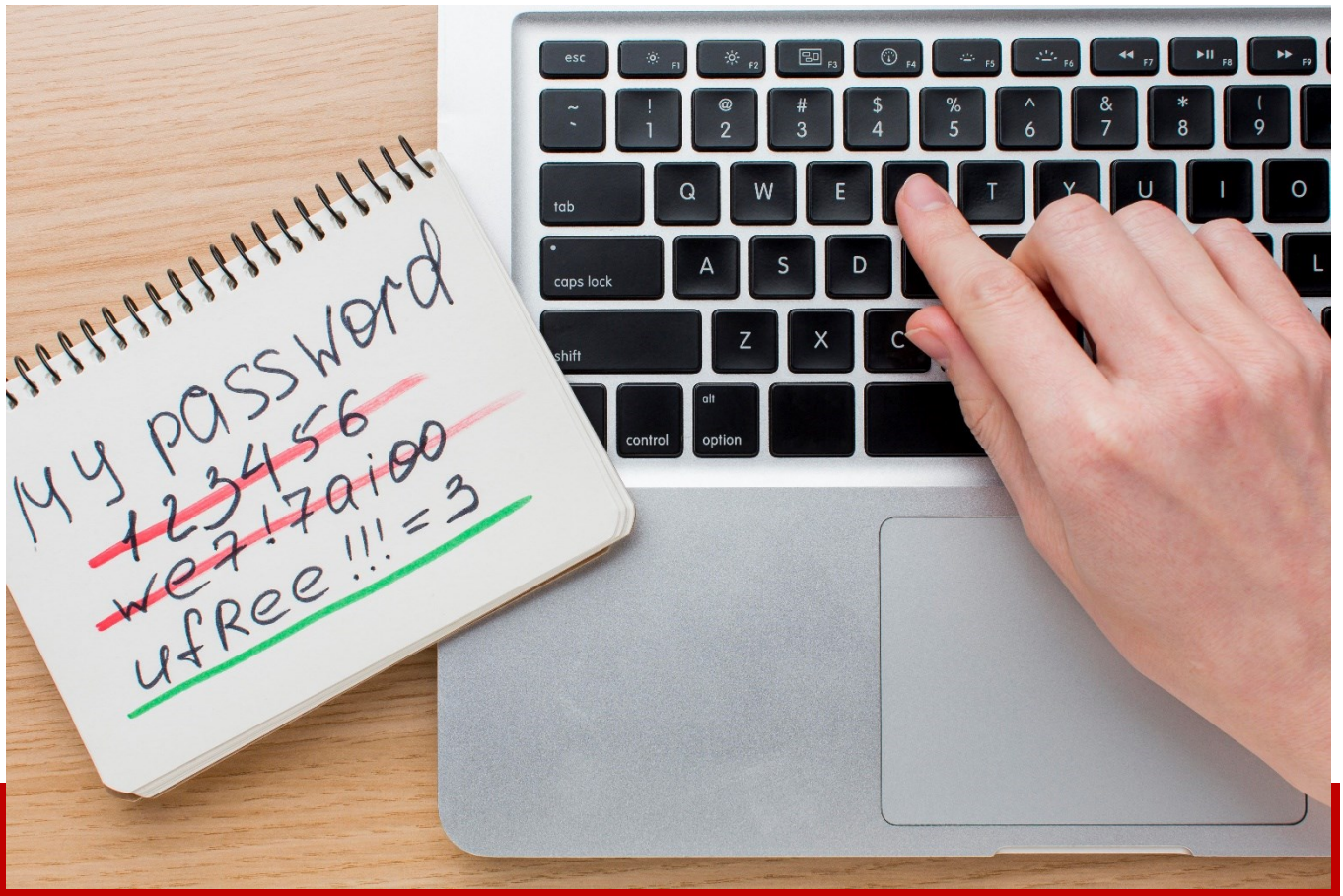
In my conversations with these cybersecurity innovators, I was inspired by their passion, dedication, and expertise in the field. Their relentless pursuit of cutting-edge solutions and commitment to securing our digital landscape is commendable. As I reflect on the insights gained from the RSA Conference, I am filled with optimism for the future of cybersecurity. The work of these innovators gives me confidence that we are on the right path towards a more secure digital world. I look forward to witnessing the continued growth and impact of these companies as they shape the landscape of defense-in-depth strategies. Together, we can build a resilient and secure digital future.

About the Author

Annabelle Klosterman is a Cybersecurity Reporter for Cyber Defense Magazine (CDM) and CDM's first Women in Cybersecurity scholarship awardee. She is a Cybersecurity Engineer for Southwest Airlines, Co-Founder/Program Director of the Cyber Community Club, and a Master's Cyber Defense student at Dakota State University. Her areas of focus are offensive and defensive security, governance, risk and management, security consulting, program management, and cybersecurity training/outreach.

Throughout the years, Annabelle has competed in numerous competitions and placed nationally at the Collegiate Cyber Defense Competition in 2022 and 2023 and was a national finalist in CyberPatriot in 2019 and 2020. Additionally, she earned 1st place in the 2022 Idaho National Laboratory CyberCore CTF, and Women in Cybersecurity (WiCyS) CTF in 2021 and 2022. She holds SANS certifications in Cybersecurity Technologies (GFACT), Cloud Security (GCLD), and Incident Handling (GCIH).

Annabelle has spoken on cybersecurity and career topics at various events and organizations including US Cyber Games, RSA Conference, Secure360, Texas Cyber Summit, BSidesSATX, South Dakota InfraGard, Civil Air Patrol, and more. Annabelle's goal is to be in a position that changes the way people view and handle security, for their protection and safety, and the benefit of everyone. Annabelle can be reached online at https://www.linkedin.com/in/annabelleklosterman and at her website https://www.annabelleklosterman.com/.



Has MFA Had Its Day?

By Ori Arbel, CTO, CYREBRO

Multi-factor authentication (MFA) has become the authentication standard for nearly all types of businesses – from banks to bicycle rentals and everything in between. Yet, like so many security schemes, the more prevalent MFA becomes, the potentially less secure it also becomes. Today, MFA is increasingly under attack, begging the question: Has MFA had its day? Is it time to adopt a more secure login scheme or is MFA still viable?

2FA and MFA: A Brief History

The predecessor of MFA, two-factor authentication (2FA), has been around – believe it or not – since 1986, when RSA introduced its first password-generating key fob. Throughout the 1990s, it found mostly niche use. Even in the first decade or so of the new millennium, only a limited number of security-conscious organizations used 2FA schemes – usually based on RSA public-key

cryptography that used two separate authentication tokens to validate user logins. Although the systems themselves were fairly reliable and secure, users found the solution burdensome and annoying. Password-generating tokens were frequently lost – forcing users to call a help desk to have IT circumvent the security system, which negatively impacted productivity. To top it off, token-based systems were expensive to purchase and operate.

Only once smartphones went mainstream did 2FA/MFA start taking off. Suddenly, nearly everyone had a surrogate token system (a smartphone) in their pocket or purse. Users could easily receive authentication codes via SMS or email, making MFA far more palatable. Then, as hacks and breaches started to not only affect millions but also grab headlines, MFA slowly moved mainstream – bringing us to the point where today it's so mainstream that it's squarely in the crosshairs of high-powered threat actors.

What is MFA Fatigue?

Like any security paradigm, MFA is not foolproof. Threat actors can get around MFA authentication using stolen credentials, smartphone spoofing, stealing authenticated session cookies after user logins, and - most notably - via social engineering techniques.

One of the most common types of social engineering MFA attacks is the MFA fatigue attack. The incidences of these attacks are on a precipitous rise, as users continue to fall victim to fake login approval requests.

When leveraging MFA fatigue, threat actors first gain access to user credentials – obtained via phishing or frequently the Dark Web. Then they attempt to login, bombarding users with MFA push notifications to trick them into authenticating the login attempts. According to research by Microsoft, 1% of users will accept an approval request like this on the first try. Others will respond simply to get rid of the annoyance of multiple authentication requests in a short time via SMS or email. To bolster these attempts, more sophisticated attackers impersonate a help desk email account, asking the victim to accept the MFA prompt just sent to his or her device.

Whatever the exact methodology, MFA fatigue attacks illustrate a serious weakness in the widely adopted MFA paradigm. The question is: is it a fatal weakness?

Five Tips to Counter MFA Fatigue Attacks

There are, in fact, numerous ways companies are attempting to counter MFA fatigue attacks. Here are five ideas to consider implementing at your organization:

1. **Strengthen employee education** – Like with many social engineering-based attacks, educating users to recognize spoof login attempts is an excellent first line of defense.
2. **Tighten authentication regimes** – Make sure your authentication regime takes into account all known user identity parameters. For example, is the user attempting to log in

actually on vacation? Is the ostensible login happening in the middle of the night in their time zone?

3. **Adopt double authentication** – Consider requiring users to first log into a VPN using MFA, then again use MFA to get into the application or resource they require. Alternatively, you can adopt a single sign on (SSO) solution.
4. **Add number matching to authentication requests** – Rather than just confirming a login attempt, require users to type in a two-digit code from the login screen to authenticate. A threat actor that didn't initiate the sign in won't know the two-digit code.
5. **Add additional context to push notifications** – To ensure users understand the origin of a sign-in and lower the chances of accidental approval, add context to push authentication requests. For example, the user's sign in location based on their IP would need to match where they are based. Context can also be added according to their responsibilities and the app they are trying to access (e.g. denying access to an HR employee trying to use a Finance app).

MFA: Not Dead Yet

MFA is still alive and kicking, but it's not a silver bullet. By implementing some or all of the additional MFA layers of security listed above, companies can extend the lifespan of their MFA security schemes – and the ROI of the systems supporting them.

However, forward looking security professionals already have their eyes on the next generation of authentication technology. More secure than MFA, passwordless security enables users to seamlessly log into systems or services without entering a password or knowledge-based secret.

Usually built on the FIDO2 standard, which defines a set of specifications such as Web Authentication (WebAuthn), Client-to-Authenticator Protocol, passwordless already has several implementations, including Windows Hello (that uses biometrics) and Microsoft Authenticator (an application).

That said, MFA will be with us for the foreseeable future. MFA has had its day…but that day is not quite over yet.

About the Author

Ori is CYREBRO's CTO, coming from a strong technical cybersecurity background, specifically with years' operating and managing global monitoring and investigation teams. He brings in-depth working knowledge with cutting edge cybersecurity platforms and innovative technologies. Ori can be reached online at LinkedIn and at CYREBRO's website http://www.cyrebro.io.

Boost Your Business Security: How Cyber Insurance Shields You from Cyber Threats

By Simon Pascoe, Director, FD Beck Insurance Brokers

As the digital landscape evolves, cyber threats have become a significant concern for all businesses. Protecting your business from these risks is crucial, and one effective solution is investing in cyber insurance. This article will explore how cyber insurance can safeguard your company, its benefits, and why it's essential to your overall security strategy.

What is Cyber Insurance?

Cyber insurance, is a specialized form of insurance designed to protect businesses against various cyber risks. It covers the financial losses arising from cyberattacks, data breaches, or other cyber-related incidents. A comprehensive cyber insurance policy can help businesses navigate the challenges of recovering from a cyber event, minimizing the potential damage to their reputation, finances, and operations.

Why Your Business Needs Cyber Insurance

1. Growing Cyber Threats

Cyber threats are becoming more sophisticated and widespread. With technological advances and the growing dependence on digital platforms, businesses are now more vulnerable to cyberattacks than ever. Cyber insurance is a proactive measure to guard against potential cyber incidents and their consequences.

2. Financial Protection

A cyberattack can result in substantial financial losses for businesses. The expenses can quickly increase, from the cost of investigating the incident to legal fees and regulatory fines. Cyber insurance helps mitigate these financial risks by covering various expenses associated with a cyber event.

3. Reputation Management

A data breach or cyberattack can significantly damage a company's reputation. Cyber insurance can help businesses manage the fallout of a cyber incident by providing access to public relations and crisis management services, helping restore confidence in the affected industry.

4.Swift Recovery

A quick response to a cyber event is essential to minimize its impact. Cyber insurance policies typically include access to a panel of expert service providers, such as forensic investigators, legal counsel, and IT security consultants, to assist businesses in navigating the recovery process.

Key Components of Cyber Insurance Coverage

1. First-Party Coverage

This coverage protects the policyholder against direct losses from a cyber incident. It may include coverage for:

· **Business interruption**: Covers the loss of income and extra expenses incurred due to the disruption of business operations caused by a cyber event.

· **Data recovery**: This covers the cost of restoring, recollecting, or recreating lost or damaged digital assets.

· **Cyber extortion**: Covers the cost of responding to ransomware attacks or other extortion attempts.

· **Notification and credit monitoring**: Cover the expenses of notifying affected parties and providing credit monitoring services following a data breach.

2. Third-Party Coverage

Third-party coverage protects the policyholder against claims by other parties affected by a cyber incident involving the insured business. This may include coverage for:

· **Network security liability**: Covers claims resulting from unauthorized access, data theft, or harmful software transmission.

· **Privacy liability**: Covers claims arising from the unauthorized access, use, or disclosure of personal or confidential information.

· **Media liability**: Covers claims related to intellectual property infringement, defamation, or invasion of privacy resulting from the insured's online content.

How to Find the Right Cyber Insurance Policy

Selecting the right cyber insurance policy involves considering your business's unique risks, the extent of your existing cybersecurity measures, and your budget. Evaluate your business's specific needs and work with a trusted insurance provider to customize a policy that best suits your requirements.

Proactive Measures to Complement Cyber Insurance

While cyber insurance is a vital component of your business's security strategy, it is essential to implement additional measures to strengthen your defenses. Here are some proactive steps to bolster your cybersecurity:

Employee Training and Awareness

Teaching your employees about possible cyber-attacks and safe internet practices is vital to decreasing the chance of cyber-related incidents. Implement regular training sessions to inform your staff about the latest dangers and best practices for protecting sensitive information. In addition to cyber insurance, it's essential to consider other forms of protection, such as professional indemnity insurance, to safeguard your business from a wide range of potential risks.

Regular Security Assessments

Conducting routine security assessments can help identify vulnerabilities in your systems and networks. Addressing these weaknesses can reduce the likelihood of a successful cyberattack.

Data Encryption

Encrypting sensitive data can protect it from unauthorized access or theft, even if your system is breached. Implement strong encryption practices for data at rest and in transit to safeguard your valuable information.

Multi-Factor Authentication

Implementing multi-factor authentication (MFA) adds an extra layer of security to your digital platforms, reducing the risk of unauthorized access. MFA needs users to provide two or more forms of identification to access an account, making it harder for cybercriminals to gain access.

Regular Data Backups

Regularly backing up your data can minimize the impact of a cyber incident, as you'll be able to restore your systems quickly and efficiently. Ensure your backups are stored securely in a separate location, and periodically test the restoration process to verify the integrity of your data.

Incorporating Cyber Insurance into Your Overall Risk Management Strategy

Cyber insurance should be integrated into your organization's broader risk management framework. This holistic approach ensures that your business is well-equipped to deal with cyber threats and that all aspects of your security strategy are aligned.

To achieve this, collaborate with your insurance provider, IT professionals, and risk management experts to assess your organization's risks and develop a comprehensive security plan. This plan should address the technical aspects of cybersecurity and the human and procedural elements that contribute to a robust security posture.

By performing a proactive approach to cybersecurity and incorporating cyber insurance into your risk management strategy, you can safeguard your business from the ever-evolving landscape of cyber threats, ensuring its continued growth and success.

Conclusion

In today's digital era, cyber threats are an ever-present risk to businesses. Investing in cyber insurance is crucial to fortifying your organization against potential cyber incidents and their consequences. By understanding the various aspects of cyber insurance and selecting the right policy for your business, you can effectively shield your organization from the financial and reputational repercussions of cyberattacks and data breaches.

About the Author

Simon Pascoe, Director at FD Beck Insurance Brokers

Simon Pascoe - For the past 26 years Simon has enjoyed a career in the Insurance industry as both a broker and underwriter. Prior to being a director at FD Beck Simon had a successful 8-year management career with one of the world's largest general insurers, which saw him deal with and structure insurance programs for some of Australia's largest insurance purchasers. Simon can be reached online at simon@fdbeck.au and at our company website https://fdbeck.com.au/.

Bridging the Widening Gap in Cybersecurity Talent: Addressing the Urgent Need for Skilled Professionals

By Travis Doe, Marketing Executive, Secure IT Consult

Introduction

In today's digital age, where technology is deeply integrated into our personal and professional lives, the importance of cybersecurity cannot be overstated. With the increasing frequency and sophistication of cyber threats, organisations are facing a critical challenge – a growing gap in cybersecurity talent. This article delves into the reasons behind this gap, its consequences, and potential solutions to bridge it.

The Widening Gap

The demand for skilled professionals has skyrocketed in recent years, but unfortunately, the supply has not kept pace. Several factors contribute to the widening gap:

1. Rapid Technological Advancements: The rapid evolution of technology has led to an increased attack surface, creating new vulnerabilities cybercriminals exploit. Keeping up with these advancements requires a diverse skill set and continuous learning, but the education system often struggles to adapt quickly enough.

Rapid technological advancements are contributing to the widening cybersecurity talent gap by introducing new challenges and complexities that require specialised skills to address. These advancements include the proliferation of IoT devices, which increase the attack surface for cyber threats, the adoption of cloud computing requires expertise in securing virtualised environments, the utilisation of AI and ML techniques by both attackers and defenders, the management and analysis of big data, the need for mobile security expertise due to the widespread use of mobile devices, and the emergence of new technologies like quantum computing and blockchain.

Keeping up with these advancements demands continuous learning, practical experience, and specialised knowledge, creating a shortage of skilled professionals who can effectively navigate and mitigate the risks associated with these evolving technologies.

2. Cybersecurity Skills Shortage: The cybersecurity industry faces a shortage of skilled professionals who possess the necessary technical expertise and hands-on experience. The complex and ever-changing nature of cyber threats demands individuals with a deep understanding of network security, encryption protocols, risk assessment, incident response, and more.

The rapid growth and complexity of cyber threats requires a diverse skillset, and a constant, continuous development plan to stay abreast of the ever evolving and shifting landscape, in which educational institutions find themselves struggling to stay relevant.

This is further compounded by the necessity of hands-on experience, and expertise across sectors of the industry. Finding individuals with a comprehensive understanding is challenging, as time & exposure are both needed to develop proficiency in the cybersecurity arena.

The high demand for professionals stems from increasing numbers of cyber-attacks and the growing value of data – organisations globally are facing a constant barrage of threats and are in dire need of skilled professionals.

3. The Lack of awareness of cybersecurity is a significant contributing factor to the cybersecurity skills shortage. Many individuals, particularly those who are potential candidates for careers in cybersecurity, are unaware of the opportunities and importance of the field. This lack of awareness has several implications:

Limited Talent Pool: The cybersecurity field requires a diverse range of skills and expertise. However, when individuals are unaware of the potential career paths and the demand for professionals, they may not consider it as a viable option. This limited awareness narrows the talent pool and exacerbates the shortage of skilled professionals.

Missed Career Opportunities: As technology continues to advance and cyber threats become more prevalent, the demand for professionals across industries is growing rapidly. However,

individuals who are unaware of these career opportunities may choose other paths or fields. This results in missed opportunities for both the individuals and organisations seeking to strengthen their cybersecurity workforce.

Lack of Preparedness: A lack of awareness of cybersecurity among the public also leads to a lack of preparedness in dealing with cyber threats. Individuals may not understand the importance of securing their personal devices, using strong passwords, or practicing safe online behaviour. This ignorance creates a larger attack surface and makes it easier for cybercriminals to exploit vulnerabilities.

Inadequate Cybersecurity Culture: Lack of awareness also contributes to a deficiency in cybersecurity culture within organisations. When employees and decision-makers are not aware of the potential risks and the value of cybersecurity measures, they may not prioritise or invest in appropriate security practices and technologies. This can leave organisations vulnerable to attacks and hinder the development of a robust cybersecurity posture.

Consequences of the Gap

The consequences of the growing gap in cybersecurity talent are far-reaching and pose significant risks:

1. Increased Vulnerability: Leaving organisations exposed to a wide range of cyber threats and risks. The consequences of this increased vulnerability can be significant and include the following:

Exploitation of Weaknesses: Cyber attackers are constantly scanning for vulnerabilities in systems, networks, and applications. Without enough skilled professionals to identify and patch these weaknesses, organisations are more likely to fall victim to exploits. Attackers can exploit vulnerabilities to gain unauthorised access, steal sensitive data, disrupt operations, or compromise critical infrastructure.

Inadequate Risk Management: Skilled professionals play a vital role in assessing and managing risks. They conduct thorough risk assessments, identify potential threats, and implement appropriate security controls to mitigate risks. However, in the absence of enough talent, organisations may struggle to accurately assess risks or prioritise them effectively. This can result in inadequate or misaligned security measures, leaving critical assets and systems exposed to potential threats.

Delayed Incident Detection and Response: Timely detection and response are crucial to minimising the impact of cyber incidents. Skilled professionals are adept at monitoring systems, analysing suspicious activities, and responding promptly to security incidents. Without enough talent, organisations may experience delays in detecting and responding to incidents, allowing attackers to persist within their networks and inflict greater damage over an extended period.

Ineffective Security Measures: Skilled professionals possess the knowledge and expertise required to implement effective security measures. They are familiar with the latest security

technologies, best practices, and industry standards. However, with a lack of cybersecurity talent, organisations may struggle to deploy and manage robust security controls. Inadequate security measures can leave vulnerabilities unaddressed, increasing the likelihood of successful cyber-attacks.

Limited Security Awareness and Training: Skilled professionals play a crucial role in raising security awareness and providing training to employees. They educate staff about safe computing practices, social engineering threats, and best practices for safeguarding sensitive information. In the absence of enough talent, organisations may not have the resources or expertise to deliver comprehensive security awareness programs. This can result in employees being unaware of potential risks and inadvertently becoming a weak link in the security chain.

Compliance and Regulatory Issues: Organisations often need to comply with various industry regulations and data protection laws. Skilled professionals ensure necessary security controls and practices are in place to meet these requirements. However, a lack of talent can hinder compliance efforts, exposing organisations to legal and regulatory consequences.

2. Talent Poaching: Talent poaching refers to the practice of actively recruiting and enticing skilled cybersecurity personnel from other organisations. Some of the key aspects of talent poaching arising in cybersecurity are:

Increased Competition: Organisations face intense competition in recruiting cybersecurity professionals due to the limited supply of qualified individuals. This competition drives up salaries, benefits, and incentives offered to attract top talent. Organisations may engage in aggressive recruiting tactics, such as offering higher salaries, signing bonuses, flexible work arrangements, and career advancement opportunities.

Skills Drain: Talent poaching can create skills drain within organisations. As skilled cybersecurity professionals are lured away by more attractive offers, organisations are left with a depleted workforce, impacting their ability to address ongoing security challenges effectively. The loss of experienced personnel can disrupt projects, compromise knowledge transfer, and hinder the overall security posture.

Negative Impact on Organisational Stability: Frequent talent poaching can lead to a lack of stability within organisations. The constant turnover of cybersecurity personnel disrupts team dynamics, reduces institutional knowledge, and may impact the consistency and continuity of security operations. This instability can create gaps in coverage, increase vulnerability to attacks, and hamper organisational resilience.

Impact on Industry Collaboration: The practice of talent poaching can strain collaboration and cooperation between organisations in the cybersecurity industry. Instead of sharing knowledge and best practices, organisations may become more guarded, fearing their skilled professionals will be targeted by competitors. This can impede the industry's ability to collectively address evolving cyber threats and find innovative solutions.

Adverse Effects on Small and Medium-sized Enterprises (SMEs): SMEs often struggle to compete with larger organisations in terms of compensation and benefits. As a result, talent

poaching tends to disproportionately affect SMEs, making it more challenging for them to attract and retain skilled cybersecurity professionals. This talent drain can leave SMEs more vulnerable to cyber-attacks, as they may lack the resources to invest in comprehensive cybersecurity measures.

3. Innovation Stagnation: When there is a lack of skilled professionals, organisations face challenges in driving and sustaining innovation in the field of cybersecurity. The following factors contribute to innovation stagnation:

Limited Capacity for Research and Development: Skilled professionals are instrumental in conducting research and development activities to explore new approaches, techniques, and technologies in cybersecurity. However, the talent shortage restricts the capacity of organisations to invest in research and development initiatives. The lack of resources and expertise hinders the exploration of innovative solutions and slows down the pace of progress in the field.

Inability to Keep Pace with Emerging Threats: Cyber threats are constantly evolving, with attackers finding new methods to exploit vulnerabilities and bypass existing security measures. Skilled professionals play a crucial role in understanding these emerging threats, analysing attack patterns, and developing effective countermeasures. The talent shortage limits the ability of organisations to keep up with the rapidly changing threat landscape, resulting in outdated and ineffective security practices.

Reduced Adoption of Cutting-Edge Technologies: Innovations in technologies such as artificial intelligence (AI), machine learning (ML), blockchain, and quantum computing have the potential to revolutionise cybersecurity. Skilled professionals are needed to understand, implement, and adapt these technologies to enhance security measures. However, the talent shortage limits the adoption of these cutting-edge technologies, hindering organisations from harnessing their full potential in addressing emerging cyber threats.

