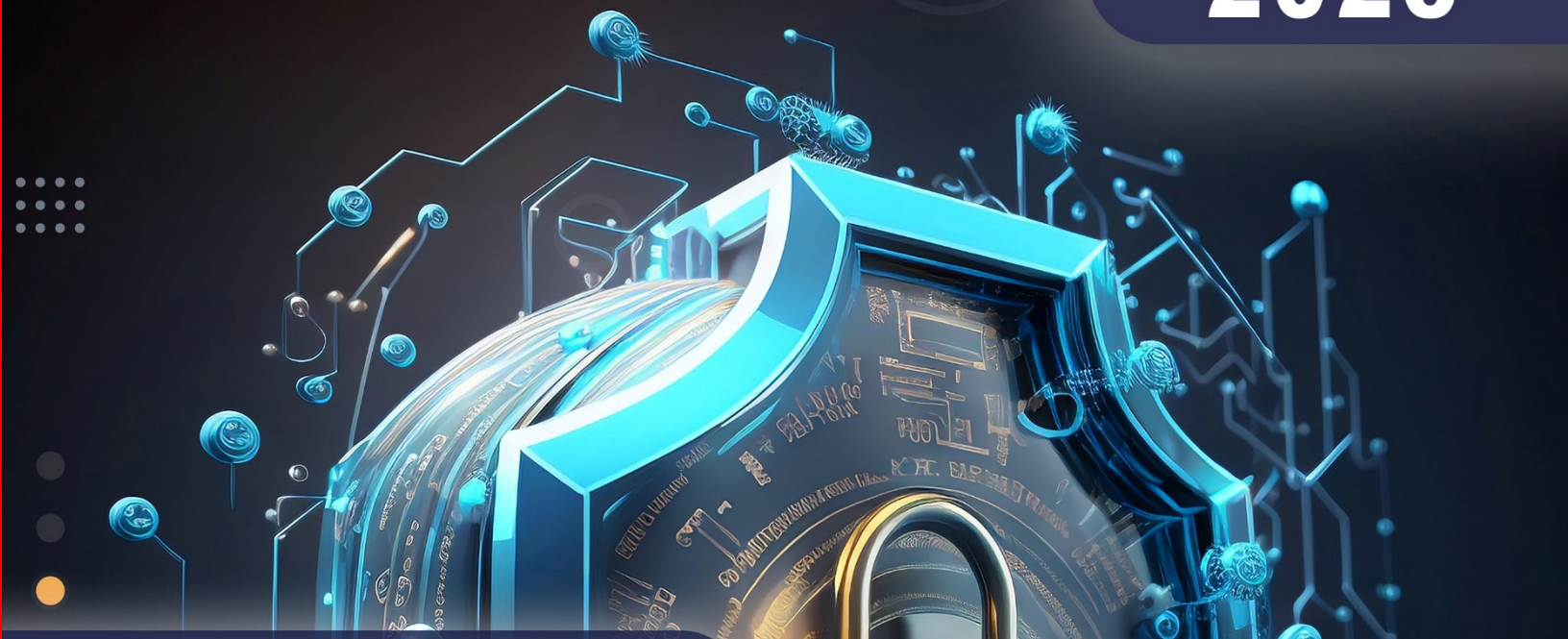
CYBER DEFENSE MAGAZINE

eMAGAZINE

MAY 2023



In This Edition

5 Benefits Of SIEM To The Cybersecurity Of Any Business

A Look At The Damages Covered By Corporate Cyber Insurance

At the Start of 2023, the FAA Grounded Planes Nationwide Due to a Computer Glitch; Is It Any More Secure Now?

...and much more...

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

Dear Friends,

As Publisher of Cyber Defense Magazine, it has been my honor and pleasure to participate in the annual RSA Conference again this year. Coming out of the past several years of restriction and postponement, it was heartening to experience a renewed sense of mission and solidarity among the cyber security professionals who attended this important annual event. Let me extend our thanks to the RSA organization for the strong working relationship we have forged together.

If you're interested in going in 2024: don't miss out, here's your chance for a super early bird signup, here https://go.rsaconference.com/rsac-us2024/us2024-super-early-bird-ryi.

In addition to the very positive reception we received to the Special RSA Issue of Cyber Defense Magazine, being physically present and enjoying many encounters with our readers and contributors was a fulfilling and enjoyable way to stay connected with the people and issues at the forefront of our industry.

On behalf of the entire Cyber Defense Media Group organization, I would also like to express our congratulations to the hundreds of Global Cyber Defense Awards recipients. We are pleased to provide this link to the full list of award winners: https://cyberdefenseawards.com/global-infosec-awards-for-2023-winners/.

With the support of our contributors and readers, we continue to pursue our mission 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

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 May 2023 Issue

From the Editor-in-Chief

This issue of Cyber Defense Magazine for May 2023 comes hard on the heels of the Special RSA edition, which carried a huge body of cutting-edge information of interest to all participants in the cybersecurity industry. We are especially pleased to have included the CDMG Global Awards to so many of our active individuals and organizations.

In my capacity as Editor-in-Chief, I was called upon recently to admonish another online source for infringement of our copyright of exclusive material published in Cyber Defense Magazine. While it is said that "imitation is the sincerest form of flattery," we zealously protect the integrity of our copyrighted content. We are always pleased to grant permission for reposting of articles under appropriate circumstances, but this incursion unfortunately did not comply with this requirement. Once again, we are grateful to our hundreds of contributors who provide actionable information for our thousands of readers.

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™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

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

RSA Conference 2023 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From April 24 – 27, 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

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/

STOP BEING REACTIVE. START BEING PROACTIVE.

Get the Zero Trust endpoint security solution that offers a unified approach to protecting your business, users, networks, and devices against the exploitation of zero-day vulnerabilities.

Visit our website, or speak to a Cyber Hero to learn more about how the ThreatLocker® solution can help you better protect your business.

THREATLOCKER

threatlocker.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

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

Industrial Cybersecurity. **Simplified.**

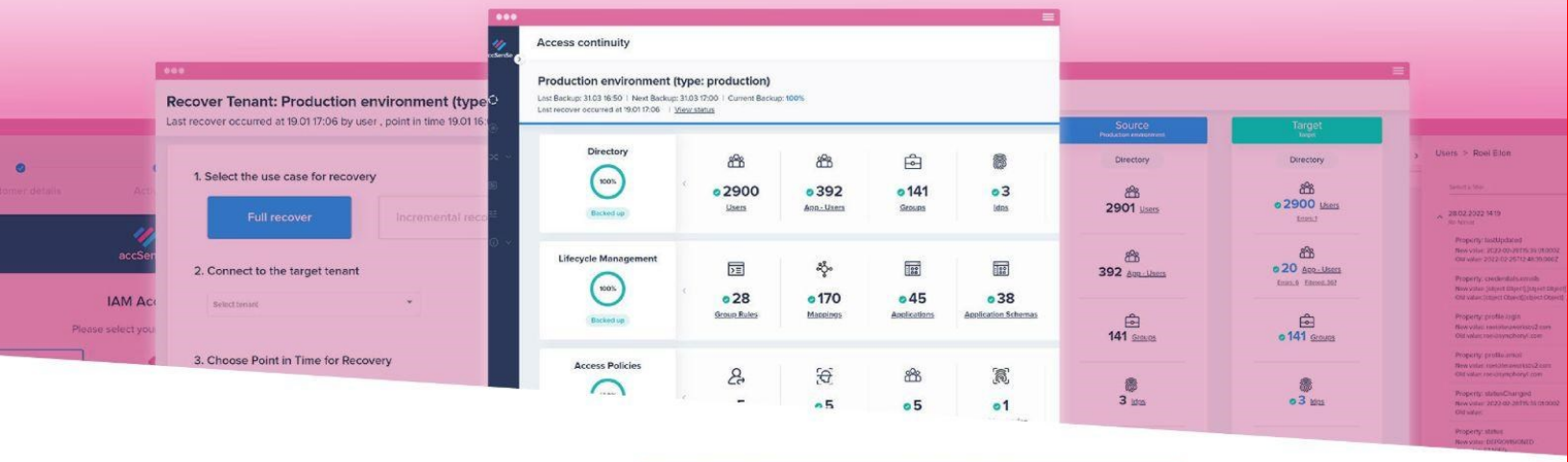
txOne networks | Keep the Operation Running

txone.com


2001
2022
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

accSenSe

A complete protection and recovery solution for your organization's most critical SaaS.
(Your IAM WF and CIAM)



The Road To Quick And Easy Recovery Starts With accSenSe and Okta

- Complete protection for your Okta tenant, which gives you full visibility to configuration and data history.
- The ability to recover means you can reduce RTO during a disaster, keeping your business running and financial loss to a minimum.
- Stay compliant with SOC2 & SOX. The audit capabilities mean you can easily control system changes.

With accSenSe you can rest secure knowing your Cloud Identity and Access Management system is fully protected and recoverable, no matter what tomorrow brings.

monday.com GLASSBOX bright data fiverr.

After running through endless Cloud Identity Access Management system implementation use-cases and disasters, the accSenSe team decided to solve the most significant problem of modern organizations relying on SaaS solutions.

We developed a platform to manage and protect cloud Identity and Access Management system to ensure business as usual isn't just a phrase.

START A 30-day TRIAL >>

https://accsense.io


CYBLE
1 Platform-
6 Capabilities
Darkweb & Deepweb
Attack Surface Management
Brand Intelligence
Cyber Threat Intelligence
Vulnerability Management
Takedown & Disruption
Learn More ▶


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


HORNETSECURITY
ALL-INCLUSIVE
SECURITY
FOR MICROSOFT
365
SPAM FILTER & ADVANCED EMAIL SECURITY
SIGNATURE & DISCLAIMER
TOTAL PROTECTION
ENTERPRISE BACKUP
EMAIL ARCHIVING, ENCRYPTION & CONTINUITY
BACKUP & RECOVERY
FROM EMAIL SECURITY
TO BACKUP & RECOVERY
ALL IN ONE SOLUTION!
START YOUR FREE
30-DAY-TRIAL
WWW.HORNETSECURITY.COM

CYBLE

Is Your Organization Protected Against External Threats?

GENERATE YOUR ORGANIZATION'S EXTERNAL THREAT PROFILE REPORT AND OBTAIN

01 Overview of vulnerabilities in your digital risk footprint

02 Risk assessment of your attack surface and threat landscape

03 Unique Risk Score as per your darkweb exposure

04 Critical information about your leaked data and security posture

SCAN ME

TO GET THE REPORT!

Phylum

The Software Supply Chain Security Company

Stop Software Supply Chain Risk at the Source

Automate software supply chain security to block new risks, prioritize existing issues and only use open-source code that you trust.

Protect the Organization

- Proactive OSS Risk Management
- Policy Standardization & Enforcement
- Improved Signal : Noise
- Modern Attack Prevention

Secure Innovation

- Developer-First Approach to Security
- Reduced Organizational Friction
- Accelerated Release Cycles
- Uninterrupted Developer Workflows

YOUR WEBSITE LOOKS GREAT!

BUT WHAT'S HAPPENING BEHIND THE SCENES?

reflectiz

Reflectiz maps all 1st, 3rd and 4th party risks, including compliance violations, web skimming attempts, and external domain threats.

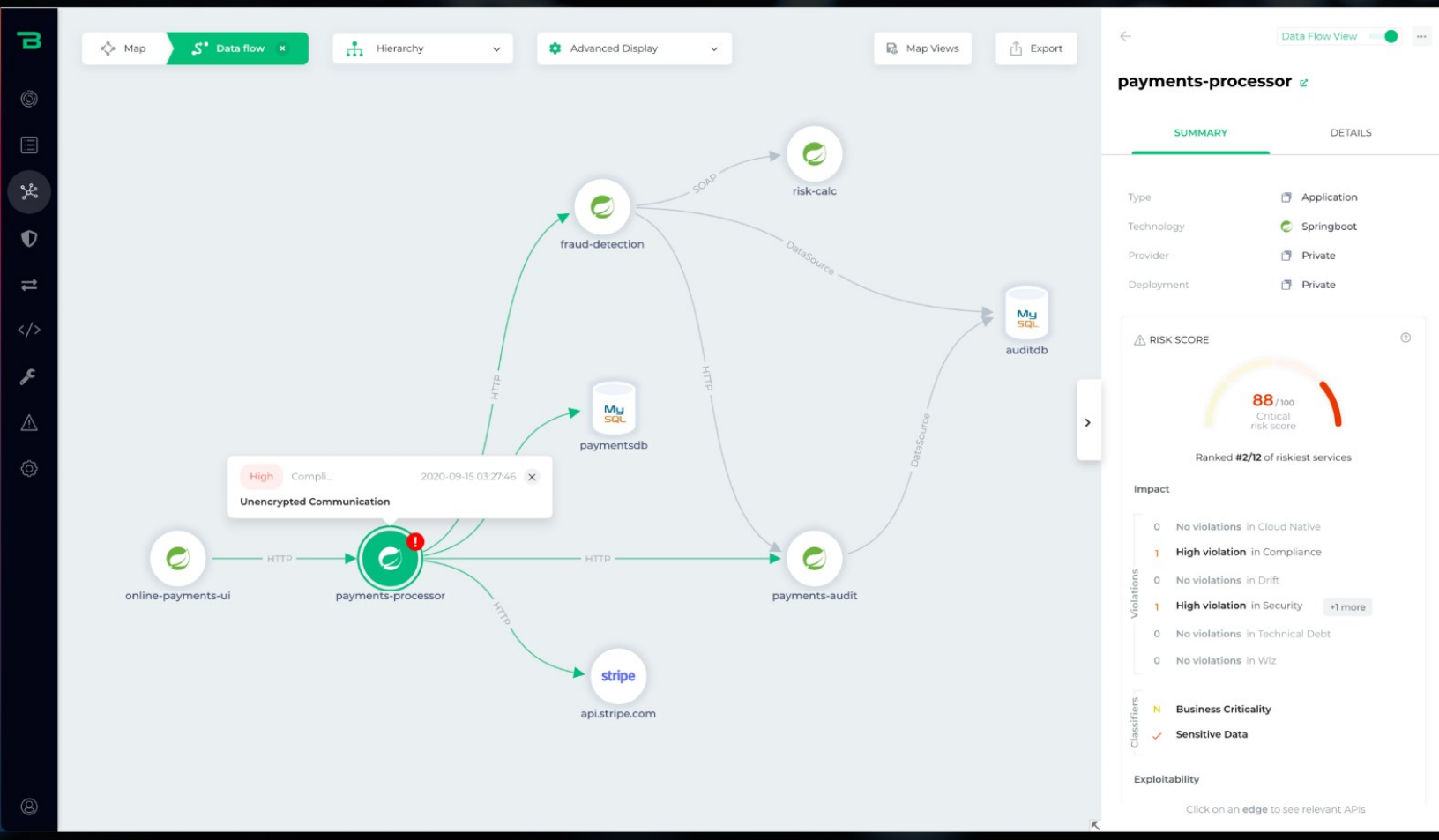
Get in touch for a quick PCI assessment.
www.reflectiz.com

BIONIC

ASPM

Application Security Posture Management

Make applications secure and resilient to significantly reduce business risk.



Start reducing business risk of apps today

www.bionic.ai

Phosphorus

Secure the Enterprise xIoT Attack Surface

FIND, FIX, and MONITOR every IoT, OT, and Network device.

See how Phosphorus can bring enterprise xIoT security to every cyber-physical Thing in your enterprise

xIoT Attack Surface Management + **xIoT Hardening & Remediation** + **xIoT Detection & Response**

Across all xIoT devices

- Enterprise IoT Devices
- Operational Technology Devices
- Smart Buildings & Cities
- Network & Cloud Connected Devices
- Industrial Internet of Things
- Internet of Healthcare Things
- Smart Ships
- Internet of Battlefield Things

Automated bot protection with 24/7 adult supervision.

From the **Top Infosec Innovator Award** winner.

TOP INFOSEC INNOVATOR
CYBER DEFENSE MAGAZINE
2022

DATADOME

datadome.co

plainID
THE AUTHORIZATION COMPANY

Power of the Policy

Move to an Identity-First Security paradigm.

Download the eBook

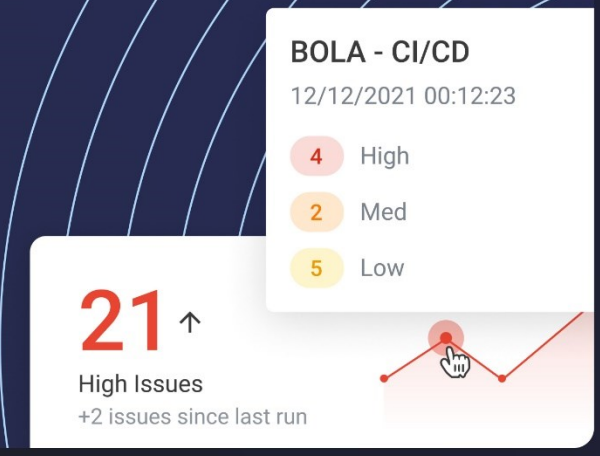
noname

The Complete, Proactive API Security Platform

nonamesecurity.com >

Shift Left with **API Security Testing**

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




ARTICLES

5 Benefits of SIEM to the Cybersecurity of Any Business

By Aaron Haynes, a Columnist at Loganix.com

Cybersecurity is a top priority for many businesses today because of the significant threats they face from hackers and cybercriminals. Companies now deal with a lot of consumer data and they are obliged to protect them from being leaked and accessed by malicious actors.

Cyberattackers use phishing attacks, data breaches, ransomware attacks, DDoS attacks, and other similar methods to infiltrate computer networks and disrupt business operations. They also improve their skills as companies upgrade their cybersecurity, causing those companies to proactively seek out threats to their IT infrastructure to nullify them.

Security Information and Event Management (SIEM) tools can provide companies with the proactive protection they need to ensure their operations run as smoothly as possible. As a business owner considering using SIEM tools, here are five benefits of using them to improve cybersecurity:

1. Threat detection and prevention in real-time

Tools with SIEM capabilities constantly monitor computer networks to detect suspicious activity and alert cybersecurity personnel when there are potential threats. Due to this constant threat detection, companies will discover incidents in real-time and prevent them from infecting the system. This real-time threat detection capability is a game-changer because a successful cyberattack can cause irreparable reputational and financial damage to the affected company.

2. Centralized log management

SIEM tools offer centralized log management which is a vital feature for business cybersecurity. They collect data from various sources like routers, servers, and switches to analyze them to provide an overview of the network. This overview allows companies to discover trends and patterns that denote specific threats. With this knowledge, they can investigate cybersecurity incidents and trace their root causes faster.

3. Better response to incidents

Companies that invest in SIEM tools can substantially increase their response times to cybersecurity incidents. This is because the tools will alert cybersecurity personnel as soon as they detect anything that needs attention. The alerts will contain information on the type of attack, its source, and the parts of the computer network affected so the personnel can immediately respond and apply the appropriate mitigation measures.

4. Improved threat intelligence

Security Information and Event Management tools help companies improve their threat intelligence by collecting and analyzing data from different sources like security logs, vulnerability databases, and threat feeds. This data gives companies extensive knowledge about the new threats they can face. They can use this knowledge to protect themselves from those threats by identifying vulnerabilities in their systems and putting control mechanisms in place.

5. Regulatory compliance

Governments around the world require companies to keep their customer data safe. This can be achieved with the real-time protection feature of SIEM tools and their ability to identify potential threats. By staying compliant with data protection regulations, companies can avoid fines and sanctions from government regulatory bodies.

Endnote

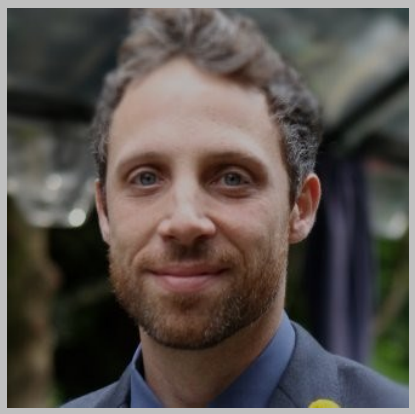
Security Information and Event Management are vital in today's business world because of the cyber threats companies face constantly. Business owners that integrate SIEM tools with their existing cybersecurity structure will be able to spot threats quickly and prevent them from harming their computer network. They also help cybersecurity personnel respond to incidents by providing all the information about threats posed to the network. These features will ensure any company using SIEM tools comply with data privacy regulations so they can avoid penalties.

About the Author

Aaron Haynes, a columnist at loganix.com

Aaron Haynes a Founder of Loganix and also, he is an enthusiastic entrepreneur and Columnist. He served as a search engine control manager in various companies.

Aaron Haynes can be reached online at https://twitter.com/myfenixpro?s=20 and at our company website https://loganix.com.



A Look at The Damages Covered by Corporate Cyber Insurance

By Taylor McKnight, Digital Marketing PR Specialist, Tivly

Consider cyber liability insurance to protect your business from a data breach or cyber-attack. This type of insurance covers the costs associated with such incidents and any legal claims that may arise. It is often called 'Cyber Insurance' or 'Data Breach Insurance.'

The Importance of Corporate Cyber Insurance

Cyber Liability Insurance or Data Breach Insurance protects businesses from expenses and legal claims resulting from cyber-attacks or data breaches. Protecting against potential incidents involving customer or employee information loss is essential, typically not covered by general liability policies. 1 in 5 businesses experiences data loss or exposure due to cyber-attacks, causing significant liabilities. Small

business owners should consider purchasing cyber liability insurance to prevent financial risks caused by such data breaches, although there might be some gaps in coverage.