Lack of Diverse Perspectives and Creative Solutions: Skilled cybersecurity professionals bring diverse backgrounds, experiences, and perspectives to the field. This diversity fosters creativity and innovation by encouraging out-of-the-box thinking and novel approaches to problem-solving. However, the talent shortage limits the availability of diverse talent, which can lead to a homogenous workforce lacking in fresh ideas and creative solutions.

Dependency on Legacy Systems and Practices: Organisations without sufficient cybersecurity talent may resort to relying on legacy systems and outdated practices to maintain their security posture. The absence of skilled professionals who can introduce and implement modern security technologies and strategies hampers the ability to adopt more advanced and effective cybersecurity measures. This reliance on legacy systems and practices increases the vulnerability to cyber-attacks and inhibits innovation.

Bridging the Gap

Bridging the cybersecurity talent gap requires a concerted effort to provide educational and training opportunities that equip individuals with the necessary skills and knowledge. Here are some key avenues for addressing the talent gap in cybersecurity:

Academic Programs: Educational institutions play a crucial role in preparing individuals for careers in cybersecurity. They can offer undergraduate and graduate degree programs in cybersecurity, computer science, or related fields. These programs should cover a broad range of topics, including network security, cryptography, ethical hacking, incident response, and risk management. Collaboration between academic institutions and industry professionals can help ensure the curriculum aligns with industry demands.

Vocational Training and Certifications: Vocational training programs and industry certifications offer practical and targeted skill development opportunities. Recognised certifications, such as CompTIA Security+, Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP), validate individuals' knowledge and enhance their employability.

Cybersecurity Bootcamps: Intensive and immersive cybersecurity bootcamps offer accelerated training programs designed to quickly upskill individuals. These programs typically focus on practical, hands-on learning and cover a range of cybersecurity topics. Bootcamps often provide real-world scenarios and industry-relevant skills, preparing participants for entry-level cybersecurity roles.

Online Courses and Massive Open Online Courses (MOOCs): Online learning platforms and MOOCs offer flexibility and accessibility, making cybersecurity education more widely available. Platforms like Coursera, edX, and Udemy offer a variety of cybersecurity courses taught by industry experts.

Industry and Government Initiatives: These initiatives may include scholarships, grants, mentorship programs, and internships, providing financial support, guidance, and practical experience to aspiring cybersecurity professionals, and collaborations with educational institutions to develop curriculum guidelines and offer resources for cybersecurity education.

Apprenticeship Programs: Apprenticeship programs provide a combination of on-the-job training and classroom instruction, allowing individuals to gain practical experience while learning from experienced professionals. These programs are particularly effective, as they bridge the gap between theoretical knowledge and real-world application. Organisations can collaborate with educational institutions and apprenticeship agencies to establish structured cybersecurity apprenticeship programs.

Continuous Professional Development: Continuous professional development opportunities, such as workshops, seminars, conferences, and webinars, help professionals enhance their skills, expand their knowledge, and stay current in the rapidly changing cybersecurity landscape.

To effectively bridge the cybersecurity talent gap, a multi-faceted approach is necessary. Collaboration between educational institutions, industry stakeholders, and government entities is

vital in developing and implementing comprehensive educational and training initiatives. By providing individuals with diverse pathways to acquire cybersecurity skills, we can cultivate a strong and capable cybersecurity workforce to meet the growing demands of the digital landscape.

Conclusion

In conclusion, the cybersecurity talent gap has emerged as a critical challenge in today's increasingly digital and interconnected world. However, the supply of qualified individuals has failed to keep pace with demand, leading to a widening talent gap.

The consequences of the cybersecurity talent gap are far-reaching and impact organisations, individuals, and society. The lack of awareness about cybersecurity and the resulting limited pool of skilled professionals further exacerbates the problem.

Addressing the talent gap requires a multi-pronged approach. It starts with raising awareness about the importance of cybersecurity and inspiring individuals to pursue careers in this field. Educational institutions must develop comprehensive cybersecurity programs, and training, bootcamps, online courses, and apprenticeship programs to acquire cybersecurity skills and enter the workforce.

Industry collaboration, government support, and continuous professional development initiatives are crucial in bridging the talent gap. Organisations should invest in training and development programs to upskill their existing workforce and attract new talent. Public-private partnerships can facilitate knowledge sharing, mentorship, and internship opportunities to nurture the next generation of cybersecurity.

Only through collaborative and sustained efforts can we build a resilient cybersecurity workforce capable of safeguarding our digital future.

About the Author

Travis Doe is a Marketing Executive @ secure IT consult – with a love for all things technology, writing every week for the SITC Website blog on topics ranging from industry leading vendors, to explaining cybersecurity, and covering recent news and events in the industry, a website developer turned marketing executive, Travis has found his love for the IT industry and enjoys work surrounding cloud and cybersecurity.

Travis can be reached online through Twitter, and LinkedIn and through the SITC website https://secureitconsult.com.

A Passwordless Future

By Sam Rehman, SVP, Chief Information Security Officer, at EPAM Systems, Inc.

Using passwords is like carrying a large set of keys everywhere you go. You can get through doors, for instance, but if you lose them, not only are you stuck and can't go anywhere, but now somebody else might be able to use them and visit places they shouldn't. When inefficiency happens, like in this scenario, a change is necessary. The same is true about passwords, which as a security contract, often give a false sense of security. A study found that two in three respondents will forget their passwords unless they record them, which is a big part of the problem. What is recorded in multiple forms increases the chance that it's stolen. Likewise, more than half of Americans perform at least five password resets each month, taking 10 minutes each time. Password resets are also a key tool for attackers to breach into systems, and since it's used so often, it's difficult for defenders to spot anomalies.

Furthermore, as people continue to shop, work, and interact online, their passwords – and by extension, the private information they protect – are becoming more vulnerable to bad actors. It stands to reason, with all of the problems of passwords, is a passwordless future possible, and what would it take to achieve it?

Passwordless and Zero Trust

In the past, ring-fencing, or the process of limiting interactions between applications and their access to the internet, was the go-to strategy for cybersecurity. However, ring-fencing no longer holds the fort, and zero trust has begun to take center stage. As zero trust matures, the public continues to recognize that it is not a single product but a concept encompassing advanced technology solutions, processes, and policies. Some of the main principles of zero trust include risk detection and evaluating authentication in the context of the user's transaction (what they accessed, where, when etc.), often called recertification.

Another chief pillar of zero trust is verifying identity frequently. And when it comes to securing one's identity, a fundamental aspect is strong authentication. One of the primary reasons why going passwordless continues to gain momentum is the push for robust authentication, as it is a fundamental component of identifying the user. Many are now aware of the brokenness of passwords since they do not comply with the authentication principles of zero trust. Similarly, anything the password holder knows, anything they remember, a bad actor can socially engineer out of them through phishing, phone scams, or some other malicious method.

The Flaws of Relying Too Heavily on Biometrics

The second reason behind the rise of passwordless is biometrics. Having a face ID or fingerprint ID on one's phone is very convenient and removes the annoyance of remembering passwords that could get stolen. Additionally, these biometric authentication methods overcome the issues of cryptographic-based authentication. Nevertheless, passwordless systems have flaws, particularly when they rely too heavily on phone biometrics and are not connected fully to centralized authentication. Using biometrics on one's phone creates a false sense of security because they don't get validated against whom the phone belongs to.

For example, many people have their child or another family member's biometric ID fingerprint enrolled on their phone. When they use biometrics to validate a transaction notification, this process can't confirm if the user validating the transaction is the account holder or any other person enrolled on the phone. Such a method does not align with zero trust because it does not confirm the end user's identity. Unfortunately, most passwordless solutions cannot bridge this gap between the account holder and the biometrics on the phone.

If there is no connection between the biometrics owner and the account holder, an attacker could access the owner's credentials by going through a fraudulent account recovery or new device enrollment process, connecting their biometrics to the owner's account. This scenario is the Achilles Heel of going passwordless, and companies wanting to adopt a passwordless model must address this gap.

Multi-Factor Authentication and Decentralized Data Storage

A passwordless biometric multi-factor authentication solution can address the gap or vulnerability in new phone or account recovery schemes. Ideally, this solution should not rely on phone biometrics but authenticate against a secure, centralized biometrics database accessible from any device or browser. Such a multi-factor method is repeatable across the user's devices – plus, it would not eliminate the convenience and authentication of biometrics.

Another key component of a passwordless biometric multi-factor authentication solution is its ability to secure biometric data over a decentralized network. This decentralized network would allow businesses to implement the infrastructure needed to safeguard biometric data (or any personal data) uniquely and innovatively; moreover, it maintains the benefits of a centralized facility to authenticate against while keeping the security of a decentralized method in which data gets stored and protected.

Typically, when people hear decentralization, they think of blockchain. However, there are better solutions to store identity or biometric data than blockchain. Although blockchain is sufficient for sharing transactions between many parties that all trust the same ledger, it cannot get edited, nor can users get removed. Today, to be General Data Protection Regulation or GDPR compliant, one needs to be able to remove users. Alternatively, businesses can store and secure biometric and other sensitive data on a decentralized network based on concepts like zero-knowledge proofs and multi-party computing.

The User Experience and Passwordless Solutions

As brands transition to passwordless biometric models, they must remember the user experience. Passwordless authentication processes should be convenient and natural – it's not optimal to have users constantly jumping through several different hoops. Likewise, businesses must remember the diverse populations they serve, especially since not everyone is tech-savvy. For some older generations, scanning a QR code could be complex. When selecting a solution (in addition to finding one with multi-factor authentication and a decentralized network for data storage), choose a vendor that offers multiple modalities that cater to different populations.

About the Author

Sam Rehman is Chief Information Security Officer (CISO) and Head of Cybersecurity at EPAM Systems, where he is responsible for many aspects of information security. Mr. Rehman has more than 30 years of experience in software product engineering and security. Prior to becoming EPAM's CISO, Mr. Rehman held a number of leadership roles in the industry, including Cognizant's Head of Digital Engineering Business, CTO of Arxan, and several engineering executive roles at Oracle's Server Technology Group. His first tenure at EPAM was as Chief Technology Officer and Co-Head of Global Delivery.

Mr. Rehman is a serial entrepreneur, technology expert and evangelist with patented inventions in software security, cloud computing, storage systems and distributed computing. He has served as a strategic advisor to multiple security and cloud companies, and is a regular contributor in a number of security industry publications.

Blockchain Technology: Strengthening Cybersecurity and Protecting Against Password Leaks and Data Breaches

By Thomas Carter, CEO, True I/O

In today's digital landscape, the frequency and severity of password leaks and data breaches have reached unprecedented levels. These incidents pose significant financial and reputational risks to organizations and compromise individuals' privacy and security.

Conventional security measures need to be modified to combat this growing threat. However, the emergence of blockchain technology offers a promising solution to bolster cybersecurity defenses. Specifically, the capabilities of emerging blockchain technology hold immense potential to mitigate the imminent, rising risk of password leaks and data breaches for organizations across a multitude of sectors.

The Growing Threat Landscape

In our interconnected world, password leaks and data breaches have become all too common. The repercussions of such incidents are far-reaching, resulting in financial losses, damaged reputations, and compromised trust. IBM's 2020 data security report says that it took businesses up to nine months to detect and contain a breach in 2020. The Mandiant Security Effectiveness Report of 2020 states that 58% of hackers gained access to the business network unnoticed, and 91% of cyber-attacks did not trigger an alert. Organizations and individuals must recognize the gravity of these threats and understand the limitations of traditional security measures. According to Cybersecurity Ventures, more than 60% of small businesses shutdown after a cyber-attack. The expenses required to remediate the problem, the divestment from investors and value lost from customers who have left often prove to be too much to handle.

Hackers constantly evolve their techniques, necessitating a proactive approach to safeguarding sensitive information.

Understanding Blockchain Technology

Blockchain is a decentralized and distributed ledger that records transactions across multiple nodes or computers. It operates on a consensus mechanism, where participants must agree on each transaction's validity before adding to the chain. Blockchain's inherent characteristics, such as immutability, transparency, and decentralization, make it a robust foundation for cybersecurity applications.

Enhancing Password Security with Blockchain

Password leaks are often the result of breached centralized databases, where user credentials are stored. Blockchain offers an alternative approach to password security through decentralized identity management. By leveraging blockchain's distributed ledger, users can retain control over their identities and personal data, reducing the risk of leaks. Additionally, blockchain enables passwordless authentication, leveraging cryptographic techniques such as public-private key pairs to authenticate users securely. This approach eliminates the vulnerabilities associated with traditional passwords and enhances overall security.

Mitigating Data Breaches with Blockchain

Data breaches expose sensitive information to unauthorized parties, leading to severe consequences. Blockchain technology can significantly mitigate this risk by employing encryption algorithms to secure data. Organizations can ensure that only authorized individuals with the corresponding decryption keys can access the information by encrypting data before storing it on the blockchain. Furthermore, blockchain's immutable nature enables the creation of audit trails, facilitating forensic analysis and identifying security incidents. Data privacy and consent

management are improved using blockchain, empowering users with greater control over their personal information.

Challenges and Considerations

While blockchain offers promising solutions, addressing the challenges and considerations associated with its implementation is essential. Scalability and performance issues have been a longstanding concern, as blockchain networks can become slower and less efficient as they grow. Additionally, regulatory and legal frameworks are still developing, posing potential compliance challenges. User adoption and interoperability between different blockchain platforms remain areas of exploration and improvement. Organizations must carefully evaluate these factors and devise effective strategies to overcome these challenges.

Real-World Examples

Numerous industries have recognized the potential of blockchain technology in enhancing cybersecurity. The finance sector, for instance, has explored blockchain-based solutions for secure and transparent transactions. Healthcare organizations are leveraging blockchain to protect patient records and ensure data integrity. In supply chain management, blockchain has demonstrated its efficacy in combating counterfeit products and enhancing traceability. These real-world examples highlight the tangible benefits of blockchain in strengthening cybersecurity across diverse sectors.

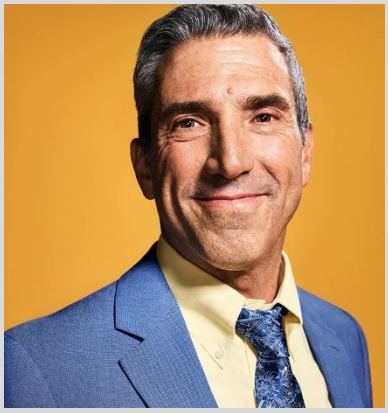
The Future of Blockchain and Cybersecurity

As cybersecurity continues to evolve, blockchain technology holds immense potential—emerging trends such as blockchain-enabled threat intelligence and secure data sharing present exciting opportunities for further innovation. Organizations can create a robust and interconnected security ecosystem by integrating blockchain with other advanced technologies, such as artificial intelligence and the Internet of Things (IoT). The synergy between these technologies can enable proactive threat detection, automated response mechanisms, and enhanced data protection. Additionally, ongoing research and development efforts are focused on addressing scalability issues and improving blockchain's performance to meet the demands of a rapidly expanding digital landscape.

In conclusion, blockchain technology has emerged as a game-changer in cybersecurity, offering unparalleled security features to combat password leaks and data breaches. By leveraging blockchain's decentralized nature, organizations can enhance password security, secure sensitive data, and fortify their cybersecurity infrastructure. While challenges exist, the potential benefits and real-world success stories illustrate the promising future of blockchain technology. As organizations strive to protect their valuable information, embracing blockchain as part of a

comprehensive cybersecurity strategy is crucial for a more secure and trustworthy digital ecosystem.

About the Author



Thomas Carter is the CEO of True I/O. A financial technology, blockchain, and digital securities pioneer, Carter is a leader and evangelist for adopting enterprise-grade FinTech and blockchain technologies with 30 years of capital markets experience. In 2016 he founded Deal Box, a capital markets consulting firm focused on helping entrepreneurs and investors by leveraging automation, artificial intelligence, and blockchain technologies.

Today, Carter is the Interim CEO of True I/O (formerly TNS), an ecosystem of blockchain-enabled solutions on a mission to transition the digital world into the blockchain economy. True I/O's flagship product, the Universal Communications Identifier (UCIDTM), is a cross-network security solution for any device connected to any network. True I/O also powers Digital Names, an alias solution for public keys that changes complex public wallet addresses into a simple Digital Name (ex: $ThomasCarter).

Carter is also the Chairman of Deal Box, leading investments and strategy. Thomas can be reached online on LinkedIn and at our company website http://trueio.io.

Adaptive DDoS Attacks Get More Sophisticated: How to Beat Attackers' New Ground Game

By Gary Sockrider, Director, Security Solutions, NETSCOUT

The rapid expansion of Internet of Things (IoT) devices, which now number in the billions, not to mention upgrades to network infrastructure and the acceleration of 5G deployments, means that network operators and IT managers have to become even more nimble at identifying and remediating security vulnerabilities. One increasing vulnerability that remains relatively elusive is DDoS attacks.

What is not often considered is that modern DDoS attacks are not what they once were several years ago. Now, such attacks are carefully orchestrated in campaigns involving reconnaissance. These campaigns identify weaknesses, tailor attacks, and monitor in real-time for efficacy, followed by adjustments in attack vectors. We call these "adaptive DDoS" attacks. And while attack methods of this nature have been perpetrated by nation-states, now they are increasing in prevalence in other sectors, such as healthcare and business.

In this article, we will explore how to prepare for these attacks so organizations don't become the unintended victims of an adaptive DDoS campaign. We will also explore how organizations can defend against these highly organized adaptive DDoS attacks by implementing edge-based detection and mitigation methods.

DDoS Attacker Evolution: From Rogue Agents to Sophisticated Operators

Today, DDoS attacks are getting more advanced by the day and are no longer the domain of rogue threat actors. This phenomenon has been observed with botnets launching attacks against Ukraine and other nation-states. Increasingly, attackers are shrewder and more brazen, performing extensive pre-attack scouting, exploiting weaknesses, and making use of botnet nodes and reflectors/amplifiers that are topologically adjacent to the target. This, in turn, minimizes the number of administrative boundaries that DDoS attack traffic must traverse, thus avoiding multiple network protection layers and making attack traffic more difficult to detect and mitigate.

While nation-state attacks are one example of the ways in which DDoS attacks are getting more organized at the ground level, businesses and other organizations are not at all immune. For example, this year, the U.S. Department of Health and Human Services (HHS) warned about DDoS attacks on the country's healthcare industry by Russian hacktivists with the goal of targeting ventilators. Killnet, a group of Russian hacktivists, already has claimed responsibility for more than a dozen DDoS attacks on U.S. healthcare organizations to date, including major hospital networks such as Cedars-Sinai and Duke University Hospital.

This is just another example of the lengths that nefarious actors go to planning, executing, and sustaining DDoS attacks. What may seem mundane is actually incredibly complex. DDoS attacks can span countries, networks, and techniques like water finding a path through any available means. Ultimately, organizations must adopt new strategies, including dynamic defenses that are just as adaptive to input as modern attacks, to combat the growing complexity.

Edge-Based Detection and Mitigation to Thwart Savvier Attackers

Because of the damage that can be done by short-duration attacks on an organization's critical business applications and services, as well as the requirement for near real-time mitigation to stop these attacks, a packet-level, stateless mitigation solution is a key consideration. This always-on technology sits on the edge of the network, and it is the foundation for a multilayered comprehensive DDoS defense against savvy attackers. Further, any edge-based solution must also be fully integrated with upstream mitigation to handle volumetric attacks exceeding the bandwidth available at the network edge.

Any DDoS protection solution must automatically identify and stop all types of DDoS attacks before they impact the availability of business-critical services. Unlike solutions that employ hard-coded logic, an adaptative DDoS defensive approach combines intelligent machine learning

algorithms with dynamically updated actionable DDoS threat intelligence, which includes historical and real-time data tracing the methodologies and patterns of attackers.

DDoS attacks are indeed challenging, but focusing on static mitigations and upstream defenses will miss attacks that are deliberately designed to evade these defenses. Ultimately, defeating these attacks requires a solution designed to adapt defense strategies to changing tactics. Only then can organizations ensure effective, comprehensive DDoS protection as bad actors become more organized and exploit more attack vectors -- and in a more methodical way -- than ever before.

About the Author

Gary is an industry veteran bringing over 20 years of broad technology experience including routing and switching, wireless, mobility, collaboration and cloud but always with a focus on security. His previous roles include solutions architect, security SME, sales engineering, consultancy, product management, IT and customer support. Gary seeks to understand and convey the constantly evolving threat landscape, as well as the techniques and solutions that address the challenges they present. Prior to joining Netscout in 2012, he spent 12 years at Cisco Systems and held previous positions with Avaya and Cable & Wireless. Gary can be reached on LinkedIn and at www.netscout.com.

Analyzing Four Diverse Attack Techniques Used by XeGroup

By Brett Raybould - EMEA Solutions Architect, Menlo Security

XeGroup is a prime example of the untold damage that sophisticated threat groups using modern attack techniques can now inflict on organizations.

Known to be active since at least 2013, the Vietnamese cybercriminal outfit, which has been linked to other cybercriminal organizations and state-sponsored hacking groups, has previously stolen more than $30 million from US-based corporations.

However, the techniques that the group leverages to attack its victims are by no means linear, nor predictable.

Over the past decade, XeGroup has been named responsible for a broad range of nefarious campaigns that have included supply chain attacks, the creation of fake websites to deceive users into revealing their personal information, compromised websites and mobile applications with malicious code, and the selling of stolen data on the dark web.

In this article, we will ll explore four diverse attack methods that the group have leveraged since their inception.

#1 – Malicious JavaScript webpage injection

One technique that XeGroup has become renowned for attacks that involve the injection of malicious JavaScript into web pages, with its adversaries successful in exploiting vulnerabilities in Magento e-commerce platforms and Adobe ColdFusion server software.

These activities were first identified back in 2013 when point-of-sale (PoS) systems at retail stores around the world were successfully penetrated with the “Snipr” malware – a credential-stuffing toolkit specifically created for this purpose.

Here, XeGroup stole financial detail directly while also attempting to gain access to corporate networks via phishing emails sent out using spoofed domains associated with legitimate companies such as PayPal and eBay.

This campaign continued all the way through to August 2020 when the attack group was taken down after researchers from security firm, Volexity, released findings about the group to law enforcement agencies globally, ultimately resulting in multiple arrests of group members.

2 – Exploiting CVE-2019-18935

Despite this, recent reports from the Cybersecurity and Infrastructure Security Agency (CISA) have suggested that XeGroup is back and actively exploiting CVE-2019-18935.

Specifically, this vulnerability can be used by threat actors to execute arbitrary code remotely on a vulnerable server by exploiting a deserialization vulnerability in the Telerik.Web.UI assembly.

It is estimated that this latest campaign has been underway since August 2021, with CISA having issued an advisory that suggests the group have successfully compromised a US government Internet-facing server running Internet Information Services (IIS).

On examining samples from various reports from CISA, Volexity, and our own telemetry on this, the Menlo Labs team has observed XeGroup’s targeting government agencies, construction organizations, and healthcare entities across our customer base.

#3 – ASPXSPY web shells

ASPXSPY web shells are also prevalent in XeGroup’s attacks.

These are scripts that have been specifically designed to enable threat actors to secure unauthorized access to web servers and carry out further attacks. A simple web application written

in C# and ASP.NET., ASPXSPY web shells provide a user interface to connect to a SQL Server database, execute SQL commands, and display the results in a table.

Interestingly, the Menlo Labs team report that a hardcoded User-Agent string is inside those scripts that, when decoded, reads “XeThanh|XeGroups”. The “ismatchagent()” function checks if the user agent matches this pattern, and it will return true if the user agent contains either “XeThanh” or “XeGroups”. If the string is not present in the communications, the web shell returns a fake error page.

#4 – Credit card skimming

Primarily, these web shells have been used to conduct credit card skimming activity – something the Menlo Labs team has observed across our customer base.

The reference to XeGroups is repeated throughout the threat actor code infrastructure, as is reference to “XeThanh”. In fact, in a 2010 sample, we see user XeThanh’s earlier card skimmers where contact information was left.

We analyzed several samples of the credit card skimmers used by this group and noticed that there were minor differences in the evolution of the code, but the overall functionality stayed the same. Through this analysis, however, we were able to retroactively look and find other samples from this group.

Indeed, as far back as 2014, the threat actor was seen creating autoIT scripts that automatically generated emails and a rudimentary credit card validator for stolen credit cards.

Combatting diverse attack methods

In examining the WHOIS history of the threat actor’s sites, the Menlo Labs team was able to uncover email addresses and other identifying information that could be used for attribution. Scouring through mounds of data, we uncovered many instances of the name Joe Nguyen together with the string “XeThanh” across the Internet.

Armed with this information, we diligently began utilizing OSINT tools to maximize data collection, leading to the discovery of additional information. Indeed, we found that Nguyen Huu Tai, who also goes by the names Joe Nguyen and Thanh Nguyen, has the strongest likelihood of being involved with the XeGroup, while the email address xxx.corp@gmail.com is also highly likely to be associated with the group.