The Damages Covered by Corporate Cyber Insurance

Cyber liability insurance covers data and technology issues that general business liability coverage does not include. Certain safeguards, such as antivirus and firewall protection, are required for coverage. Assessments of password procedures, access, and network configuration may also be necessary. Agents and carriers can guide the necessary steps.

First Party Damages

Cyber liability insurance provides liability coverage to protect against damages from a data breach. This coverage may include the cost of the following:

Loss of electronic data

This insurance covers repairing damaged software or replacing lost or stolen data from a cyber attack.

Cyber extortion

If a cybercriminal holds your data or information hostage for ransom, insurance coverage is available to assist with the ransom payment.

Business interruption/loss of income

Cyber liability insurance policies can aid in covering lost income and expenses if your business cannot operate due to a data breach or cyber-attack.

Security fixes and cyber forensics

Having cyber liability can assist in covering the expenses involved in upgrading your security and conducting a thorough investigation of the data breach.

Notification and identity protection for affected customers

Cyber liability insurance can help with the costs of notifying customers affected by data breaches. It can also cover the cost of providing identity protection services. This type of insurance is essential in today's digital world, as cyber threats are becoming more common and sophisticated. Protect your business and customers by investing in cyber liability insurance.

Fraud and credit monitoring services

Cyber liability insurance can cover the cost of credit monitoring for customers affected by a data breach. This is a professional solution to the potentially devastating impact of a data breach.

Third-Party Coverage Offered

Accidental virus transmission can result in damage to a third-party system. It is important to recognize this risk and take measures to prevent it. Such damages can have serious consequences and should be avoided at all costs. It is crucial to prioritize the protection of third-party systems and take responsibility for any harm that may be caused.

Network security and privacy liability

A network security coverage grant is important for businesses to protect from information and privacy risks such as cyber-attacks. It covers first-party costs like legal fees and IT forensics during a data breach or other cyber incident.

Privacy Liability

Privacy liability coverage is important for businesses dealing with sensitive information to protect against potential breaches or violations resulting in liability. This coverage helps with third-party costs and regulatory investigations due to cyber incidents or privacy law violations.

Network Business Interruption

If your organization depends on technology, network business interruption coverage can help address potential cyber risks. This coverage can help recover lost profits, fixed expenses, and additional costs incurred during downtime due to security breaches or system failures.

Media Liability

This policy covers any intellectual property infringement, excluding patent infringement, resulting from advertising your services. It generally applies to online and prints advertising, including social media posts.

Errors and Omissions

E&O coverage is important for professionals to protect against negligence or breach of contract claims, including legal defense costs. It should also cover cyber risk aggregation related to service failures caused by a cyber event. Purchasing the appropriate amount of insurance to cover this risk is important.

What Can Happen if You Do Not Have Cyber Insurance?

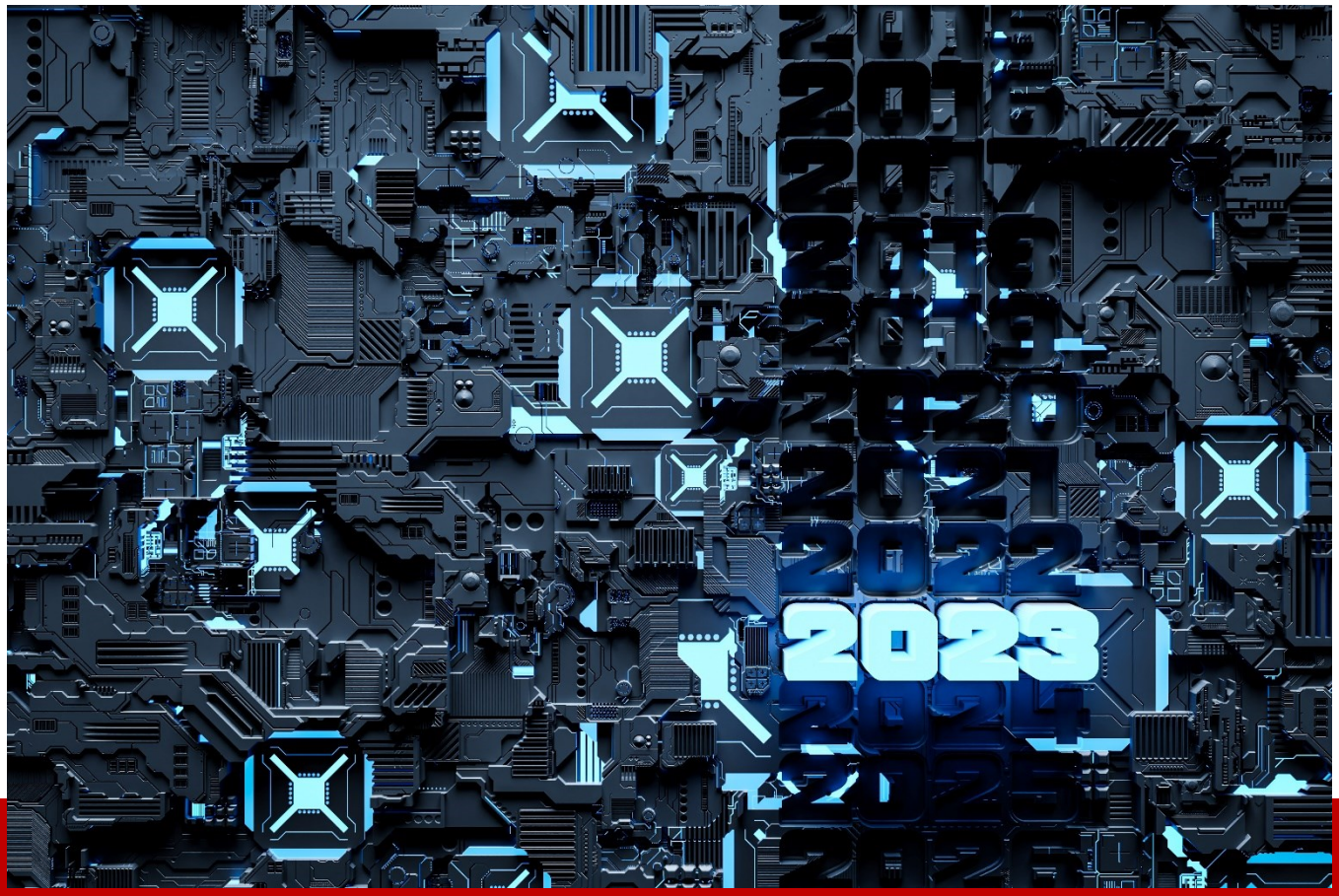
Cyber insurance is important for mitigating cyber-attack risks and reducing liability as a data owner. Not reported lost or stolen information can result in fines, and small businesses are often targeted in cyber-attacks. Cyber insurance can protect them from costs and prevent them from going out of business.

Conclusion

Cyber insurance coverage provides businesses with financial protection against data breaches and cyber-attacks. It's important to understand the available coverage options before deciding. Choosing a policy can help prevent financial losses.

About the Author

Taylor McKnight, Digital Marketing PR Specialist representing Tivly. He also associates with numerous companies across all business niches. Other than working on my clients, He also enjoy working on his social media, taking photographs, and traveling.



At the Start of 2023, the FAA Grounded Planes Nationwide Due to a Computer Glitch; Is It Any More Secure Now?

By Walt Szablowski, Founder and Executive Chairman, Eracent

Just a few months ago, the FAA grounded all flights across the nation resulting in thousands of flight delays. There was a subdued panic as the country theorized the possible and unsettling scenarios that would have led to such an extreme measure; a glitch in the system was not one of them. But that was the official determination by the FAA. How could one accidentally deleted file have such a profound impact on the largest transportation agency of the U.S. government? The White House is pushing toward Zero Trust Architecture to target the cybersecurity vulnerabilities that can so easily be exploited.

Nationwide Ground Stop. What Happened?

On January 11, 2023, the FAA initiated a nationwide Ground Stop (GS).[1] This response was a drastic measure on the part of the FAA and has not been implemented on a nationwide scale since the unprecedented terrorist attacks carried out on September 11, 2001.[2] A GS is initiated reactively due to severe weather, equipment failure, or a catastrophic event.

Speculation ran rampant on that day. Was it another terrorist attack? A cyberattack? The response from the FAA did little to assuage the media or the public at large. The FAA attributed the GS to an overnight outage that disrupted the Notice to Air Missions (NOTAM) System.[3] NOTAM issues real-time alerts triggered by any abnormal status of the National Airspace System to prevent air disasters.[4]

One Unintentionally Deleted File?

So, what happened? Federal aviation officials reported this thoroughly avoidable debacle was a result of one engineer performing routine maintenance who accidentally replaced one file with another.[5] This event was a catastrophic failure of the FAA's software fail-safe infrastructure. Was there no backup system in place?

The U.S. Department of Transportation Office of the Inspector General issued a report citing the ongoing challenges integrating the FAA's Next Generation Air Transportation System due to extended program delays. Case in point; a planned modernization of the antiquated practice of air traffic controllers using paper flight strips to track aircraft is not expected to take effect until 2029.[6]

EO 14028

On May 12, 2021, the White House issued Executive Order 14028: Improving the Nation's Cyber Security, requiring federal agencies to enhance cybersecurity and software supply chain integrity by adopting Zero Trust Architecture and mandating the deployment of multifactor authentication encryption.[7] The effective date for compliance by all civilian government agencies is September 2024.[8]

Never Trust. Always Verify.

Zero Trust Architecture eliminates blind faith in all components of the cybersecurity supply chain relationships by always presuming the presence of internal and external network threats. The Cybersecurity and Infrastructure Security Agency (CISA) is currently examining legacy government cybersecurity programs. CISA's Zero Trust Maturity Model aims to assist government agencies in developing and implementing Zero Trust strategies and solutions.[9]

If the FAA already had a Zero Trust system in place, this isolated area of vulnerability in the NOTAM system would have been immediately flagged. The necessary controls would instantly switch to the backup system in real time.

No Process = No Cybersecurity

The theoretical implementation of a Zero Trust model is only as effective as the process that monitors it and distills it into a structured and auditable process. It requires a comprehensive framework that supports, expedites, and coalesces all networks and endpoints along with their components, software applications, organizational data, policies, and audit-risk analysis.

Traditional security approaches automatically conclude that all software components are secure once they gain access to the network. In a Zero Trust configuration, every component must continually prove that it can be relied upon. Its application on a federal and corporate level is a critical IT initiative to prevent systemwide failures like what happened to the FAA.

What Needs to Be Protected?

Most importantly, businesses and government agencies need to define what they need to protect to design a cybersecurity system that fits and supports each organization's unique requirements. It's all about risk analysis. What is the size of the network? What software is on the network? What data is on the network, and where is it? Vulnerabilities need to be identified and mitigated before they can be exploited. And that requires vigilance. Holistic cybersecurity requires Zero Trust Architecture that is clearly defined, managed, and constantly evolving. It's one thing to design a process and another to make sure that it's actually happening through constant reporting.

Most companies expect their cybersecurity software to fail, assuming the fault lies within their organization, prompting them to try something else. Zero Trust is not "one and done." Successful execution requires complete network visibility within a single management and reporting platform in an automated and repeatable process.

Zero Trust vs. VPN

No one is safe from cyber threats. Any organization that sells or uses software must be vigilant. Although the FAA denies that the NOTAM system was hacked, its current lack of Zero Trust Architecture leaves it open to cybersecurity threats.

Cyber threats come in many forms — malware, ransomware, phishing, or corporate account takeover. For corporate cybersecurity that relies on Virtual Private Networks (VPNs), a compromised external device could infect an entire network. With the increased prevalence of remote and hybrid workers, VPN vulnerabilities are becoming more apparent.[10] VPNs are contained within the network's perimeter, permitting only users with access to engage with the network, assuming that anything within the boundary can be trusted.

Zero Trust takes the opposite approach, assuming nothing and no one can be trusted. It oversees the entire network and serves as the gatekeeper demanding continuous authorization to gain entry. It is imperative for organizations to implement technologies that are built on a well-defined and scheduled process that is routinely tested.

Hackers Could Be a NASDAQ Company Today

Cyberattacks have become so commonplace that corporations consider dealing with the constant threat as a cost of doing business, like dealing with the mafia. A new breed of 'ethical hackers' use ransomware attacks to bully companies by demanding money to restore access to their network. The amount demanded is 'reasonable' in that it won't put the target organization out of business. After all, hackers want repeat customers too.

There is less noise in the media about major hacks because the hackers don't want to garner too much attention; they want to build up their clientele. Hacking is a business in its own right.

Is the FAA Any More Secure?

The FAA NOTAM system is reportedly 30 years old and at least six years away from being updated.[11] The good intentions of EO 14028 can only become a reality if there are consequences for failing to implement it. Execution of the mandate is complicated, confusing, and time-consuming, and if there is no penalty for being hacked, there is no motivation to follow through on the initiative.

The FAA shutdown is a wake-up call that all government agencies and civilian organizations need to answer.

About the Author

Walt Szablowski is the Founder and Executive Chairman of Eracent and serves as Chair of Eracent's subsidiaries (Eracent SP ZOO, Warsaw, Poland; Eracent Private LTD in Bangalore, India, and Eracent Brazil). Eracent helps its customers meet the challenges of managing IT network assets, software licenses, and cybersecurity in today's complex and evolving IT environments. Eracent's enterprise clients save significantly on their annual software spend, reduce their audit and security risks, and establish more efficient asset management processes. Eracent's client base includes some of the world's largest corporate and government networks and IT environments. Dozens of Fortune 500 companies rely on Eracent solutions to manage and protect their networks. Visit https://eracent.com/.

Cyberattacks Coming?

In light of foreign conflicts and the existing rash of global, large-scale hacks, how can financial companies and institutions protect themselves?

By Bryan Keepers, Director of Channel Sales Americas, Opengear

The modern cyber landscape is undergoing something akin to the Cold War, where there are no direct confrontations between factions but clandestine attacks. Notoriously, in 2020, there was the SolarWinds hack, where suspected non-domestic hackers carried out ransomware attacks against several US corporations and government agencies. Recently, there have been multiple hacking incidents that some experts attribute to foreign conflicts, including hackers penetrating websites belonging to multiple overseas agencies and displaying anti-government and anti-invasion images and messages. Likewise, hackers linked to foreign governments breached the networks of US government agencies for at least six states. Moreover, a cybersecurity company accused the US National Security Agency of infiltrating

and monitoring companies and governments in over 45 countries. Unfortunately, businesses, especially financial services, could get hit in the crossfire.

As cyberattacks increase in frequency and sophistication, financial organizations need to protect themselves and minimize the downtime caused by cyberattacks. Last year was particularly bad for businesses in the financial services sector, with organizations suffering the largest number of known breaches in 2022, second only to government organizations. More than 60% of global financial institutions with at least $5 billion in assets were targeted by cybercriminals this past year. The average cost of a financial services data breach is $5.85 million, resulting in brand damage, lost customers and thousands of dollars in fines. Most concerning is that less than a quarter of financial service organizations feel "very well" prepared for a cyberattack and the network outages accompanying these breaches.

As the world's most regulated industry, the financial sector is constantly under pressure to meet new compliance requirements. To comply with these regulatory demands, financial institutions are integrating more Internet of Things (IoT) at branch locations, increasing the usage of mobile apps and creating more distributed sites – all requiring additional network capabilities. Nevertheless, the more complex a financial company's network becomes, the more vulnerabilities get created inadvertently. And, like a vicious cycle, more breaches lead to more network outages. The time it takes network engineers to resolve downtime is also getting longer, causing significant productivity loss, decreased customer satisfaction and increased employee turnover. In addition to focusing on encryption and security strategies to reduce and contain cyberattacks, financial businesses must also work to build a resilient network capable of bringing operations back up to keep ATMs running, branches open and apps operating.

One approach to ensuring a secure network that can also bounce back quickly from an outage is leveraging an out of band network, which provides an alternative pathway, allowing the network to continue operating even if the product network becomes unavailable. Consider that 98% of Millennials, who generate a massive portion of US income, rely on mobile apps for various banking activities. Should the network go down, these valuable customers will still have a way to use a bank's service if an out of band network is in place because engineers can separate and containerize the functions of the management plane. Similarly, an out of band network is an ideal independent management plane. It operates free from the primary in-band network giving engineers secure, reliable and – most importantly – remote access to the primary network. The ability to remotely identify and remediate network issues is invaluable, as sending engineers on-site whenever there is an issue can take hours or even days to fix.

All network devices for financial intuitions are potential targets – branch and edge devices are no exception. Every aspect of the network infrastructure needs to have built-in security and resilience. Take, for example, an ATM network with machines in many remote sites; since the beginning of 2022, there has been an increase in malware-based attacks on ATMs. Should an ATM go down because of a cyberattack, there is the risk of lost revenue, but also the threat of compromised data. Typically, when an outage occurs, a bank would send a technician on-site to resolve it, which is ineffective and time-consuming. However, with an aforementioned out of band network, engineers will always have remote access when the network is up and down. And by installing out of band management units at each ATM, companies can reduce downtime to a few minutes, bringing machines back up and running swiftly. Perhaps the most helpful aspect of an out of band network is that it eliminates the need to send an engineer physically on-site and then have them carefully and securely open up the ATM.

While an out of band network is pivotal to recovering quickly from outages caused by cyberattacks, it is not a replacement for cybersecurity hardware or software, merely a critical addition to a business's complete security posture. As society grows more dependent on financial apps and digital systems to store, transfer and deposit money, the more vulnerable it becomes to the endless cleverness of cybercriminals. From 1834, when a pair of thieves effectively conducted the world's first cyberattack by hacking the French Telegraph System and stealing financial market information, until today, our world has become embroiled in cyber thefts on a global scale – which isn't changing anytime soon. Financial services and institutions need to recognize this reality and protect themselves accordingly.

About the Author

Bryan Keepers is the Director of Channel Sales Americas at Opengear. As a channel veteran, Bryan has over 25 years of experience working in sales and with partners. He has grown Opengear's Partner Program and channel presence exponentially, becoming a thought leader on channel strategy, differentiating Opengear and building valuable relationships as a trusted advisor. Bryan can be reached online at First Name can be reached online on LinkedIn and at our company website https://opengear.com/.

Continuous On-Demand Training Is the Only Way Forward for Cybersecurity Readiness

By Taavi Must, CEO and Co-Founder, RangeForce

The days of sending cybersecurity personnel away for five days once a year for product-focused training from security vendors or a SANS course are making way for continuous, on-demand upskilling using realistic cyberattack scenarios and emulated technology stacks.

When Dataport established a security operations center in 2018 using existing employees from other IT roles, it took a three-pronged approach to bolster its cybersecurity awareness and response posture. The mid-sized German IT service provider, which caters to the public sector, focused on internal mentoring, traditional in-person training and a cybersecurity-readiness platform to better detect and defend against attacks and protect its customers' digital sovereignty.

Dataport turned to RangeForce's cybersecurity upskilling solutions as that third pillar, and its cybersecurity readiness has improved immeasurably since the engagement started in 2020. Dataport has transformed a team without any experience in running a security operations center into one of the top-performing teams using those offerings. That progress affirms the value of continuous development and assessment of cybersecurity skills using real-world threat scenarios for organizations confronting a constantly changing security landscape in which humans are the weakest link. The 2022 ISG Provider Lens™ Cybersecurity — Solutions and Services report for Germany also documents the need for more training: The war in Ukraine, disruptions caused by the COVID-19 pandemic, and the increasing digitization of enterprises have expanded attack surfaces and resulted in more cybersecurity breaches there.

Today, Dataport is able to tap innovative, interactive and on-demand training solutions that are available 24/7 for individual skills development and benefit from team threat exercises. RangeForce works with Dataport to identify skills gaps and target training. Expert-created modules cover a range of cybersecurity knowledge levels and are released weekly with content mapped to industry frameworks such as MITRE ATT&CK and MITRE D3FEND.

Team threat exercises, meanwhile, test Dataport's coordination under pressure in realistic, but controlled, threat environments. Its teams use emulated networks with commercial and open-source solutions on RangeForce's cloud infrastructure, where they can experience simulated threats, vulnerabilities and cyberattacks, and defend against them just as they would in the real world. Teams can choose from more than 15 prebuilt attack scenarios, from ransomware to data exfiltration to web defacement, based on team type and level of difficulty. After putting their skills and processes to the test, Dataport receives assessments of how well its teams should perform when dealing with actual attacks on their infrastructure or customers' infrastructures, along with follow-up recommendations to improve their cyber readiness and benchmark it against peers.

Since its initial RangeForce implementation, Dataport's platform adoption has grown three-fold with participation from security analysts and incident response and engineering operations teams. Dataport employees have completed thousands of hours of hands-on training that otherwise would be cost-prohibitive in terms of the required in-house expertise and effort to build out modules and simulated tech stack environments.

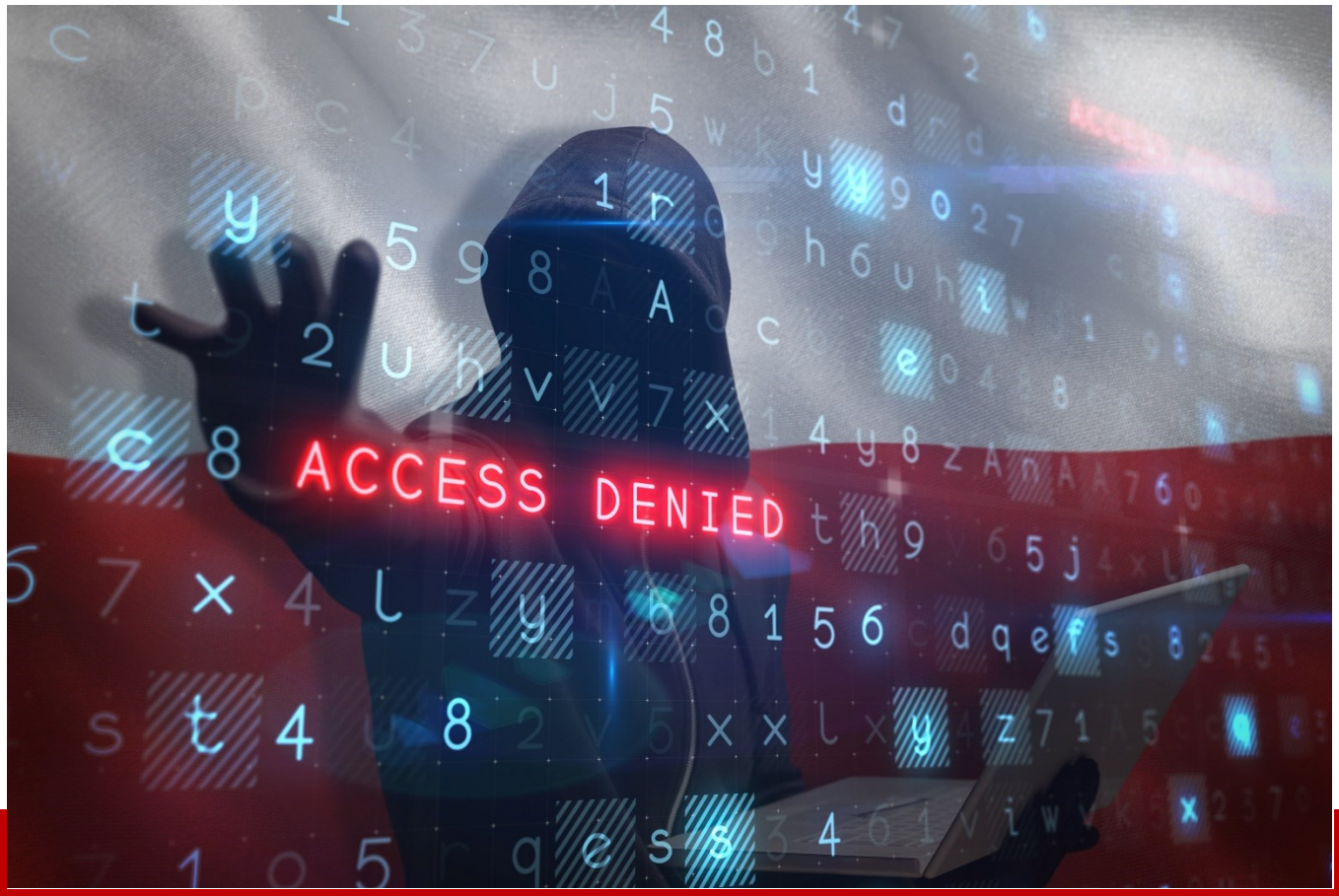
During team threat exercises, at least 90 percent of customer teams are unable to pinpoint attacks until they're provided some information via email into the threat environments. In Dataport's most recent threat exercise, however, both participating teams identified the attack and immediately started defending against it without that added intel.

A continual learning approach to cybersecurity readiness is paying dividends for Dataport and should be the way forward for all organizations. It's the only way to keep up to date with current threats while developing new employee skills and honing existing ones to keep cybersecurity teams at the top of their games.

About the Author

Taavi Must is CEO and Co-Founder of RangeForce, a leading provider of scalable, cloud-based, cyber defense upskilling solutions. He has more than 20 years of experience in enterprise technology development and leadership for global companies including Dell Technologies and Oracle. He previously served as managing director for ByteLife Solutions.

Taavi can be reached online at https://www.linkedin.com/in/taavimust and at our company website https://www.rangeforce.com/.



Progress and Barriers in the International Fight Against Cybercrime

By Ilia Sotnikov, Security Strategist and VP of User Experience at Netwrix

Cybercrime is a global issue. We all depend on information flows, communications, and production supply chains than span continents — and we are all vulnerable to the threats that can disrupt them.

The need for global action against cybercrime has been recognized for decades. Work on the first international treaty in this space, the Budapest Convention on Cybercrime, was initiated by the European Council in the 1990s. It was signed in 2001 and has been ratified by over 60 countries, including the USA, Canada, Japan and Australia. And in March 2023, the White House published the National Cybersecurity Strategy, which states that no country can efficiently counter cyber threats on its own and makes international partnerships one of its five core pillars.

This article explores the success and challenges of recent international collaboration efforts, with particular attention to the work of the United Nations in preparing its new global Cybercrime Treaty.

Recent Successes in the Global Fight Against Cybercrime

International collaboration is already enabling law enforcement agencies to work together, making the internet a safer space for everyone. For instance, one of the most powerful "cybercrime as a service" operations, Emotet, was taken down in January 2021 in a coordinated effort by the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine.

More recently, law enforcement agencies from the United States, Germany, Netherlands, Canada, France, Lithuania, Norway, Portugal, Romania, Spain, Sweden and the United Kingdom all participated in a months-long operation to disrupt the Hive ransomware network.

Challenges

Given these successes, why is the United Nations putting so much effort into drafting a new treaty? Simply put, there are still difficult issues that are slowing down or even blocking cybersecurity efforts.

One key challenge is the lack of a common international legal framework that would allow prosecution of cybercrime in all jurisdictions. While 80% of countries have adopted their own cybercrime legislation, definitions and laws vary greatly from country to country. And some major countries, such as Brazil, India and Russia, have refused to join the Budapest Convention. As a result, ransomware operators and other cybercriminals can still find safe havens.

Another issue is that many countries lack the skills and resources required to defend against cybercrime. This has resulted in cyberattacks against entire countries, which are seeking help from more developed economies. A common framework for international cooperation could set norms and enforce consequences for violating them.

The United Nations Cybercrime Treaty: A Long Journey

To tackle cybercrime at an international level, an ad hoc committee of the United Nations was formed in 2019. After significant preparation work, it began talks regarding a UN Cybercrime Treaty in 2022. This treaty is still in its early stages; four of six formal sessions have taken place to date. Since it's not easy to have almost 200 member states come to agreement on every detail of a legal document, this will undoubtedly be a lengthy process. The final draft of the new treaty is expected in early 2024.

The proposed treaty aims to establish common understanding of cybercrimes across multiple jurisdictions and facilitate international cooperation. A key goal is to make it more difficult for cybercriminals to both conduct illegal activities and get away with them by reducing safe havens where they can operate and hide.

The treaty is somewhat similar to other international treaties, such as those for fighting corruption or human trafficking. It seeks to establish common grounds on cybercrime so that national legislatures criminalize the same set of activities. The treaty will also set boundaries that give necessary powers to law enforcement without creating potential for human rights abuses.

The treaty will also establish a common legal vocabulary, which currently doesn't exist internationally, so that law enforcement agencies around the globe can better cooperate during investigation and prosecution of cybercrimes. Definitions are expected to cover many types of cybercrime, such as data theft, malicious data destruction, child pornography, financial fraud and malicious use of systems.

Larger businesses and industries that are the top targets of cybercrime will likely benefit most from the treaty, but it is really the entire international society that the UN aims to protect with the agreement.

Barriers to Treaty Development and Acceptance

While most UN member states agree that cybercrime is a vital issue to be addressed, we are likely years away from the treaty being accepted. The draft document will continue to undergo reviews and both public and non-public consultations, and legal teams from various UN member states will continue working through disagreements on descriptions and classifications.

Moreover, in most member states, the treaty must be ratified by local governmental bodies before it takes full effect. After that, countries will start implementing changes to align local legislation with the treaty, which can take years.

It's important to note that the draft UN Cybercrime Treaty does not address complex questions around cyberattacks backed by nation states. Trying to achieve agreement on this topic would probably lead to a deadlock in the process. Even with this topic left out of scope, however, there will likely still be barriers for some countries to accept and sign the new treaty.

Still, it is critically important to push for the common understanding of the cybercrimes across as many jurisdictions as possible. Even if the final treaty is reduced in scope and includes multiple trade-offs, it still gives the international community the leverage it needs to complicate the life of cybercriminals. Even countries known to be reluctant to prosecute cybercriminals will have to adjust their local laws after ratifying the treaty.

The Global Effort Is Significant

Arguably, the willingness of governments to acknowledge the problem of cybercrime and collaborate to find a solution is much more important than the treaty itself. This effort sends signals downstream and could result in more open sharing of information and tools even before the committee's work on the UN treaty comes to fruition.

In the future, adoption of common definitions of cybercrime will make international cooperation simpler and remove bureaucratic barriers to reducing cybercrime risks and holding cybercriminals accountable, so that businesses and the consumers they serve can all operate with greater confidence.

About the Author

Ilia Sotnikov is Security Strategist & Vice President of User Experience at Netwrix. He is responsible for technical enablement, UX design, and product vision and strategy. His 20 years of experience in cybersecurity and IT management include helping Netwrix build its product management function and managing SharePoint solutions at Quest Software.

Ilia can be reached at www.netwrix.com.

Navigating Your Way to Resiliency in Four Steps

By Shane Steiger, Principal Cybersecurity Engineer, MITRE

Cyber Resiliency

The concept has been around for many years. No doubt you've seen the images, such as a tiny flower emerging among bricks; one tree bending to the wind while another crashes to the ground; or soldiers successfully pushing back attackers who've breached the castle walls. And, of course, there's always the old chestnut of a tight huddle of computer experts combatting a shadowy figure in a hoodie.

These images fail to convey the most important point: that whether you run a hospital, factory, power grid, or a national security team, you have vital things to do beyond repelling cyber attackers. You can't let your business/mission grind to a halt because of a cyberattack.

Being able to achieve your organization's mission despite being under cyberattack is the most important part of cyber resiliency.

Start by assuming cyber attackers have made it over your organization's moat and are already stealing from you and eroding your business or mission. How do you proceed? Admittedly, this can seem overwhelming. But while it is a complex challenge, it's not insurmountable if you approach it with a solid plan.

To simplify this, my company, MITRE, released the Cyber Resiliency Engineering Framework (CREF) Navigator™. This free visualization tool allows organizations to customize their cyber resiliency goals, objectives, and techniques, as aligned with NIST SP 800-160, Volume 2 (Rev. 1), the National Institute of Standards and Technology's (NIST) publication on developing cyber-resilient systems.

The CREF Framework follows the four guiding steps below, and I've included some key questions for you to explore:

#1 Anticipate: Maintain a state of informed preparedness to forestall compromises of mission/business functions from adversary attack. This means plan, plan, plan. Know your high-value assets or critical points in your cyber assets. Work with your stakeholders to determine what your business/mission needs to operate. Determine what systems and services *must* be up at a bare minimum? Also, learn what cyber events others in your sector have experienced. Then, once you have a plan, ***test it***. Even a simulated tabletop exercise often will reveal undiscovered gaps in planning. Lastly, plan for worst-case scenarios, including events outside of computing that might exacerbate cyber risk—such as hospitals dealing with ransomware during a global pandemic.

#2 Withstand: Continue essential business/mission functions even when an adversary has successfully attacked. Okay, so you've been cyber attacked. As discussed in Step 1, if you planned for it, you are more likely to withstand it. First, what is happening to your assets? Can you easily move them around physically or logically—with virtualization? Can you reposition assets where an attack is not occurring? Do you have more than one system to achieve some business or mission functionality, such as a redundant system? Or do you have another way to achieve the same function if all similar systems are targeted? Is it a diverse system? Do you have key backup of systems in place? Do you have access to your cyber resiliency plan if systems or backups are completely unavailable? (You'll need access to this information later to fight through and recover.) Is there an adaptive response from some of your tools? During this initial phase, and despite the intense pressure, I recommend you stop to take a breath. Amid fear, uncertainty, and doubt, take time to be clear which assets are being affected—and how that's impacting your business/mission. If you do this "withstand" step well, you should be able to keep at least a minimum level of functionality in place and thus continue to achieve your core business/mission.

#3 Recover: Restore mission or business functions during and after adversity. This is where you bring your organization back from minimal to normal functionality. You'll need to recover from backups or build new systems that are not vulnerable to the same attacks. Think about how to segment your systems or realign them to restrict access. Cyber adversaries may try to overcome your recovery steps as you proceed by adapting their responses to assumed capabilities. Remember, this step is often happening during the fog of adversity. Can you segment your recovery to keep an adversary from re-compromising it? Do you trust the integrity of the recovery? Can you coordinate your response with

orchestration? Did you plan ahead and put forensic tools in place so you can better understand the event—and be confident you've fully recovered a trustworthy system?

 # 4 Adapt: Modify business/mission functions and supporting capabilities to account for likely changes in the technical, operational, or threat environments. Take this opportunity to make things unpredictable for future attackers. Distributing different tools across the environment in waves can reveal things that a static environment does not. Furthermore, make things non-persistent. Create systems or services that live only as long as needed and then can be destroyed. (Sounil Yu, CISO of JupiterOne and creator of the Cyber Defense Matrix and DIE Triad, has an informative and entertaining discussion on this very concept). Lastly, think about putting in a "canary in the coal mine" or trip wires. By salting your system with deceptive information or capabilities, you'll receive warnings about active cyber threats. Plus, the mere existence of information like this may cause an adversary to pause—thereby slowing their advance or making them distrust all information, true or not. If you make things hard enough for them, they'll go someplace else.

For more detail about the cyber resiliency concepts I've outlined, check out the CREF Navigator. This interactive website contains definitions, mappings, relationships and visualizations to other frameworks and standards to help you navigate your cyber resiliency journey.

A final note: We've all heard the rough definition of insanity is doing the same thing repeatedly while expecting a different result. This holds true in cyber. Resilient folks adapt. They don't repeat unsuccessful actions. A quote often attributed to Charles Darwin is as accurate now as it was well over a century ago: "It is not the strongest species that survive, nor the most intelligent, but the ones most responsive to change."

About the Author

Shane Steiger is a Principal Cybersecurity Engineer with MITRE, with more than 24 years of experience across multiple large enterprises and industries with emphasis on cyber architecture and strategy. Steiger was an early adopter of MITRE's Cyber Resiliency Engineering Framework (CREF) and the MITRE ATT&CK® Framework, incorporating each framework into the threat modeling, emulation, and defensive strategy choices of his organizations. He also contributed directly to NIST SP 800-160 Volume 2 (Rev. 1): Developing Cyber Resilient Systems: A Systems Security Engineering Approach. Steiger received his Bachelor of Arts in Mathematics and Latin from Susquehanna University and his Juris Doctor from Widener University Commonwealth Law School. He is a Certified Information Systems Security Professional (CISSP) and a member of the Pennsylvania Bar. Shane can be reached online at ssteiger@mitre.org and https://www.linkedin.com/in/shane-steiger-esq-cissp-6073a41/ and at MITRE's website https://www.mitre.org.

Do Highly Intelligent Language Models Pose a Cyber Threat?

By Brett Raybould, EMEA Solutions Architect, Menlo Security

It is estimated that as many as 100 million users have engaged with AI chatbot, ChatGPT, since it was released at the end of November. Developed by OpenAI, ChatGPT has surprised with its ability to complete a range of tasks in a highly sophisticated and human-like way.

Since then, others have jumped on the AI bandwagon. Microsoft has already announced the launch of a new version of its Bing search engine that taps into a version of OpenAI's cutting edge large language model that is customised specifically for search, the platform taking its key learnings and advancements from ChatGPT. Google has also said that it would be introducing Bard, an experimental conversational AI service positioned as a direct rival.

The headlines are hard to ignore, but not all the feedback to these highly advanced large language models has been positive. For many there is the worry that ChatGPT can be used as easily for negative purposes as is it for positive ones.

A professor at Wharton, University of Pennsylvania's business school took an MBA exam using ChatGPT. The University found that it didn't just pass the test but scored an impressive B/B-. With ChatGPT able to write an advanced essay on a subject within just a few seconds, the platform could easily be used by students to cheat. Is this a sign of how different the post-AI world will be perhaps?

Cybersecurity presents another growing concern. Blackberry reports that 71% of IT professionals believe that foreign states are likely to be using ChatGPT already for malicious purposes, such as nation state attacks. CyberArk also published findings about how it was able to create polymorphic malware using ChatGPT, while Check Point Research suggests that cybercriminals have been using it to create spear-phishing emails and share information-stealing malware code on criminal forums.

We decided to ask ChatGPT whether it could be misused by malicious actors to develop Highly Evasive Adaptive Threat (HEAT) attacks, a class of attacks capable of bypassing many traditional corporate security solutions such as firewalls, secure web gateways and phishing detection tools.

The initial response was: "Is it possible for ChatGTP or any other language model to be misused to generate malware? If a malicious actor has access to the model and trains it on malware samples, could it generate malicious code or be used to create phishing campaigns or other malicious activities? In this sense, ChatGTP generated malware could be considered a HEAT threat, as AI-generated malware can be sophisticated, adaptive and difficult to detect."

So, the initial answer was yes, it can be used to generate HEAT attacks. However, in the same response the chatbot clarified that the creation of malware using AI language models is not an inherent capability of the models themselves, but rather the result of malicious use.

We then asked similar questions, and it concluded that ChatGPT does not pose a HEAT threat. One reply said: "While it is possible for a threat actor to misuse ChatGPT for malicious purposes, such as generating misleading or false information, it is not capable of generating malware on its own."

Can ChatGPT democratise cybercrime?

OpenAI has been keen to reiterate that ChatGPT is not always correct, and therefore its responses should not be relied upon as fact. However, both the bot's initial response and the studies conducted by Blackberry, CyberArk and Check Point Research suggest there may be cause for concern.

What we do know is the ChatGPT is centered around machine learning, so the more inputs it receives, the more sophisticated and accurate it will become.

The concern is that ChatGPT could be used to democratise cybercrime. By this, we mean that would-be threat actors with limited to no technical skills could learn to write credible social engineering or phishing emails, or even code evasive malware, using the ChatGPT platform or similar tools.

We have experienced the catastrophic damages that democratised cybercrime can cause already. Indeed, a major reason why the volume of ransomware attacks has increased so dramatically in recent years is because of a booming ransomware-as-a-service industry.

Therefore, given the potential cyber threats that these bots can bring, it is more important than ever that organisations properly protect themselves against HEAT attacks. We recommend that organisations incorporate isolation technology into their security strategies as an effective way of combating highly evasive threats – even potential ones created by AI.

This ensures that all active content is executed in an isolated, cloud-based browser, rather than on users' devices. In doing so, it blocks malicious payloads from reaching their target endpoints, preventing attacks from happening in the first instance.

Highly evasive adaptive threats are already on the rise. Given the potential for threat actors to take advantage of the capabilities of language models in coordinating attacks, companies will need to enhance their security strategies as a priority.

About the Author

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.

Now is the Time for the Thoughtful Regulation of Crypto

By Hugh Brooks, Director of Security Operations, CertiK

The rapid expansion of the cryptocurrency industry has brought technological innovation and financial inclusion, while promising a freer and fairer global financial landscape. However, this growth has also introduced some growing pains, such as the more than $3.7 billion lost to hacks, scams, and other exploits in the past year alone. Furthermore, the recent collapse of FTX, the world's second-largest crypto exchange, underscores the inadequacy of existing regulation to appropriately protect users from risk. On the flipside of this coin are all the potential benefits of a truly crypto-native approach. By voluntarily adopting stringent and effective security and transparency measures, the crypto industry can ensure it'll be around to realize its transformative potential.

Without delving too deeply into the potential motivations of such policy, the fact remains that external regulation of the crypto industry has often proven to be contradictory, unclear, and ineffective. This uncertainty hinders the growth and stability of a burgeoning trillion-dollar global industry that transcends geographical boundaries. Aggressive regulators inadvertently drive innovation and investments offshore,

undermining the potential of the sector. And major nations have learned painful lessons about the importance of resilient systems over the last few years, from the supply-chain disruption of the pandemic to the unknown cost of cybersecurity incidents such as SolarWinds. Punishing some of the brightest minds in the country for their online experimentation is not just a great way to discourage innovation of all types, it's a national security risk.

Meanwhile, the FTX debacle highlights the drawbacks of government-led regulation, which can be manipulated by outside special interest groups. A crypto-native approach, based on the open, auditable, and transparent foundation of blockchain technology, however, offers a solution devoid of coercion. Compliance with such an approach is binary: the math either checks out or it doesn't.

One of the best examples of a crypto-native solution is Proof of Reserves. This innovative approach enables users to access real-time, on-chain data that verifies the solvency of a Web3 platform. Unlike traditional financial reports which come just once a quarter, Proof of Reserves offers instant, transparent, and verifiable information. The widespread implementation of this self-regulatory measure would be a major step towards the crypto industry boosting its credibility in the eyes of regulators and users alike.

Another powerful tool for proactive self-regulation is Know Your Customer (KYC) verification for project teams. By having legitimate founders verify their identities, the industry sets a higher bar for trust and transparency. While the anonymous nature of Bitcoin, brainchild of the still-pseudonymous Satoshi Nakamoto, is essential to the crypto ecosystem, projects soliciting financial investment from the Web3 community must strike the right balance between their right to privacy and their responsibility to transparency.