XeGroup ultimately remains a low to medium threat level hacking group. However, the fact that it continues to threaten a variety of sectors with a variety of techniques despite significant efforts to dismantle the group is concerning.

Indeed, the group's use of a combination of increasingly sophisticated attack methods again highlights the importance of organizations advancing their security setups, moving away from an overreliance on outdated detect and remediate solutions and towards technologies capable of stopping 100 percent of attacks in their tracks.

About the Author

Brett Raybould - EMEA Solutions Architect, Menlo Security. Brett is passionate about security and providing solutions to organisations looking to protect their most critical assets. Having worked for over 15 years for various tier 1 vendors who specialise in detection of inbound threats across web and email as well as data loss prevention, Brett joined Menlo Security in 2016 and discovered how isolation provides a new approach to solving the problems that detection-based systems continue to struggle with.

How Ai Can Be Used as A Tool to Help Monitor for Cybercrimes and Keep Kids Safe From Cyberbullying And Scams

By Ron Kerbs, CEO of Kidas

Machine learning (ML) and classifiers have been used as cybersecurity tools for years. Starting in the 1990s, machine learning techniques began detecting known attacks and deviations from normal system behaviors. In the beginning of the 21st century, machine learning tools analyzed traffic and communication to understand abnormalities. This was the rise of data-driven approaches. The availability of copious amounts of data and computational power in the 2000s enabled significant advancements in machine learning. At first, machine learning was used at the network and system level which gave rise to intrusion detection systems (IDS) emerged. These systems used ML algorithms to analyze network traffic and identify suspicious activity to find viruses and malware.

In the last few decades, companies like Meta, Google and Twitter have relied on Natural Language Processing (NLP) to detect other types of threats - social threats like scams, hate

speech and bullying on social media. The NLP solution to monitor communications on social media is accurate but not accurate enough to cut moderation team budgets. In fact, these companies have large moderation teams.

Recent developments in large language models (LLM) like OpenAI GPT-4 enable companies to improve the performance of moderation task accuracy.

The Problem

Currently, I see three main challenges to getting these models to a place where they are good enough.

1. Availability of data

The models are trained on big data sets. To monitor gaming or social media DMs correctly, you need access to this specific data. However, this data is private and/or not accessible as it is private between users. This is not the core competency for many of these businesses. Though they may recognize the need to develop these systems internally, it often detracts from the company's core mission. Furthermore, these companies are reluctant to share data externally as it's extremely valuable. Take, for example, Reddit and Quora - both started charging for data even though it is available online. In a TechCrunch article, Reddit CEO Steve Huffman said that the data shared on Reddit is extremely valuable. He goes on to say that many of the users feel so comfortable in the community, that they share things that they may not feel comfortable sharing elsewhere. "There's a lot of stuff on the site that you'd only ever say in therapy, or AA, or never at all," Huffman is later quoted saying. With access to that information, Reddit saw an opportunity to sell it instead of giving it to large companies for free.

2. Change in slang and communication type

Slang is an ever-evolving aspect of language that changes over time. It reflects the cultural, social and generational shifts within a society. The evolution of slang can be influenced by numerous factors, including technology, pop culture, social movements and globalization. For example, current movies, television shows and music influence the slang that people use. Catchphrases, expressions and words popularized by celebrities or influencers can quickly enter mainstream language. Technology and the internet have also had a significant impact on slang as it has created spaces for people to communicate in an abbreviated language with words like "LOL," "OMG" or even emojis. In short, people change their slang words and use new emojis, etc. either to intentionally mislead the algorithm or because language changes very quickly. As long as these models are not trained regularly, they will miss a lot as language evolves. However, training such a huge model costs a lot of money and computation power, so it is almost impossible to train on a day-to-day basis with current computation power and costs.

3. **20/80.**

In general, there is an unwritten understanding that if it takes 100 percent effort to get to 100 percent accuracy - 20 percent of the effort is invested in getting to 80 percent accuracy, and 80 percent of the effort is needed to improve accuracy by an additional 20 percent. In other words, the last improvement and movement towards perfection in the finetuning of machine learning is always the longest stretch. Moving from 95 percent accuracy to 99 percent is hard but from 99 percent to 99.5 percent accuracy is the hardest.

The Solution

While it is tempting to try to use LLM for monitoring, a better bet would be to use specific models for each task. For example, a model for scams, a model for hate speech, and so on. This results in a much more cost-efficient and easier-to-train algorithm. LLM can undoubtedly assist in creating or validating training sets, but it muddles efficiency.

AI can be a powerful tool in monitoring and addressing potential cybercrimes to keep children safe from cyberbullying and scams, however, at this time, it's best used to assist in monitoring and mitigating potential cybercrimes. It should be complemented with human judgment and oversight. At this stage, human involvement is crucial for interpreting AI generated alerts, addressing false negatives or positives and providing emotional support and guidance to those, especially children, in potentially harmful situations.

I believe we will achieve artificial general intelligence (AGI) at some point, but in the next decade, specific expert-trained algorithms will continue to outperform LLMs for these tasks at a fraction of the cost.

About the Author

Ron Kerbs is the Founder and CEO of Kidas. Ron has a decade of experience in leading technology teams and investing in early-stage startups. After volunteering in various children-focused NGOs, he decided to address the problem of gaming toxicity. Ron can be reached online on Twitter, Instagram and at Kidas' company website https://getkidas.com/.

What to Consider When Choosing Cybersecurity Insurance Coverage

By Richard Clarke, Chief Insurance Officer, Colonial Surety Company

Despite the fact that marquee corporate names like Meta, T-Mobile, and Morgan Stanley have shelled out hundreds of millions of dollars in fines and settlements for data breach lawsuits in the last few years, cybersecurity victimization is no status symbol, nor is it confined to enterprise companies. In the endless battle of attrition against cyber criminals, CISOs and leaders deploy automated security software solution stacks, rigorous corporate policies and procedures, and education-awareness programs. Since cyberattacks succeed despite their best efforts, they are adding cybersecurity insurance to their cost of doing business.

The costs associated with a data breach have grown staggering, including costs of forensic investigations, legally mandated customer/employee notification costs, business interruption costs, expenses in identifying the cause of the breach, and non-compliance fines – and now there's the cost of legal defense and settlements in fighting lawsuits. Attorneys and consumers have become increasingly aware they can sue the companies if data is compromised. The cyber insurance market is growing at a 20% clip every year, and the cyber liability insurance market increased 3.9% in 2022. Yet when examining cyber insurance proposals, executives may have

difficulty in distinguishing individual insurance policy provisions, as well as pinpointing the exact differences between cyber liability insurance and data breach insurance, often unsure as to what these insurance policies may or may not cover.

Small businesses are not spared from data security lawsuits

According to the 2023 Data Security Incident Response Report, lawsuits being filed in response to breach incidents has grown rapidly since 2018, including a marked increase in lawsuits responding to incidents where fewer than 100,000 people were impacted and even four suits in which 1,000 people or less were impacted. For smaller organizations in particular, cybercrimes can be catastrophic. In a National Cybersecurity Alliance study, 25% of small businesses that experienced a data breach filed for bankruptcy and 10% went out of business. Yet, only about one quarter of small to medium-sized businesses carry cyber insurance. SMBs leaders are under particular pressure to acquire the best possible data breach and liability protection at the lowest possible premium, a difficult task given the rising premiums.

Certainly, not all cyber insurance products address the same exposures. Some policies may offer an enhanced approach to coverage that includes breach response services, mitigates damage, provides for business interruption loss, and insures the obligatory investigation and notification are included and properly addressed. Some offer defense for litigation expenses, as well as regulatory actions. To execute proper due diligence when selecting cyber insurance protection, buyers need to fully understand what their cyber exposures are, what comprehensive cyber liability insurance protection can provide as opposed to breach insurance, and its coverage approach.

Data breach insurance defined

Data breach insurance confers very specific protection in the event that the insured organization suffers a data security breach. Individual insurers may vary in the way they define a data breach, so it bears close attention when shopping. A breach might come in the form of anything from stolen customer/employee data to a dumpster diving situation in which a third party is able to commit identity theft by piecing together correlated customer/employee information after going through the organization's discarded files. Many cyber insurance policies cover some variation of these exposures. Ideally, the insurance policy covers assistance at every stage of incident investigation and breach response, helping businesses navigate their legal obligations in the event of an attack.

However, data breach insurance does not necessarily require allegations of negligence, nor does it provide defense expense coverage, in many cases. Coverage either exists for the specific data breach situation or not, depending on the circumstances of the claim being made and coverage provided (or not) by the specific cyber insurance policy.

Cyber liability insurance defined

The term “cyber liability insurance” is not universal terminology, but generally refers to one or more insuring agreements in a cyber insurance policy, which would defend the insured organization/persons from covered allegations as well as pay settlements/judgments on behalf of the insured organization. The core insuring agreement in most cyber insurance policies usually involves insurance for allegations of “network security liability” or “breach of privacy liability”, or some combined version of both. Simply put, the coverage provides generally broad insurance protection primarily involving allegations of negligence, with a focus on defending the insured organization, including insured persons, and payment of settlements/judgments.

Data breach policy or cyber liability?

Organizations can pick and choose which coverages they wish to insure; although the majority almost always opt for both coverages. Most business insurers have similar policy forms for basic liability insurance, commercial general liability, and directors & officers liability insurance. But there are usually significant variations between one cyber insurer and another. Both buyers (and sellers) of cyber insurance should carefully review their coverage policies, and ideally have a basic understanding of their risk exposures to ensure that the coverage purchased is technically adequate in addition to being acceptably priced.

Depending on the individual policy, in some cases endorsements for data breach situations could be added to another type of commercial insurance policy such as property insurance. This is a less costly but much more limited approach to coverage than a specific cyber insurance policy, which almost always includes coverage for the cyber liability exposure. Not only are companies trying to adapt to the emerging cyber risk vectors, but insurance carriers are as well. Security leaders should seek out non-traditional providers or insurtechs that have online tools, flexible term and payment options, flexible coverage options, and customized value-added services instead of traditional policies that are inflexible and limiting, within a commoditized market.

Vigilance against cyber threats, diligence in mitigating cyber risk

How does the buyer know which cyber insurance is most appropriate for their exposures? It’s an answerable question that requires some due diligence. Business leaders can rely upon a trusted insurer or agent to provide acceptable coverage. If they have successfully assessed their cyber risk exposure, they can employ a basic coverage checklist cross-referenced against the policy proposal. Insurance buyers would be wise to do some easy research into whether the insurer tends to pay claims promptly and without friction, checking websites that track data breach situations, like www.privacyrights.org and www.idtheftcenter.org.

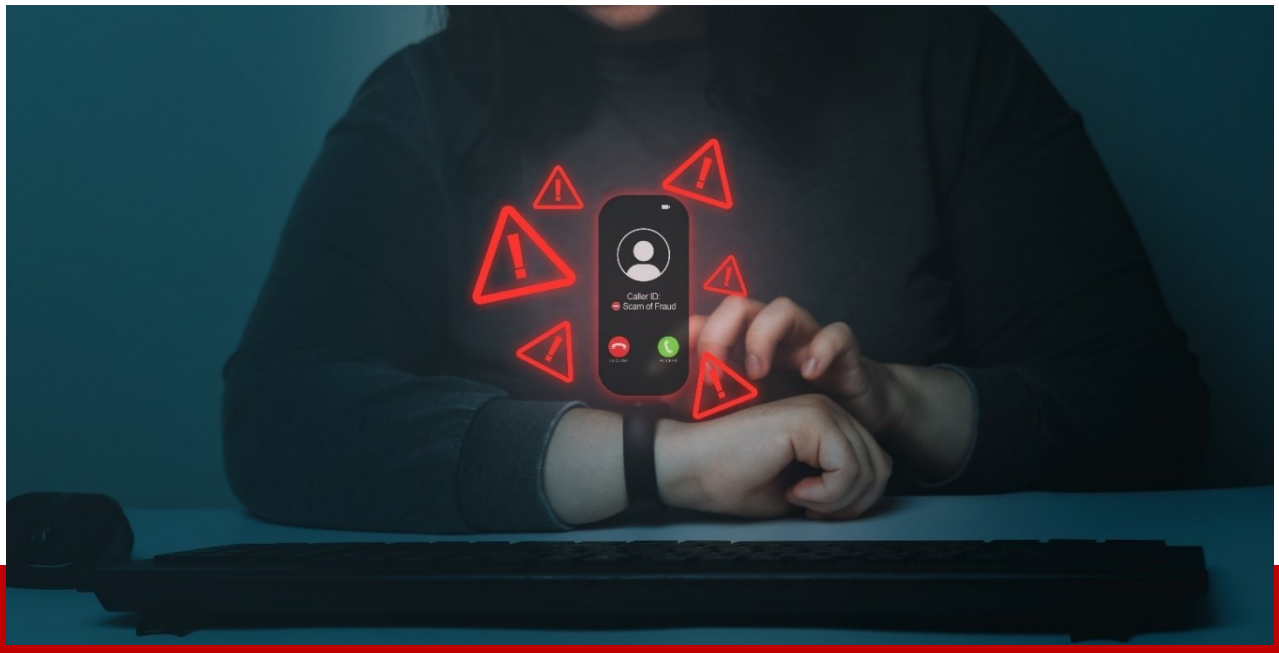
Cyberattacks are rising, despite numerous cybersecurity solutions and zero-trust approaches in the market, feasting on an ever-widening attack surface from the proliferations of hybrid work, enterprise cloud adoption, IoT, blockchain, and now generative AI tools. To mitigate the unwieldy

risk environment and to stay competitive in recessionary times, it has become mission critical that organizations, especially small and medium-sized enterprises, find insurance solutions that insulate their businesses from destructive cyber threats and data breach lawsuits that hit the bottom line and the brand reputation.

About the Author

Richard Clarke, Chief Insurance Officer, Colonial Surety Company. As an insurance industry veteran with more than three decades of experience, Richard is a Chartered Property Casualty Underwriter (CPCU), Certified Insurance Counselor (CIC) and Registered Professional Liability Underwriter (RPLU). He leads insurance strategy and operations for the expansion of Colonial Surety's SMB-focused product suite, building out the online platform into a one-stop-shop for America's SMBs.

For more information about Colonial Surety Company visit our website: https://www.colonialsurety.com/.



TikTok Ban: The Death Knell for Free Access to the Web?

By Sebastian Schaub, CEO, hide.me

Chinese tech company TikTok is firmly in the headlights as authorities in the US continue to scrutinise the App due to worries over a possible threat to national security. Things have just significantly ramped up with Montana becoming the first US state to ban TikTok. This move has seen Governor Greg Gianforte signing legislation that would prevent mobile application stores from offering the app state-wide by next year. Is this series of escalations against TikTok in the US justified in the face of national security concerns or are we seeing yet another example of a nation state looking at ways to throttle free access to the web for its citizens?

There is clearly concern about the use of Chinese technology given the backdrop of tensions between the West and China on the geopolitical stage. We have witnessed similar unease in the UK with respect to Huawei. The UK government has ruled that Huawei technology must be removed from the UK's 5G public networks by the end of 2027 under legal documents that were handed to broadband and mobile operators. In the US, both the federal government and more than half of US states, have prohibited the TikTok app on government devices. In response, TikTok's parent company Bytedance has repeatedly denied that it has ever shared data with the Chinese government and has also stated that it would deny any such request should it be asked to do so in the future.

And governor Gianforte has taken things a step further by prohibiting the use of all social media applications that compile any personal information / data to perceived foes on any government-issued devices. Specifically, we are talking about WeChat (Chinese parent company) and Telegram Messenger (established in Russia).

As a VPN service provider, we know only too well that the folk in Montana can easily bypass any such ban by using a virtual private network. By using such a service, users are effectively encrypting their data traffic and denies others from snooping on their web browsing activity. But there is already mounting anger by those who consider the moves as nothing more than authoritarian deception; indeed, those who advocate for a 'free' internet are openly critical of the US authorities, decrying their actions as overall censorship.

The situation in Montana is yet another example of living in an era where the concept of internet freedom is very much under threat. We have witnessed a whole host of examples just over the last couple of years whereby governments in countries such as India, Russia, Indonesia, and China have taken steps to exert greater control over their internet territory. It is a common defence to claim that their actions are to strive for greater good - to provide safety for citizens, to prevent crime or to uphold a particular moral standpoint. What they really want is greater control over their citizens. They want the power to spy on them or be able to eliminate any platform from which they can exercise freedom of speech - banning such a popular app like TikTok is precisely doing this. Blocking or limiting access to 'undesirable' social media platforms or apps all boil down to one thing - denying internet freedom. To enjoy true internet freedom citizens everywhere should be able to freely share ideas, knowledge and opinions. This is the cornerstone of free speech and democracy. TikTok has already stated that the Montana bill basically infringes on the first amendment rights of the people of Montana by unlawfully banning TikTok. The company has also declared that they intend to defend the rights of their users both inside and outside of Montana.

The concept of internet freedom covers a whole host of considerations - net neutrality, freedom of information and the right to internet access as prime examples. We believe that establishing a free global internet should be an international priority. The current sentiment of governor Gianforte and the powers that be in Montana, certainly fly in the face of internet freedom. We can only hope that this sort of ban is short-lived and doesn't spread across the country - otherwise, what technology is next in the crosshairs?

About the Author

Sebastian is the Founder of hide.me VPN and he has been working in the internet security industry for over a decade. He started hide.me VPN to make internet security and privacy accessible to everybody.

Sebastian can be reach through our website http://www.hide.me.

Three Ways to Protect the Data Powering Summer Vacations

By Amit Shaked, CEO and Co-Founder, Laminar

The travel industry is in the midst of rapid recovery following the COVID-19 pandemic. In 2022, there were over 747 million passengers who took to the skies, a 125.9% increase from the year before. Experts predict that travel will recover to pre-pandemic levels before the end of 2023.

The hidden force behind each airline powering safety, travel paths, aircraft repairs, and the customer experience is data. It is estimated that the average aircraft creates more than 20 terabytes of engine information an hour — and this is only a portion of the story. From purchasing a ticket, to scanning an ID, and any meals or drinks bought on a plane, airline employees and customers are constantly creating and exchanging data. All of this data can be used to contribute to a better experience overall for pilots, flight attendants, and passengers. However, businesses must act judiciously to safeguard the security, privacy, and governance of such data.

The aviation industry has seen a steady rise of cyberattacks since 2020. At the beginning of the year, the Transportation Security Administration (TSA) said it was investigating a potential

cybersecurity incident after a researcher discovered a copy of the 2019 no-fly list on an unsecured internet server. The list contained names and birthdays of individuals prohibited from flying on commercial flights going to, from, or within the U.S. Adversaries aren't just interested in data pertaining to national secrets, they seek sensitive personal information too. Last year, threat actors also breached Pegasus Airlines and were able to access 6.5TB of sensitive data, which included source code, staff data, and electronic flight bag data.

As the busy summer travel season begins, it is critical that the aviation industry and its partners take the right steps to protect its most valuable assets: its data.

Cloud Apps in the Clouds

To stay competitive, domestic and international airlines are compelled to focus on two main elements of business: first, elevate the goods and services they provide to meet the ever-growing expectations of the modern traveler, and second, constantly innovate new ways to improve things like safety standards, on-time arrivals, comfort, price, and so on. In both of these instances, speed and freedom to innovate are essential.

When it comes to innovating the customer experience, it's clear that in 2023, in-flight WiFi is just the beginning. Now, airlines are offering more ways of entertainment and convenience with a long list of cloud-based amenities. Passengers on a flight can connect with other passengers to compete against them in games and connect socially. Travelers can even shop for last-minute merchandise in the clouds to be picked up at their destination terminal. The extent to which airlines will go to please their customers is unmeasurable, yet it may come at a cost. These amenities, while alluring, contribute to the proliferation of data, often sensitive data such as payment information or access credentials. In this environment, it's common for unknown or "shadow" data to lurk unknowingly throughout the organization's network.

Visit any major airport around the world and you'll notice travel has been one of the biggest beneficiaries of the world's move to the cloud. Facial recognition, wearables, and virtual reality are all being applied by many airlines to improve travel experiences and make flying easier and safer for passengers. AI is also being used to help the industry advance sustainability efforts, such as the conservation of fuel, reduction of food waste, predicting logistical disruptions, and more.

The proliferation of data in the aviation industry translates to a higher risk of adversarial activity and has led to user data ending up in the wrong hands many times over. Unfortunately, data democratization, which has enabled the activities that create the biggest advantages for cloud-based businesses, are the same activities that introduce the most risk. This is mainly due to the fact that cloud data is extremely challenging to produce largely due to lack of visibility.

Taking Visibility & Security to New Heights

Over the years, cloud computing and digital transformation have expanded the exposed attack surface that IT teams need to defend. Developers using SaaS applications and cloud storage platforms don't hesitate to deploy new databases without the consent of knowledge of IT, which leads to an extremely limited view of data across the environment. This problem is compounded by the fact that there is often a lack of context – whether the data is sensitive/confidential or not – that leads to inefficient allocation of resources.

The exposure of data across a hybrid or multi-cloud environment, combined with this lack of comprehensive visibility, makes it impossible for many organizations to assess their data security posture accurately. Not all data is created equally, some require more protection than others. Still, security controls are often applied uniformly for the entire environment rather than understanding the context and prioritizing data security efforts accordingly. The complexity of the environment also makes it virtually impossible to monitor for attacks in progress or detect data leaks effectively.

Protecting data across an increasingly complex web of platforms and applications is a challenge facing the aviation industry. However, it is possible to take advantage of the agility and scalability of cloud computing without sacrificing data security.

Elevating Data Protection

It's clear that the cloud has significant benefits to the aviation industry, from improving travel safety to enhancing traveler comfort. However, today's aviation industry must adopt modern cloud data security solutions in order to address the unique challenges of protecting its data in the cloud.

The aviation industry can create value by empowering developers and data scientists with stronger data protection techniques that safeguard sensitive, regulated, and proprietary data in the cloud while still offering a high level of speed, convenience and innovation. This is often referred to as agile cloud data security.

Agile cloud data security is built on four primary components: discovery, prioritization, security, and monitoring. Starting with discovery, organizations need complete data observability for everything in their hybrid, multi-cloud environments. They must know what data they have, who owns it, and where it is located. Data security and data governance both require that there is a way to find, characterize and classify known data and "shadow" or unknown data across the entire environment. That data must also be prioritized by understanding the context of the data and prioritize protection accordingly. Analyze the data and where and how it is used so that data security can be analyzed based on a variety of factors, including the sensitivity of the data, the current security posture, governance and compliance mandates and exposure.

Only after an organization's data is discovered and prioritized can it then truly begin to strengthen its security posture. This entails a reduction and minimization of the attack surface and enforcing data security best practices and established data policies. Lastly, effective cloud data security requires vigilance. IT teams should be detecting new data assets or changes to existing assets

and continuously monitor the environment for access anomalies and indications of data leaks or compromise.

The benefits of agile cloud data security are more control over data, a reduction in the innovation attack surface, and more secure support for the daily activities of the value creators. Most importantly, agile cloud security transforms the role of security teams from gatekeepers to gate openers, which is critical to enabling innovation in the aviation industry. With more innovation, the aviation industry can help protect its own bottom line as well as the millions of passengers it serves every year.

About the Author

Amit Shaked is CEO and Co-Founder of Laminar, the first agile data security platform that provides organizations the visibility and control they need to achieve data security, governance, and privacy in the cloud. The Laminar Data Security Posture Management (DSPM) solution continuously discovers and classifies all cloud data, structured and unstructured, across managed and self-hosted data stores, including unknown shadow data, without the data ever leaving the organization's environment.

Prior to founding Laminar, Shaked served in Unit 8200, an Israeli Intelligence Corps unit of the Israel Defense Forces where he was focused on collecting signal intelligence and code decryption. In the military, Shaked earned a master's degree in AI and deep learning. Following Unit 8200, Shaked went to large-stage startup Magic Leap which gave him valuable internal security experience.

Triple Tactics

How APIs are being Targeted with Trinity Attacks

By Andy Mills, VP EMEA, Cequence Security

Application Programming Interfaces (APIs) are growing twice as fast as traditional web traffic but their popularity and their exploitability also makes them a prime target. Out of just over 20 billion transactions observed during the first half of 2022, 16.6 billion were found to be malicious, according to the CQI API Protection Report 2022, equivalent to around 83 percent. But the ways in which these interfaces are being abused is evolving.

The primary ways in which APIs are attacked or abused have been documented in the OWASP API Top Ten. The report found that two types of attack led the pack: the exploitation of Improper Assets Management (API9 in the OWASP list) and Insufficient Logging and Monitoring (API10). The former was favoured by those deploying shopping bots while the latter was used to carry out content scraping. But the report also unearthed a previously unobserved pattern. Malicious attackers were now combining the tactics, techniques and procedures (TTPs) detailed in the OWASP Top Ten in order to abuse perfectly coded APIs.