By undergoing KYC verification, project teams can confidently stand behind their work without necessarily publicly *doxxing* themselves, while investors can make informed decisions based on accurate, reliable information. This approach safeguards the interests of all parties and cultivates a more stable and secure environment for growth.

All those who believe in the future of the blockchain industry share a collective interest to ensure the industry's success and prosperity. It is vital that we address the significant losses attributed to hacks, exploits, and scams in order to guarantee the industry's long-term viability. By adopting a proactive approach, we can demonstrate our commitment to security and transparency, outpacing regulators in the process.

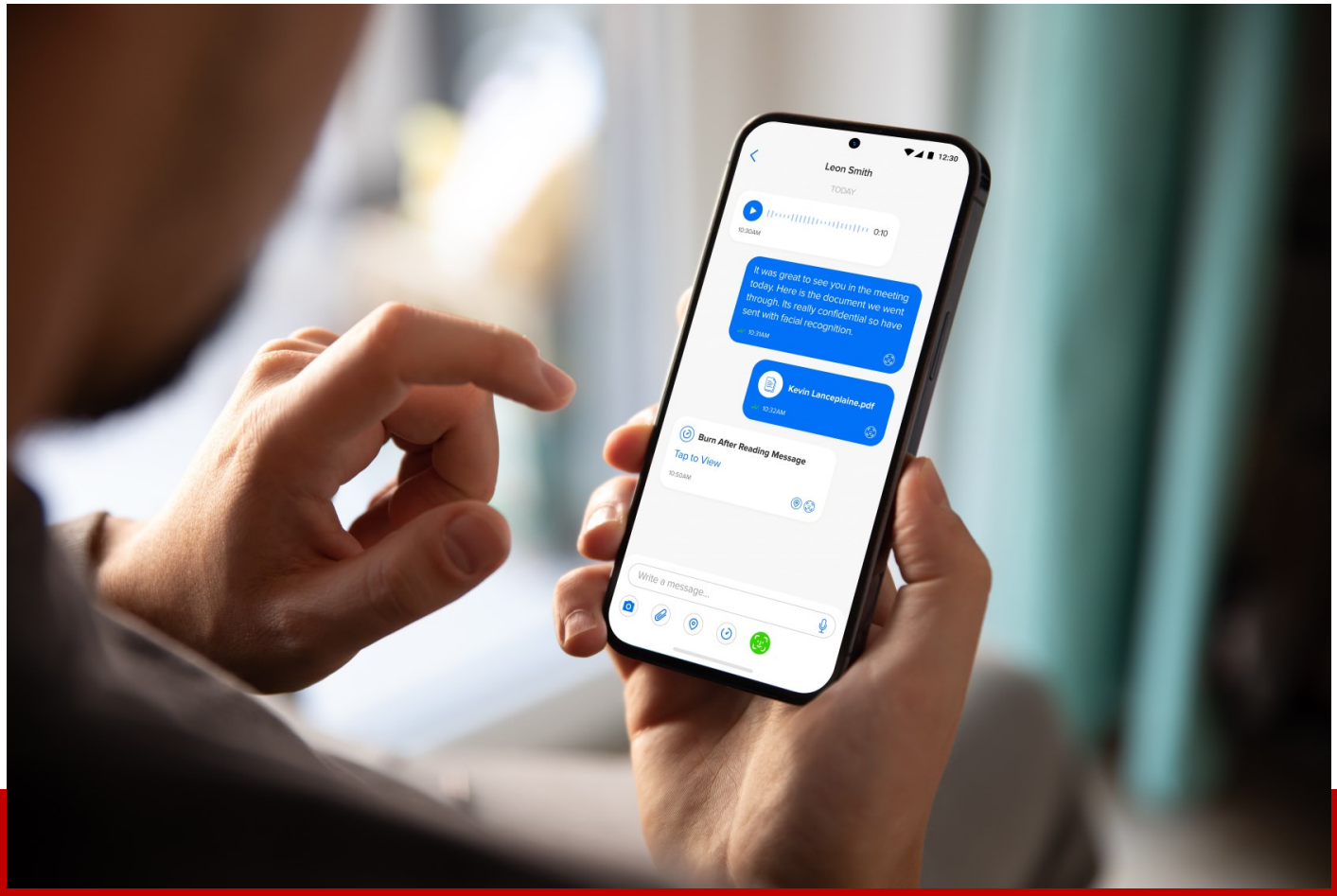
Embracing self-regulation and implementing native solutions like Proof of Reserves and KYC verification allows the crypto industry to confront its challenges head-on. And the flexibility of blockchain technology enables the development of new solutions as fresh problems arise.

The *self*-regulation of the crypto industry is of paramount importance. As the sector continues to evolve, it is crucial to come up with native solutions that address its unique challenges in the most effective, hands-off manner possible. By fostering transparency, trust, and security through self-regulation, the crypto community can lay the groundwork for a more sustainable and successful future of the industry.

The cryptocurrency industry is doing good things, and it's better for all involved if we come up with meaningful solutions to our own problems.

About the Author

Hugh Brooks is the Director of Security Operations of CertiK. Hugh can be reached online at (@Crypto_tauros) and at our company website http://www.certik.com.



How Secure Communication Can Enhance Your Organization's Cyber Defence

By Luca Rognoni, Chief Security Officer and Co-Founder, YEO Messaging

Cyber threat landscape has dramatically expanded in recent years due to an exponential increase of interconnected devices, systems, infrastructures inside and outside an organisation. New IT technologies means new cyber threats to assess, extended organisation network perimeters, new attacking surfaces to defend, new attacking vectors to be aware, reduced margin of error in cyber risks evaluation, but along with the increasing number of cyber threats also the amount of processed, transmitted and stored data has increased in any organisation.

Providing confidentiality and integrity of data in transit in this fast-growing cyber threat landscape is more critical than ever in an organisation's cyber defence strategy, and secure communications play a key role in preventing data breaches and other cyber-attacks.

A secure communication involves several components including: encryption, authentication, authorisation, integrity, non-repudiation. Encryption plays a crucial role in protecting confidentiality and integrity as it is a data security control that can be applied to the data when it is in all three different states of its lifecycle: at rest, in transit and in particular scenarios, to data in use too. In a layered security model, encryption is a direct information-protection technique that perfectly integrates in a defence-in-depth approach to data security.

Authentication and authorisation mechanisms ensure that only authorised personnel can access sensitive data. Authentication and authorisation have evolved into identity and access management systems allowing an organisation to ensure that only authorised individuals or entities are granted access to resources and determining what the individual or the entity is allowed to do based on their role or permissions, creating segmentations or isolations of systems, workspaces and personnel. A segmented approach to data access reduces escalation and impact of data breach. Identity and access control systems provide a comprehensive set of frameworks to enhance authentication and authorization through MFA, Contextual authentication, Single Sign-On and Federation.

Integrity of data ensures that the information transmitted is not tampered or altered during the communication and non-repudiation proves the authenticity of the data and the identity of the sender.

Looking at the cyber risk landscape of an organisation, mitigation of data breach for data in transit is one of the most important defence challenges that an organisation has to face as it involves several organisation areas through which data travel through, within and outside the organisation perimeter.

Fast emerging threats involving supply chains can be mitigated and the impact reduced with secure communications. As organisational data is moving within and outside of the network perimeter, passing through several organisations and infrastructures in complex supply chains, often difficult to risk assess completely, a direct information-protection technique like data encryption, policy-based access control and continue monitoring allow you to establish secure communication for data transfer, mitigating severe data breach along these long supply chains where data visibility is often reduced or lost at the edge of the organisation network perimeter. Secure tunnelling protocols like VPN (IPSec, WireGuard) using on-premises or cloud VPN proxy are fundamental to providing site-to-site secure connection between multiple networks. A secure supply chain management can rely on secure data exchange protocols like AS2/AS4, OFTP2 that provide strong security and flexibility in a B2B environment. Traditional S/MIME, SFTP, HTTPS and E2EE are still the solid foundation for secure communication of emails, web content and data exchange in general.

Cloud services from SaaS to IaaS are the lifeblood of any organisation but they also force the organisation to extend the defence perimeter outside where on-prem risk mitigation strategies are not applicable. Secure communications between organisation and its cloud infrastructures protect ingress and egress data traffic from sensitive user data to management plane network traffic. VPN protocols and VPN gateway services secure management plan network traffic, Secure Web Gateway, CASB and DLP creates secure communications to/from cloud infrastructures by enforcing organisation security policies and visibility in the everyday network traffic detecting and preventing data leak, policy violation and malicious content.

On-prem data traffic in particular north-south network traffic should always require secure communications implemented by segmenting networks and using firewalls and access control policies to control access to sensitive data. Internally to organisation the most difficult threat to mitigate a data leak, unintentional or not. Secure communications limit access to data and provide accountability and monitoring through DLP (data loss prevention) and Secure Web Gateway solutions that can monitor communication channels for sensitive data and prevent it from being shared with unauthorised parties, allowing secure collaboration solutions to be deployed to help organisations securely share data and collaborate on projects without exposing themselves to the risk of cyber-attacks. Secure communication can protect email messages by encrypting their content, using digital signatures to verify the sender's identity, and scanning email attachments for malware.

With the recent pandemic, remote or hybrid working environments have increased. They provide great flexibility and cost efficiency but they also expanded the attacking surface for an organisation, the defensive network perimeter of the organisation extends beyond on-prem or cloud infrastructures to remote worker infrastructures and networks, increasing the organisation inbound and outbound traffic of sensitive data. Secure communications are critical to protect and monitor confidential data like emails, video/audio conferences and now messaging. Secure communication is critical for mobility and can be implemented on mobile devices through the use of end-to-end encrypted and continuously authenticated secure messaging apps like that we designed and developed at YEO messaging, encrypted email protocols like S/MIME, mobile remote-access VPN and organisation managed Web-Application proxy and Secure Web Gateway.

Secure communications are essential for organisations that need to comply with industry regulations such as HIPAA, PCI DSS, or GDPR. These regulations require organisations to protect sensitive data and maintain secure communication channels to prevent data breaches by implementing secure communication protocols that provide end-to-end encryption, digital signatures, access controls, and other security features.

Finally, secure communication is a critical component in an organisation's incident response plan. The plan should provide steps that should be taken in the event of a cyber-attack, including how to maintain secure communication channels to prevent further data breaches and to continue to provide safe internal and external communications between incident response teams, executive management, legal counsel, law enforcement agencies, and other third-party vendors or consultants to quickly and securely facilitate coordination and collaboration between all parties involved.

About the Author

Luca Rognoni, Chief Security Officer & Co-Founder YEO Messaging, secure messaging that uses patented continuous facial recognition to authenticate users. Luca is a highly experienced software engineer, with over 25+ years' experience in design and coding digital rights management (DRM), anti-virus, encrypted systems and other security software. He started his career as a software and hardware reverse engineering and device driver developer on Microsoft and Linux platforms back in 1999, with a focus on file system filter and network filter drivers. This gave him a strong foundation in developing core system software with interesting security applications, which sparked his interest in developing antivirus and anti-malware solutions.

Luca then moved into developing antivirus and anti-malware kernel engines and DRM solutions for software and data, including the DRM solution used by Microsoft Game Studio to protect Windows PC games, mobile security software development and penetration testing.

Luca Co-Founded YEO Messaging in 2017 and is responsible for developing YEO's internal security, penetration resistance and global threat tolerance. YEO is available for business and individual users who want to know that the messages, files and media they share are secure, private, and only being viewed by the intended recipient, whether that's a private picture or sensitive documents. As well as end-to-end encryption and geofencing features, YEO is the only app of its kind to use continuous facial recognition to verify not just the device, but the person looking at it.

Luca can be reached at Luca@yeomessaging.com and at our company website www.yeomessaging.com.

The 2023 State of Ransomware: A Resurgence Is Brewing

By Bob Maley, CSO at Black Kite

After last year's good fight against ransomware gangs, CISOs thought they won. Overall attacks were down and ransom payments dropped 40%. In fact, this year even brought some false hope: several reports indicated ransomware was in decline. Rumors spread that hackers were actually being laid off due to the reduction in extortion money.

We were wrong, again – and the hackers capitalized on our complacency. While we celebrated the decline, they regrouped and got stronger. With the start of the new year, new players emerged and mass-ransomware attacks plagued major businesses. In fact, the number of ransomware victims announced in March 2023 was nearly double that of April 2022 and 1.6 times higher than the peak month in 2022.

CISOs can't afford to be blindsided again. It's time to understand the complexities of the ransomware landscape to close the agility gap once and for all. By recognizing today's top vulnerabilities, culprits and strategies for resilience, leaders can get ahead of attacks and never underestimate a quiet period again.

The Evolving Landscape: New Trends and Targets

According to the new Ransomware Threat Landscape 2023 Report, ransomware attacks experienced a period of stagnation last year as several major ransomware groups were shut down. Various other external factors also contributed to a decrease in attack frequency. However, the lull came to a sudden end in 2023 as new ransomware gangs such as Royal, BianLian, and Play hit the scene. The time was ripe with opportunity, with advanced AI and ML technology creating new vulnerabilities, as well as geopolitical tension and economic turmoil rising. Coupled with mass-ransomware attacks that were executed by major players like Lockbit and Clop and new trends like encryption-less ransomware, the battlefield has gotten serious.

The rise in ransomware should be on every organization's radar – but several industries are at particular risk. From April 2022 through March 2023, Manufacturing and Professional, Scientific, and Technical Services accounted for nearly 35% of all ransomware victims. Educational Services, Retail Trade, and Health Care and Social Assistance accounted for 17%. The United States was the top targeted country, accounting for a staggering 43% of all victim organizations.

The report also uncovered ransomware groups often target companies with annual revenues of around $50M to $60M, as they may have the financial resources to pay ransoms but potentially lack the robust security and resilience measures of larger corporations. However, organizations of all sizes must still beware; many are targeted through third-party vendors that fit this profile. In fact, ransomware was the second most common cause of third-party cyber breaches in 2022.

Whether your organization fits the bill or not, chances are a vendor (or a vendor's vendor) does, and in turn, is vulnerable to ransomware attacks that could cripple your own operations. Ignorance may be bliss in some situations – but here, it's expensive and devastating. The first step toward preparation is understanding warning signs and thinking like a hacker.

On The Radar: Top Criminals Seek Common Vulnerabilities

According to the report, LockBit Ransomware Group, which was responsible for 29% of attacks over the last 12 months, remains the top player in the cyber-criminal space. What makes them so effective: LockBit has a dedicated team of hackers and operators responsible for ransomware development and deployment. They view themselves as a business rather than a criminal operation.

The other top ransomware gangs in the last year include AlphaVM (BlackCat), responsible for 8.6% of attacks, and Black Basta, a ransomware-as-a-service (RaaS) group responsible for 7.2% of attacks. Lastly, Clop was responsible for 4.8% of attacks. The group resurfaced this March, announcing over 100 victims and launching a mass-ransomware campaign that exploited a high-severity Fortra GoAnywhere vulnerability.

No matter the gang, the vulnerability criteria remain mainly the same. Poor email configuration (such as missing DMARC records) is present for 67% of victims, leading to successful phishing and spear-phishing campaigns, allowing attackers to gain an initial foothold in the organization's network. Sixty-two percent of victims saw leaked credentials as a component of their attack, which provides attackers with easy

access to systems and networks, enabling them to bypass security controls and move laterally within the organization. Lastly, public remote access ports account for 42% of victim attacks.

In today's rapidly evolving threat landscape, organizations must remain vigilant to these common vulnerabilities. It is crucial to note that many ransomware victims are also third-party vendors for other organizations. Monitoring these common ransomware indicators in third parties is essential to reduce the risk of being targeted by ransomware via a distant entry point in your extended network.

The Three Phases Toward Agility & Resilience

Ransomware groups are evolving into new-age tech companies with sales teams, customer success departments and more. Every action is geared toward expanding their illicit businesses – and they're moving faster than the good guys can keep up with.

Getting informed with the latest data on ransomware trends is the first line of defense – but your approach shouldn't end there. Ensuring agility and protection can be broken into three main phases: prevention, response, and recovery.

Prevention is proactive: Taking a proactive approach to internal security measures can greatly reduce the likelihood of a ransomware attack. There are a number of best practices to ensure your organization is not an attractive target for ransomware groups, such as to monitor your ransomware indicators (such as checking for open critical ports or leaked credentials), regularly backup critical data and systems to allow for quick recovery, and develop a comprehensive incident response plan.

However, implementing internal measures alone still leaves the door half open. To mitigate the risk of ransomware attacks due to third-party vendors, organizations should also evaluate the cybersecurity posture of third-party vendors using sophisticated tools, require vendors to adhere to industry best practices, perform regular audits of vendors' security practices and more.

Response is rapid: In the event of a ransomware attack, taking immediate action is critical to mitigate the damage. Steps to take when hit by a ransomware attack include isolating affected systems to prevent spread, notifying relevant authorities and stakeholders, engaging with cyber experts for remediation options and documenting the incident for future reference and potential legal actions.

Recovery is resilient: After a ransomware attack, it is crucial to learn from the experience and strengthen your organization's cybersecurity defenses. Post-attack steps include conducting a thorough analysis of the incident to identify root causes and vulnerabilities, implementing recommended security measures to prevent similar attacks in the future, and sharing information about the attack with relevant parties and collaborating with industry peers to improve overall cybersecurity.

Looking Ahead: Remaining Vigilant Amid Resurgence

Don't let any lull fool you – the current state of ransomware is growing more dangerous by the month. With new players, bigger attacks and economic volatility that's causing some businesses to cut staff and innovation, we can expect disruption to continue throughout 2023.

It may feel as though there's no way to beat the adversaries. Ransomware criminals have no ethics, and therefore, can increase agility without the concerns of a responsible business. But when examining the data, you'll find the answers for agility and resilience right in front of you. By implementing a combination of internal security measures and third-party risk management, organizations can stay off the radar of ransomware groups, protect sensitive data, and minimize the potential damage caused by ransomware attacks. It takes a village -- let's work together to ensure resurgences are a thing of the past.

About the Author

Bob Maley, Inventor, CISO, Author, Futurist and OODA Loop fanatic is the Chief Security Officer at Black Kite, the leader in third-party cyber risk intelligence. Prior to joining Black Kite, Bob was the head of PayPal's Global Third-Party Security & Inspections team, developing the program into a state-of-the-art risk management program. Bob has been named a CSO of the Year finalist for the SC Magazine Awards and was nominated as the Information Security Executive of the Year, North America. His expertise has been quoted in numerous articles for Forbes, Payments.com, StateTech Magazine, SC Magazine, Wall Street Journal, Washington Post, Dark Reading and more.

Bob can be reached on LinkedIn and at our company website https://blackkite.com/.

Protecting Sensitive Information Within Translation

Strategies for Preventing Data Breaches in the Translation Industry

By Ofer Tirosh, CEO, Tomedes

When it comes to translation, it's not unusual to come across sensitive information such as financial reports, legal documents, and medical records. It doesn't need to be explained that such important details must be kept confidential and secure, as the resulting data breach can be disastrous to both the translation company and its clients.

This comes with its own set of hardships. Thus, safeguards must be in place in order to ensure the privacy, integrity, and security of both service provider and customer. Sharing information during business transactions is a show of trust, and failing to do their part can have terrible long-term repercussions, a loss of credibility, financial and clientele loss, and a damaged reputation for the translation company among them.

For clients, the consequences of a data breach can be even more severe. Exposed sensitive information can lead to identity theft, financial and reputation loss, and damage to personal and career life. Clients may also be subject to legal action if they cannot protect the private information of their customers. Therefore, it is critical for translation companies to take measures to prevent data breaches and protect the sensitive data they handle.

The Risks of Data Breaches in Translation

No matter how secure a translation company thinks it is, it is still vulnerable to cyberattacks and data theft. Hackers and other cybercriminals may attempt to gain access to confidential information by exploiting vulnerabilities in the company's systems. This can come in the form of malware, spyware, and other malicious software on the company's systems. These attacks can result in the theft of sensitive information, such as financial information or personal data, which can be used for identity theft, fraud, and other criminal activities.

Insider threats from employees and contractors are another major risk for translation companies. Employees and contractors with access to sensitive information may deliberately or accidentally leak confidential data. Employees who are disgruntled or have been terminated and contractors who may not be properly vetted can easily be bought or convinced to reveal what they know. Insiders can also fall prey to phishing attacks and other social engineering tactics used to gain access to sensitive information.

Additionally, one of the main challenges translation companies also face is the sheer volume of data that translation companies have to process. This can lead to errors and oversights, which can put sensitive information at risk. Another potential issue is the diversity of the information that is being handled, as confidential knowledge can be delivered in a range of different formats, including audio recordings, video files, and written documents.

On a brighter note, there are some defenses already in place. Some countries and organizations have already put privacy and data regulations that all companies, including those in the translation industry, should comply with. This includes the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) among others. This bolsters companies to implement data protection measures that are appropriate for the types of data they handle, including policies and procedures for data collection, storage, and sharing. It also pushes businesses to secure systems and processes for handling this data, including encryption, secure storage, and access controls. Failure to comply with these regulations can result in significant fines and reputational damage.