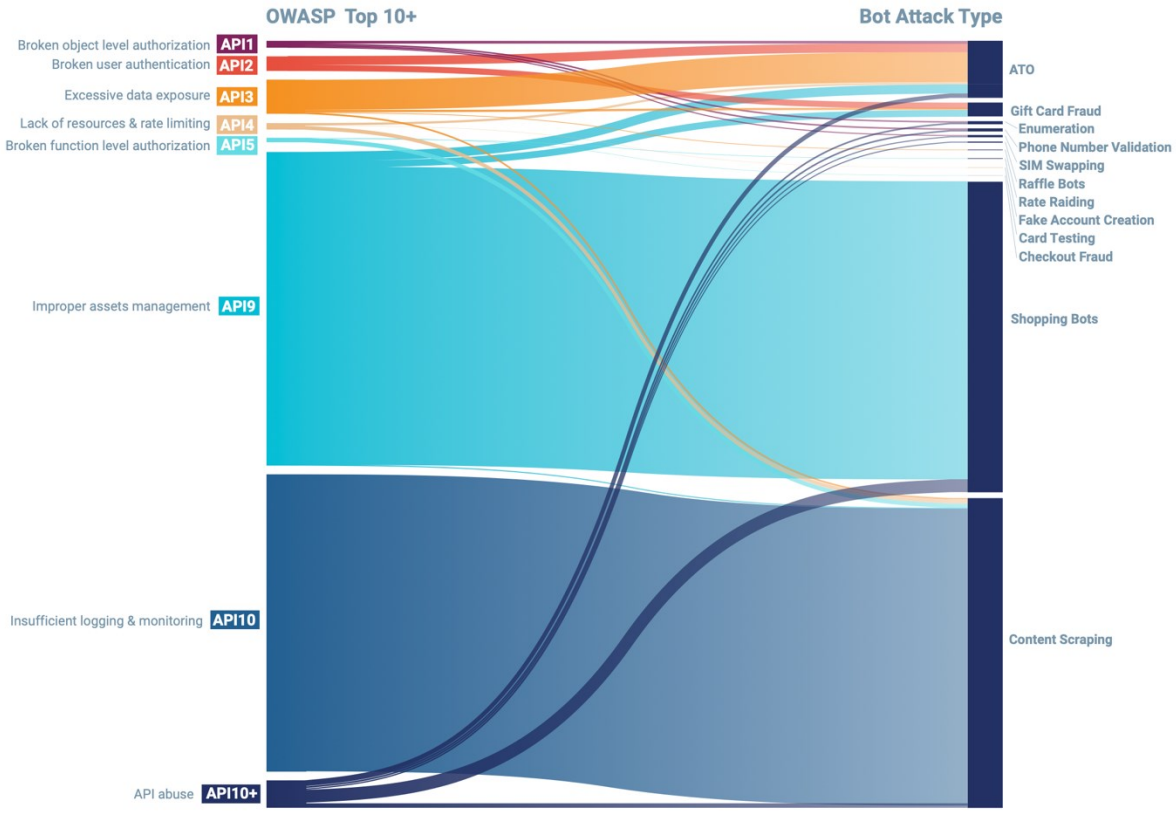


Figure 1: Mapping of OWASP API Top 10 attack types and bot attacks 1H 2022

Contrary to popular belief, even if the API is coded perfectly correctly, adheres to the API specification it is designed against, is properly inventoried and has been tested to ensure it is not susceptible to any of the OWASP Top Ten API Threats, it can still be probed and compromised. This is because, while shift left efforts to test APIs pre-production are beneficial, no measures will stop a persistent automated attack. If the assets being protected by that API are attractive enough, attackers will persist and will compromise it usually by using its own functionality against it in an attack known as business logic abuse.

Perfectly coded and inventoried APIs do, of course, take much more effort to compromise. They need to be studied to see how they work, how they interact with one another and what the expected outcome of any API call should be to avoid triggering an alert. Learning and exploiting an API and using its own functionality against it is often referred to as Business Logic Abuse and it's this that is now on the up as API development and security during production improve.

Trinity Attacks and API10+

One such form of abuse is the trinity attack. This sees the combined use of Broken User Authentication (API2), Excessive Data Exposure (API3) and Improper Assets Management (API9) from the former OWASP Top Ten to create a chimera of an attack. Trinity attacks are a form of combined or API10+ attack that are still relatively small in number, with 100 million registered by the report, but the rate at which they are occurring is ramping up, as can be seen from the graph. It's a worrying trend, as it suggests more attackers are catching on to using this approach.

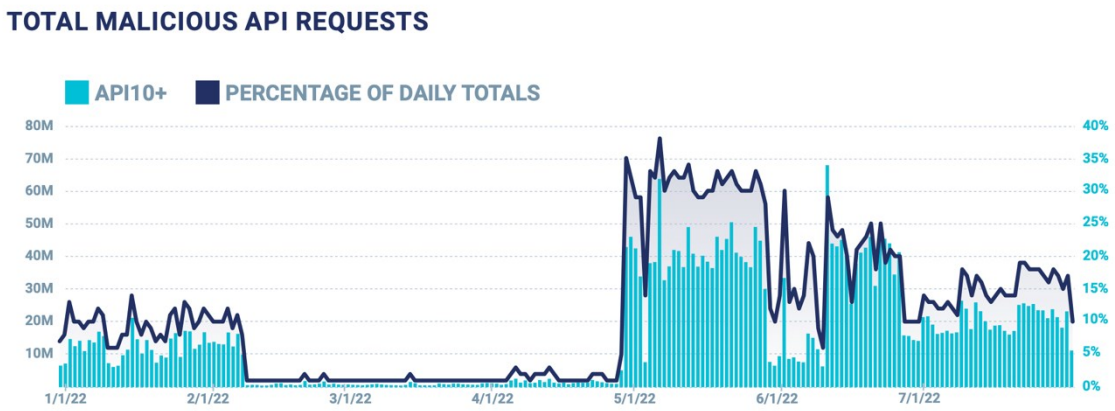


Figure 2: Growth in the number of API10+ attacks during 1H 2022

Trinity attacks can be devastating. So how might they manifest? Broken User Authentication can result in credential stuffing, whereby the attacker targets the authentication mechanisms that protect user integrity. A successful credential stuffing campaign will often utilise a checker functionality that checks user confirmation APIs for sensitive customer data which can be stolen immediately after login. Excessive Data Exposure results when the checker APIs return more data than necessary, giving the developers a false sense of security because the user confirmation happens after authentication.

The combination of APIs exposing too much (personal) data and those that are vulnerable to credential stuffing therefore makes this deployment a ripe target for API abuse. And finally, the attacker can further the attack through Improper Assets Management. This typically resulst in Shadow APIs ie APIs that fly under the radar of the security team which are to all intents and purposes invisible. These shadow APIs allow the attacker to then enumerate the victim's infrastructure using the known API patterns to discover and establish other APIs that are unprotected and vulnerable to the credential stuffing and exposed excessive data vulnerabilities we've just covered.

An eCommerce Attack

Such attacks are highly organised and well executed. Take, for instance, the case of an ecommerce platform that was targeted last year in a bid to automatically purchase items with stolen credit card data.

Reconnaissance was conducted by mapping the entire site using commonly known vulnerability scanning tools from a single IP address. This included some basic behaviours like SQL injection, command injection (OWASP API8), directory traversal, and searching for exposed sensitive files. When basic recon did not yield any low-hanging fruit, the attacker moved on to mapping the API ecosystem.

The attackers then began using existing attack configurations from well-known bot automation tools like OpenBullet to perform basic credential stuffing and account creation attacks. During a 24-hour period, they initiated more than 1.5 million requests from 130,000 IP addresses, which were effectively mitigated through the use of over 1,000 behavioural fingerprints.

However, the attack continued even as it was mitigated, leading to the discovery that this was ultimately a feint by the attackers and was not the end goal. During the following attacks, the reconnaissance behaviour returned, this time focusing on account creation and checkout APIs.

The attackers discovered that upon creation of a brand-new account, and before email verification had taken place, the checkout APIs (particularly those to add a payment method) could be invoked by the user. This is an example of Broken Function Level Authorisation, because this API functionality was intended to be used only by users who were both authenticated and authorised.

The focus of the attack then shifted to account creation, and the attackers immediately began stuffing new (fake) accounts with stolen payment information, targeting retail products for purchase. They did not care that the credential stuffing campaign was failing because they were watching which of the new accounts they had created would be able to successfully access payment APIs, iterating through the stolen credit card details until they found one eligible to continue with the purchase.

Mitigating Multi-Faceted Attacks

As can be seen from this example, spotting trinity attacks is difficult without behaviour-based monitoring and analysis. If the business is not looking for attacks that seem to be making legitimate requests but in large volumes, this activity won't be seen as a red flag.

Many organisations have seen their API infrastructure grow organically over time and so they start out with, and continue to rely upon, security solutions designed to monitor and detect web applications such as Web Application Firewalls (WAFs). These solutions use a signature-based alert mechanism and are therefore unable to detect and block let alone defend against trinity attacks. Others may rely on their bot tools but these use Javascript to determine and block an

attack. RESTful APIs use JSON or XML, not Javascript, which means they cannot be monitored by bot software.

As there is usually a bot element to trinity attacks, it also makes sense to join up API and bot monitoring security. Such attacks enumerate at speed across the infrastructure so are often automated by bots. But given that WAFs are blind to high volume attacks making legitimate requests from the API and that the bot solutions cannot read API payloads, these attacks simply bypass them both undetected and unchallenged. Unfortunately, this lack of understanding of the relationship between bots and APIs continues to persist with the two often treated as separate problems by security vendors.

It's an artificial distinction that plays right into the hands of the attackers which is why it makes more sense to look at API protection as an issue that requires bot detection and mitigation as well as management of the API's security through discovery, detection and defence. So where should the business start?

Discover, Detect and Defend

Initially, it's imperative that you get on top of your APIs by determining how many you have, what they do, and that you make provisions to be able to document any changes on a continuous basis using a runtime inventory. Surprisingly, those responsible for their API ecosystem often rarely know how many they have and routinely underestimate the numbers, as a result of which it can be easy to get overwhelmed when this discovery is performed. However, as the risks posed by APIs will differ, it's relatively simply to prioritise them.

Some APIs will be purely informational while others may expose sensitive data such as personally identifiable information or credit card data. Some may not be properly authenticated, while others may be prone to business logic attacks like account takeovers or scraping. Risk assessing the APIs will therefore allow the business to prioritise the inventory but keep in mind that the risk posed by an API can change over time. Attackers can and will continue to probe APIs for weaknesses, and a problem with configuration or a connection to a less secure system could introduce new vulnerabilities.

With the inventory in place, you can consider what runtime protection to put in place. This should scan for business logic abuses, data leaks and other common attack types as covered by the OWASP Top Ten but it should also be able to cope with changes in the attack landscape by drawing upon machine learning technology to carry out threat based and behavioural analysis. This can determine the intent of the transactions (whether performed by bots or individuals) and continually track sophisticated API attacks as they retool to evade detection. Action can then be taken to block or deflect the attack, from basic block and rate limiting to HTTP header insertion and deception.

The API Lifecycle

It's only by looking at the entire API lifecycle that the business can hope to protect its APIs from both current and emerging forms of attack. From security testing at development, through to managing the API as part of an ecosystem that is tracked and managed using a runtime inventory, to active defence that looks for attack patterns, there needs to be a cradle to grave approach.

The trinity attack indicates that attackers are getting much more adept at analysing how each API works, interacts and performs. It's a significant upping of the ante in the API security stakes and, at the moment, many of these attacks are going undetected and unchallenged simply because organisations don't know they're happening until it's too late.

To stop them, we need to take a new approach to how we secure APIs and start using the same joined up thinking that the attackers have already demonstrated. API attacks are no longer separate and distinct, they're becoming elements of much more ambitious persistent campaigns and so any approach to security needs to adopt the same tactics, by using a wide angle lens to capture every element of the attack.

About the Author

Andy Mills is VP of EMEA for Cequence Security and assists organisations with their API protection strategies, from discovery to detection and mitigation. He's a passionate advocate of the need to secure the entire API lifecycle using a unified approach.

Prior to joining Cequence, he held roles as CRO for a major tax technology provider and was part of the original worldwide team of pioneers that brought Palo Alto Networks, the industry's leading Next-Generation Firewall, to market.

Andy holds a Bachelor of Science Degree in Electrical and Electronic Engineering from Leeds Beckett University. Andy can be reached online at andy.mills@cequence.ai and at our company website https://www.cequence.ai.

Criminals are Bypassing Authentication with Stolen Session Cookies

By Trevor Hilligoss, Director of Security Research, SpyCloud

The last 12 months revealed a concerning trend in credential exposure. According to SpyCloud's 2023 Identity Exposure Report, nearly half of the 721.5 million credentials recovered from the criminal underground in 2022 were exfiltrated by infostealing malware.

Compromised credentials are traditionally one of the simplest entry points in carrying out a successful cyberattack. Using freshly stolen credentials, criminals can avoid setting off alarms when infiltrating networks by posing as legitimate users, giving them free rein to carry out their objectives. One step further than your run-of-the-mill breach credentials is infostealer malware, which is designed to exfiltrate high-quality and quantity authentication data, such as session cookies/tokens, credentials, PII and more.

Security teams are addressing the threat by emphasizing cyber hygiene and implementing solutions like multi-factor authentication (MFA) and, more recently, passkeys to protect valuable

corporate and user data. But while these solutions offer improved security compared to traditional methods, they are still susceptible to compromise.

To truly address the ongoing threat of identity exposure from stolen data siphoned from malware-infected devices, organizations must understand what is driving the growth in infostealer malware and adopt new security approaches that allow them to proactively protect against the threat.

The growing trend of malware

The rise of infostealer malware directly results from the high return on investment (ROI) it provides criminals and the ability to remain undiscovered, even given today's advancements in intrusion prevention.

Often, the primary motivator for Initial Access Brokers (IABs)—individuals and groups who package and sell malware-stolen data on the darknet—is financial gain. The rise of passwordless technology, such as passkeys, aims to provide more secure user authentication and create additional barriers for cybercriminals. However, despite these efforts by security leaders, criminals continue to adapt their strategies to focus on approaches with higher rewards, and these authentication methods are not without their own vulnerabilities.

Infostealer malware is virtually undetectable and often designed to be non-persistent on a victim device, enabling execution and exfiltration of sensitive data in seconds, leaving little to no trace. This low-risk (many infostealers are widely sold online for less than a few hundred dollars per month of use), high-reward investment for criminals has created a bustling underground market where network access is weaponized for monetary gain.

The data exfiltrated by malware is highly attractive to criminals because of its superior quality. Last year alone, SpyCloud recaptured nearly 22 billion malware-exfiltrated device and session cookie records, a number expected to continue growing.

Cookies authenticate users on a platform for a set duration of time. If exposed, they allow threat actors to bypass authentication methods such as MFA and passkeys without needing credentials in a process known as session hijacking.

Breaking passkeys and MFA with session hijacking

Session hijacking occurs when cybercriminals use stolen cookies/tokens to take over an active authenticated web session by importing malware-exfiltrated cookies into anti-detect browsers used by the adversary. This process bypasses authentication security mechanisms and grants access to criminals, allowing them to masquerade as legitimate users and affording all the permissions a real user would have without raising alarms.

Session hijacking can enable criminals to access confidential business data, change or escalate privileges, and launch follow-on attacks like ransomware, as using a valid, already-authenticated

session provides the threat actor essentially unfettered access to internal corporate systems and applications.

Because these cookies, while they remain valid, represent an already-authenticated web session, the method of original authentication—be it a passkey, MFA-validated, or logged-in using a Single Sign-On (SSO) solution—one stolen cookie is all it takes to bypass the entire authentication and login process.

The recent CircleCI breach, for example, was brought on by cybercriminals employing malware to steal an employee's 2FA-backed SSO session token. According to CircleCI, the threat actor used that token to pose as the employee from actor-controlled infrastructure. The company's antivirus protection failed to identify the infection due to the difficult-to-detect nature of malware, and the attacker was able to pose as the employee undetected.

The way forward: post-infection remediation

While solutions like passkeys are not a cure-all, they are not entirely ineffective. They are a strong option for reducing password fatigue and decreasing overall friction in the login process. With over 72% of consumers reusing previously exposed passwords, according to SpyCloud research, they are a beneficial tool for increasing overall security.

But as stolen cookies become a popular method of entry for criminals, its important organizations don't put their full efforts behind one tool. Instead, they should look to processes and solutions that enhance their protection against session hijacking in addition to actively monitoring for stolen data.

The most effective way to protect against session hijacking is to leverage a post-infection remediation (PIR) approach to proactively address the threat before it can become a full-blown security incident.

PIR is an identity-centric approach to malware infections that consists of a series of steps to fully address the exposed data putting your organization at risk. Since malware-siphoned cookies can remain active for months after being stolen, gaining a holistic view of malware-compromised devices is the first step to addressing the problem.

Visibility into what criminals know about your business through recaptured data from the darknet that has been properly ingested, curated, analyzed and automated is an excellent way for security teams to stay a step ahead. With this actionable data, security teams can quickly and seamlessly view when valuable data has been compromised, align it to the user, and then link it to the original malware-infected device for proper remediation.

Next, teams can isolate the infected device and remove the malware before requiring employees to invalidate compromised SSO sessions and data. With insight into the exact devices and data criminals accessed, teams can review all activity and access logs to confirm actions are driven by an authorized user. Future access to sensitive data, regardless of whether it was expected or

not, can also be monitored to ensure that it was initiated by an authorized user. These steps provide an enhanced layer of protection by giving enterprises a comprehensive understanding of their highest-risk users.

An effective PIR approach disrupts cybercriminals before they can harm users and businesses. While passkeys and MFA are great strides forward for the security industry, cybercriminals continue to innovate. By swiftly and proactively preventing unauthorized users from accessing customer and employee accounts, enterprises can effectively address vulnerabilities in their current security frameworks. This approach safeguards employees, customers, brand reputation, and overall company profit.

About the Author

Trevor Hilligoss is the Senior Investigator at SpyCloud and is an experienced security researcher with a background in federal law enforcement. Before leaving government service, Trevor spent nearly a decade tracking both cybercriminal and nation-state actors for the DoD and FBI and has presented at the US and international conventions as a threat intelligence expert. He holds a BA in Sociology, multiple federal certifications in the field of cyber investigations, and two Global Information Assurance Certifications (GIAC).

Trevor can be reached online at https://www.linkedin.com/in/thilligoss/ and at SpyCloud's company website https://spycloud.com/.

Cyber Attacks on Municipalities

What attracts cyber criminals to municipalities and how they can be prevented.

By Veronika (Nikki) Jack, Student Majoring in Information Technology-Cybersecurity, George Mason University

Cyber-attacks on municipalities have been increasing at an alarming rate, this is a cause for concern. The reason that municipalities are such an appealing target to hackers is that they store valuable information and records of many citizens. As local and national governments are changing their method of keeping records from paper to digital and as technology advances, it makes hackers extremely interested in breaking into the systems to extract the data. Municipalities are easier targets compared to private companies because it is known to hackers that their systems can be outdated, making them easier prey to catch.

Our reliance on technology is growing, and more information is being stored on digital platforms. Technology has many benefits and does help speed up every day processes, however, when the proper security measures are not in place they can be hacked.

The breach of a municipality's data can be devastating. When digitally stored data and the IT (Information Technology) infrastructure are compromised, it can cause significant disturbances

and disruptions to normal city functions. For example, a breach in a municipality can impact the city's utilities, emergency services, and local law enforcement, and the community will be affected in a negative way. Attacks on cities threaten the integrity of confidential data. People's information and records are stored digitally, the release of this data includes individuals' personally identifiable information (PII). Data including important documents, records, and information about a person can be leaked to the public or lost.

It is known that local government data are using old and dated technology that is not updated and is running on outdated software versions that could be vulnerable to attacks. When technology is not updated this leads to increased exposure to risks because patches and other security fixes are included in the latest update.

When a system is compromised even by paying the ransom you are not guaranteed that you will get access to all the data, and it can be permanently deleted. Hackers can find exploits online that run specific code or commands to compromise a system. When a zero-day attack occurs, it is especially important that affected systems are isolated from the network so that they are not further affected or contaminate any other devices.

One of the most recent attacks was a breach at a healthcare administrator which targeted employees and staff of the House of Representatives in March of 2023. Information of over a hundred lawmakers was released. When there are breaches like this substantial amounts of personal information could potentially be released and could get into the hands of the wrong people.

One effective way of understanding how cyber-attacks work can be found in the speech delivered last year at the Fairfax County Public School Boards Annual Conference by Adib Sarkar, founder, and CEO of CYB3R8. He stated that "Everything's interconnected these days, from our smartphones to the cloud systems we use. And guess what? Each connection is a potential weak spot for hackers to exploit. It is like playing a game of "Find the Vulnerability," and all it takes is one tiny crack to bring the whole system crashing down."-Adib Sarkar

Devices need to be secured because any small vulnerability can compromise the entire system. There are many ways that hackers can try to get into systems. They can try getting in through vulnerabilities in code or try brute forcing (putting thousands of password combinations until they crack the password) their way into a system, but an easier way is to trick employees using social engineering, which means tricking people into giving out information. For example, some hackers will send out emails disguising themselves as someone else just to get information about a system that they can later get into.

To solve this problem, local governments must make sure their staff are trained to know how to spot and avoid being tricked by something that is malicious. They should have routine password changes and the stored data should be encrypted so it is not easily accessible.

One big reason cities are such a big target for breaches is that their systems are outdated because they are underfunded or do not have enough security measures properly implemented at the scale needed. Investing more money into IT security can help to avoid being a target. Trying to

recover from a disastrous incident such as a large amount of data loss can be detrimental to a city and can lower its reputation.

The reason hackers want this information is to sell people's data on the web and to get insight into companies. A large driving factor for attacks is money, and the more information a hacker can extract, the more they make. If the data the hackers are taking is more current, it is more valuable. Information is usually sold in bulk, and quickly before it can be caught.

"These hackers might want to cause chaos, disrupt services, or steal sensitive information to use as leverage."- Adib Sarkar

To have a secure system, it is important that the technology is updated to comply with new laws and regulations. Data on systems should be audited regularly to check for any anomalies. Old tech should be replaced, and modern technology should be updated regularly because technology constantly evolves and changes. Investing in new security systems and training will be a better way to manage their funding, rather than dealing with a breach which can be devastating.

About the Author

Veronika (Nikki) Jack, and I am a student at GMU (George Mason University) majoring in Information Technology-Cybersecurity. I was named a winner in Cyber Defense Magazine's Young Women in Cybersecurity scholarship program in 2022.

Nikki can be reached online at njack4682@gmail.com.

Six Tips to Ensure a Strong Patch Management Strategy

By Ashley Leonard, CEO and Founder, Syxsense

The proliferation of software applications and updates across the market today has put pressure on enterprise security teams to implement strong patch management strategies in defense against known and unknown threats. In 2022, ethical hackers found over 65,000 new software vulnerabilities, which makes sense in the context of reports that 43 percent of IT and security teams are unable to secure devices at speed and scale. Yet the stakes are simply too high for organizations to forgo patching vulnerabilities, with or without having a dedicated patch management solution in place. Let's dive into some helpful tips to ensure your organization bolsters its security posture and protects its endpoints effectively.

Implement Proper Access Rights

It has become a common practice for organizations to grant employees admin rights, leaving crucial vulnerability patching activities to them. This almost guarantees some level of human error when it comes to patching. IT teams should never trust end-users with patching. Instead, IT teams should follow strict patch management protocols informed by exclusive access policies that restrict users to installing specific applications only after entering their password and block them from installing potentially dangerous software.

Prioritize Patch and Vulnerability Risk

The volume of patches, vulnerabilities, and potential threats can quickly become overwhelming for enterprise IT teams, so it's important to rank patches and vulnerabilities by risk level. To do so, examine the severity ratings for each patch or vulnerability, then assess your environment to understand how exposure could affect your system. If there's a critical vulnerability on one machine in an enterprise environment of 10,000 devices, the risk is different than if you had that same critical vulnerability on 5,000 of your 10,000 devices. Once you've prioritized, focus on applying the most critical updates first.

Don't Rely on "Free" Patching Services

Despite what many users may think, "free" patch tools don't provide all the security needed to safeguard against vulnerabilities. Strictly speaking, many don't offer the reporting needed to guarantee that systems are fully protected. Instead, for instance, they might concentrate on supplying system-specific patches, neglecting other apps (for everything from browsers to business software) that might run on your system. Furthermore, these tools often require coding expertise or integrations to other solutions to actually close up security holes. The total cost of ownership on "free" patching tools, in fact, is generally fairly high. There's a simple fix for this. Invest in solutions offering cross-platform support, reliable third-party patching, and the necessary reporting capabilities to substantiate comprehensive patching coverage.

Never Delay Patching

For patching to be most effective, it needs to be continuous. No software is ever fully protected against bugs. Organizations know this and prioritize patch releases. Nonetheless, the majority of security incidents involve vulnerabilities IT teams haven't gotten around to patching yet. A recent survey reported that 78% of IT teams don't patch critical vulnerabilities within 24 hours – enough time for a threat actor to wreak havoc on a system.

Delayed patching can lead to catastrophe. The Equifax breach in 2017, which exposed 143 million users' personal information, was a consequence of a vulnerability going unpatched for 76 days. Considering that Microsoft deploys patches every month, that's almost three months of ignored patch updates. Organizations that delay patching put employees, partners, and their brands at risk. To be safe, IT teams should automate the patching process to ensure all patches are updated promptly.

Don't Allow Vendors to Auto-Update

Most operating systems and third-party applications run their own auto-updates. At first glance this is great, however users may not be able to install these updates if their devices are locked down, a practice many IT teams do to make sure updates don't break critical business

applications. Additionally, automatic updates can create a false sense of security and often interrupt productivity if triggered during the workday. Instead, IT teams should create their own update schedule and work against their patch management best practices to quickly evaluate new patch releases, test them, and release them into the workflow with the help of automated tools.

Look at the Big Picture

What is considered a risk for the most protected security environments changes daily. For example, WSUS doesn't protect Linux devices and applications running on Java may still be open for attack. A vulnerability in the much-used Google Chrome can provide hackers a way into your company's networks. Do you know what's been updated? Are you sure? It is crucial to stay current on what's happening in your environment, yet the required certainty can be frustratingly elusive. The key is to ensure that you have a patch strategy and protocols in place – and the visibility to assess new threats and make sure updates are happening as needed.

Patch management will continue to evolve alongside the growing number of devices to protect. Sadly, so will the tactics and approaches that cyber criminals use to encroach on your organization's endpoints. Leveraging these tips is one way to ensure that you're prepared for what's next, but the onus is on you to make sure you're not left behind in this fast-paced environment.

About the Author

Ashley Leonard is the CEO and Founder of Syxsense—a global leader in Unified Security and Endpoint Management (USEM). Ashley is a technology entrepreneur with over 25 years of experience in enterprise software, sales, marketing, and operations, providing critical leadership during the high-growth stages of well-known technology organizations.

Ashley manages U.S., European, and Australian operations in his current role, defines corporate strategies, oversees sales and marketing, and guides product development. Ashley has worked tirelessly to build a robust, innovation-driven culture within the Syxsense team while delivering returns to investors.

Ashley has founded several successful technology companies, including NetworkD Inc., with operations in 7 countries. NetworkD made several strategic international acquisitions and then completed a successful exit to Sparxent in 2008. In 2012 he founded Verismic Software and launched Syxsense in 2019.

Ashley can be reached online at the Syxsense company website https://www.syxsense.com.

Overcoming Challenges in Cyber Defense Business Naming in The Age of AI

Actionable Naming Strategies for Founders

By Darpan Munjal, CEO and Founder, Squadhelp.com

Establishing a strong brand identity is key to success in the cyber defense space, and it's becoming more difficult as the industry grows and more businesses open.

Cyber defense businesses are built on trust, and that trust is often created through strong branding. This poses a challenge in a couple of ways – firstly, standing out in any crowded market is hard, but in a market that hinges on trust any big, unexpected branding or naming moves that would usually be a logical way to differentiate yourself as a business have to be approached carefully. Secondly, as naming conventions are so strong in cybersecurity and cyber defense, names are simply running out!

Many names that evoke safety, for example, are taken. The name "Check Point", as in Check Point Software Technologies Ltd, is one example, creating an idea of a vigilant and proactive

approach to cybersecurity. It conveys the idea of safeguarding and controlling access to critical points within a network.

Other more modern naming conventions within the cyber security industry, such as mixing evocative images with the usual conventions of safety and security, have also been around for long enough that many names using this method are taken. FireEye is an example of this sort of name. "FireEye" is impactful and attention-grabbing. It conveys a sense of urgency and alertness, symbolizing the detection and response to cyber threats. The term "fire eye" evokes imagery of intense scrutiny and surveillance, indicating a focus on monitoring and identifying malicious activities.

These narrow conventions and the recent proliferation of new players in the industry in no way means it's impossible to name new cyber defense businesses, but it does mean that as a cyber defense founder you'll have to employ new strategies to come up with brandable, trustworthy, appropriate names. One of those strategies is using AI as a tool to generate great cyber defense naming ideas. We'll look at this, as well as other useful naming strategies for cyber defense businesses.

Creating Trust Through Naming: Choose Names Cyber Defense Customers Will Believe In

According to research, customers associate certain words with reliability, expertise, and security - using this insight, cyber defense businesses can craft names that inspire confidence while setting themselves apart from competition. Here are a few tips to maximize the psychological effect of a name in the cyber defense space:

1. Evoke Emotion: Naming that stirs positive associations such as FortifyShield or SecureHaven can evoke feelings of safety and trust with customers on an intimate level. By emphasizing emotional connections through your name, your business could reach customers further down their psychological spectrums.

2. Create Familiarity and Authority: By including words or phrases which evoke trust from potential clients such as CyberExperts or TrustShield, businesses can establish credibility and gain their confidence. At Squadhelp, we've found that our customers lean towards the following root words for cyber security and cyber defense names: Secure, Encrypt, Firewall, Safeguard Protect, Lock, Shield, Defense, Privacy, and Fortress

3. Stick with Simplicity and Clarity: Simply stated names are easier for customers to remember and project an air of professionalism, while omitting difficult terms or technical jargon will increase accessibility while broadening its appeal. Names like McAfee, BAE, and Sisco all achieve this.

4. Know the Norms: As I mentioned earlier, the cyber defense space is not a place to wildly innovate with naming and branding. So, before you name your business, you should be aware of industry norms.

Usual name types for Cyber defense firms include:

- Made Up/Abstract: Sisco, Sofos
- Acronyms: IBM, BAE
- Mashup: Fortinet, Mimecast
- Founder name: McAfee, Kaspersky Lab
- Evocative: Forcepoint, CrowdStrike, CyberArk

Integrating AI into the Cyber Defense Naming Process: The Possibilities and Limitations

Language models, such as ChatGPT, can be used to generate naming ideas. By providing prompts and parameters, you can tap into the creative capabilities of AI to generate a wide range of potential names for a cyber defense venture. Specifically, AI is great at the brainstorming stage. You can ask ChatGPT to provide words similar to the names of cyber defense firms with names you think are great, for example, or words on a theme such as strength, security, or power.

You can then search for available names that have these words as a part of them or use them as a prompt for an AI-powered name generator such as Squadhelp's to find hundreds of available names and domains suitable for your venture. It's important to note here that AI is a tool and should be treated as such. While AI can generate a vast number of naming options, the human element is still crucial in making appropriate and original choices. Creativity, intuition, and cultural sensitivity are all needed to pick a genuinely great name that aligns with your company's vision and values and resonates with your target audience.

Trademarks and Cyber Defense Naming

It's important to keep trademark checks in mind when naming, particularly in a crowded industry. My advice is always to run trademark checks and audience testing on a handful of names before getting too attached to one. It may simply be too close to another business name in the same sector, particularly in an area like Cyber Defense where naming trends are strong and don't change at speed.

Modern Naming: Challenge and Opportunity Come Hand in Hand

Naming a cyber defense business in 2023 presents unique challenges due to growing competition and an ever-evolving industry landscape. But by understanding trust psychology, leveraging language norms, and welcoming innovative new technologies as solutions, businesses can effectively navigate these hurdles.

Crafting compelling yet trustworthy names helps establish brand recognition, and strong brand identity elements around a name – such as logos and taglines – can give you that extra push you need to stand out in the cybersecurity and cyber defense sector. Remaining adaptable and forward thinking are necessary traits necessary for cyber defense companies' lasting success, so integrating AI into their naming processes for new businesses and products is a logical step forward for the industry as a whole.

About the Author

Darpan Munjal is the CEO and founder of Squadhelp.com, a brand-naming platform with more than 30,000 customers and 300,000 creatives globally. Munjal is a serial entrepreneur and has over 25 years of experience leading internet-focused businesses.

Darpan can be reach at @darpanmunjal.

Why IT Governance and Mitigating Risk is a Critical Part of Cyber Defense

Organizations must recognize how every solution they implement works together and as part of their larger defense-in-depth strategy.

By Vincent Tran, CISSP, Co-Founder and Chief Operating Officer, Liongard

So much of the discussion around cyber security focuses on the need to bolster defensive systems and procedures, but these discussions are missing the most basic components of a security posture: IT governance and mitigating risk.

The continuous proliferation of systems and configurations, along with threats facing businesses, are real and ever-growing, and organizations have endless options they can consider as they build out their security posture.

Organizations must recognize how every solution they implement works together and as part of their larger defense-in-depth strategy. More importantly, they need to have visibility “left of boom,” looking further upstream of the event and ensuring that the governance and change detections to system configurations are in place to allow the security tools to mitigate risks downstream.

A well-designed and carefully managed cybersecurity program can help protect against and mitigate a wide range of threats while ensuring critical business operations remain secure and uninterrupted. By establishing a solid foundation of asset and user inventory paired with visibility into changes, policies and procedures, organizations can ensure that their investments and cybersecurity strategy is comprehensive and effective.

IT Governance is the glue

To effectively safeguard against cyber threats and mitigate risks, it is crucial to have a solid IT governance strategy in place that incorporates Configuration Change Detection and Response (CCDR). As the Center for Internet Security (CIS) recommends in controls 1, 2, and 5, this requires establishing an inventory of assets, software, and user accounts, respectively. This is then maintained by continuously detecting and documenting changes from the prior state. Only then, can proper response and remediation processes be effective.

Governance requires circling back to assess that the security configurations have not drifted or have been misconfigured, and team members continue to follow the protocols, procedures, and processes over time. This tenet is the focus of the US NIST 800-128 guide, which recommends a need for security-focused configuration management and configuration change detection to be adopted. This is integral to an organization's ability to respond with proper context and recover from incidents. In some ways, foundational IT governance is as important as the security solutions themselves.

Too often, teams overlook this critical piece of the security framework. Instead, they "set it and forget it" with their defensive tools and fail to develop a clear line of sight into change and drift. They're unable to account for new assets, software, and users that may have been added and are unprotected. That's precisely the mindset threat actors will take advantage for their benefit, causing potentially catastrophic — and expensive — problems for companies.

Companies are forced to compromise

Security measures used to be rigid and unyielding in the past, but this outdated approach is no longer effective. Today, companies must balance security and flexibility, treating security as adaptable processes and protocols that can adjust to ever-changing circumstances.

Consider security to be an offensive line in a football game. The goal is to protect the users, remain fluid, and allow for the user to progress forward without running out of bounds or scrambling into unprotected areas.

As part of that, security teams need to allow for a certain level of flexibility, shifting more of the effort — and the burden — onto the IT governance side and develop the agility to react to change. This compromise places greater responsibility to clearly establish and maintain inventory and

policies for what is and is not allowed. This way, the end-user can focus on their tasks and have what they need to be productive while being assured of a successful — and secure — outcome.

Companies need new ways to look at old problems

Businesses must adapt to the changing times and update their security measures accordingly. Those who don't have visibility across their surface area, changes to their assets and users under management are susceptible to ever-increasing risks and may become more and more vulnerable over time.

While adopting digital transformation and innovative systems and services is essential in today's business world, these strategies can also present new risks to organizations. To stay ahead, companies must continuously assess and tune their security processes. Often this requires examining and removing manual work that should be automated to enable continuous auditing overtime.

Teams need to select systems and automation that provide them with agility, which, in turn, would generate substantial value and return for the organization. Ensuring that continuous auditing, change management, and security assessments are in place will maximize the benefits while minimizing potential drawbacks.

Ultimately, the focus is creating a win-win situation for everyone involved, where the end users receive the best possible experience, and the organization can confidently achieve its security objectives while safely navigating the modern technology landscape.

About the Author

Vincent Tran, CISSP is the Co-Founder and Chief Operating Officer of Liongard. He is a multi-disciplined entrepreneur with more than 25 years of experience in marketing, design, UX/UI, technical project management, developing business intelligence automation platforms and secure web applications. Before joining the Liongard team, he owned and operated multiple professional managed services organizations, representing a wide variety of agency clients. Vincent received his Bachelor of Science from the University of Texas at Austin and is a Certified Information Systems Security Professional with ISC2.

Vincent can be reached online at https://www.linkedin.com/in/vincenttran/ and at our company website https://www.liongard.com/.

Gartner's Calling for a Human-Centric Approach to Cybersecurity - Here's How to Implement It

By Roy Zur, CEO, ThriveDX Enterprise

Gartner, earlier this year, published a report stating that the future of cybersecurity lies with the very people helping businesses to operate and gain revenue, its employees. In fact, the report's number one prediction is that by 2027 at least 50% of CISOs globally will formally adopt a human-centric approach. It's no surprise as employees are the top risk to enterprise security, and Gartner's research shows that more than 90% of employees admit to undertaking actions that they know increase their company's cyber risk.

Security leaders have long grappled with an imbalance between technology and the human element when it comes to implementing an effective cybersecurity strategy. The key to changing this is looking beyond awareness to building a culture of security within the organization at every level, with a renewed focus on human factor security.

There are several steps to implementing this successfully, starting with the tips below.

Cultivate a culture of security from the top down.

A comprehensive program that combines technology and culture to change mindsets and skillsets is the key to addressing human factor security. This begins with training, education and "beyond

awareness" mindset on all levels from the C-suite down to make sure that every team member knows what security policies and controls exist and what threats they are likely to come across. All employees should be receiving regular training, testing and further touch points to keep cybersecurity top of mind at all times. This focus on human factor security is the only way to build employee confidence in their cybersecurity skills, ultimately cutting down on human risk and cyber threats.

Go beyond security awareness to build learning processes that work.

By now, most enterprises have some type of security awareness program in place to at least satisfy compliance requirements. However, simply gathering employees every few months to review a list of security procedures is not enough. Organizations should strive to engage employees in active learning processes, helping them internalize and apply cybersecurity best practices in their day-to-day work. Training should be regular and unscheduled, and include education on cyber risks employees are likely to encounter in their daily work. The ultimate goal for every security professional is to get buy-in for security awareness and training from every employee, creating a culture where the entire team essentially forms a human firewall inside the organization, identifying threats and preventing attacks. Generic security awareness training does the exact opposite. It accomplishes nothing other than checking a compliance box and it can be potentially damaging to your security culture. Human-factor security goes beyond awareness and builds a strong security culture by involving employees and customizing security awareness training to their needs.

Implement tailored training for every role inside the organization.

One size simply does not fit all when it comes to security training. For example, non-technical employees on your marketing team are not going to have the same security aptitude, skills or educational needs as developers or engineers on the dev-ops team. They also receive different types of communications and are likely to encounter different types of cyber attacks. Training should be customized to suit every role in the organization, from non-technical employees to IT team members, engineers, DevOps, developers, and security professionals. By providing role-specific training, employees can develop the cybersecurity skills they need to protect themselves and the organization.

Don't forget about secure code and application security training.

When creating a tailored security awareness training program, do not forget about the importance of secure code and AppSec training. It is simply essential for developers and engineers to ensure that the software and applications they create are resistant to potential cyber threats. Effective secure code training helps the developers in your organization understand cybercriminals' intents, identify vulnerabilities in their code and protect the organization from future attacks.

Finally, create an executive workshop program along with continued training and education initiatives throughout the organization.

C-suite executives set the tone for the entire organization, so it's crucial that they are well-versed in cybersecurity best practices. Executive workshops can help establish a security culture that begins at the top and trickles down to every level of the organization. In addition, a regular education program to create consistent, positive cyber hygiene habits across the organization is of the utmost importance. This, coupled with effective communication, reduces human risk and ultimately cuts down on cyber threats. By continually reinforcing good practices and keeping employees informed, they will be better equipped to protect themselves and the organization.

In light of Gartner's report, embracing a human-centric approach to cybersecurity has never been more critical. By focusing on human factor security and fostering a security-driven culture from the top down, organizations can build employee confidence in their cybersecurity skills and create a more secure environment in the face of ever-evolving threats. Achieving this requires a combination of technology and cultural change, transforming both mindsets and skill sets to make a lasting impact.

About the Author

Roy Zur, a serial entrepreneur, is CEO of ThriveDX's Enterprise Division the global education company committed to transforming lives through digital skills training and solutions. In August of 2021, ThriveDX acquired Cybint Solutions where he also served as CEO since founding the company in 2014. Roy is a 15-year veteran of the vaunted Unit 8200 of the Israeli Defense Force, where he served as a Major, which instilled in him early a passion for addressing the "human factor" of cybersecurity training – currently the #1 vulnerability across the threat landscape.

In addition to steering the vision of ThriveDX's Enterprise Division, Roy serves as adjunct professor of risk management in cybersecurity at IDC Herzliya in Israel. He is also Founder and Chairman of the non-profit Israeli Institute for Policy and Legislation, and a member of the Forbes Business Council.

Roy can be reached online at roy.zur@thrivedx.com and https://www.linkedin.com/in/royzur/ https://www.squadhelp.com/.

How Continuous Authentication Is Changing the Game for BYOD And Contracted Employees

By Jasson Casey, Chief Technology Officer, Beyond Identity

Five years ago, utilizing your personal device for work was considered a trendy perk. Now, it's become a standard practice for many organizations. From contract workers who empower organizations to expand their capabilities without adding to their headcount, to BYOD employees who prefer the flexibility and familiarity of their own device, unmanaged devices are now considered the status quo in many workplaces.

While this unlocks new forms of work and uplevels productivity, personal devices also open up new attack vectors for threat actors, leaving companies' networks, applications, and data exposed. Removing personal devices from work isn't the answer, so what is?

BYOD and contract employees are a cybersecurity blind spot

When employees work on an unmanaged device, there are natural concerns about the security posture of that device, and whether the individual accessing company data from it is actually authorized to do so. When the user initially logs in, a platform authenticator that runs on the device requesting access can validate that the device is not jailbroken and that key security settings are configured correctly and active (e.g. local firewall is on, lockscreen is active, the disk is encrypted, and security software is installed and running).

But what about after? As security practitioners know, things change. It's not hard to imagine the user purposefully or inadvertently changing an important setting that could lead to a security breach during the duration of their session. The device could be left in a cab, stolen, or innocently loaned to a friend without logging out first. In the time between that initial security check and final log-out, security teams are blind to who is actually behind the keyboard, and whether the device security posture remains within policy. This directly undermines organizations' efforts to transition to a zero trust model.

The consequences of such a breach can be dire, costing companies their time, capital, and reputations. In 2022, organizations like Toyota, The Red Cross, Cash App, and the US Department of Veterans Affairs all suffered contractor-related cybersecurity breaches, despite having robust cybersecurity policies in place. The solution to this problem isn't to suspend BYOD and contractor activity, which has become so essential to the modern workplace, but to fortify defenses to best support and protect work on personal devices.

Device Trust coupled with continuous authentication provides 24/7 peace of mind

Continuous authentication is rapidly becoming a best practice for BYOD and contract workers. Through this security solution, organizations can expand risk-based policy checks beyond that initial log-in, monitoring user behavior and risk signals from the endpoint every few minutes to re-assess whether the user identity remains trustworthy and that the device remains compliant with security requirements.

If the user and device pass the initial security check at log-in but fails a security check at any point during their session, the organizations' SOC team can be immediately alerted and the device can be quarantined to prevent potential data leaks. This round-the-clock monitoring provides real-time insight into who is accessing company data even when they are on an unmanaged device.

The greatest advantage offered by BYOD and contract work is productivity, therefore it is critical that continuous authentication offers a streamlined, frictionless user experience. Integrating passwordless MFA delivers a smooth experience that facilitates work rather than interrupts it. By autonomously screening for changes in user behavior or device security posture, without requiring any user intervention, the company remains secure and workers remain uninterrupted.

As new regulations and best practices around zero trust models continue to gain steam, organizational leaders are increasingly searching for new avenues to achieve compliance. The consistent reassessment provided by continuous authentication makes it a vital component of organizations' zero trust architecture, ensuring no device or user is inherently trusted.

The freedom to empower BYOD and contractors

With passwordless identification, device trust, and continuous authentication in place, organizations are free to empower contracted and BYOD employees without sacrificing cybersecurity. Productivity can be realized while granting security teams previously unheard-of real-time insight into their overall security posture.

As the threat landscape continues to evolve, the modern workplace can't afford any blind spots; continuous authentication is the key to filling the gap between log-in and log-out and maximizing productivity and security.

About the Author

Jasson Casey is the Chief Technology Officer of Beyond Identity. Prior to his current role, he served as the CTO of SecurityScorecard, VP of Engineering at IronNet Cybersecurity, VP of VoIP Product Development at CenturyTel, and as Founder and Executive Director of both Flowgrammable and Compiled Networks. He received his bachelor's degree in computer engineering from The University of Texas at Austin and holds a PhD in computer engineering from Texas A&M University.

Jasson can be reached online at https://www.linkedin.com/in/jassoncasey/ and at our company website https://www.beyondidentity.com/.

How The Growing Adoption of Cloud Is Giving Rise to New Security Challenges

By Joseph Carson, Chief Security Scientist & Advisory CISO, Delinea

The cloud has become a necessity for modern businesses. More and more organizations are seeing the value of the cloud and taking the leap, but that doesn't mean they're prepared for the challenges that come with it, including new cybersecurity considerations.

According to the Cloud Security Alliance's 2021 report, "State of Cloud Security Concerns, Challenges and Incidents," almost half of those surveyed were uncertain if they had a cloud security incident in the previous year.

Many organizations have attempted to protect their cloud environments with existing security solutions and fail to adopt native cloud security solutions.

Organizations understand that cloud security is important, but they're not always sure how to protect themselves or address the growing threat. Worse yet, they may not even realize a breach has occurred.

Education and Awareness

Employees are a key consideration for protecting your organization from cyber threats and crime. Cyber awareness and resilience should be a top priority and part of the organization's culture which puts employees in a position of strength. They should be taught to identify suspicious activities, report potential threats and never be afraid to ask for help.

This can be accomplished in a number of ways, including:

- Teaching online vigilance and safety
- How to Identify suspicious applications
- Reporting suspicious emails with links or attachments from unknown sources
- Limiting activities that take place on insecure Wi-Fi networks

Having empowered employees helps strengthen your employees' cyber knowledge and increase their ability to report potential incidents earlier. If employees know how to identify breaches or suspicious behavior, they can be a key part of preventing a problem. In addition, employees also learn how to protect themselves and their personal data outside of the workplace.

This needs to be a top-down strategy. Managers and leaders are accountable for the adopting and consistency of cyber security protocols. They are responsible for training employees to perform their job safely and assess risks, as well as being cyber ambassadors and mentors if they need to report something.

Implement and Enforce Mobile App Security

Mobile apps can be a big source of risk and exposure to security breaches. Apps may seem simple and harmless, but the wrong app can introduce risks that expose sensitive data to malicious attackers. This information should always be protected, no matter where it appears.

Developers often include options to help design applications with security, but at the end of the day, it’s up to the user to protect themselves.

These risks may include:

- Using inappropriate authentication and authorization checks that malicious actors can exploit
- Leaking data that could be discovered by malicious applications
- Using weak encryption methods
- Transmitting sensitive data without encryption
- Vulnerable APIs that expose sensitive data

Mobile app security can be enhanced by:

- Using certificate pinning to mitigate intermediary attacks on unsecured networks
- Reducing the amount of sensitive information that's stored in the app
- Allowing only the necessary permission for an app's function
- Implementing data security policies and guidelines for mobile app use
- Enforcing session logouts after use
- Avoiding saved passwords or reused passwords on apps
- multi-factor authentication (MFA) to create more of a barrier for users with weak or outdated passwords
- Continually assessing the risks of mobile apps and monitor for security updates

Analyze Logs for Suspicious Activity

Security logs can be valuable for identifying suspicious or unusual activities. These logs should be reviewed and analyzed regularly to find odd behaviors, such as logins that occur after normal business hours.

This not only helps your organization identify possible criminal activities, but it can be used for forensic purposes to trace a breach if it occurs.

Keep Systems Patched and Current

Patches are necessary to fix bugs, improve features, and keep an app functioning as it should. All systems and applications will need regular patches, and they're an important part of preventing criminal activities.

A patch can identify any gaps or vulnerabilities that could allow a malicious attacker to launch an attack. While this isn't enough to prevent cyber crime on its own, it can make it more challenging.

Use Strong Passwords and Protect Privileged Accounts

Rigorous password protection is vital to cyber security. Employees should be trained to use strong passwords such as passphrases.

A passphrase is a sequence of words or other text used to authenticate a user or secure a cryptographic key. It is similar to a password, but usually longer and more complex, and it can be made up of words, phrases, numbers, and symbols.

Passphrases are often used to protect sensitive data or resources such as online accounts, encrypted files, or digital wallets. They are considered more secure than traditional passwords because they are longer and more difficult to guess or crack using brute force attacks.

Worse yet, employees often reuse passwords on multiple accounts creating a bigger risk. If this is the case, implement an enterprise password manager to secure credentials across your organization. Help employees move passwords into the background with a solution that can auto generate strong complex unique passwords for each account and automatically rotate them on a frequent schedule.

The same is true for privileged accounts. An employee with privileged access can be exploited to provide access to the whole network. Just one compromised account gives a malicious hacker the advantage they need, and it could happen from something as simple as clicking the wrong link.

You should always identify and vault privileged accounts, and limit administrator rights if they're not necessary implementing strategies such as the principle of least privilege. Every account needs multi-factor authentication to protect against weak or outdated passwords as well.