Strategies for Preventing Data Breaches in Translation

However, even with these safety nets in place, securing confidential data should start at the company ground level. There are already a few general steps that a company can do to begin the process, but for translation companies, these strategies should be more stringent. They can range from putting strong security protocols and procedures in place, training employees on best practices for secure information

management, ensuring secure data storage and transmission, and conducting regular security audits and assessments.

For security protocols and procedures, use secure encryption methods to protect sensitive data, ensure that all software and hardware is up-to-date and regularly patched for security vulnerabilities, and put into practice access controls to restrict who has access to sensitive information. Other security protocols may include multi-factor authentication, firewalls, and intrusion detection systems.

However, using machines may not be enough. Employees also play a critical role in preventing data breaches. It is essential that translation companies train employees on best practices for secure information management, including how to identify and report potential security threats, how to handle sensitive information, and how to protect data during transmission. Employees should also be trained on how to avoid phishing scams and other social engineering tactics used by cybercriminals to gain access to sensitive information.

Once human and machine are trained and prepared for any breach possibilities, companies must then ensure that the data is stored and transmitted securely. This can be done through secure cloud-based platforms for data storage and transmission, implementing secure file transfer protocols, and using encryption to protect data during transmission. The information should also be backed up regularly and stored in secure locations to prevent loss in the event of a security breach. These procedures can also be automated to reduce human error.

Finally, to keep security effective in the long term, conduct regular security audits and assessments to check and discover potential vulnerabilities in their systems and processes. Do regular penetration testing to identify potential security weaknesses, and perform regular audits of their security protocols and procedures to ensure consistent compliance with data protection regulations. These assessments should be conducted by qualified professionals and include a comprehensive review of all security controls and procedures. Any identified vulnerabilities should be addressed promptly to minimize the risk of data breaches.

Best Practices for Secure Information Management in Translation

In the translation industry, secure information management has become essential. This is conducted through a combination of sensitive data encryption, access controls, authentications, data backup and recovery, and monitoring and logging access to confidential data.

First and foremost, sensitive data, such as personal information, financial records, and confidential business information, should be encrypted during storage and transmission. For instance, translation company Tomedes has its certified translation orders go through a Secure Sockets Layer ("SSL") protocol to ensure that data cannot be accessed by unauthorized users, even if it is intercepted or stolen. Other industry-standard encryption methods, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS), can also be used to encrypt sensitive data.

Another method of preventing unauthorized access to sensitive information is access controls and authentication measures that open or restrict the types of data employees receive based on user roles and responsibilities. Common examples include biometric or two-factor authentication for programs, which can also enhance security by requiring users to provide additional forms of identification before accessing sensitive information.

Translation companies should additionally provide secure methods for regular data backup and recovery to prevent data loss in the event of a security breach. All backups should be stored in secure locations to prevent unauthorized access, and disaster recovery plans put in place to ensure that potentially lost data can be restored quickly in the event of a security breach or any other disaster.

Steps can be followed to maintain security even during company operations. Monitoring and logging access to sensitive information can be a dealbreaker for detecting and responding to security incidents. Implement systems that track and log access to sensitive information, including who accessed the information, when it was accessed, and what actions were taken. These logs should be reviewed regularly to identify potential security threats, and to ensure compliance with data protection regulations.

Conclusion

No matter how secure a translation company may be, the threat of data breaches and compromises will always be around the corner for as long as there is the knowledge of private, sensitive information being traded back and forth between clients and service providers. Privacy and data protection regulations are an attempt to keep on top of the danger, but there is only so much that can be done if companies themselves do not put their best foot forward and prevent, if not minimize, the risks that are already present and waiting for an opportunity to strike.

The translation industry is constantly evolving, and companies must adapt their security strategies to keep up with emerging threats and new technologies as best they can. By implementing best practices for secure information management, translation companies can minimize the risk of data breaches and protect sensitive data from cyber threats and other security risks, keeping clients safe, happy, and secure in their translator choice.

About the Author

Ofer Tirosh, the CEO and Founder of Tomedes, a leading professional translation company that specializes in providing customized language solutions for businesses and Fortune 500 companies. With over 15 years of experience in the translation industry, my team and I work collaboratively with a network of expert translators in more than 150+ languages and multiple fields to deliver exceptional translation services.

As the head of a company that regularly handles sensitive information, I understand the importance of cybersecurity and its impact on businesses. I have gained valuable knowledge and expertise in implementing robust security measures to safeguard our clients' data from cyber threats. My experience has equipped me with a deep understanding of the various cybersecurity challenges that businesses face, and I am committed to sharing my insights and recommendations with the broader community.

Innovation or Threat?

ChatGPT increases the risk of cyberattacks.

By Markus Cserna, CTO, cyan Digital Security

The whole world looks with amazement and appreciation at the achievements of the publicly available voice bot ChatGPT - especially after the release of version 4.0 in mid-March. But what many do not yet suspect: With the triumph of AI, the danger of cyberattacks is also increasing. Even laymen have the tools for digital attacks at their fingertips. Companies must therefore urgently equip themselves, demands guest author Markus Cserna, CTO at cyan digital security. He says: Companies can already benefit from intuitive solutions that offer effective protection.

When we look back on 2023 in the future, we will remember it as the year when Artificial Intelligence (AI) became fully viable on a mass scale.

The AI software of the US company OpenAI, which was released in November 2022, took its successful course around the globe at breathtaking speed. In Germany, too, curiosity and euphoria were and are great - especially after the release of the software's much more powerful successor.

ChatGPT: All-rounder with problematic properties?

The technology now delivers thoroughly useful texts for almost every area of life in seconds, while other AI programmes produce creative-artistic images at the touch of a button. But despite all the euphoria, justified doubts are also growing in places.

"Since the upgrade to the AI language model GPT-4, the chatbot ChatGPT has been writing misinformation more frequently and convincingly," reported the media with reference to investigations by the network research service NewsGuard, which monitors and investigates disinformation on the internet.

In the new version, the AI responded with false and misleading claims to 100 out of 100 suggestive questions that it was asked. These questions dealt, for example, with disproved theories of vaccination opponents or conspiracy theories. The current version GPT-4 thus generated false messages more frequently than the previous version GPT-3.5.

According to NewsGuard, passing the US bar exam seems to be easier for the AI than recognising erroneous information. While GPT-4 performed better than 90 per cent of all examinees on the bar admission exam, the latest version of OpenAI's AI software received a critical rating on a NewsGuard test that reviewed the software's ability to avoid spreading clear misinformation.

Using the opportunities of AI - but please with a sense of proportion

To clarify: This is anything but a general reckoning with AI. The opportunities that this new technology offers, especially to companies from Germany and Austria, are welcome in many constellations and can be used for the benefit of the business locations.

However, this must be done with a sense of proportion and a clear mind. The examples cited show how close genius and madness can be, even with artificial intelligence.

Caution is also advised when the human factor is added. After all, the same technology can be used to pursue and realise both honest intentions and fraudulent motives. Most AI products such as ChatGPT have certain barriers built in to prevent misuse, but the distinction is difficult in many cases - and can therefore still be tricked again and again.

The speech bot is based on probabilities, reassembling familiar things at breathtaking speed. But it is precisely these reproduction capabilities that could make ChatGPT a dangerous assistant for cybercriminals.

ChatGPT turns programming amateurs into dangerous cybercriminals

Thanks to the new software, even IT laymen without deep programming knowledge can mature into professional IT attackers. For hackers, the triumph of AI makes it extremely easy to combine or modify malicious code in such a way that it can no longer be detected by existing security systems.

The cyberthieves do not even have to get their own fingers dirty, but can conveniently abuse AI for their criminal purposes. This represents the next step for cybercrime-as-a-service, now criminals don't even have to be experts.

New attackers require a new security infrastructure

Chatbots are trained with billions of data sets from all areas from social sciences to programme code. This also opens the door wide for amateur hackers. IT abuse could become a mass phenomenon in the next few years.

The reaction time windows between an attack via chatbot and the recognition as well as neutralisation of the attack could thus unfortunately become smaller. Attacks will be carried out more professionally with less effort, which means new demands on cyber security.

Affected IT departments of corporations and large companies cannot guarantee perfected digital protection with established thought patterns. Without rethinking and rethinking the existing security infrastructure, complete digital resilience will hardly be possible in times of disruptive technologies.

Attackers from Asia, Africa and increasingly Russia, for example, no longer have to fear language barriers either: With the new version of ChatGPT, foreign language barriers can be easily bridged. Those affected in Germany will no longer realise, or at least too late, who they are actually dealing with. The times of bungling spam addresses with grammatical errors seem to be over.

Content placed in malicious messages by cybercriminals thus appears more "real". The distinction between legitimate and illegitimate traffic becomes much more complex. Increased IT vigilance is therefore the order of the day for companies and organisations.

About the author

Markus Cserna's work lays the foundation for cyan's success: technological progress against Internet fraudsters and competitors. He started his career as a software specialist for high-security network components before founding cyan in 2006 with the vision of protecting internet users worldwide from harm. Since then, he has led the company as CTO with a restless passion for cyber security technology that steadfastly keeps ahead of the curve in dynamic markets.

Markus Cserna can be reached online at our company website https://www.cyansecurity.com.

Deception Technology Can Derail Cyber Attackers

By Brett James, Director, Transformation Strategy at Zscaler

In recent years, federal agencies have expanded remote work dramatically, and in response IT teams have done the same for edge computing deployments. increased use of cloud computing, and continued other important government IT modernization efforts. These are all positive developments that help agencies meet their missions more effectively.

But they also come at a cost – an expanded cyberattack surface – and cyber attackers are taking advantage. For example, Microsoft's Digital Defense Report showed that 46 percent of nation-state cyberattacks in one year were directed at the U.S. government.

Public trust is at risk, while the price tag of cyber breaches is rising. The IBM 2021 Cost of a Data Breach report found that data breaches became 10 percent more expensive in 2021, and the average cost of a breach in the public sector was $1.93 million. Moreover, the average time to detect and contain a breach was 287 days, driving up costs and increasing the danger.

With an increase in the number and severity of cyber threats, government agencies that rely on traditional detection technologies could be at a serious disadvantage.

Confronting the Growing Danger

Cyber attackers are using increasingly sophisticated methods that are difficult for government agencies to detect:

- **Stealthy attacks:** Advanced adversaries use purpose-built playbooks and an in-depth understanding of their target's environment to get in and stay hidden. As a result, 91 percent of incidents do not generate a security alert, representing a threat to even well-defended and prepared agencies.
- **Human operated:** Traditional defenses are designed to detect malicious code, but 68 percent of attacks do not use malware. With ransomware, for example, an agency is not simply fighting a software program; the attack is directed by a person. Sophisticated adversaries use advanced tactics like legitimate credentials or built-in tools to bypass traditional defenses and challenge security teams' limited resources to hunt for threats.
- **Hiding in false positives**: Most agency security operations default to compiling as much data as possible, collecting it in a security information and event management (SIEM) system, and then seeking evidence of an attack. The sheer volume of resulting data overloads security teams with alerts, 45 percent of which are false positives. Research shows 99 percent of security teams say excessive alert volumes are a problem. Frequently, big threats are flagged, but they are buried in all the noise.

Implementing Active Defense

Zero trust architectures directly connect authorized users to permitted applications and data, reducing the attack surface and lateral movement. But what happens when a bad actor slips through those defenses? How does your agency defend against insider threats and sophisticated nation-state and ransomware attacks?

In these situations, the best defense is active, making it nearly impossible for attackers to achieve their aims. This is the idea behind deception technology.

Deploying Honeypots

Deception technology provides a fake attack surface to intruders, to distract them from sensitive data or systems. This attack surface is composed of honeypots, or false assets, that set off an alarm when an attacker touches them. These decoys can be fake endpoints, files, services, databases, data, passwords, users, computers, user paths, OT, IOT and other resources that mimic production assets.

Deception technology can leverage cloud-based delivery and can be expanded to every possible identity system. Because nine out of 10 attacks involve an Active Directory infrastructure, creating fake, but attractive objects to monitor is a good place to start, followed by fake network attached resources.

Once an alert is triggered, defenders can track attackers' movement in a secure, isolated environment, identify the assets the attackers are interested in, slow them down, and monitor their tactics, techniques, and procedures.

Deception technology provides:

- **Pre-breach warnings**: Perimeter decoys detect stealthy pre-breach activities that often go unnoticed.
- **Lateral movement detection**: Application decoys and endpoint lures intercept adversaries that have bypassed perimeter-based defenses and limit their ability to maneuver and find targets undetected.
- **Defense against ransomware**: Decoys in the cloud, network, endpoints, and Active Directory act as landmines to detect ransomware at every stage. Simply having decoys in your environment inhibits ransomware's ability to spread by providing early warning.
- **Real-time threat containment**: The best deception technology integrates seamlessly with your ecosystem of third-party security tools such as security incident event management (SIEM), security orchestration automation and response (SOAR), and other security operation center (SOC) solutions to shut down active attackers with automated rapid-response actions.

Integrating With Zero Trust

One of the most powerful approaches to cybersecurity integrates deception technology into a zero-trust system. No single security technique is 100 percent effective at stopping attackers; for maximum protection, multiple technologies must work together and share information.

While the core of zero trust does not include a threat detection component, incorporating deception technology into a zero-trust architecture adds a powerful capability. Deception decoys act as tripwires in a zero-trust environment, identifying compromised users or lateral movement across the network.

Conserving Time and Money

Deception technology is a very efficient form of threat detection that can save time and reduce costs for government agencies. Agency personnel can simply set up honeypots and wait, detecting advanced attacks without high operational overhead. Because legitimate users have no reason to touch fake assets, agencies drastically reduce the rate of false positives and add a powerful layer of threat detection across the enterprise.

About the Author

Brett is an IT Infrastructure and Security Leader with 20 years' experience spanning operations across six continents. Prior to joining Zscaler, Brett led Bechtel Corporation's journey towards Zero Trust while directing multi-disciplinary teams across the globe. Brett's career has evolved from help desk support, server, and datacenter operations, through to leading regional and global teams with responsibilities across operations, engineering design and architecture disciplines. That wide experience gave him in-depth knowledge of a diverse range of technologies and disciplines plus the capability to direct teams who manage them.

Brett James is the Director, Transformation Strategy of Zscaler. He can be reached online at bjames@zscaler.com, LinkedIn and at our company website https://www.zscaler.com/.

Data Privacy and Data Protection: What Enterprises Need to Know

By Anurag Lal, President and CEO of NetSfere

Digital transformation is exponentially increasing the amount of data companies collect, use and store. In fact, it is projected that the total amount of data created, captured, copied, and consumed globally will increase from 64.2 zettabytes in 2020 to more than 180 zettabytes in 2025, enough to fill approximately 10 million DVDs.

That's a lot of data. As companies generate and become stewards of more and more data, strong data protection and data privacy strategies are essential to enterprise success.

Data protection and data privacy are both critical to keeping sensitive data safe. While data privacy and data protection are interconnected, it is important to understand the distinction between the two terms, their implications for business and best practices for mitigating data loss and reducing compliance risks.

Data protection

Data protection is a broad term that refers to the processes, policies, tools and strategies aimed at securing data availability, integrity and privacy. In today's digitally transformed enterprises, data protection is mission critical for preventing unauthorized access to data and securing data as it travels across devices.

Data protection is especially critical to business continuity considering the expanded attack surface created by remote and hybrid working models and the increasing frequency and severity of cyberattacks. According to the Identity Theft Resource Center's Annual Data Breach Report, the number of data compromises reached 1,802 in 2022, impacting approximately 422 million people.

As data grows more valuable and cyberthreats continue to evolve, actively protecting data must be a key focus of every enterprise.

Data privacy

A subset of data protection, data privacy relates to who has authorized access to data. Data privacy essentially dictates how data is collected, handled, and managed by organizations. Enterprises, especially those in highly regulated industries such as healthcare and financial services, must understand and comply with a growing number of data privacy regulations. According to a Gartner prediction, by 2024, over 75% of the world's population will have its personal information covered under modern privacy regulations.

Businesses that don't comply with the patchwork of data privacy regulations are at risk of data breaches, fines, loss of trust and brand reputation, and operational disruptions. Today, compliance risk is increasing as regulators step up enforcement, cracking down on organizations that don't meet compliance standards.

The most recent annual report from the Data Protection Commission (DPC), the Irish supervisory authority for the General Data Protection Regulation (GDPR), revealed that in 2022 the DPC concluded 17 Large-Scale inquiries, with administrative fines in excess of €1billion. In 2022, U.S. regulators from the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) fined banking institutions $1.8 billion for employee use of unsanctioned communications apps.

Stricter enforcement of evolving regulatory frameworks requires organizations to develop a robust approach to data privacy that works to prevent unauthorized access to data.

Data protection and data privacy best practices

As stewards of an ever-increasing amount of data, enterprises must ensure data protection and data privacy. Organizations can protect data and privacy by following the best practices outlined below.

Educate employees

It is important to educate employees on cybersecurity best practices and ensure they understand that cybersecurity is the responsibility of all stakeholders in an organization. Employee cybersecurity training is especially critical considering that 82% of breaches reportedly involved the human element.

To minimize cyber risk, enterprises should make it a continuing practice to educate employees to recognize phishing scams and other threats, understand cybersecurity best practices and recognize the importance of following security protocols to comply with regulations such as HIPAA and GDPR.

Encrypt all data

Protecting data in transit and at rest requires true end-to-end encryption (E2EE). E2EE makes it impossible for cybercriminals to intercept this data, locking down sensitive information to ensure data privacy, security, and compliance.

E2EE is one of the best cyber defenses against threat actors and is mission critical in business applications such as mobile messaging and collaboration technology.

Create Bring Your Own Device (BYOD) Policies

With the rise of remote and hybrid working, devices and data are increasingly travelling outside of the company network, creating a wide variety of security and privacy risks.

To minimize BYOD cyber vulnerabilities, organizations must establish and enforce “acceptable use” policies including requiring the use of passwords with multi-factor authentication, requiring employees to use VPNs when working remotely, prohibiting the downloading of unsanctioned apps, and banning the use of unauthorized messaging apps in workflows.

Understanding the nuances of data protection and data privacy and how to proactively approach both can mitigate the threat of data breaches and help ensure success for today’s data-driven enterprises.

About the Author

Anurag Lal is the President and CEO of NetSfere. With more than 25 years of experience in technology, cybersecurity, ransomware, broadband and mobile security services, Anurag leads a team of talented innovators who are creating secure and trusted enterprise-grade workplace communication technology to equip the enterprise with world-class secure communication solutions. Lal is an expert on global cybersecurity innovations, policies, and risks.

Previously Lal was appointed by the Obama administration to serve as Director of the U.S. National Broadband Task Force. His resume includes time at Meru, iPass, British Telecom and Sprint in leadership positions. Lal has received various industry accolades including recognition by the Wireless Broadband Industry Alliance in the U.K. Lal holds a B.A. in Economics from Delhi University and is based in Washington, D.C.

Investing Wisely

Where to focus spend during the economic downturn

By Tim Wallen, Regional Director, UK, US & Emerging Markets, Logpoint

There remains a great deal of uncertainty when it comes to how IT budgets will play out this year. According to the ESG 2023 Spending Intentions Survey, 53 percent expect it to increase, but 30 percent say it will stay the same and 18 percent think it will go down. Yet regardless of how things play out, cybersecurity is liable to get a bigger piece of the pie, with 65 percent expecting spend in this area of the IT budget to increase.

Although cybersecurity is widely regarded as a business priority warranting higher spend, it's proving much harder to ensure there's enough to go around. Inflation is seeing costs such as software licensing rise, plus the sector is experiencing a significant skills shortage, and coupled with the cost-of-living crisis, this is seeing wages increase. The ISC(2) Workforce Study 2022 found that the workforce gap has increased by 73.4 percent year-on-year in the UK, with The Department for Digital, Culture and Sport (DCMS) projecting an annual shortfall of 14,100 per year, it's a problem set to get worse before it gets better.

Compounding these challenges is a highly competitive market. According to the 2023 Gartner Board of Directors Survey, 64 percent of board directors intend to increase the risk appetite of the business in order to compete more aggressively, with 46 percent willing to accept greater risk to achieve growth. CISOs will therefore need to adjust their risk management strategies to capitalise on opportunities, but as a result, can expect to see the risk exposure of the business increase, putting yet more pressure on cybersecurity resource.

All of these factors mean the CISO will need to utilise the data at their disposal more effectively to justify their decisions and guide investment. They'll need to look at how they can measure the effectiveness of security controls against those of other organisations and evaluate the maturity of the business' capabilities, for instance.

Using meta-analysis to drive decision making

Such meta-analysis will help CISOs report to the C-suite about general cybersecurity performance and justify their decisions to the board whether that be to invest, consolidate or outsource. In addition, meta-analysis will allow the CISO to evaluate technology and determine opportunities to reduce costs by using it as a benchmarking function. Using a data-driven approach will in turn, prove the business case for investment in automation, which will be essential in helping to ease staff shortages.

Automation can unlock real gains, particularly in the mid-market which struggles with alert overload/fatigue. Advances in AI and machine learning are seeing these alerts treated not as standalone occurrences but as part of a bigger picture. They are regarded as indicators of a possible compromise that is then qualified using contextual information to determine the level of response needed, helping to reduce the problem of false positives and to prioritise investigations.

Crucially, organisations with fully deployed security AI and automation save $3.05 million per data breach compared to those without (a 65.2% difference in average breach cost, states the 2022 IBM Cost of a Data Breach Report), so it can certainly deliver ROI and should be prioritised. But where else should CISOs focus spend?