Don't Allow Installation of Unapproved or Untrusted Applications

Privileged access is vulnerable in a number of ways, including allowing employees to install and execute applications without authorization or without verifying the application reputation. Depending on its source, this can provide an ingress point for attackers to install ransomware and infect the system, or to install hidden backdoors to gain access at a later date and launch an attack.

The best way to protect against this risk is with privileged access management. With this security measure, employees have only as much privilege as they need, and only for the length of time they need it to complete a task. Then, if an employee makes an error that could leave the network vulnerable, such as reading an email and clicking on a suspicious link, and a malicious hacker gets in, they are limited in how much damage they can do.

Be Deceptive

Malicious hackers count on predictability and routine. If they know when scans and patches are run, what users have access to, and when routine tasks take place, it gives them an edge.

Always be deceptive and unpredictable in your behaviors. Take an as-needed approach to assessments and updates to limit their opportunities to attack and make it more difficult to hide in your system and await the best moment to strike.

Fight Cyber Crime in Your Organization

Cyber crime is everywhere and growing. As cloud adoption increases, organizations are facing greater risk from malicious actors seeking sensitive data. Taking a proactive approach to cyber

security puts you in a strong position to defend against cyber threats, and if one occurs, mitigate its effects.

About the Author

Joseph Carson is a cybersecurity professional with more than 25 years' experience in enterprise security and infrastructure. Currently, Carson is the Chief Security Scientist & Advisory CISO at Delinea. He is an active member of the cybersecurity community and a Certified Information Systems Security Professional (CISSP). Carson is also a cybersecurity adviser to several governments, critical infrastructure organizations, and financial and transportation industries, and speaks at conferences globally.

Joseph can be reached online at (Linkedin, TWITTER, etc..) and at our company website https://delinea.com/.

Simplifying your Approach to the Zero Trust Journey

By Chris Cullerot, Director of Technology and Innovation, iTech AG

Earlier this year, the Cybersecurity and Infrastructure Security Agency released its Zero Trust Maturity Model 2.0 to help agencies develop zero trust strategies and actionable implementation roadmaps.

CISA's updated maturity model aligns with previous efforts, continuing to provide resources and roadmaps to help agencies protect their most sensitive data and meet security standards required by the end of FY24.

Effective zero trust architectures combat persistent threats by validating every user and device, and continuously validating identities within the environment before authorizing access. It's an approach that benefits organizations of all kinds—and the maturity models put out by CISA can provide a roadmap for all sectors as well.

Improving the detection of cyber incidents and creating standard playbooks greatly assist agencies in addressing common challenges agencies may encounter and will empower agencies to face cyber incidents head on, complementing zero trust principles for a more secure organization.

Improving detection of cyber incidents

Effective cyber defense requires enhanced speed and agility to stay ahead of dynamic threats. An advanced or optimal zero trust posture requires automated controls and centralized visibility into the IT environment. This starts in the security operations center (SOC).

Even with zero trust principles in place, incidents will inevitably occur so addressing the most significant threats first is essential to managing the deluge of events that SOC analysts face. The volume of tickets can mean more severe alerts get lost in a rush of information. Analysts need a detection and event management process that helps them prioritize those events deemed most critical.

To enhance threat detection and response, one federal agency implemented an incident detection and response solution that allows them to collect, interpret and store audit logs to perform analytics and detect anomalies.

Teams are then alerted once a threat is detected, and the solution automatically creates actionable tickets that are managed through the incident response workflow for validation, response, and remediation. The incident response system also provides threat context to assist in validating an event and informing the appropriate response.

Security teams now draw critical insights that help them identify and prioritize cyber incidents and take the appropriate actions to contain and eradicate the threat. Approaches like this demonstrate realistic ways that agencies can address zero trust requirements, recognizing that not every incident can be immediately investigated.

Creating standard playbooks

When responding to a cybersecurity incident, descriptive playbooks equip security teams with the proper resources to support containment, eradication and recovery from the threat.

As organizations continue their zero trust journeys, security leaders may notice common threats. In these situations, standard playbooks can identify patterns and provide a repeatable response to remediate these attacks. The playbooks also allow IT leaders to automate responses to security incidents such as email phishing, malware, and denial of service.

These automated solutions can be tailored to an organization's specific needs to better respond to threats moving forward. Furthermore, by automating security responses, SOC teams become more efficient and effective by reducing the amount of time spent on identifying and remediating taxing events, and instead allocating the time and resources to higher priority or more complex cyber incidents.

For example, to better position the team in its zero trust journey and progress its modernization posture, another federal agency was focused on improving response time to evolving threats and streamline enterprise security operations. By implementing functions such as security orchestration and automation response (SOAR), errors resulting from manual processes were eliminated across teams. These standard playbooks and dashboards helped expedite investigations, response processes, and corrective actions across the agency's IT, security, and risk teams.

The agency cultivated a more uniform approach to cyber incidents and improved its ability to respond to emerging threats.

Looking ahead

Achieving zero trust is a significant undertaking as agencies need to protect their data while meeting evolving security standards and mandates from CISA and other federal agencies. To meet these expectations and upcoming deadlines, advance their zero trust journeys and best protect government holistically, agencies will benefit from approaches that streamlines and helps automate important functions.

Taking incremental, concrete steps to improve detection of cyber incidents and creating standard playbooks will accelerate and advance security postures as organizations continue a zero trust journey, better positioning them in today's digital threat landscape.

About the Author

Chris Cullerot is a security leader and strategist with over 18 years of experience in security management and operations. He has led numerous security programs and initiatives during his career including the incident response program for the 2016 Presidential Transition Team. He is driven by a passion for innovation with the ability to integrate the security function with corporate goals and business strategies. Chris currently serves as the Director of Technology and Innovation for iTech AG, overseeing the delivery of the company's technical portfolio of services including digital innovations and cybersecurity. Learn more about iTech AG at https://www.itechag.com/.

No Cloud, No Problems: Why Dynamic DNS Reigns Supreme Over Cloud Applications

By Dan Durrer, Founder & CEO, No-IP

Whether you are gaming with friends or game planning your next business venture, it is likely that you are relying on the cloud for data storage. On the surface, paying a monthly fee and keeping all your information stored in a cloud application or service sounds great; but there's another cost that's lurking: the cost of uncertainty. Uncertainty in how the vast amount of your personal data is being protected. How much do you value protecting the privacy of your baby monitor, security camera or sensitive workplace documents? Do you want more control over your network performance and monthly service costs?

To truly understand if cloud solutions are your best bet, it's important to understand the inherent drawbacks of the cloud and consider the cost you are willing to pay for the "convenience" of the cloud.

Data Visibility Shouldn't Be Clouded

Anytime you sign up with a cloud data service, it's hard to validate whether their end-to-end is secure, or what tools they're using to stay secure. There's ambiguity around most companies' internal data protection policies, and it would take some serious sleuthing to find answers. You don't know where your data is stored (it could be on a server in another country) and whether the /"terms and conditions" you breezed through entitled the provider to sell your data to advertisers.

Let's consider IoT devices as an example: most security cameras, smart doorbells, and baby monitors have low profit margins. The provider makes their money from the cloud subscription services required to keep these devices online. It just so happens that most of these security camera companies are owned by a large corporation — Nest by Google, Blink and Ring by Amazon, etc. It's very much a black-box situation; what happens to your security feeds and personal info when they pop up into the cloud? Should you be worried about data usage like we've seen from TikTok and Facebook recently?

Choosing the right data storage and remote access solution comes down to the value you place on data protection, performance, and flexibility. A few questions to ask yourself if you are trying to decide whether to go the cloud or DDNS route:

- Where is this device manufactured?
- Who owns this company?
- Where are the cloud servers hosted?
- Could I explore a self-hosting situation that might save me stress or money?
- Do I even really care about any of this? Or do I just want to get set up and move on?

Key Considerations of the Cloud

Reliability: Anytime you're pushing your data up to the cloud and then out to the internet, there's an opportunity for extra latency. The cloud often brings slower connections and higher bandwidth requirements as data is uploaded from your IoT devices to the cloud, and then down to the phone or app you're using to view or control it. This doesn't occur when you're directly connecting with your devices through DDNS services.

Relying on the cloud also makes you subject to outages, which last year affected companies as large as Twitter, Zoom and British Airways. Plus, 80% of organizations experienced a serious cloud security incident during the last year, according to Snyk's State of Cloud Security 2022 report.

Vendor Lock-In: Once you sign up for a recurring cloud subscription service, it's often difficult to get out of the engagement. You might experience high switching costs (like replacing the equipment you've already purchased that isn't compatible with any other service), or have large

amounts of data that become difficult to migrate to a different cloud server. You could be stuck paying for a service you're not truly smitten with.

Recurring Costs: You've heard of "death by 1,000 papercuts." But what about "death by 1,000 cloud SaaS subscriptions?"

You might pay $1.99/month to upload your phone's photos to Google Photos. Then you realize you already signed up for iCloud storage through Apple last year. If you set up six security cameras around your house, you'll need six different subscriptions to keep each of them connected. Now add your new baby monitor….and so on and so forth.

Sure, $1.99/month here and $30/month there might not seem like a lot on the surface, but those costs can add up: especially in an uncertain economy. The cost of easy setup can sometimes be outweighed by long-term, recurring subscription fees.

Staying in Direct Contact with Your Devices: DDNS

When truly having control over data, network quality and spend is a priority, it might make sense to curtail use of the cloud altogether in favor of a Dynamic DNS (DDNS) solution.

DDNS allows access to devices from any location, without relying on the cloud. Your hostname stays active with your current IP address so you are always able to access your devices (computers, security cams, etc.) remotely. Because you are directly connecting with your devices, you – and only you — control what is shared, and with whom.

The Distinct Differences of DDNS

DDNS can provide you with some potentially game-changing advantages, including:

Security: Cloud servers are often vulnerable to security breaches that occur because of high traffic and cyber attacks. With DDNS, you control your connection and data; your DDNS provider has no visibility into the data being transferred. This gives you greater control and security over your information, as you can ensure that your data is not being accessed or monitored by any third-party.

Control: When using cloud servers, you'll have less flexibility and control of your network and ports. DDNS puts you in control of your network, meaning you control which ports are open and who can view your device.

Visibility: Any data that's passed through cloud servers could theoretically be viewed by cloud providers and any third parties they associate with. Dynamic DNS, meanwhile, is simply a private connection to your remote devices. Your DDNS provider doesn't even have the ability to view your data, even if they wanted to.

Price: You can often find DDNS solutions for free, or extremely low monthly fees. Plus, it's a one-stop shop; one subscription will cover all of your bases.

Like with any weather forecast, stormy weather in the forecast doesn't mean you will be rained on, but it is important to understand the implications of what you are signing up for and what can lie ahead. Signing up with a cloud application could lead to some stormy days.

About the Author

Dan Durrer is the Founder and CEO of No-IP, a company based in Reno, Nevada, that provides Dynamic DNS services and other Internet infrastructure solutions. Durrer is well-known for his passion for technology and his commitment to providing reliable and affordable internet infrastructure services. He has been the driving force behind No-IP's growth and success, and his leadership has helped No-IP expand our offerings to include domain registration, SSL certificates, email services, and more.

Dan can be reached online at ddurrer@noip.com and at our company website https://www.noip.com/.

Promoting Safety Across Your Digital Supply Chain

No organisation is an island. Last month's attack on payroll software Zellis, reminds us how the effects of one breach can very quickly cascade across the business network to third parties, resulting in a much larger number of victims. And it's not just the business that suffers.

By Guy Golan, CEO at Performanta

No organisation is an island.

Last month's attack on payroll software Zellis, reminds us how the effects of one breach can very quickly cascade across the business network to third parties, resulting in a much larger number of victims. And it's not just the business that suffers.

Promisingly, according to the Government's latest breaches survey, the majority of large businesses (55%) are reviewing supply chain risks for the first time. However, this is still relatively uncommon across organisations overall.

Just over one in ten (13%) businesses say they review the risks posed by their immediate suppliers.

The industry needs to shift its mindset from one of security to one of safety. Assessments are carried out every day to determine whether an organization is deemed 'secure' by compliance and industry standards, but this doesn't mean that all parties involved are safe.

We need a global data-driven strategy that prioritizes accuracy, transparency and context when it comes to cybersecurity across the entire supply chain, for the sake of each business and every single individual involved.

An agreement is a partnership

When part of a supply chain, businesses essentially sign up to an industry partnership, meaning you share the responsibility of digital security.

As a first step, organization must recognize that cybersecurity is not just about compliance; it is about ensuring the safety and resilience of their operations. As the cyber industry continues to grow and adapt, the threats organisations face are becoming more sophisticated and pervasive, meaning that one breach in the supply chain could spell trouble for countless businesses.

The cyber industry is dynamic, with new technologies, applications, and threats emerging constantly. Acknowledging the evolving nature of cyber threats is vital to promoting safety across digital supply chains.

We are still in the early stages of the cyber evolution; there are areas of technology and new kinds of risk that the industry is yet to uncover. Only through recognising this and preparing for changes to come can true safety be achieved.

Businesses should aim to create a culture of safety that permeates all levels of the organization. This culture includes proactive risk assessment, continuous monitoring, and ongoing training and education for employees.

Instilling a mindset of safety across the supply chain

Defending against the unknown – which the industry has come to see as common practice – was long viewed as being impossible, but we can now take proactive measures within digital supply chains to enhance our preparedness.

Although the industry has yet to establish an official definition of what it means to be 'safe' in the cyber realm, assessments based on compliance standards alone do not guarantee safety for all involved parties. Nevertheless, the industry is already well-positioned to make this transition from security to safety.

Three core elements shape a comprehensive cyber safety strategy: accuracy, transparency, and context.

To effectively navigate the evolving risk landscape, digital supply chains must accurately identify potential risks, understand the impact of these threats, and develop appropriate solutions. This necessitates real-time, precise data and user-friendly methods for assessment and presentation that facilitate effective response from teams.

As data accuracy increases, transparency naturally follows. Transparent communication and shared insights are crucial for all stakeholders within a cyber safety strategy, both internal and external. Within a supply chain, transparency becomes paramount to align all parties and respond effectively to threats.

Furthermore, it is imperative to ensure that security insights are accessible to all areas of the digital supply chain, not just those with cybersecurity expertise. Translating data into understandable terms for stakeholders such as CEOs and CFOs fosters company-wide awareness of risks. This widespread understanding is essential for securing buy-in and implementing a comprehensive safety strategy.

As our lives and identities become increasingly intertwined with the digital realm, feeling safe is fundamental. Merely achieving compliance is no longer sufficient for businesses. Even organisations that claim to be shielded by robust security defenses have faced vulnerabilities time and again.

The connections within supply chains can very easily turn from being a business advantage to a catastrophic vulnerability. After all, the Zellis breach resulted in stolen customer data from large organisations like the BBC, Boots and British Airways.

Clearly, the traditional security approach has reached its limits. The industry must seize this opportune moment to unite under the banner of safety, prioritizing the holistic wellbeing of digital supply chains.

About the Author

Guy Golan is a Cybersecurity Expert with over 20 years of experience in the industry. He started his career in the Intelligence Brigade for the Israeli Defence Force before leading several large organisations as CISO. He's now the CEO and Founder of global cybersecurity firm Performanta, with over 150 security professionals spanning three continents.

Recruiting and Retaining Women Talent in Cyber Amidst the Cyber Shortage

By Oriana Vogel, Chief Human Resources Officer, Trustwave

With over 2.5 million cybersecurity positions unfilled globally, the cybersecurity field is facing a severe shortage of talent, with an increasing demand for skilled professionals to combat the ever-evolving threats in the digital landscape. One crucial aspect of addressing this shortage is to focus on recruiting and retaining women in cybersecurity. Gender diversity brings unique perspectives, insights, and problem-solving approaches that are invaluable in the field. To combat the talent shortage, organizations must be committed to building an environment that's focused on inclusivity and career development to attract and retain the best talent in cybersecurity. Here are six inclusive methods industry leaders should implement to advance gender diversity within the cybersecurity industry:

Creating an Inclusive Environment

As a core component of building a diverse workforce, equal opportunities must be provided for all employees. By fostering an environment of mutual respect and trust, it allows individuals, regardless of gender, to have a real impact within their organization. Creating an inclusive company culture allows employees to feel empowered and encouraged to facilitate meaningful change in the organization. It is critical that internal teams, such as the HR department, align with these values and focus on providing the necessary resources and tools to support their employees' success.

Skills Development and Learning Opportunities

One significant barrier to entry for women in cybersecurity is the perception that they must possess all the required skills from the start. Recruiting and retention teams should proactively address this concern by offering extensive learning and development opportunities. These education initiatives can include formal programming to teach proprietary skills as well as industry knowledge. It's imperative to extend learning beyond the structured paths and enable employees to create their learning journeys. External certifications are also a great way to further bolster professional growth. Organizations should consider how they can entice employees to participate in these programs.

Knowledge Sharing and Mentorship

By promoting a culture of knowledge sharing and mentorship, employees can feel encouraged to learn from one another. Employees must have the opportunity to work on challenging projects alongside industry leaders inside the organization and leverage their expertise to expand their skill set. This collaborative environment allows all genders to feel included, fostering an atmosphere where everyone's opinions and contributions are valued.

Flexibility and Work-Life Balance

In this new hybrid world, it's important to recognize that women often have different travel needs and strive to provide a flexible work environment. Embracing a 100% virtual culture and enabling individuals to work from anywhere, is imperative to retaining top talent. Take an approach that prioritizes a commitment to flexible working hours, ensuring all employees can maintain a healthy work-life balance.

Removing Barriers to Entry

Often women won't apply for a job if they don't meet all the criteria, while men tend to be more willing to take the leap. An effective recruiting process specifies that the organization is willing to invest in training individuals who may lack certain skills initially. This approach encourages women to pursue cybersecurity careers, knowing that their employer will support their growth and development.

Global Opportunities and Leadership

Organizational commitments to inclusivity must extend globally. Think about the aspects within your operations that could benefit from being more inclusive – for example, consider holding town halls or all-staff meetings at different times of the day to accommodate a global workforce. Leadership teams must also think globally to ensure consistent opportunities and experiences are available for employees worldwide.

By fostering an inclusive environment, providing extensive learning opportunities, promoting knowledge sharing and mentorship, and offering flexibility, organizations can begin to fill the millions of job openings with talented women who will drive the future of cybersecurity.

About the Author

Oriana Vogel is the Chief Human Resources Officer at Trustwave. She is responsible for the company's global human capital and for optimizing Trustwave's talent and culture.

Prior to Trustwave, Oriana served as a top human resources leader at Discover Financial Services. She led all Business Partners and Talent Centers of Excellence and set up Discover's first-ever HRIS and Shared Services function. Oriana has also held senior human resources leadership roles at Amazon and American Express.

Oriana has a proven ability to drive value through large-scale transformation initiatives and to create agile and talent-rich organizations. Her extensive background and strong leadership skills ensure Trustwave cultivates a performance culture.

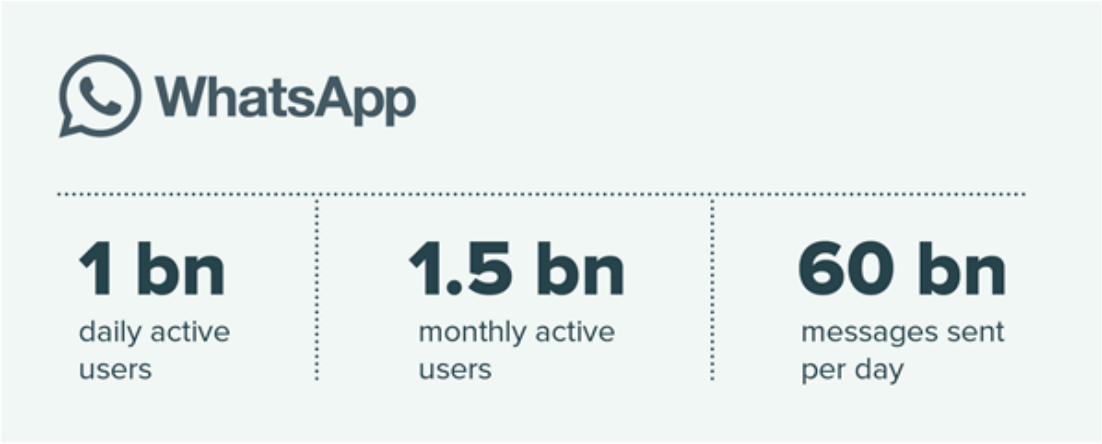
Oriana holds a bachelor's degree from Wellesley College and a master's in business administration from Harvard University.

Oriana Vogel can be reached online on LinkedIn and at our company website https://www.trustwave.com/en-us/.

4 Reasons Why Not to Use Whatsapp for Secure Communications

By Nicole Allen, Senior Marketing Executive at Salt Communications

Don't settle for just using WhatsApp for secure communications. Check out these 4 reasons why you should consider a WhatsApp replacement.



WhatsApp is a communications app that is widely utilised for personal use, however using WhatsApp for business could include risks related to productivity, compliance, improper management of workflows, tracking, data administration, and, lastly, company security.

What potential concerns could there be while utilising the personal messaging service, WhatsApp for corporate communications? Look closely at the following observations:

A breach of compliance

Recently many financial institutions are being fined for using “pervasive off-channel communications” along with widespread failure to preserve records of communications. Executives violated federal security laws and suffered the consequences thanks to their actions.

For the compliance violations, in September 2022 eight companies and five affiliates agreed to pay $125 million each. These firms include affiliates of Barclays, Bank of America, Citi, Credit Suisse, Deutsche Bank, Goldman Sachs, and Morgan Stanley. With these fines in mind organisations need to focus on enabling the best tools that ensure communications are private, secure and in alignment with their compliance policies.

Zero corporate admin controls therefore no protection

WhatsApp provides a limited number of admin controls that are limited to groups. It does not provide a wide variety of corporate admin control capabilities to restrict user access to the organisation's data because it is a personal messenger. Anyone can create unauthorised groups and converse privately (from a company’s perspective!) because you cannot control the lines of communication within the app. For example, once you begin using WhatsApp for routine business communications, there is a chance that former staff members will misuse any sensitive information they have access to, or sensitive internal information is being discussed with external parties.

If you use WhatsApp for business purposes and your mobile device is lost or stolen, you should presume that all of your official data is also lost and potentially stolen. Since WhatsApp does not offer a security layer to guard against data loss or theft, organisations are leaving themselves open to attacks and leaks.

Decreased productivity

Adopting WhatsApp at work may reduce your productivity because it is not designed for continuous office job operations. Given that the interface makes them think of personal messaging, employees' attitudes towards professionalism are altered. The use of WhatsApp for business purposes also encourages staff to regularly participate in non-work-related conversations - directly impacting their productivity.

Using a personal messenger for confidential information is not encouraged by many businesses throughout the world. They can instead rely on specialised secure communication systems designed specifically to manage efficient work schedules.

Lack of control over your data

Do you want to be the owner of your organisation's data or not? The choice is yours. Message exchanges are non-compliant, insecure, disorganised, and unchanneled on WhatsApp.

For organisations the lack of control of message data is vital. Whether it is a police force who need complete control over their communications from hosting to storage for sensitive disclosure obligations, financial organisations who need to remain compliant, or law firms who need to maintain client confidentiality, the way in which your data is being managed should be YOUR CHOICE. Popular messaging platforms do not give this option, businesses still trust a system where we have zero control or visibility to where data is being hosted, what is being done with their data and who has access to it.

It's time organisations communicate with confidence and take control of their communications.

Common WhatsApp attacks

With many high-profile WhatsApp hacks, organisations need to ensure that they have full control over their technology solutions, and have the capability to manage how their metadata is stored and used.

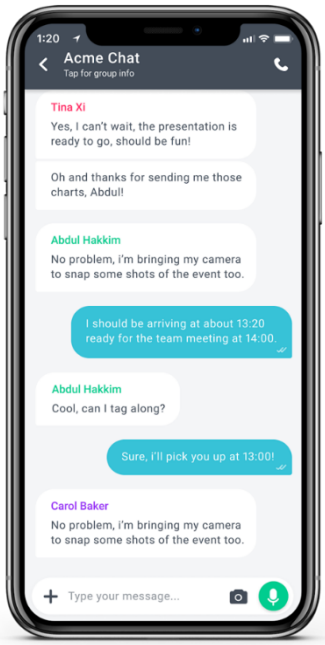
WhatsApp along with numerous other solutions such as Viber, Signal and Facebook Messenger are all 'consumer' messaging applications. These apps do offer end-to-end encryption within their app, but the negative thing about these solutions is that the users believe 'Encryption' is full 'Security'. Salt Communications don't think that this is the case. We believe that enterprises should see 'Security' as Encryption working hand in hand with control and management.

A common example is Pegasus. Pegasus is frequently appearing in the news. A few WhatsApp users, notably journalists and activists, received messages informing them that Pegasus had compromised their phones early 2019. This is when everything started. However, one could argue that news of the Pegasus spyware never really stopped being a topic. It seems to be used by different governments so frequently that there are allegations of phone hacks utilising it virtually every few months.

Why you should use a Secure WhatsApp replacement

It bears underlining that WhatsApp was created with the consumer in mind and thanks to its 2 billion users, it has grown into a very potent product for Facebook. It is a prime example of how surveillance capitalism operates: provide free access to a practical tool while charging third parties to profile users and target content to them according to predetermined criteria using the gathered data.