Where to allocate spend

According to Forrester, top priorities for cybersecurity in 2023 include the replacement of legacy Security and Incident Event Management (SIEM) with systems that can analyse security behavior. Using a converged SIEM, for instance, provides the business with additional capabilties as it comes with Security Orchestration and Response (SOAR) fully integrated to provide automated detection and response, User Entity Behaviour Analytics (UEBA) for threat modelling, and with additional modules such as Business Critical Security (BCS) allowing previously siloed applications, such as SAP, to be brought into the SIEM security fold. So how does each of these helps ease the pressure on cyber security resources?

The automation conferred by SOAR sees security data and alerts gathered and prioritised to help identify and resolve incidents fast. Workflows and playbooks automate repetitive tasks, such as dealing with false positives, and guides security analysts to the right response. All the analyst has to do is approve or execute a decision while security teams are presented with data that has been automatically correlated and analysed together with contextual information and intelligence. This action speeds up the triage process so security teams can respond quickly ensuring Mean Time to Detect/Respond (MTTD/MTTR) is reduced. Plus, it also mitigates data breach impact because built-in response capabilities on the endpoints can be used to isolate hosts, block incoming connections from malicious sources, and disable users.

UEBA is invaluable in enabling the business to identify activity that deviates from the norm and to apply context to indicators of compromise (IoCs). It can detect security incidents that would be impossible to detect under other circumstances because it applies machine learning to peer grouping and baselines to identify normal/abnormal behaviour. And because it looks at data from across the organisation and its security infrastructure, it can apply that behavioural analysis to eliminate false positives.

UEBA also helps teams make sense of alerts by supplementing them with environmental and situational information. Environmental context can include details such as, whether a user was an IT admin or highly privileged user, or if they own the asset in question, while situational context may seek to establish if the incident has happened before and whether it falls within normal parameters. Moreover, high-fidelity risk scoring makes it easy for analysts to know which alerts to investigate first, helping to reduce the time it takes to resolve incidents.

A converged solution can also help the business extend its security management across previously siloed applications. SAP, for instance, is used to carry business critical data to systems responsible for everything from digital enterprise resource planning (ERP) and human capital management operations to sales, stakeholder relationship management (SRM) and customer relationship management (CRM) processes. However, these are usually protected using SAP security which then prevents the correlation of information and achieving enterprise-wide oversight.

Bringing such applications onto the SIEM using BCS enables SAP systems to be continuously monitored for IP theft, fraud, access violations, and compliance to enable threat detection and response. Suspicious transactions and SAP user behaviour can then be captured in near real-time and activity tracked with UEBA, while integration with the SIEM and SOAR automates checks, dramatically reducing time to compliance. Monitoring SAP in this way can also prevent costly downtime by acting as an early warning system.

Creating a single pane of glass

Automating SIEM, SOAR, UEBA and BCS over one platform not only eliminates the complexity associated with integration and management but also enables these data feeds to be combined to provide qualified insights. The severity of an incident can be validated and the response automated, freeing up precious human resource. Moreover, the dashboard provides the CISO with a single pane of glass through which to view the security posture of the business, keep track of compliance obligations and to carry out reporting.

Converged solutions will be a primary focus for investment going forward because CISOs can conserve significant spend by consolidating the cybersecurity stack. An ESG report found 70 percent of businesses run more than ten tools, with some managing up to 50 point solutions, often with overlapping functions in a bid to close security gaps.

This can result in high operational overheads as these solutions come from a myriad of suppliers with their own proprietary technologies that the security team needs to master in order to use them and keep them up to date. Reducing the number of solutions and the number of vendors can therefore cut

management costs because there's no longer the need to spend out on training or to hire those with specialist skillsets.

For this reason, a staggering 75 percent of CISOs are pursuing a vendor consolidation strategy, according to Gartner's Top Trends in Cybersecurity 2022 report. These CISOs said motivation included the need to improve overall risk posture, derive efficiencies from economies of scale and eliminate the time and expense required to integrate separate tools. But what's notable is that almost a third (29 percent) said they were actively pursuing a consolidation strategy now compared to back in 2020.

However, while consolidation may seem a no-brainer it can become difficult to execute and extract savings from due to software licensing models. These are typically based on data volume, which does of course increase exponentially overtime, leading to runaway costs. Tied in to specific providers, CISOs face something of a Hobson's Choice: pay these rising costs or cut back on their security monitoring.

Limiting the amount of data coming into the system simply doesn't make sense in a security context, because it means curtailing visibility, but it can also directly impact business growth. Unable to reach their security objectives without worrying about restricting what they ingest and from where, the CISO may choose instead to delay security projects. For this reason, it's vital that CIO/CISOs look not just at the functionality but the scalability of the solutions available to them.

Scalability is also key for another reason. The current economic climate is likely to see threat actors intensify their efforts because they are equally feeling the effects of the downturn. Those attackers will also be looking to leverage automation to create maximum return for minimum effort, which will equate to an increase in the volume and veracity of attacks. So CISOs cannot afford to cut back; they must invest to curb the threat and protect the company's assets. The trick is to do so wisely and in such a way that costs become contained, human resource conserved and automation used to confer accuracy and reduce workloads. Consolidation can deliver on all three fronts.

About the Author

Tim Wallen is Regional Director for the UK, US and Emerging Markets at Logpoint. With almost 20 years of cybersecurity experience, he has held senior sales and management positions within both high-growth and established vendors, including FireMon, ForeScout, Check Point, McAfee, and IBM. He is responsible for driving strategic growth in the regions and for leading the growing team of Logpoint sales, marketing, and technical professionals. Tim can be reached online at https://www.linkedin.com/in/timwallen/?originalSubdomain=uk and at our company website https://www.logpoint.com/en/.

Online Privacy Statistics

By Milos Djordjevic, Online Privacy Expert, VPN Central

Online privacy is a burning issue in our modern threat landscape. It concerns both companies and individuals — no one can afford to ignore it.

The first step in tackling this question is informing yourself. We've rounded up the most important online privacy statistics, including facts about social media, online shopping, and data protection.

Let's have a look at the numbers.

Here's our pick of the most relevant statistics concerning online privacy:

- 79% of Americans aren't confident that companies would admit to misusing and compromising their data.
- The average cost of a data breach in the US is $9.44 million.
- 92% of consumers don't trust shopping recommendations from chats or pop-ups on websites.
- In 2022, 70% of global internet users have taken steps to protect their online activities.
- Out of all social media, Facebook collects the most data about you.

- 77% of US adults know about companies using their data to target them with ads.
- 48% of respondents feel they have no control over the search terms they use.
- Less than half of US consumers say they trust social media and other online services to protect their data.

Internet Privacy Statistics

Let's check out some eye-opening stats about internet privacy in general:

1. 48% of respondents feel they have no control over the search terms they use.

(Statista)

Nearly half of US adults are concerned about their online searches. In addition to that, they stated that they felt no control over their:

- Visited websites — 41%
- Online purchases — 45%
- Private conversations and text messaging — 37%
- Posts on social media — 35%
- Physical location — 28%.

2. Nigerian internet users are the most concerned about their online privacy.

(Statista)

According to Statista's global 2019 study, 82% of internet users in Nigeria are worried about online privacy. They're closely followed by Egyptians at 76% and Indians at 73%.

The US is near the bottom of the list, in 20th place with 47%. Interestingly enough, German users are the least worried, at 26%.

3. 41.4% of all websites use cookies.

(W3Techs)

Cookies are one of the most popular tools used by websites and advertisers to track online activities.

Out of them, non-secure and non-HTTP Only cookies are the most prevalent, both at 75.2%. Furthermore, session cookies (69.9%) are more common than persistent ones (55.9%).

4. 47% of respondents updated their website's cookie policy in the last 12 months.

(IAPP and TrustArc)

Online privacy statistics show that nearly a half of companies have updated their cookie policy in the last year. Additionally, 80% have updated their website's privacy policy one or more times.

There are also other changes: 42% of respondents have deleted their clients' personal data more regularly in 2019.

5. In 2022, 70% of global internet users have taken steps to protect their online activities.

(Statista)

As of December 2022, seven in ten respondents have taken steps to safeguard their identity online. Given the worrying digital footprint statistics, this comes as no surprise.

The most popular form of protection was parental control, at 36%.

Other commonly used security measures were:

- Multi-factor authentication — 36%
- Privacy settings on devices — 30%
- Identity theft protection services — 28%.

Social Media Privacy Statistics

Social media platforms are among the most vulnerable online spaces. The following facts are hard to dispute:

1. Out of all social media, Facebook collects the most data about you.

(Clario)

Facebook is the most data-hungry platform. It collects 79.49% of personal information, like your hobbies, pets, favorite shows, and more.

Instagram is next on the list, with 69.23%. TikTok is in third place, at 46.15%. Finally, Clubhouse and Twitter are evenly matched with 33.33%.

2. Less than half of US consumers say they trust social media and other online services to protect their data.

(Deloitte)

According to internet privacy statistics, 47% of consumers trust social media and websites to keep their data safe. The majority wishes for better privacy practices.

Still, the same study has shown that they're not doing all in their power to protect their data. 41% have used different passwords across websites as their dominant security measure.

One look at password reuse statistics proves this is a step in the right direction. But it's not enough on its own.

3. 79.2% of people have adjusted the privacy settings on their social media profiles or reduced their usage.

(DuckDuckGo)

In the past year, most social media users have changed their privacy-related settings or spent less time on these services. On top of that, 23% of respondents have "deleted or deactivated a social media profile due to privacy concerns."

Among those users, 28.5% have deleted their Twitter accounts and 30.5% have deactivated their Instagram.

Online Shopping Privacy

Online advertising is often at the top of concerns about internet privacy. Here's why:

1. 50% of American adults think that online advertisers shouldn't save any information about their visits.

(Pew Research)

The majority of US adults expect limits on how long their data is stored. Out of them, 50% believe that online advertisers shouldn't keep any of their data.

They're also not comfortable with social media, video sites, and search engines keeping records. At the same time, 28% of respondents didn't mind credit card companies logging their activities for a few years.

2. 77% of US adults know about companies using their data to target them with ads.

(Pew Research)

Online privacy statistics have revealed that US adults are knowledgeable about ad targeting. 77% are aware that companies build user data profiles based on their online browsing. Out of them, 75% believe that all or most businesses rely on this tactic.

3. 92% of consumers don't trust shopping recommendations from chats or pop-ups on websites.

(Chain Store Age)

It's becoming increasingly difficult to influence consumers with technology. A whopping 92% steer clear of pop-ups and chats when it comes to shopping recommendations.

In addition to that, 81% don't trust ads on mobile devices. Only 23% of consumers think that social media ads are reliable.

Data Privacy Statistics

Here are some interesting trends surrounding privacy regulations and practices:

1. The average cost of a data breach in the US is $9.44 million.

(IBM)

Data breaches can be an expensive mistake. According to IBM's 2022 report, the US is in the first place, with $9.44 million. The global average cost of a data breach is $4.35 million.

2. 25% of Americans are asked almost daily to agree to a privacy policy.

(Pew Research)

One-quarter of adult Americans say they are asked to agree to a privacy policy almost every day. 32% say this happens about once a week.

Still, only 22% thoroughly read the policy before agreeing to the terms and conditions.

3. Indian internet users are the most aware of their country's data protection and privacy rules.

(Statista)

60% of Indian internet users are familiar with their domestic data protection and privacy rules. They're closely followed by Germany, at 59%. Egypt and Great Britain are tied at 57%.

The US is near the bottom of the list, in 18th place.

4. 79% of Americans aren't confident that companies would admit to misusing and compromising their data.

(Pew Research)

Data privacy statistics show that most Americans don't believe companies will admit mistakes and take responsibility for data misuse. What's more, 69% don't trust companies to use their data in ways they'll be comfortable with.

Conclusion

Netizens and consumers are becoming increasingly aware of how pervasive internet privacy issues are. In turn, companies and organizations are hard-pressed to win back their trust.

Our digital privacy statistics show that there's a rift slowly growing between them. Additionally, more users are taking their first steps in minimizing their digital footprint and protecting their information.

Still, strong security measures and a transparent privacy policy will always inspire confidence.

FAQ

Why is online privacy important?

Online privacy is important because your data is a valuable asset. Even information that you might find trivial is useful to companies and cybercriminals. It can be used against you or sold for profit, so it's essential to keep your data safe.

How to protect your privacy online?

There are several ways you can protect your online privacy, such as:

- Creating strong passwords
- Refraining from oversharing on social media
- Using a password manager
- Enabling multi-factor authentication
- Adjusting your privacy settings on apps
- Installing a VPN.

How many people are affected by internet privacy?

Internet privacy affects everyone who has a digital footprint. According to online privacy statistics, 62% of American netizens believe it's impossible to go through daily life without companies collecting data about them.

About the Author

Milos Djordjevic is a Digital Marketer passionate about technology. He has pursued a cybersecurity and online privacy career to helping organizations and individuals stay secure in an increasingly complex digital world. Milos holds a master's degree in Marketing and more than ten years of experience on the WEB. He can be reached online at milos_djordjevic@vpncentral.com and at our company website www.vpncentral.com/.

Empowered Encryption

Why organizations must take back control of their data

By Dimitri Nemirovsky, Co-Founder & COO, Atakama

Sometimes, what a change represents is more meaningful than the change itself. Case in point is Apple's recent launch of an advanced encryption suite to help customers keep their data private. Among a handful of new security tools is a feature that expands on current end-to-end encryption facilities, giving users the option to fully encrypt data stored in its iCloud service.

The fact Apple takes encryption seriously should surprise no-one. Apple has long set the standard for data privacy for consumers, with the tech giant's security measures among the most trusted in the industry. Apple's record $26.25 billion spend on R&D in its 2022 fiscal year is another testament to its continuing commitment to innovation.

But what has changed is Apple's approach to the end user. In granting control of the encryption keys that protect customers' sensitive data to users, Apple has put the user in the driving seat. Now, users can take responsibility for their data even in the event of an Apple data breach.

This represents a sea change in mindsets around data privacy, doubtlessly driven by regulatory pressures, media scrutiny, and the direct financial and reputational losses incurred by organizations facing evolving cyber threats.

But what does this mean for enterprise data security?

There is an opportunity for Apple's approach to become normalized and adopted as a standard across the enterprise. This approach is pivotal in preparing for inevitable data breaches – and with the right tools, organizations can take control over their encryption keys and stay in charge of their security infrastructure, without relying on a third party.

Third parties: a fast-growing risk to data security

Enterprises and consumers alike have historically relied on intermediaries to secure their data, and there are regulations and standards in place which govern levels of compliance and security. No executive wants to sit in front of a Congress committee investigating a data breach and admit that they failed their compliance obligations. Yet, as the third-party landscape changes, and data-bridges linked by APIs bring disparate third parties closer together, the responsibility for securing data can variously shift from party to party. Responsibility for the security ultimately rests with the owners of the data, and that's exactly why organizations must have absolute control over the keys that secure their data.

Enterprises, which appreciate the value of the data they own, cannot afford to rely on bulk encryption techniques or centralized Identity Access Management (IAM) solutions to defeat breaches. Even if organizations encrypt data, it is vulnerable to theft if they rely on centralized encryption key management. Organizations must shift from locking away their critical data in a centralized, third-party-owned vault along with everyone else's data. Recognizing that securing the perimeter is just one aspect of securing the data inside it, firms also need their own safety deposit box within the vault – and only they should have access to the key. This will empower organizations to control their data and better protect themselves.

Hacking is not a question of when, but how often

There has been an alarming rise in ransomware breaches globally, with attacks against organizations up by 13% in the space of a year. It's a reminder that determined cybercriminals will stop at nothing to access, steal, and ultimately leak data for financial gain.

It is no longer a question of if an organization is going to be attacked. It's not even a question of when – organizations now need to consider how often they will be attacked. Any organization that fails to embrace an assume breach mindset is setting itself up for catastrophe.

Notwithstanding the traditional problem of organizations focusing on keeping threats out via IAM and thinking that nothing can be done to secure data from bad actors already within the perimeter, organizations have no excuse not to seize control over their encryption keys. Unsurprisingly, companies which have been hacked take securing data within the perimeter much more seriously.

But while Apple is making strides to empower the consumer, the enterprise world continues to lag behind. Few organizations are taking advantage of Bring Your Own Key (BYOK) capabilities that enable them to manage their own encryption – often this is due to complexity. Administering keys is not a simple task, it's far from frictionless and there are significant penalties, including permanent data loss, for making mistakes. Even the most sophisticated entities can get tripped up by key management, as the recent AWS security incident demonstrates.

Multifactor encryption

Organizations need new tools to control their data, independently manage their keys, and strengthen their defenses in the face of growing security threats. The latest advances in multifactor encryption eliminate the reliance on third parties and IAM for data protection, protecting organizations from data exfiltration by empowering them to secure their critical information on their own.

Conventional encryption relies on centralized keys and places a heavy reliance on user credentials and identities, leaving organizations vulnerable to mass exfiltration of data as soon as a user is authenticated. Encryption on its own doesn't provide any meaningful level of defense unless it is created independently from the centralized access management system that the attacker has already breached.

With multifactor encryption, data at rest is encrypted using AES-256 keys. A unique key is generated for each object and then automatically fragmented and distributed across physical devices, eliminating central points of attack and central points of failure. Utilizing this approach, bad actors find that they are in a vault which requires keys that they can't access.

For users, decryption is frictionless – with just a few clicks on a file, a user can approve a notification prompt on a mobile device, and policies can be designed to map organizational workflows to provide automation that ensures security while granting users the agility and flexibility to work with documents seamlessly. This allows organizations to maintain complete control of their encryption, without falling into the common trap of sacrificing data accessibility for data security.

Flexible deployment gives organizations the freedom to secure their data in the way that best suits their environment, offering unrivalled data protection even when rules-based access controls fail and facilitating innovation and productivity.

Decentralized multifactor encryption transforms the way enterprise data is protected, putting organizations in the driving seat of their own data security by giving them full control over their most sensitive assets.

About the Author

Dimitri Nemirovsky is the Co-Founder & COO of Atakama. Dimitri holds BBA and MBA degrees from Baruch College and earned his JD from Brooklyn Law School. Prior to co-founding Atakama, Dimitri spent 15 years as an attorney, most recently practicing regulatory and enforcement law at Bingham McCutchen where he represented large financial institutions in high-stakes matters. Dimitri began his career at Merrill Lynch.

Dimitri can be reached online at LinkedIn and at our company website https://www.atakama.com/.

Most Commonly Overlooked Attack Surface Vulnerabilities & How to Fix Them

By Marc Laliberte, Director of Security Operations at WatchGuard

Over the last decade, many organizations have rapidly accelerated their digital transformation. The rise in cloud hosted Software-as-a-Service (SaaS) applications, continued proliferation of Internet of Things (IoT) devices, and a global pandemic forcing an overnight transition to a remote workforce have forced most IT teams to quickly adopt and deploy new technologies to keep the business moving. While these new technologies have obvious productivity benefits, they also significantly expand an organization's potential attack surface. If security isn't a motivating factor when acquiring or managing new technologies, it can lead to significant gaps in your organization's defenses.

Your attack surface is the total collection of all possible attack vectors that could enable an adversary to access, cause an effect on, or extract data from a system in your organization. To understand this better, you can split your attack surface into three main components: digital attack surface, physical attack surface and human attack surface.

Digital Attack Surface

Your digital attack surface is, put simply, anything digitally accessible to an adversary. This includes known assets like your corporate website, server infrastructure, and user workstations. It also includes unknown assets like shadow IT, forgotten or employee-installed software and devices. Your digital attack surface also includes rogue assets, malicious infrastructure and systems set up by a threat actor like existing malware infections or typo-squatted domains.

Physical Attack Surface

Your physical attack surface includes all vulnerabilities an attacker could access with physical access to your office or an endpoint system. This includes everything from exposed network jacks in your lobby to unencrypted user laptops left in a car. While an attack against your physical attack surface may feel unlikely, it often enables effortless privilege escalation and lateral movement to adversaries who target it.

Human Attack Surface

Your human attack surface is the total number of individuals in your organization who are susceptible to social engineering. We've all experienced the common forms of social engineering like Phishing and Smishing (text message phishing), but this also includes techniques like media drops, in which adversaries ship a malware-laced USB drive to victims hoping a curious individual connects it to their laptop. Your human attack surface can also include fake employees tricking your real employees into performing a damaging action.

The most common shortfall for an IT or security team in managing their attack surface is simply not understanding the breadth of it. It's very easy for technical debt to accumulate over the years or to spin up "quick fixes" which are then neglected or long forgotten. To address this, make a regular asset and data audit a part of your security program. At a minimum, identify business owners and run a risk assessment to understand the data or system's value and risk of compromise. You can lean on the business owners themselves to complete questionnaires for their environment and asset discovery tools to identify things that are missed.

A recent Thales research study found only 40% of non-IT staff have adopted multi-factor authentication (MFA). While this is better than previous years, it's still a significant gap for organizations that have not fully adopted MFA. Compromising a user's credential is unfortunately a very low bar for threat actors and, without MFA, that is enough to get a foot in the door. Even with unprivileged accounts, you won't meet a seasoned penetration tester that doesn't have a near 100% success rate of elevating their access in an organization from any account at all.