By passing the buck onto you, WhatsApp is protecting themselves: "You provide us, all in accordance with applicable laws, the phone numbers of WhatsApp users and your other contacts in your mobile address book on a regular basis, including for both the users of our services and your other contacts."



Salt is the pioneer in providing a comprehensive solution for encrypted communications between smartphone users and secure systems within their organisation. Our product offers centralised control for administrators, integrating with trusted internal services, providing secure voice and video calls, messaging and WhatsApp replacement, and file transfers for users making critical decisions on-the-go.

In a nutshell, to be more efficient amongst your organisation and keep all your communications in one secure place and communicate on one official platform rather than relying on several communication channels like emails and personal messengers. Utilise a secure communications system, to secure all of your business communications and data.

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/.

How To Ensure Information Security of An Organization Basing on Business Requirements

By Sergio Bertoni, The Leading Analyst at SearchInform

There is a global trend of strengthening the legislation related to the information security related issues. Besides the regulators' requirements, due to the steep increase in the amount of information security related incidents, more and more people begin to understand the importance of ensuring appropriate level of information security safety. Organizations and businesses all over the world are motivated to ensure the safety of data they gather and process.

The first group of specialists who have to deal with more responsibilities and work are information security officers. It is especially true for the young experts in the field. And especially for those, who are employed in a company, which doesn't have an advanced information security protection system. This isn't a fantasy scenario, if this resonates with your case, this article is for you.

So, let's start with some basics. If you work for a company, which doesn't have a well-developed information security protection yet, you have two primary options:

- Base on the business requirements.
- Base on the regulator's requirements.

The most efficient one is to complement regulator's requirements with business's needs. In this article, we will provide recommendations on how to do it.

The business way

Preliminary stage. Choose the protection paradigm.

Even if you are lucky enough to have a chief who really understands the importance of information security aspect, you should be initiative and proactive – offer some kind of a plan on how everything should be done. At least, prepare a plan, containing information on what should be done "at least", starting with the inventory (hardware, software and content); explain measures how to identify the most significant risks and reveal methods of their mitigation.

In order to customize the plan it's required to initiate interaction with employees of different departments. Conduct a survey of each department employees in the form of a round table or private conversations – choose the method you like more.

It's required to find out answers to the following four questions:

- What do specialists consider as the information asset?
- What are the risks posed to these information assets?
- What are the possible consequences of these risks for an organization in their opinion?
- What they will consider as an incident and how do they assess its criticality?

It's impossible to develop adequate organizational and technical measures for data protection if there are no precise answers to these 4 questions.

It's very important is that not only the method of action, but also the penalties for not meeting the established standards should be discussed during the survey and conversations with other employees. The auditor, the employee, who is in charge of ensuring information security, has some tools with the help of which it's possible to influence the violators. But it's crucial to precisely develop the set of rules, which will be easy for understanding beforehand and only after it proceeds to discuss the penalties. By the violators, I mean the following types of employees:

- Employees, who don't comply with information security rules.
- Managers, who don't agree on a budget allocated to the information security needs in a timely manner.
- IT specialists, who are in charge of ensuring IT systems uninterrupted work (in case something fails).

Proceeding to the realization

Below you can find the list of measures, aimed at protection of information and infrastructure. However, it's important to notice, that actions, related to these processes should be iterated permanently.

1) Inventory

I mean the real life inventory, not the nominal one. Perform the initial check of the infrastructure, as you have to understand what do you have:

- Which hardware and software is used
- What are the current versions of firmware
- Which ports remain open
- Which connections are there
- Which data is kept in the Storage Area Network; is there any personal or confidential data; who has access to it.

It's the ideal scenario if this process is automated, because inventory should be performed regularly. Typically, each time the inventory is performed, there are some unexpected findings. And the first time you perform the inventory, you'll definitely find open ports and documents kept in inappropriate folders.

2) Cryptoprotection

Just after you finish with the inventory it's required to ensure crypto protection. If you have a node, which interacts with others or a data storage, containing crucial information, it's required to protect them immediately. I'd like to remind that there are options for crypto protection for both data and channels and it's required to protect both of them. Nothing should remind unprotected. And, of course, don't lose your passwords/keys 😊.

3) Access rights management

This requires, at least, appropriate distribution of access rights to folders and computers in Active Directory. However, in this case you can only implement attribute based access control (not based on the content, in other words, access control to a specific file or folder).

It's better to implement content based access control. It can be done with the help of specific solutions, which analyze the file content. Depending on how confidential data in the file is, the solution allows or prohibits interaction with the file. For instance, advanced DCAP class solution deals with the task.

4) Audit of security events

It should be total. It's required to perform audit of all the existing sources (software and hardware). Bad news is that it's impossible to analyze everything manually. Good news is that almost all the IT systems log actions, and, typically, in a quite detailed manner. Automated systems are capable of processing these logs, turning an event (or a link of interconnected events) into an incident. You can choose such a system for almost any budget allocated, what's more, there are even free, open-source (ELK etc.) ones.

5) Editing security policies

As soon as the incidents are detected in the event flow, you may start to complement ready-made security policies with your own ones. Both ready-made and customized policies should be edited from time to time according to the current business-processes and infrastructure needs. In our case, policies stand for any settings in any data protection tools, ranging from antiviruses to NGFW.

6) Enhancing employees' awareness in information security related issues

Numerous information security problems originate from the lack of knowledge and understanding. That's why educating and training employees is so crucial and mustn't be neglected. Large companies even develop specific educational portals, and organize education process in different forms, including the form of a game. In some organizations, for instance, governmental bodies, instead of gamification, the practice of development of regulations and organization of trainings is implemented. Regardless the exact methods used for organization of education process, plenty of free materials, which you may use in this process are available publicly. For instance, we regularly extend the list of useful materials, which can help to enhance the digital literacy.

7) Protection analysis

This is the process, aimed at examination of existing vulnerabilities in the inventoried software, ports and hardware, performed manually or automatically.

You can manually check all the sources and reveal, whether there are unpatched versions, default passwords and access rights violations are present. Honestly, this is a laborious method. If you're a beginner, but an inquisitive specialist, you'll cope with the task. Nevertheless, a fair amount of skill is required to succeed. That's why the best option is to hire a team of professionals which will perform the protection analysis once a year (the period is to be specified according to the organization's peculiarities and requirements). Despite its expensiveness, this option is typically the most beneficial one.

Another option is the automated one – you can use the specific software, vulnerability scanner, which can be both commercial and open source.

This is an important stage and it's great if you don't neglect following the protective measures mentioned at this stage. If you'll decide to deal with the issue on your own, here is he list of helpful resources:

- Vulnerability scanner https://nmap.org/download.html
- Database of known vulnerabilities https://cve.mitre.org/
- Database of exploits for obtained vulnerabilities https://www.exploit-db.com/

8) Dealing with incidents

At this stage the work processes, related to incident investigation, analysis and prevention starts. The main aim at this stage isn't simply to fix all the critical events, but, what's more, to make the corresponding conclusions: why, despite the security policies set, negative events happened, how is it possible to mitigate their outcomes and how to prevent such incidents occurrence in future. This isn't a simple tuning of policies for elimination of incidents and false positives, but enhancing of the information security protection in general, not only with the help of technical measures, but with the help of organizational ones as well. What's more, it may be a useful option to organize cyber trainings, aimed at practicing of respond to different types of threats.

Obviously, this is not the exhaustive list of all the actions. In order to ensure the information security protection it's required to consider numerous issues and peculiarities of the corporate infrastructure. However, if you are have no idea what to start with or if you are thinking of what to do next and checking whether you haven't missed something, this to do list should be helpful.

About the Author

Sergio Bertoni, the Leading Analyst at SearchInform which is the global risk management tools developer.

Sergio has plenty of hands-on experience in the sphere of information security and has been contributing to the company's success for years. Sergio comments on different infosec topics, including information security trends and new methods of fraud (from simple phishing to deepfakes), provides advice on how to ensure security of communication channels and shares best practices for organizing information security protection of businesses.

Sergio can be reached at our company website https://searchinform.com/.

The Power of Policy: The Best Weapon in Your Defensive Arsenal Isn't New Tech

By Craig Burland,CISO of Inversion6

The default mental image of a 1970's Ford Pinto shows a car ablaze with the rear end mildly crumpled and the hapless driver nowhere in sight. The Pinto came to epitomize the flaws in consumer safety regulations and the downside of callous cost benefit analysis. Ford's leadership had determined that redesigning the car's fuel system was more costly than the legal impact of mass producing a dangerous vehicle. They were wrong. The Pinto spurred a revolution in product safety that saw manufacturers face dramatic changes in requirements to protect consumers. Fast forward 50 years and we're facing a similar dilemma in digital products, seemingly waiting for a virtual explosion and flaming wreckage before taking action.

The idea of Secure by Design has been around for decades. One of the earliest references can be found in a paper called, "The Protection of Information in Computer Systems" by JEROME H. SALTZERAND MICHAEL D. SCHROEDER. The authors called for attention to least privilege and data privacy in the new arena of multi-user systems. In 2022, Microsoft celebrated the 20th anniversary of Bill Gates' now-famous email announcing the creation of the Trustworthy

Computing (TwC) initiative. The initiative sought to put customer security at the forefront, emphasizing the need for security over adding new features.

Inexplicably, adoption of these ideals remains aspirational rather than foundational. Companies across the world continue to emphasize speed and efficiency in development, choosing to launch products and deliver features at pace with minimal attention paid to application or security. It's DevSecOps minus the Sec. Day in and day out, we read about product design flaws that expose customer data or reveal significant vulnerabilities. The lack of commitment to security can be seen across the technology landscape from industrial control systems to cloud platforms. Within the last month, CISA announced multiple issues with input validation flaws opening the door to compromise. Input validation is one of the most basic checks a developer should perform. Skipping this check is development malpractice. It's like strapping a gas tank to the back of a small car and hoping rear-end collisions won't happen.

The good news is that adding security to the DevOps pipeline and moving toward Secure by Design doesn't take innovative genius. Organizations like OWASP and MITRE have done the hard work by building the components of a sound program. All it takes is an awareness of risk, a focus on strategic prioritization, and a matter of will.

First, it's essential to raise awareness with the development teams and leaders about why security warrants investment. Developers don't typically spend their mornings reading about the latest vulnerabilities and compromises. Development leaders worry about release dates, price points, and key features. In their minds, the only guaranteed way to fail is never to launch. Injecting a cybersecurity perspective into the decision process is vital to reshaping the dialog. Every product with technology faces threats. Those threats may be large or small. They may require a big response or a minor adjustment. They may potentially impact the company's reputation or affect a minor aspect of product data. From a cyber perspective, the biggest mistake a company can make is choosing to remain ignorant of the risks. Tools like threat assessments for the leaders and secure development training for the developers can spark a change and build buy-in for long-term, cultural change.

Next, it's critical to establish cybersecurity as a stakeholder in product development. By inserting cyber requirements alongside product features, security has a designated seat at the table and a voice in the outcome. Too often, security is engaged just before a product launch shoved into the precarious situation of trying to stop the business or ignoring risk. This is an unwinnable 11th hour trap. Including security-centric elements at the start of the effort lets the process flow normally, allowing a genuine, unbiased dialog about risk and compliance happen. Requirements may be broad like adoption of a secure development framework or narrow like insisting on static code analysis before every release. Like most business requirements, these cyber elements should be negotiable. It's rare that a product feature doesn't spawn a design discussion about different ways to meet the need. If fully meeting a requirement would undermine the product or eliminate the business opportunity, other options or compensating controls should be considered.

With awareness and requirements in place, the final step is testing and validation. In contrast to the 11th hour trap, security issues discovered during the development pipeline can be treated rationally, discussing time, cost, and scope – the core elements of project delivery – to find win-

win scenarios. Good requirements have tangible success criteria and named ownership. Validation should be an objective, fact-based exercise rather than a contentious series of events.

Secure by Design will continue to grow in importance as the negative impacts of unsecure development practices drive headlines. The Biden Administration recently announced a shift in liability for flawed technology products, intended to increase protections for customers. CISA followed with more detailed guidance about how to meet this challenge. In June, Google called for security-by-default as its first element of responsible AI development. As the famous saying goes, “Those who fail to learn from history are doomed to repeat it.” Smart companies will heed this advice and embrace secure development before their product becomes the Ford Pinto of the 2020s, engulfing the company’s reputation in lawsuits and flames.

About the Author

Craig Burland is CISO of Inversion6. Craig brings decades of pertinent industry experience to Inversion6, including his most recent role leading information security operations for a Fortune 200 Company. He is also a former Technical Co-Chair of the Northeast Ohio Cyber Consortium and a former Customer Advisory Board Member for Solutionary MSSP, NTT Security, and Oracle Web Center. Craig can be reached online at LinkedIn and at our company website http://www.inversion6.com.

The Basics of Digital Forensics

By Milica D. Djekic

The digital forensics is a field that assists us to find the clues within a cyberspace regarding some cybercrime or computer breach. The majority of tools used for a digital forensics serve to extract data from a memory, hard drive, removable storage or even websites and transfer them further to a skillful investigator for an analysis. Following all of these, we can conclude that digital forensics investigators may get specialized to some fields. Through this book's chapter, we would also recommend how forensic staffs could get trained to their tasks.

Why digital forensics matters?

So often, the practice would bring us many cybercrime cases or data breach scenarios which would need a skillful investigation to get proved in a reality. When some cyber incident occurs, the first step being taken would include a good incident response. Next, we should deal with the digital forensics trying to assure the evidence of what happened.

All the staffs working on digital forensic tasks should get prepared to respond to a certain situation which is possible only through regular training, education and exercises. The next phase with a digital forensics would cover data collection using an adequate data acquisition tools and software. Also, those collected information must get analyzed and such a produced finding should get put in a skillfully created report.

Researching this area of cyber defense, we would notice that a digital forensics marketplace is very well-controlled and in the majority of cases – you need to leave your personal details before you get a permission to download any application. In addition, we would mention that this sort of tools is quite expensive, so we would recommend to some beginners or low-budget organizations to try to download some software for free.

Many web locations would offer some freeware or open-source versions of forensic tools and we would like to highlight the Forensic Control website as one of the best forensics tools marketplace offering you a wide spectrum of free applications. Also, in order to gain some experience and knowledge in dealing with digital forensics – we would advise you to take advantage over web resources including learning materials, tutorials and video sessions.

Some commonly used forensic tools

The forensics tools may get used for many different purposes such as disk and memory capture, removable storage history, website data acquisition, operating system registries and much more. Through this book's chapter, we plan to provide only some basic examples of forensic tools usage and discuss why those matter in a practice. In a Figure 1, we would demonstrate how to use a RAM memory capture forensics tool being suitable for a RAM data collection.

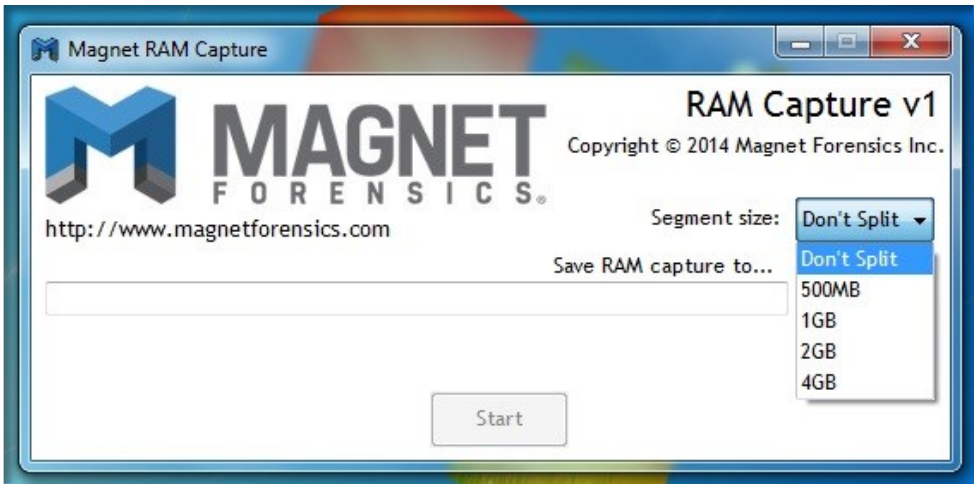


Figure 1. The Magnet RAM Capture

The purpose of tool illustrated in a Figure above would be to capture the RAM memory segment and transfer it to a certain destination for an analysis. That task would require a well-trained investigator that would analyze data and provide an expert's report to some trusted organization. Many defense and justice systems would rely on these findings taking them into a consideration in a case of deciding on someone's legal status. The Figure 2 would illustrate Forensic Acquisition of Website software.

Figure 2. The Forensics Acquisition of Website

As it's represented through the previous picture, the Forensic Acquisition of Website tool is quite easy to handle for the reason it would need a case ID and detective details at its beginning. The next step with this application would get provided through a Figure 3 illustrating how such a software may capture the entire website and gather all the data.

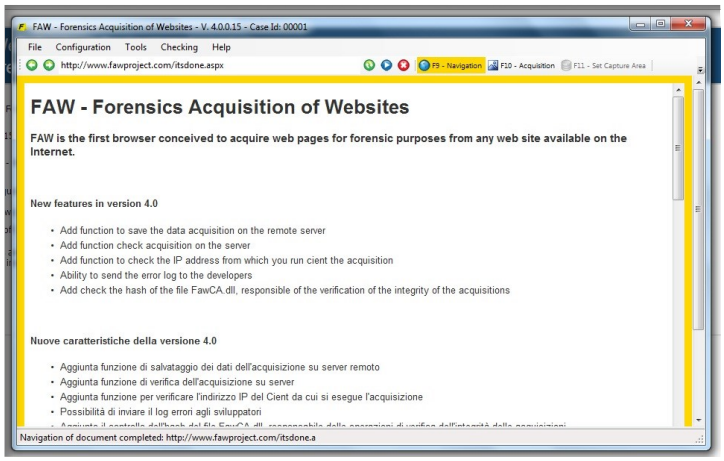


Figure 3. The FAW tool perspectives

The FAW software would capture the entire website offering you navigation, acquisition and setting of capture area. We would highly recommend to everyone to try testing tools being given at the Forensics Control website. Also, some developing societies could attempt to select some of these free tools for their digital forensics investigations. We believe some comparative analyses and researchers could offer the answer to a question if these freeware tools may replace the commercial ones in some sense.

The goals of such a conducted investigation

The primary goal of digital forensic investigation would be to find the evidence about a cyber breach that occurred. Also, the reporting as such an important step with the investigation should offer us a better understanding how such an incident happened and who the key players of that campaign could be. Also, as this sort of investigation is so important to a court process, we would advise the investigators to prepare as good reports as they could – giving lots of information and examples to justice sector staffs.

Some developing countries would still struggle – not having enough skillful staff with policing and justice system that could deal with this modern time and its technological advancements. For such a purpose, we would strongly recommend to those societies to pay more attention to education and training of their employees making them qualified to cope with these new challenges.

The finishing talk

The role of this book's chapter would be to get a closer look at all the concerns and challenges of digital forensics. This practical part of the book would guide us through some basic concepts and could also get used as a training material trying to demonstrate some of the tools being available through the Forensics Control webpage. For more advanced courses, we would suggest much deeper research being conducted in order to contribute with a better insight in an analysis and reporting within a digital forensics.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books"The Internet of Things: Concept, Applications and Security"and "The Insider's Threats: Operational, Tactical and Strategic Perspective"being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with a disability.

Why Power Matters in Cyber Protection

Defending power management equipment in an era of more connectivity

By James Martin, Global Connectivity Product Manager, Eaton

It's well understood that as digital evolution continues opening doors for greater connectivity of devices, enterprises must ensure that new potential entry points are protected from potential cyber attackers. Businesses that strike this balance stand to capitalize on IoT while reaping the benefits from advancing solutions like predictive analytics to help streamline operations and make more proactive, data-driven decisions.

Power devices are becoming a bigger priority for cyber defense as enterprises bring them into their expanding network infrastructure. Earlier this year, the Cybersecurity and Infrastructure Security Agency and the Department of Energy issued a warning concerning network-connected uninterruptible power supply (UPS) devices, urging organizations to take steps now to stave off potential attacks.

Enterprises should evaluate their current cybersecurity game plans now and incorporate power management, considering the steps that follow.

Assess current readiness

Protecting power devices can not only boost enterprises' cyber defenses, but also strengthen trust with their customers. Gartner predicts that by 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements. Having a well-rounded cybersecurity approach that includes power management can serve as example to customers or partners that an enterprise takes network threats seriously across the board.

Global safety standards offer a strong benchmark for IT teams to work from when deploying power devices and solutions. Underwriters Laboratories (UL) and the International Electrotechnical Commission (IEC) provide important guidelines for the implementation of appropriate cybersecurity safeguards in network-connected devices, including those in the power management space. Deploying UPSs with network management cards that carry UL 2900-1 and ISA/IEC 62443-4-2 certifications can give teams peace-of-mind that their devices were developed with cybersecurity in mind.

Employ best practices

In addition to leveraging power management solutions with baked-in cybersecurity capabilities, enterprises should use best practices with power management technologies that apply across an interconnected network. Examples include using firewall and industrial security solutions as well as encrypting information; conducting routine security assessments; regularly updating antivirus software and antispyware; using advanced email filtering; establishing powerful password policies and end point protection; and offering employees cybersecurity awareness training.

Enterprises should also look to execute remote firmware updates to keep current with the latest features. Selecting power devices that require cryptographic signatures for all firmware updates can help IT teams avoid cybersecurity risks. Additionally, looking for vendors that offer 24/7 monitoring across converged IT/operational technology (OT) environments will add an extra layer of protection and visibility for critical infrastructure.

Although primarily developed to monitor and manage power devices – as well as gracefully shut down critical loads during outages – power management software can also be used to provide an inexpensive, highly viable air gap solution. This measure helps keep secure networks physically isolated from unsecured ones including the Internet. Organizations such as Grandeur Housing use this method to safeguard against ransomware attacks while enhancing overall cybersecurity.

Embrace the evolution

By leveraging power management software, enterprises can stay on top of emerging cybersecurity threats like the Ripple20 vulnerabilities , which surfaced during the early days of the pandemic and put many internet-connected devices in jeopardy. Power management software allows IT teams to keep up with the latest patches and secure their power management components from Ripple20 and other new threats that develop.

Enterprises may also find it useful to partner with technology and solutions providers that demonstrate an ongoing commitment in protecting against cybersecurity risks as the proliferation of smart, connected devices link together more elements of IT operations. A key advantage that comes with this

type of collaboration is the ability to continuously monitor distributed networks and make necessary updates quickly as new threats are identified.

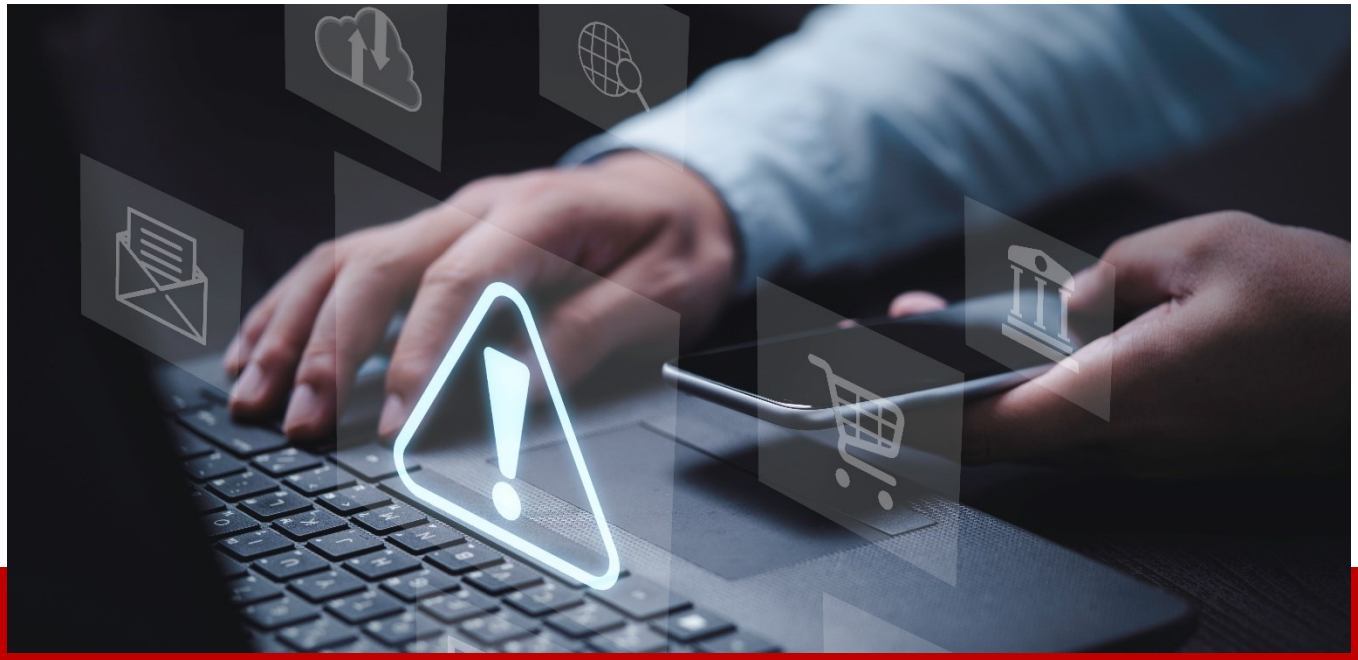
Some enterprises could be tempted to overlook physical security when it comes to protecting power devices and other IT equipment. However, this should be given careful consideration since attackers can use physical infrastructure to target critical data. Measures such as putting smart security locks on IT racks can be helpful to ensure only authorized personnel have access to these components.