Eliminating complexity is another important step towards reducing your overall attack surface. Complexity often masks configuration or management mistakes that can lead to additional gaps in your defenses. This is especially important when it comes to your protection and detection capabilities. A Gartner survey

earlier this year found 75% of organizations are pursuing security vendor consolidation to help reduce complexity and speed up response times.

No attack surface management program can be successful without addressing the human element too. Make sure your social engineering training covers not just traditional email phishing but other common social engineering techniques and risky behaviors as well. As we've seen throughout the course of 2022, with major breaches targeting Uber, Microsoft, and others, the strongest technical controls can often be circumvented by a single employee mistake.

Addressing your attack surface isn't a one and done type of event. It is an ongoing and evolving process that requires continuous focus and iterative improvements over time. It also isn't an easy task, especially for large or old organizations. If you start with the basics though, you can knock out enough low hanging fruit to make your organization a less vulnerable target to cyber adversaries and continue strengthening your security program over time.

About the Author

Marc Laliberte is the Director of Security Operations at WatchGuard Technologies. Marc joined the WatchGuard team in 2012 and has spent much of the last decade helping shape WatchGuard's internal security maturation from various roles and responsibilities. Marc's responsibilities include leading WatchGuard's security operations center as well as the WatchGuard Threat Lab, a research-focused thought leadership team that identifies and reports on modern information security trends. With regular speaking appearances and contributions to online IT publications, Marc is a leading thought leader providing security guidance to all levels of IT personnel. Marc can be found on LinkedIn at https://www.linkedin.com/in/marc-laliberte/.

An Interview with Greg Van Der Gaast

By Megan Lupton, Senior Content Executive, Champions Speakers

From one of the most wanted hackers to being featured in the Top Trending Ethical Hackers list, Greg van der Gaast has been on both sides of the fight against hackers. In this exciting interview, he reflects on the UK's biggest cyber threat and reveals what he believes to be the next big style of cyber-attack.

In your opinion, what is the biggest cyber threat the UK faces?

“Everyone will say ransomware, but ransomware is basically a payload; it's a way of monetising a breach. I think the really shocking thing is the way companies get breached, the way that people get in the door, because it really hasn't changed in the 25 years that I've been doing this.

“People are still not building systems properly, they're still not maintaining them properly, they're still not doing asset inventory. They're not patching properly, they have poor processes, they have a lack of consistency in processes. You're basically living in a house with a thousand doors and a thousand windows, and some constantly being left open - that's how people get in.

“For large businesses and organisations, you need a holistic and business-aligned security approach that's truly proactive and in line with the business, in line with how things actually work. Then, you come up with effective, sustainable ways of doing things rather than the security status quo, which is just ‘buy another tool’.”

What would you say is the weakest link in the cyber defences of a business or organisation?

“Everyone says people - ‘people are the weakest link’ - but they're also your first line of defence.

“It's, in a word, sloppiness. Lack of maturity, lack of processes, lack of integration, not having that full holistic view of your environment. But also, your IT and your security not understanding the business processes themselves, not knowing what there is to protect. Those are the real issues.

“You hear a lot about ‘Dave from Marketing clicked an email and that's how everything went wrong’. He clicked on an email, so an attacker had Dave's level of access on his laptop.

“But... how did they get the admin? Because you hadn't configured that laptop properly. And how did they get through your VPN? And how did they get through your firewall? Because you hadn't updated the firmware, you hadn't changed the default password.

“Let's blame it all on Dave from Marketing, instead of the security and IT teams who didn't do their jobs.”

What do you predict will be the next big style of cyber-attack?

"Ransomware is very disruptive, we've got more and more critical infrastructure being hit. I think that's going to continue to grow, continue to scale up.

“We're still not taking the problem seriously. We usually just blame an intern and go from there. I think someone told me that T-Mobile has been hacked six times in the last three years... that's probably a bad sign.

“I think it's going to be a bit more of the same, but it's going to get more and more damaging. The scale of things will get worse and worse.”

This exclusive interview with Greg van der Gaast was conducted by Mark Matthews.

About the Author

Megan has managed the internal content for Champions Speakers since 2019 when she joined the company as a Digital Copywriter. In 2020, she progressed to Content Executive and only a year later, Megan was promoted to Senior Content Executive, where she now manages the Champions Speakers YouTube channel and PR outreach.

Continuing her passion for writing, Megan started a PhD at De Montfort University in October 2021. She previously earned her Bachelor of Arts in Film & Creative Writing at the University of Essex and her Masters of Arts in Creative Writing from Teesside University. In her current course, Megan is studying the ethics of such digital forms as podcasts and is conducting metafictional research on the creative process.

In her role, Megan has interviewed several exciting names including Dr Alex George and Sir Mo Farah. She is particularly passionate about LGBTQ+ pride and female empowerment, digital media and journalism – topics Megan enjoys writing about at Champions and researching for her PhD.

What are NIST Encryption Standards? Why Do They Matter a Lot?

By Amar Basic, Co-Founder CyberArrow

Data encryption is essential in today's technologically advanced world to safeguard sensitive information against hacker assaults and data breaches, as an estimated 30,000 websites are hacked each day globally. The National Institute of Standards and Technology (NIST) has developed a set of recommendations and rules for encryption and cryptography protocols to guarantee high security. These are referred to as NIST Encryption Standards, and they offer businesses a foundation for creating robust security protocols to safeguard their sensitive data.

This article discusses the NIST Encryption Standards and some of the forms of encryption and cryptographic protocols they advise. It also discusses the importance of these standards for preserving the privacy, accuracy, and accessibility of sensitive data in the present digital era.

Importance of NIST Encryption Standards

The US Department of Commerce's National Institute of Standards and Technology (NIST) is a non-regulatory organization fostering inventiveness and economic competitiveness. One of NIST's key responsibilities is creating and maintaining standards for the cryptographic protocols and algorithms used in information security. Poor security measures, such as insufficient encryption or weak passwords, might leave data vulnerable to hacker assaults and illegal access.

NIST encryption standards are essential for keeping sensitive data confidential, authentic, and intact. Cryptographic methods and protocols are employed during the encryption process to transform plaintext data into ciphertext to prevent unauthorized access. The standardized foundation provided by NIST standards for encryption provides compatibility between various systems and devices and contributes to the security of the encryption techniques.

NIST Encryption Standards

Cryptographic algorithms are deployed in every piece of equipment and applied to every link in the digitally connected age to secure data during its transfer and retention. NIST has taken a unique and

pioneering role in creating critical cryptographic standards to meet the security standards of today's world. The following are the four most significant NIST encryption standards:

Data Encryption Standard (DES)

The National Bureau of Standards (NBS), which is now known as the National Institute of Standards and Technology (NIST), initiated the Data Encryption Standard (DES), a symmetric-key encryption method, as a standard in 1973. With a 56-bit secret key, the block cipher technique DES encrypts data in 64-bit blocks. The algorithm operates in multiple rounds, each using a different subkey generated from the original secret key.

DES encrypts and decrypts data using a symmetric-key technique. The invention of this ground-breaking encryption standard played an essential role in advancing contemporary cryptography. However, due to its short key length and other flaws, it has been replaced by newer and more secure encryption techniques.

Advanced Encryption Standard (AES)

The National Institute of Standards and Technology (NIST) created the Advanced Encryption Standard (AES) in 1997, a popular encryption algorithm, to replace the outdated Data Encryption Standard (DES). AES employs the same key to encrypt data, making it a symmetric-key encryption technique.

The block cipher algorithm AES supports three key lengths: 128 bits, 192 bits, and 256 bits, and it operates on 128-bit blocks, while the algorithm consists of rounds that perform substitution and permutation operations on the plaintext input. The data is encrypted in each game using a set of round keys created using the secret key.

It offers robust encryption protected from assaults, such as brute-force attacks. The US government has certified AES for use with classified material.

Public-Key Cryptography

Asymmetric cryptography, commonly called public-key cryptography, invented in 1976, encrypts data using two public and private keys. The public key is distributed, but the private key is kept private, and due to their mathematical link, data encryption with one key can only be decoded using the second key.

Public-key cryptography is frequently employed for secure communication, digital signatures, and online authentication. One of its main benefits is public-key cryptography's ability to offer safe communication without requiring a shared secret key. Instead, every participant has a unique set of keys that they can use to encrypt and decrypt data.

Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) is made to withstand assaults from quantum computers, while quantum bits, also known as qubits, are used in quantum computers. They may execute some calculations far more quickly than conventional computers, which could leave many encryption techniques open to intrusion.

PQC is still an emerging field, but growing in significance as quantum computing technology develops. Even if the attacker has access to many qubits, PQC algorithms are made to be impervious to attacks from quantum computers.

Conclusion

NIST Encryption Standards are essential for assuring the safety of sensitive data in various applications. They offer a collection of recommendations and standards for encryption and cryptographic methods that assist enterprises in safeguarding their data against unwanted access and possible cyberattacks.

Following the standards and recommendations set forth by NIST is crucial to maintain robust security measures, given the constantly shifting nature of cybersecurity threats. Organizations may significantly lower the risk of data breaches and ensure their sensitive data's security, integrity, and availability by adhering to these guidelines.

FAQs

1. **What is NIST Special Publication (SP) 800-131A Revision 2?**

Special Publication (SP) 800-131A of the NIST Version 2 is a set of recommendations for using cryptography in applications that must adhere to FIPS 140-2 of the Federal Information Processing Standards. The document lists accepted cryptographic algorithms and protocols appropriate for usage in governmental organizations and other businesses that must adhere to FIPS 140-2.

2. **Why are there so many different types of encryptions?**

There are numerous encryption standards since there is no one-size-fits-all encryption solution because various applications and systems have varied security needs. However, as technology develops, new dangers and weaknesses are found, necessitating the development of new encryption standards to solve these problems.

3. **Which is the most widely used encryption standard?**

The Advanced Encryption Standard (AES) is the most popular and widely used encryption standard. It is a type of symmetric key encryption that encrypts and decrypts data using the block cipher algorithm.

About the Author

Amar Basic is a dynamic and accomplished cyber security entrepreneur. He has been selected to represent the UAE in ISO SC 27 working group which is responsible for drafting and publishing many information security standards such as ISO 27001. As Co-Founder of CyberArrow, Amar has been instrumental in helping global organizations automate compliance and cybersecurity awareness.

Amar's in-depth understanding of cyber security risks and mitigation techniques has earned him a reputation as a sought-after speaker and thought leader in the cyber security community.

In addition to his entrepreneurial pursuits, Amar is a strong advocate for cyber security awareness and education. He believes that building a safer digital world begins with educating people about cyber threats and best practices for protecting sensitive data.

Amar Basic can be reached online at LinkedIn https://www.linkedin.com/in/cyberamar/, and at CyberArrow's website https://www.cyberarrow.io/.

Hacks And Data Leaks

How to protect businesses from cyberattacks

By Sergey Ozhegov, CEO, SearchInform

Hacks and data leaks: how to protect businesses from cyberattacks

Hardly a week goes by without a hack or data breach incident occurrence. Quite often, large organizations, such as banks, state bodies and corporations become attacked, despite the fact that they are well-sponsored and their employees are usually quite well informed in the information security related issues. Thus, even large enterprises are often incapable of protection against cyber threats. So, the questions arises – what should executives of SMEs, which information security budget is much smaller do? The SearchInform CEO shares advice on how to strengthen an organization's information security protection.

SMEs are in the focus

Owners of small businesses quite often don't take cyber security issues seriously, because they believe that intruders aren't interested in their companies due to their small size. Such approach leads to serious consequences, as it turns small businesses into perfect and vulnerable target.

One of the core risk is critical data leak. Such data includes, but isn't limited to:

- Client database
- Critical data on some business processes
- Commercial data on business deals etc.

Businesses should also take data privacy laws seriously. There is a global trend of adoption of various acts, aimed at regulation of data-related processes. The new regulations, coming into force worldwide motivate companies to implement specific protective software. The consequences of such norms ignorance become more and more serious. For instance, in case a company doesn't comply with a regulator's requirements, it has to pay fines, which, in turn, are also permanently increased.

The main problem is that implementation of information security measures requires significant financial expenditures and takes time. Nevertheless, law requirements and data leak risks must not be ignored anyway. That is why it is strictly important to address risks properly and deal at least with main vulnerabilities and security "holes".

First of all, let's identify where to expect threats to occur.

Who poses a threat to your organization's security?

There are four categories of intruders, which pose threats for information security.

External accidental intruders

These are intruders who hack any poorly secured IT infrastructure. With the help of automatized vulnerabilities scanners, they reveal unpatched vulnerabilities, open ports and weak passwords. Typically, small and mid-size businesses face such problems, because they often don't have a staff information security officer and system administrators usually deal with information security tasks.

External deliberate intruders

Cybercriminals who refer to this group choose their victim deliberately. They usually attack companies because they know, that the companies have some valuable assets or simply because somebody paid them for the hack. For instance, market competitors can perform a DDoS-attack to disrupt "Black Friday" sale.

Internal malicious insiders

Malicious insiders typically pose more threats to businesses than hackers do. Due the fact, that such intruders initially have access to the IT-infrastructure they have more options for committing fraud, data leaks and other destructive actions.

Internal accidental violators

Despite mentioned above, employees much more often become accidental violators: they are typically tricked by phishing methods, accidentally send confidential data to the wrong recipient etc.

Which tools do intruders use most often?

Below is the list of most popular tools, used by intruders to attack organizations.

Password cracking

Most users use not complicated passwords, which are cracked in minutes, sometimes in seconds. That is why in most cases intruders do not use advanced tools for password cracking. Instead, they simply brute force passwords.

A vivid example – the case of insurance company TransUnion South Africa. The intruders hacked company's server, access to which was protected with the following password - "password". Intruders demanded a ransom equal to $ 15 million to provide employees with the access to the encrypted server.

Phishing

When a phishing attack is conducted, fraudsters use seemingly legible, but factually fake email or website. Any SMS, link or attachment in the mail, which at first glance looks like a normal one, in fact may be a malicious one and may infect a computer with spyware or ransomware.

BEC-attacks

BEC-attacks (Business email compromise) is the corporate email compromise. Intruders hack counterparties' or company employees' mailboxes, examine correspondence, imitate the continuation of the conversation for their own purposes. Sometimes, thread in an email may contain only two-three letters, sometimes correspondence lasts for months. Attackers' aim is to induce employees to conduct a payment to a fake account, gain access to infrastructure or confidential information.

The most important aspect of a successful attack is social engineering. Employee's attentiveness can protect a company from such type of attack.

DDoS-attacks

Hackers overload company's server with requests until it starts to lag or simply fails. This issue is often critical, because business processes are interrupted. DDos-attacks specific issue is that they are usually used as a tool for performing deliberate malicious actions. Sometimes DDoS may hide the start of an attack, which aim is to find out, which vulnerabilities does the organization's IT-infrastructure have. This endangers companies, operating in all business spheres.

Malicious software

Malicious software stands for any programs, deployed on devices with the intent to harm users or gain unauthorized access. The list includes: viruses, worms, trojans, ransomware, and various spyware.

One of the most significant threats for small and middle size enterprises is encryption of company's data by a ransomware virus. After data is encrypted, intruders demand a ransom. Business processes of the attacked companies may remain interrupted or totally stopped for weeks, and the ransom sum may be large, up to millions of dollars. In case the victim refuses to pay the ransom (and, in fact, even in case the ransom is paid), there is a chance that data will be compromised and exposed.

Attacks on unpatched software

Such attacks logic is as follows: the vendor publishes detailed data on the vulnerability and releases an update, a client forgets to install the newest version of software or operation system and hackers benefit from this user's delay. They have the precise data on the vulnerability and the attack costs nothing to them.

How to protect a company against internal and external threats

Sooner or later your business may turn into intruders' target, it's just a matter of time. First of all, intruders attack those organizations, which are not protected properly. That is why it is crucial to ponder, whether company's infrastructure is protected well enough and if there are no deliberate malicious insiders among employees.

Below you can find the least of minimal required technical measures for ensuring organization's protection against internal and external threats:

- Do not neglect usage of antivirus protection and use licensed software, update it regularly
- Distinguish access rights to confidential data (at least in Active Directory)
- Set the two-factor authentication to access services, critical for company's business processes
- Use corporate email instead of free public one
- Perform monitoring of phishing activities cases, when your brand is impersonated

- Back up your data
- Use only encrypted data transmission channels
- Use tools for monitoring employees' activities (DLP-systems) to mitigate insider-related risks.

What else can be done

A company doesn't always have an onboard information security specialist; what's more, it's often too expensive for companies to purchase software licenses. That's why I would recommend to consider information security outsourcing.

However, you can implement numerous protective measures absolutely free of charge. Set the regulations for interaction with critical data, for instance, specify, which employees should have access to specific documents, where exactly the documents should be kept etc. Implement the trade secret mode – this helps to enhance discipline, because not all the employees understand, that corporate data is an asset, and its misuse is a kind of crime, equal to an ordinary theft of company's equipment from a warehouse.

Training employees in the sphere of information security helps to mitigate the number of accidental mistakes and incidents. It's crucial to acknowledge staff about phishing attacks and internet safety rules; provide employees with regulations on how to work with sensitive data; implement the safe passwords policy; explain, why it is so important to log out the system when leaving workplace.

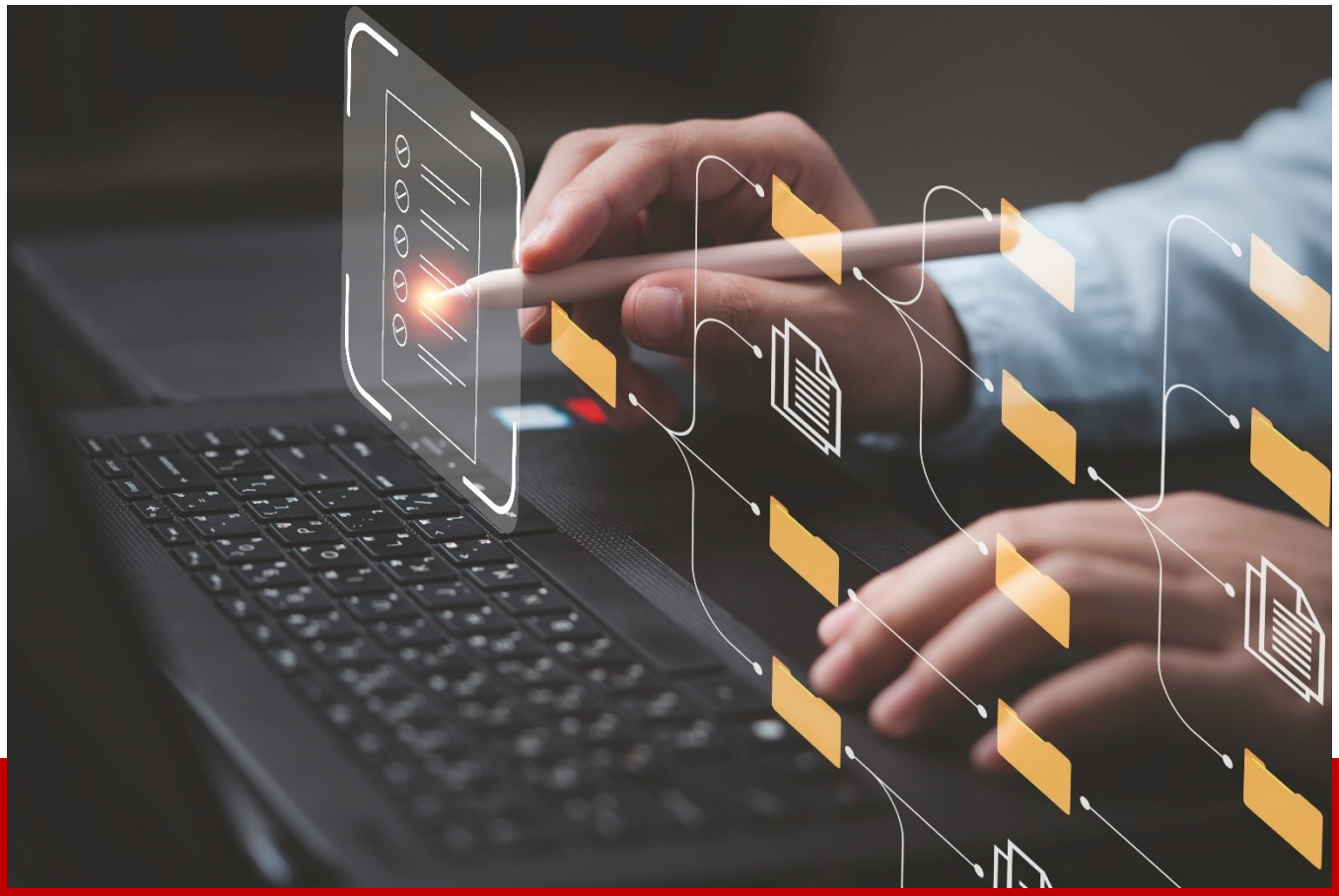
Complex implementation of even minimally required measures significantly enhances company's protection.

About the Author

Sergey Ozhegov, CEO of SearchInform. Sergey is the Chief Executive Officer at SearchInform, which is the global risk management tools developer.

For over a decade Sergey has been contributing to the company's success, handling business processes and strategic decision making. Sergey is a co-founder of annual SearchInform Road Show.

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



How Sandboxes Protect Organizations from Malware — Known and Unknown

From Detecting Threats to Collecting Rich Signature Data — Sandboxes Help Malware Researchers Keep Defense Systems in Sync with An Evolving Threat Landscape.