Secure for the future

Enterprises will need to get used to the concept of weighing cybersecurity capabilities for their power management equipment, as this will only grow in importance as IT infrastructure becomes more interconnected. Every network access point needs to be safeguarded from potential cyber threats. By securing power devices as part of a full network defense, enterprises and their IT teams can have peace of mind knowing that they aren't enhancing connectivity at the expense of cybersecurity.

About the Author

James Martin is the global connectivity product manager at Eaton. He has promoted Eaton's software and connectivity solutions for the past 10 years and built trusted technical adviser relationships with channel partners, field sales, and sales operations. James can be reached online at (jamesmartin@eaton.com) and at our company website https://www.eaton.com/us/en-us.html?percolateContentId=post%3A1



With Increased Cybersecurity Awareness, Why Does Phishing Still Work?

By Zac Amos, Features Editor, ReHack

With the costs of cyberattacks rising and the effects becoming more severe, many decision-makers realize cybersecurity awareness training must be an ongoing part of employee education. Many of the most successful and widely used attacks relate to phishing. They happen when a cybercriminal imitates another person or organization to gain information from a victim.

However, these attacks still happen even as workers sit through hours of training and go through realistic phishing simulations. Why is that the case?

1. Cybersecurity Training Programs Are Not Sufficiently Effective

Adding cybersecurity training to employees' schedules is not enough. The educational content they receive must also be actionable enough that they can apply it to their daily lives — whether at home or work. However, a 2023 Fortinet study suggests that's not happening.

About 90% of leaders polled believed additional cybersecurity training for employees would reduce cyberattacks. Another 85% of respondents said they taught workers cybersecurity best practices. However, over 50% said employees still lacked knowledge in this area. That suggests aspects of the training make it less than maximally effective.

Company representatives in charge of training might improve it by digging into internal data to determine where shortcomings exist. Alternatively, they could gather information through quick, informal quizzes. How many employees can correctly identify phishing attack characteristics? What percentage know the best practices for creating and using passwords? Answering those questions can show trainers which areas to focus on in future sessions.

2. Many Workers Juggle Numerous Responsibilities

People under constant pressure don't have as much time and may not feel clear-headed enough to accurately judge what constitutes legitimate communication versus a phishing scam. That can compromise data integrity in more ways than phishing attacks.

A 2022 Tessian study revealed that more than two-fifths of respondents mentioned distraction and fatigue as their reasons for falling for phishing attacks. Another 52% said they were tricked by phishing attacks that impersonated a company executive. People who are tired and dealing with duties that pull their attention in all directions may be less likely to identify phishing attacks, even after getting the appropriate training.

However, the study also showed other things can compromise data security. For example, 40% of respondents sent emails to the wrong person and 29% said their companies lost customers or clients because of that mistake.

Training employees about data-handling procedures is as important as teaching them to recognize phishing attempts. One frequent suggestion is to minimize the number of people with access privileges. Many companies do that by setting security parameters so users can only see information directly related to their task or role.

3. More Employees Use Personal Devices for Work

Many employers have started implementing bring-your-own-device (BYOD) policies. Doing that to handle some workplace tech needs has numerous advantages. Workers can use items they already know well, which could result in higher productivity and greater satisfaction. Plus, companies can reduce their hardware and software spending.

However, one BYOD downside is that employees may not update their devices as often as they should. Cybercriminals frequently exploit known vulnerabilities during their attacks. That could make personal devices used for work particularly useful targets for perpetrators.

A 2023 SlashNext study found 43% of employees experienced work-related phishing attacks on personal devices. It's also problematic that 90% of security leaders identified protecting employees' equipment as a top priority, but only 63% said they had the tools to do it adequately.

Another takeaway was that 50% of phishing attacks happen outside of email. Plus, 95% of the security leaders in the study identified phishing via private messaging apps as an increasing problem.

It becomes more difficult for IT teams to secure personal devices employees use for work. It's harder to ensure the equipment has the most updated software and operating system versions.

4. Cybersecurity Awareness Is Only Part of What's Needed

A study published in 2023 by Zscaler ThreatLabz showed a 47.2% rise in phishing attacks for 2022 compared to the previous year. The researchers also found that cybercriminals deployed increasingly sophisticated attacks. That could mean the cybersecurity awareness training attendees receive must be more in-depth to prepare them for most potential attack methods.

Elsewhere, a 2022 study from The National Cybersecurity Alliance and CybSafe showed 58% of those who had cybersecurity training believed they were better prepared to recognize phishing and related attacks. Even so, 34% of that group still experienced at least one type of cybercrime.

Lisa Plaggemier, executive director of the National Cybersecurity Alliance, explained that these findings highlight how cybersecurity training is crucial for helping people protect their data. Still, it is only one component of what internet users must do to keep themselves and their devices safe. She said that since cybercriminals are becoming more aggressive and successful when targeting everyday users, there must be a total overhaul in what's done to help people build cybersecurity practices into their lives.

Phishing Education Must Evolve as Cybercriminals' Tactics Do

Teaching people to spot and avoid phishing attempts remains relevant and necessary. However, trainers, IT teams and others involved in such processes must not treat education as a static effort that happens once throughout someone's time at a particular workplace.

Cybercriminals increasingly use newer and more advanced approaches to trick their potential victims. Cybersecurity training about phishing and other notable topics must also be updated. People must understand the importance of using best practices for online security whenever they use the internet — not just at work. When these things happen, phishing attacks should become less successful.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on Twitter or LinkedIn.


EVENTS

DEFENSE STRATEGIES INSTITUTE PRESENTS:
THE 3RD ANNUAL

CRITICAL INFRASTRUCTURE SECURITY SUMMIT

PROTECTING US INFRASTRUCTURE THROUGH ADVANCED CYBER CAPABILITIES

JULY 26-27, 2023

MARY M. GATES LEARNING CENTER

ALEXANDRIA, VA

INFRASTRUCTURE.DSIGROUP.ORG

JOIN THE CONVERSATION AND REGISTER TODAY

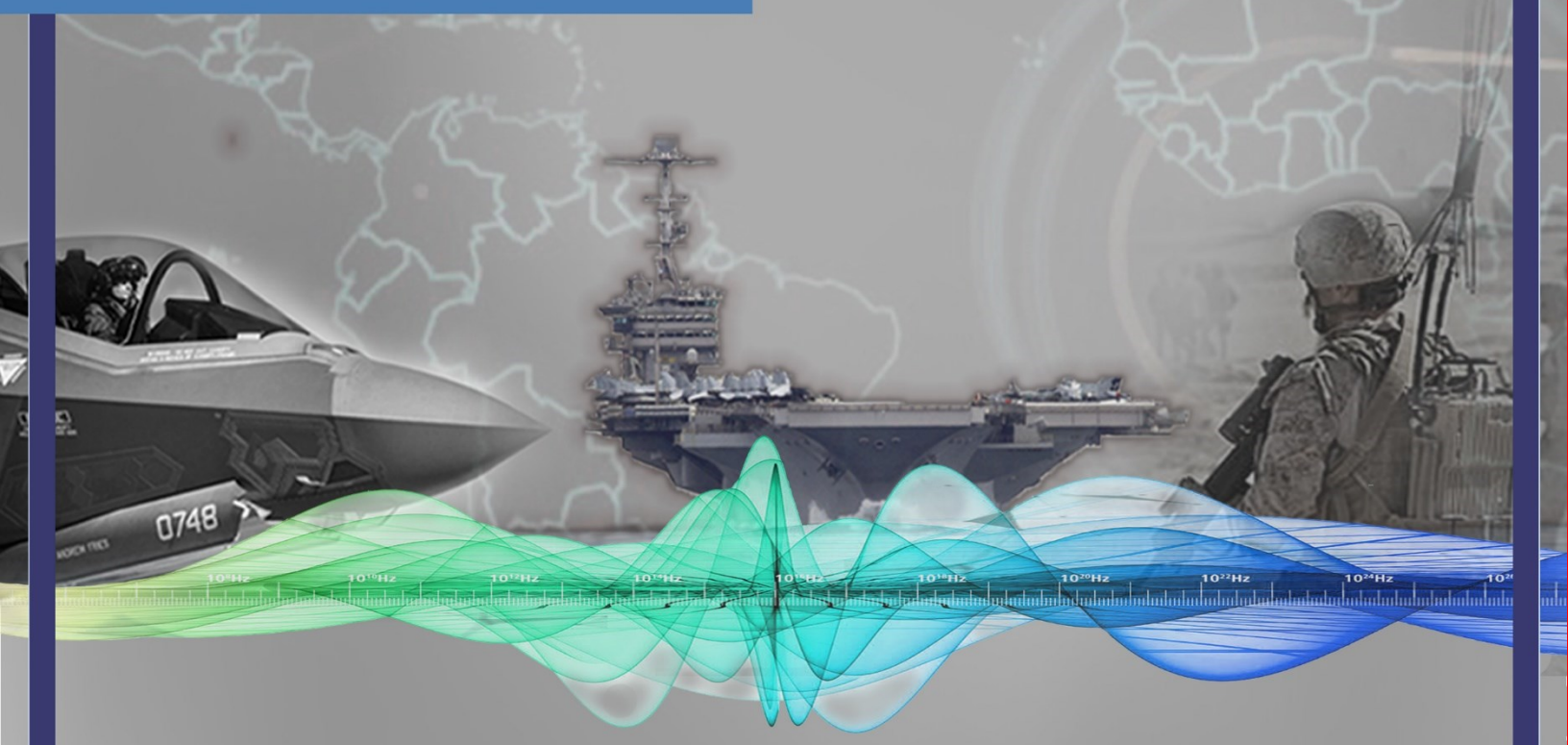
ACTIVE MILITARY AND GOVERNMENT EMPLOYEES ATTEND FREE

5TH INFORMATION WARFARE SYMPOSIUM

MILITARY/GOVT ATTEND FREE

NATIONAL HARBOR, MD

JULY 26-27, 2023



INFORMATIONWARFARE.DSIGROUP.ORG

Organized and Conceptualized by

3rd Edition

CONNECTED AFRICA

Africa's premier Telecom Event

"Transforming to Telco's of the Future"

July 25, 2023

Johannesburg, South Africa

For More Details

CYBER DSA 2023

15 - 17 AUG 2023 | KUALA LUMPUR CONVENTION CENTRE

ADVANCING DIGITALISATION & SECURITY THROUGH COLLABORATION

Have You Registered?

Get ready to connect with the top players in the **cybersecurity industry** at **CyberDSA 2023**

Scan the QR:
Register for **FREE Visitor Pass** to Exhibition.

Scan the QR:
Ticket for attending **All Access Conference** is now **ON SALE**

Forum & Tracks Schedule:
https://bit.ly/ForumTracks

www.cyberdsa.com | CyberDSA

SUPPORTED BY:
MINISTRY OF COMMUNICATIONS AND DIGITAL | MALAYSIAN ARMED FORCES | ROYAL MALAYSIA POLICE

STRATEGIC PARTNERS:
DEFENCE CYBER AND ELECTROMAGNETIC DIVISION (MAF) | CyberSecurity MALAYSIA

HELD IN CONJUCTION:
SIBER SIAGA 2023 | MALAYSIA CYBER SECURITY AWARDS | WBF WORLD BLOCKTECH FORUM

ENDORSED BY:
MATRADE

ORGANISER:
AEROSEA EXHIBITIONS SDN BHD (1357130-A)

IndoSec®

29-30 AUG 2023

AWARDS & GALA DINNER

★ ★ ★

31 AUG 2023
5:00 PM - 9:00 PM

THE RITZ-CARLTON JAKARTA PACIFIC PLACE

Organised by

TRADEPASS

WORLD CyberCon MIDDLE EAST 2023

MEET ESTEEMED SPEAKERS

Abdullah Alfahaid
CIO, Ajlan & Bros Holding

Abdullah Marghalany
Cybersecurity Chief Officer, Madinah Health Cluster

Ali Abdulla Alsadadi
Chief Of Information Technology, Ministry of Oil and Environment, Bahrain

Wael Fattouh
Chief Information Security Officer (CISO), Bank Aljazira

Abdullah Alahmade
Chief Information Security Officer & BCM Director, Tamweel Aloula

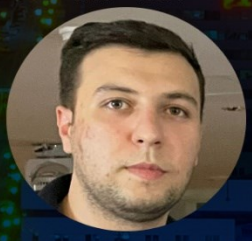
Shenoy Sandeep
Regional Director – META, Cyble Middle East

Dr. Nasser Alamri
Cybersecurity Executive Director, Institute of Public Administration – IPA – KSA

Eng. Ala Zayadeen
Head of Information Security and Data Privacy, BinDawood Holding

Jeevan Badigari
Director of Information Security, DAMAC Properties

Isabelle Meyer
CIO, Zendata Cybersecurity



Ilkin Javadov
Senior Penetration Tester & Ethical Hacker

Augustin Kurian
Editor-In-Chief, The Cyber Express

Ayad (Ed) Sleiman
Head of Special Projects, KAUST

Mousab AlSaaydeh
CS Risk Management Consultant, stc

AUG 30, 2023,
RIYADH, SAUDI ARABIA

REGISTER NOW

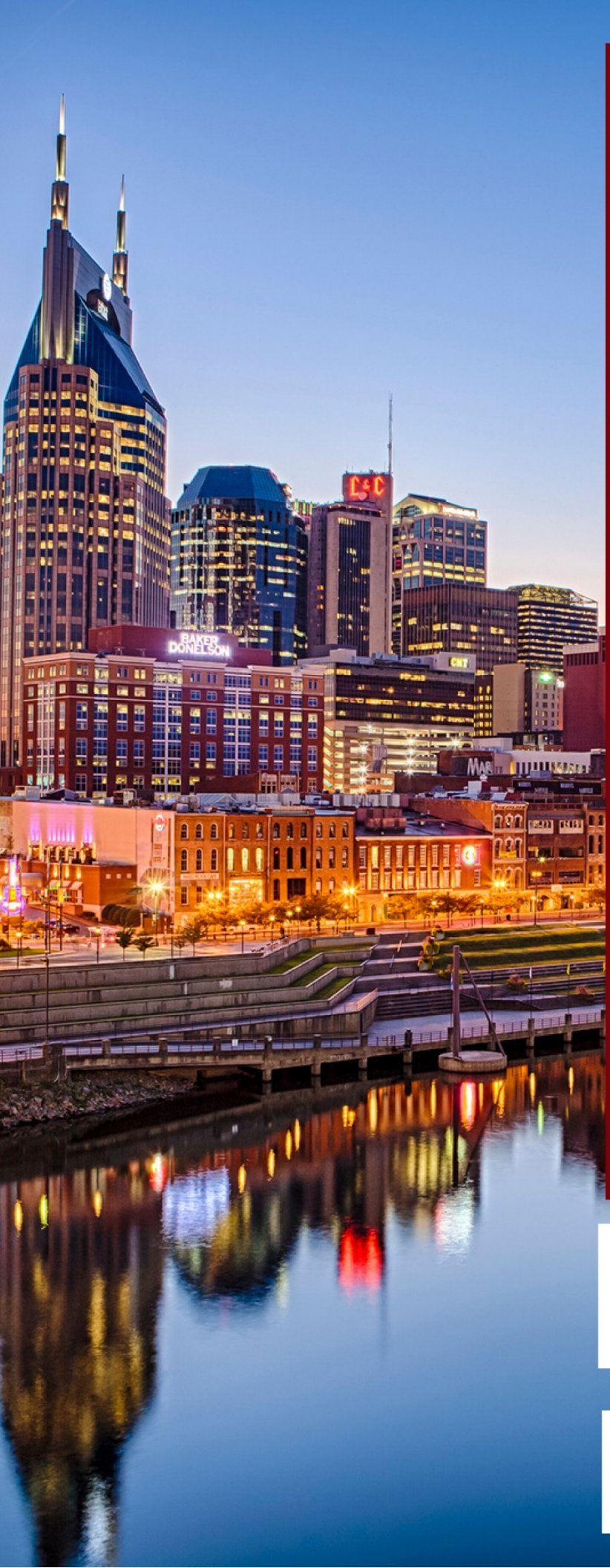
thecyberexPress.com/events

EVENT PARTNERS

CYBLE · potech · ZENDATA · INOEX GLOBAL

MEDIA PARTNERS

CYBER DEFENSE MAGAZINE · INTERNATIONAL BUSINESS MAGAZINE · ACNNEWSWIRE · CIO · WORLD BUSINESS OUTLOOK · siliconindia · GlobalRisk Community · WIRE19



10th annual

Control Systems Cybersecurity USA

NASHVILLE TN SEPT 19-20

www.cybersenate.com

marketing@cybersenate.com

Headline Sponsor

FORTINET®

VERACITY
INDUSTRIAL NETWORKS

TECHEX
EUROPE

Co-Located Events:

CYBER SECURITY & CLOUD EXPO
EUROPE

IOT TECH EXPO
EUROPE

BLOCKCHAIN EXPO
EUROPE

AI & BIG DATA EXPO
EUROPE

EDGE COMPUTING EXPO
EUROPE

DIGITAL TRANSFORMATION WEEK

Contact:
> www.**techexevent**.com
> enquiries@techexevent.com

CYBER SECURITY & CLOUD EXPO

EUROPE

26-27 September 2023, RAI, Amsterdam

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.

6 Co-Located Events

8 Conference Tracks

250+ Speakers

150+ Exhibitors

6,000+ Attendees

76% of attendees are **Director Level & above**

Register now for free tickets!

> www.**cybersecuritycloudexpo**.com/northamerica
> enquiries@techexevent.com

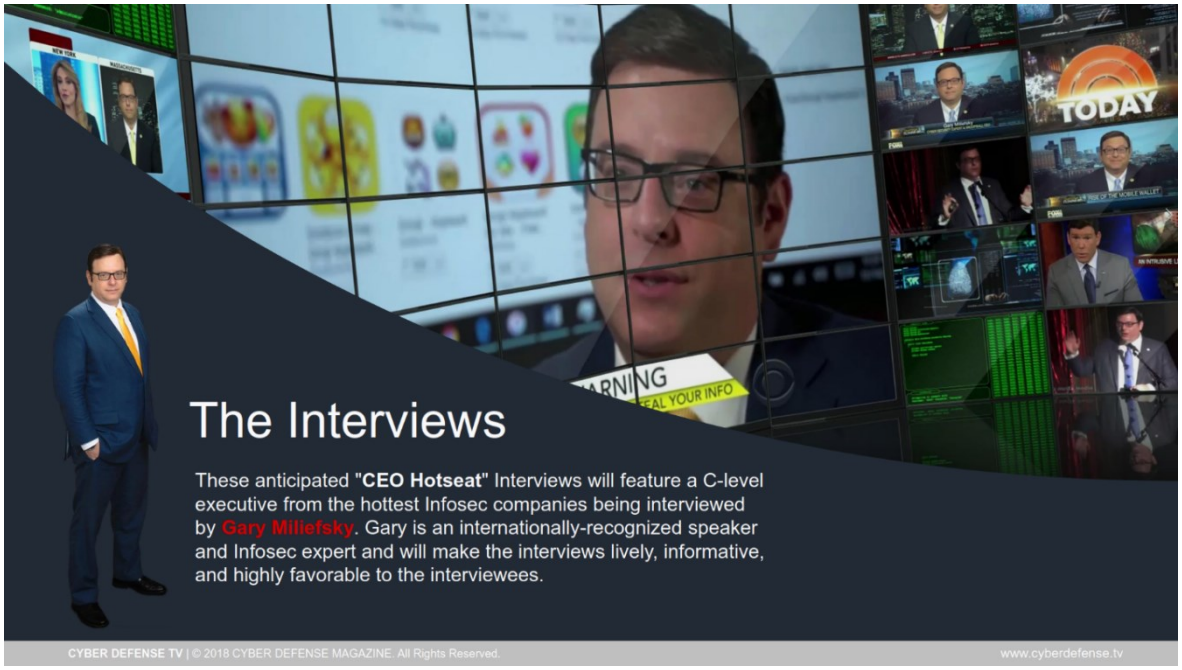
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

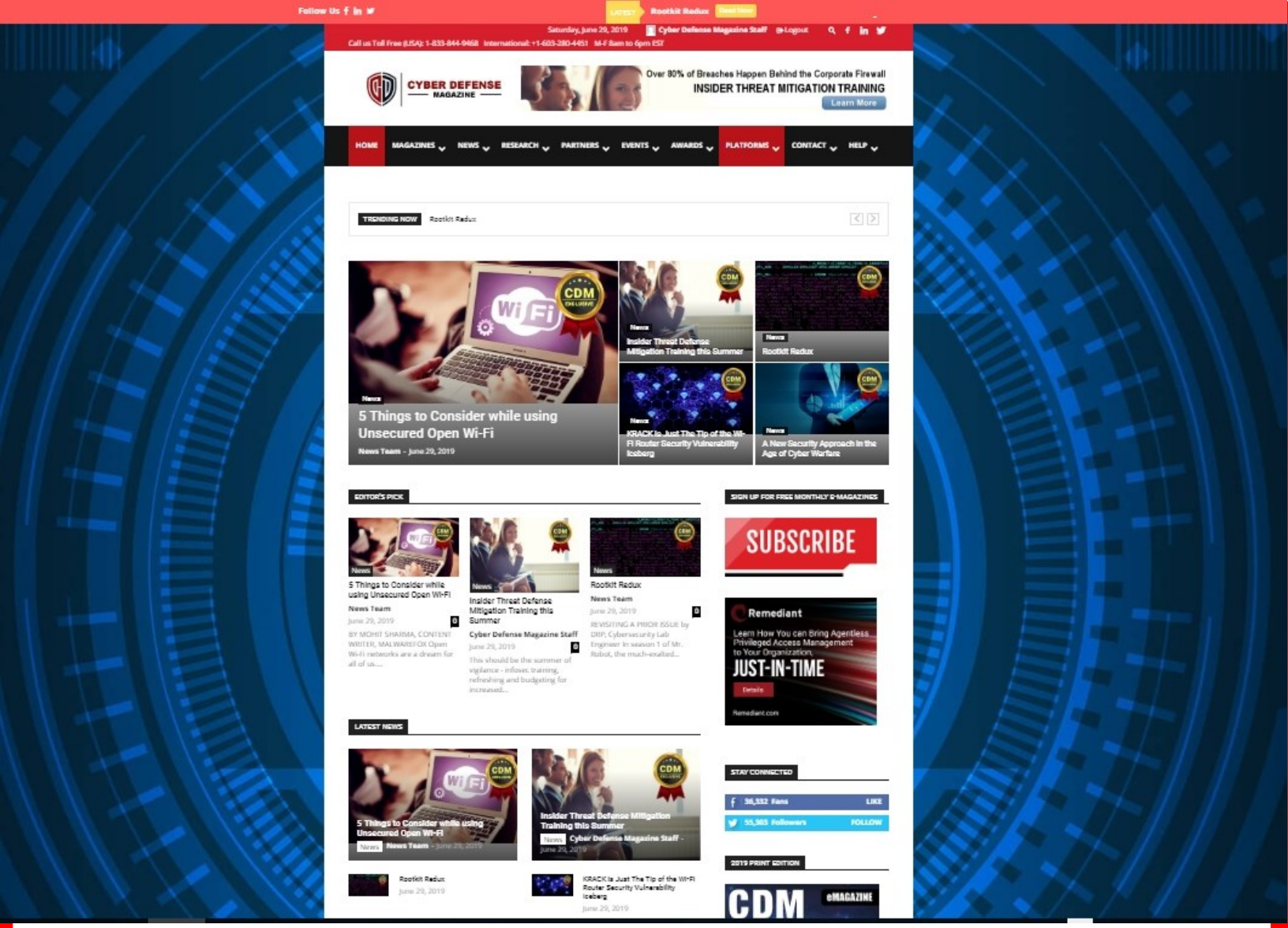
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 07/04/2023



Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

11 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. We successfully launched https://cyberdefenseconferences.com/and have another amazing platform coming soon.

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

RSAConference™2024

San Francisco | MAY 06-09 | Moscone Center

Stronger Together

See for yourself why we are **Stronger Together.**

RSA Conference 2024 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From MAY 06-09 , you'll get the chance to:

- See what the future holds in expert-led Track Sessions covering the hottest topics and emerging trends.
- Expand your knowledge and be inspired by forward-thinking Keynotes.
- Demo the latest products to find real-world solutions from over 600 companies.
- Enhance your career through valuable networking opportunities.

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

FOLLOW US

*** with help from writers and friends all over the Globe.**