By Jack Zalesskiy, Technology Writer, ANY.RUN

Over 270,000 new malware variants were detected in the first half of 2022 alone — up 45 percent from the same period last year. These previously unidentified strains — known as zero-day or zero hour malware — are among the most unpredictable curveballs adversaries can hurl at our security systems. Under the right circumstances, they can even become completely unstoppable.

That's because of how firewalls, endpoint protection platforms (EPP), and intrusion detection and prevention systems (IDPS) — the tools we use to automatically ward off cyberthreats — separate what they discern as malicious from benign.

These systems are predominantly signature based. Although there are advances to incorporate AI and behavioral-based detection into antivirus software, the technology isn't completely reliable yet. Consequently, these systems rely on examining files for known hashes, static patterns, or behavioral patterns and comparing them to established signatures in threat databases.

But what if a signature hasn't been added to a database yet? That's when malware has a chance to pierce the defenses.

Incidents involving new or modified malware exploiting zero-day vulnerabilities are among the most notorious: Sony pictures breach in 2014, attack on RSA in 2011, Operation Aurora which put 20 high-profile organizations in the line of fire. More recent incidents include an attack on General Bytes and a phishing campaign involving Magniber, a ransomware aimed at Windows users.

This situation creates a paradigm where the defense team's success hinges on identifying new signatures before a potential infection occurs. In part, this is what fuels the ongoing arms race between adversaries and security specialists — and the surge in new malware variants we saw last year.

Sandbox in a security system

If you imagine endpoint detection systems as alarms that notify you about break-ins, a sandbox is like a lie detector, crime lab, and forensic artist all fused into one. It gives researchers a faster way to analyze malware, collect Indicators of Compromise (IOCs), and add them to various end-point detection products that make up an organization's protective barrier.

At its core, a sandbox is a specially configured monitoring environment designed to emulate a real operating system. Researchers use it to detonate and observe malware without jeopardizing the host machine. Sandboxes employ a combination of AI, ML, heuristic-based, and behavior-based detection, along with manual fine-tuning and proprietary techniques unique to each vendor, to effectively identify threats where signature-based detection falls short.

There's been an explosion of sandboxes in recent years, as we wrestle with increasingly sophisticated malware. They vary from virtualized environments and cloud services to on-premises server racks that mimic end-users' hardware configs.

If you imagine that firewalls are at the very edge of the defensive network, while tools like data loss prevention systems sit close to the organization's core, sandboxes fit somewhere in the middle.

They come into play when researchers encounter suspicious objects and need to examine them to extract malware configurations. Sandboxes can also assist with malware detection and incident response, but their application in these areas is more situational.

After processing a sample — usually a suspicious file or link — the sandbox assigns its verdict (malicious or not) and displays rich analysis data: strings, like C2 addresses and file hashes. Then it's up to the analyst to decide whether to dig deeper manually or use the signatures obtained from the analysis output to configure end-point detection programs.

Sandboxing still requires the supervision of a trained security researcher, but it can significantly reduce the time required to obtain results. It can even enable junior, mid-level, or broader-scope security specialists to complete a task that would otherwise need to involve a senior malware researcher.

It is through this continuous cycle of analyzing new threats, extracting signatures, and strengthening endpoint detection that an organization's security perimeter becomes hardened against emerging threats.

Sandboxing Limitations

While sandboxes are incredibly helpful in accelerating malware analysis, they are not infallible. To surveil processes for signs of malicious activity, sandboxes deploy monitoring hooks, which leave artifacts that can clue the malware into the fact that it's being observed. Nowadays, when most malware detects that it's running within a sandbox, it either halts the execution or performs a benign action instead.

Other anti-evasion techniques involve scanning the execution environment for files containing names of known sandbox vendors, setting an execution timeout, or waiting for user input before the malware triggers.

Some sandboxes counteract anti-evasion techniques by mimicking user actions (like moving a cursor and clicking on documents), using non-intrusive monitoring techniques, while others give control over the execution flow back to the researcher.

In most sandboxes, the workflow is such that you configure the VM environment, hit the run button and wait for results. If the malware detects the sandbox in the middle of the simulation, it can try to erase itself from the disk, terminate execution, or hide malicious actions, and there's nothing you can do to prevent that.

In an interactive sandbox, however, researchers can control the simulation by performing actions that would typically trigger the malware. From the user's perspective, the simulation process resembles using a standard virtual machine. However, behind the scenes, the sandbox continues to gather behavioral artifacts. Right now, this is the closest one can get to running the simulation on a physical system that's been set up for malware analysis, without actually going through the hassle of setting one up.

An essential part of a security system

As the threat landscape evolves, sandboxes like ANY.RUN have become crucial in the arsenal of cybersecurity professionals. They provide a safe environment for analyzing malware, extracting valuable intelligence, and informing the configuration of defensive systems. By staying ahead of emerging threats, organizations can strengthen their security posture and mitigate the risk of potential breaches.

However, sandboxes are just one component of a robust cybersecurity strategy. They should be part of a comprehensive approach that includes firewalls, intrusion detection and prevention systems, data loss prevention, access control systems, and ongoing security training for employees.

By combining these elements, organizations can create a multi-layered defense that protects against both known and unknown threats. This ensures a secure and resilient network in the face of an ever-changing online environment.

About the Author

Jack Zalesskiy is a technology writer at ANY.RUN with five years of experience under his belt. He closely follows malware incidents, data breaches, and the way in which cyber threats manifest in our day-to-day lives.

Jack can be reached online at support@any.run and at our company website ANY.RUN - Interactive Online Malware Sandbox.

How Should CMMC Impact Your Remote Work Policies?

By Zac Amos, Features Editor, ReHack

Cybersecurity Maturity Model Certification (CMMC) is another compliance framework defense industrial base (DIB) contractors can add to their toolkits to work for the Department of Defense (DoD).

Government contractors must look to the newest version of this framework to stay on top of security as new working habits and conditions expand outside of traditionally secure purviews. How will CMMC address the mobile working revolution for safety, especially for high-profile government jobs?

What Is CMMC, and How Do Contractors Achieve Compliance?

CMMC, previously known as the Defense Federal Acquisition Regulation Supplement (DFARS), is a comprehensive cybersecurity framework to ensure defense contractors' skills, knowledge and trustworthiness. Companies and individuals bidding for government contracts must adhere to stay relevant in a highly competitive cyber landscape. Many people wonder if it leaves room for contractors to be remote — it does, but with extra stipulations.

Third-party assessors and self-evaluations analyze intimacy with government protocols and cybersecurity know-how. How can these entities protect government data, like controlled unclassified

information (CUI) or federal contact info (FCI)? Do they know how to work with high-stakes, priceless data if a threat actor breaches defenses?

Achieving compliance requires navigating the three levels of qualification, undergoing interim assessments and third-party audits, and drafting a plan of action and milestones. There's plenty to unpack before getting the seal of approval, but it ensures contractors earn trust and prove their commitment to digital protections.

How Does CMMC Impact Remote Work?

Previously, government contractors were in controlled environments with company-sponsored cybersecurity infrastructure. The rise of remote work expands an attack surface area beyond comprehension, so CMMC made guidelines for adapting to these lifestyles by looking at cloud computing and quality assurance while on the go. However, many remote work compliances circle the various facets of remote access.

Contractors must practice monitoring remote access points and connectivity. Remote access is a streamlined way to reach protected machines in safe venues, but the connection should be encrypted and secure to be foolproof. Networks permitting access must install additional verification measures like intrusion detection and cryptography and keep detailed reports to prove to auditors their permissions are minimal and recorded. It will help prevent cyberattacks primed for remote environments.

Apart from reigning in remote access, companies must also evaluate permissions. What can administrators do, and can they control more or less with remote sessions? Could they perform these tasks — maintenance or operational — on and off the network, or is connectivity required?

The varying work-from-home measures are specific to designated CMMC levels, so not all precautions are required if contractors don't plan to advance to Level 3. These are all the specific controls to access CUI that remote contractors should pay special attention to, among others:

- 3.1.12
- 3.1.13
- 3.1.14
- 3.10.6
- 3.13.7
- 3.5.3

For example, not all levels require two-factor authentication, but only 57% of organizations used these authentication tools in 2019. Their effectiveness is sound, so why not incorporate it into remote work procedures?

How Can Companies Make Remote Policies Compliant?

One of the best ways to achieve compliance is by incorporating secure tools. These are a powerful start in outfitting remote contractors:

- Multifactor authentication (MFA) software
- Hardware-based virtual private networks (VPNs)
- Tokenization
- External device connection indicators, like for microphones

More advanced operations could further restrict access by collecting data on contractor activity. Companies can set alerts for when irregular access locations occur or contractors log in at erratic hours. It can also monitor if non-company-approved devices seek access.

Contractors can also reference NIST 800-171 to bolster remote compliance. It's the backbone of CMMC, and every cybersecurity framework, local or remote, can benefit from reviewing what it offers.

Another less formal way of ensuring workers achieve CMMC compliance for remote desks is to assert professional conduct. Working from home has its perks, like more lax dress codes, but the change in mindset shouldn't detract from attentiveness and security. Companies hiring contractors can set clear expectations with them on how to maintain productivity and awareness despite working in less-than-traditional settings.

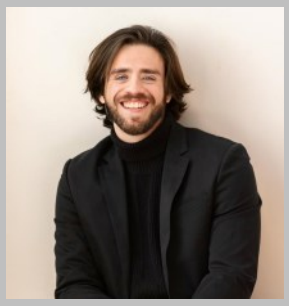
Stretching Compliance Beyond Office Doors

CMMC is preparing contractors for the next phase of the remote work revolution. The space for threat actors to nudge into sensitive areas increased to potentially every geographic point on the planet. Compliances are the touchstones for solidifying a safe digital workplace.

The resources to forge safe spaces for government data are here, and protective digital tools and assets improve daily. The revision of CMMC shows it is willing to adapt to new work environments and global change, so contractors should stay on top of updates at all costs.

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.



How Professional Human Hackers Choose Their Targets

By Peter Warmka, Founder, Counterintelligence Institute

Over the past few years, Cybersecurity professionals have acknowledged the increasing need of security awareness training to combat the growing threat from social engineering. However, while such training today focuses on what an attack may look like as well as how the target should respond, seldom is it discussed *how* and *why* particular individuals are selected as targets by professional human hackers. Understanding this methodology will better prepare potential targets from falling victim to more advanced social engineering techniques.

Target Selection

In my previous career with the CIA, and in response to intelligence requirements, I would carefully select my targets based upon their perceived ability to help facilitate the breach of their organization. In many cases, the starting point was acquiring an organizational chart and then speculating on their access based upon their title and position on the chart.

Today's threat actors, whether intelligence services, industrial competitors, activist groups or organized criminal rings, undertake this same objective while using the best available tools. Their number one resource for the identification of potential targets is the LinkedIn platform. Specific searches of individuals can be conducted by organization, title, geographic location, academic degrees, professional certifications, etc. While general searches may yield thousands of profiles, refined search parameters will identify a manageable pool of attractive candidates.

Target Assessment

As a CIA recruiter, I would have to develop a suitable pretext for contacting a potential target of interest and then spend several hours over multiple lunches or other social engagements to get to know them. This information would help me "assess" whether they were truly viable targets. Did they have access to the intelligence we wanted and what made them tick as a person? What information could I leverage to manipulate them into becoming sources?

Today, professional human hackers do not need to personally expose themselves to obtain such information. Their principal resource for collecting such assessment information are the social media accounts established and maintained by potential targets. A multitude of information is provided within such accounts to include profile background, pictures, posts and interactions with others.

What do such profiles reveal? Let me share four popular platforms and what a hacker can glean regarding a prospective target.

From LinkedIn

- Academic and work experience
- Career aspirations
- Certifications and licenses
- Affiliations with associations
- Volunteer work
- Network of professional contacts

From Facebook

- Hobbies
- Interests
- Favorite sports teams
- Music genre and favorite artists
- Favorite foods and restaurants
- Travel (where, with whom, and future travel plans)
- Social economic status (revealed from pictures)
- Close friends and family members

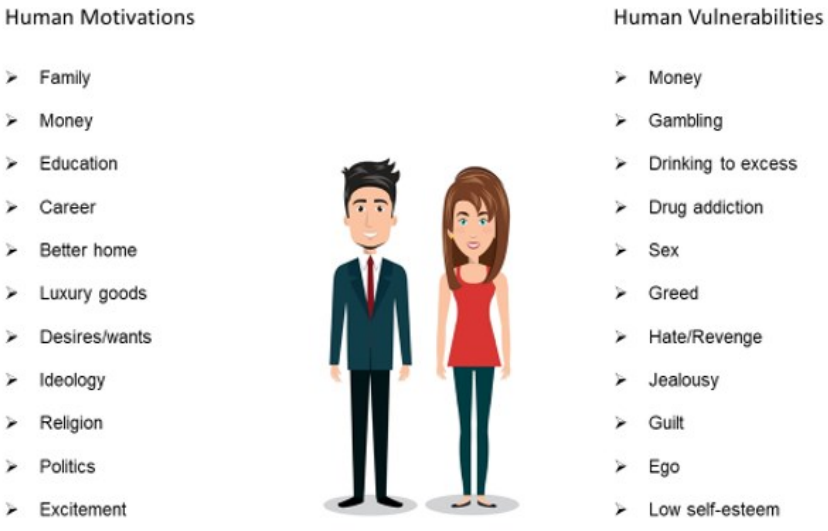
From Twitter

- Insight into what the target thinks.
- Opinions
- Religion
- Pet peeves

From Instagram

- Pattern of life activity
- Target's routine
- Where can a human hacker casually bump into the target.

With this assessment information, a professional human hacker develops a personality assessment profile on a target, identifying specific motivations and vulnerabilities.



These motivations and vulnerabilities are then used as a guide to develop specific social engineering ploys, whether they be spear-phishing, smishing, vishing or face-to-face encounters.

Let me give you two examples of how this methodology works.

1. An intelligence service is interested in securing proprietary information from U.S. defense contractor, Patriot Technologies. When evaluating prospective insiders at Patriot, they identify CEO Brandon Phillips as a very attractive target. In addition to access to sensitive information on his media devices as well as to the IT network, he has a very revealing social media profile. Of particular interest are his regular posts on Facebook where he uploads photos showing sunrises and sunsets with family and friends aboard his sailboat. He has mentioned several times that one of his life's dreams would be sailing the Mediterranean.

With his strong motivation identified, the intelligence service decides to send an email appearing to come from Brandon's local nautical club. It announces an upcoming excursion to the Mediterranean on a first come, first serve, basis. More information and registration information are said to be contained in the attachments. Even though everyone at Patriot Technologies, including the CEO, has had basic phishing training, Brandon never imagines that this email was a phishing attempt. It played to his strong motivation and utilized the influence technique of "scarcity" manipulating him to immediately open the attachments before losing the perceived opportunity. As a result, malware is uploaded into his personal laptop which in turn is also used to gain access to the firm's network. Success!!

2. A criminal group wishes to penetrate financial service provider, Maxwell Wealth Group, to gain access to sensitive information regarding the firm's high net worth clientele. While identifying over 15 potential insider candidates, the group took special interest in Christine Summers whose updated LinkedIn profile revealed that she recently joined Maxwell as a new receptionist. Professional human hackers find new receptionists as attractive targets as they are frequently isolated from the rest of the workforce and sometimes must make unilateral decisions. Furthermore, it takes time for them to become familiar with all the firm's policies and procedures.

Christine receives an incoming *vishing* call from "Doug" posing as Maxwell's outsourced IT management provider. Doug welcomes Christine to the firm and wants to let her know that if she ever has an IT issue, she should immediately telephone him. In passing, Doug mentions that he reviewed her IT account profile prior to making the call and had noticed several files which were corrupted and not working properly. While not urgent, he stated that it could eventually lead to a crash of her hard drive. Leveraging fear, Christine begins to panic and asks Doug for help. Doug sends to her an email with a link for her to approve his taking over of her account to ostensibly conduct the repair.

While Doug is creating a backdoor into the network for his team to enter later, he keeps Christine on the line and distracted by talking about one of her passions as revealed from her Facebook profile – animal rescues. After 15 minutes, Doug confirms that he is all finished. Christine is so grateful that Doug has saved her from a potential crash of her system not realizing that she has just facilitated what will become a $5 million data breach of Maxwell.

Understanding how professional human hackers select and assess their targets, individuals should have a better appreciation regarding the sensitivity of personal information that they may post to their social media accounts as well as the need for greater privacy settings. Cognizant that human hackers can leverage such information, unsolicited incoming communication incorporating an individual's motivation or vulnerability should be treated with judiciousness.

About the Author

Peter Warmka is a former Senior Intelligence Officer with the CIA having over 20 years of experience in breaching the security of target organizations overseas. He is the Founder of Orlando, Florida based firm Counterintelligence Institute, LLC and author of the non-fiction book "Confessions of a CIA Spy - The Art of Human Hacking."

In addition to conducting his signature training program, Mr. Warmka is a frequent conference speaker, guest podcaster, and author of numerous publications on social engineering and the manipulation of insiders.

He received a bachelor's degree in liberal arts from the University of Wisconsin-Milwaukee and a master's degree in international business management from Thunderbird School of Global Management. Mr. Warmka is a Certified Fraud Examiner (CFE), a Certified Protection Professional (CPP) and Certified Instructor at CIA University (CIAU).

Peter can be reached online at pgwarmka@counterintelligence-institute.com, https://www.linkedin.com/in/peterwarmka; and at our company website http://www.counterintelligence-institute.com/.

Oh, Great and Powerful Cloud, I Wish to Be Free of The Burdens of Infrastructure!

By Craig Burland, CISO, Inversion6

The Cloud's booming voice, stunning light show and smoke fill the room. "Faster! More agile! Cheaper! Business aligned! Strategic! I have the answer to all your technology problems. Imagine everything that could be accomplished if no one spent time taking care of infrastructure!"

From the start of the cloud conversation, it should have been clear that there was something hiding behind the curtain. Like the Great and Powerful Oz, the Cloud has a secret: it isn't really magic.

Disappointing, but not surprising.

Regardless of the ratio of ingredients [Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS)] in your cloud cocktail – say, ½ SaaS, ¼ IaaS, ¼ PaaS – divesting yourself of infrastructure isn't a panacea. It doesn't make obsolete applications disappear, instantly fix poor hygiene practices or absolve you of security or compliance governance. It doesn't suddenly make users cyber-smart. And it's not cheaper without a thorough understanding of and diligent focus on usage. The cloud is quite literally just someone else's data center.

Smart organizations recognize this reality and come into the conversation with their eyes wide open, understanding that moving to the cloud is a trade, not a boon. Smart cybersecurity leaders should leap at the opportunity of using the cloud as a green field. They should insist on principles like "secure from the start" and "proactive, data-driven governance" to build solutions that are more scalable, flexible, secure and cost-effective than those they replaced.

Focusing specifically on the challenges of a cloud infrastructure transformation, the obvious thread is a lack of governance with a sub-plot of cybersecurity woven in. Interestingly, these challenges aren't new –they're equally present in on-premise architectures. They just present themselves differently when planning a pivot to the cloud. Let's take these challenges one at a time.

Application obsolescence is a failure of lifecycle management. On-premise, obsolete applications create a chain of technologies unable to upgrade, support teams unable to evolve standards and a steep escalation of risk. The cloud doesn't solve these problems, but it does force the lifecycle conversation to the front. Obsolete applications can't be moved to the cloud. If the business wants enhanced performance and agility, they need to upgrade. If the business wants to avoid being on the wrong side of the IT strategy, they need to upgrade. Cyber leaders should double-down on any one-time changes to establish a principle about remaining on supported solution components, to avoid making the same mistake again.

Poor technology hygiene comes down to ignorance of the risk presented by vulnerabilities and misguided prioritization. Poor hygiene is not an "on-prem problem"– it's a people and process problem. Hosting infrastructure in the cloud doesn't automatically address vulnerability and patch management. Hygiene can be ignored in cloud workloads just as easily as on-prem. The cloud does offer automation and visibility that can be lacking in on-prem environments, but it takes the other elements to execute. Processes like scheduling maintenance windows, validating applications following patches and communicating to customers still need to be resourced. Cloud transformation effort opens a window where cyber leaders can build in an effective vulnerability and patch management process with fewer legacy roadblocks.

Security and compliance remain the most misunderstood aspect of the cloud. Cloud service providers (CSPs) operate under what is called the "shared responsibility model." In simple terms, they protect what they bring to the table – data center, hardware, core network. The organization must protect everything else. The data, access, virtual servers, applications, identities, all of it. These are the responsibility of the customer. CSPs provide the tools to help with security, but they don't enable, configure or maintain them. Making matters worse, most security platforms implemented on-prem typically can't be extended to the cloud. Security teams must learn new tools and develop new processes to protect the cloud. Almost daily, there are reports of cloud compromises as hackers target poorly managed SaaS platforms or exploit unprotected storage buckets. As for the data lost in these incidents, addressing compliance violations falls to the organization as well.

The last area of cloud governance is cost. While not typically part of cybersecurity, controlling operating costs is part of every leader's role. On-premise, finite amounts of licenses, hardware and rack space limit the pace of expansion and control cost. The cloud removes that governor, letting the business run full throttle. Without strong financial controls and precise cost allocation models, new workloads will sprout like dandelions. Left untended, these assets will cause a serious budget disruption. Articles going back to 2021 discuss the likelihood that organizations will overspend their cloud budgets unless there is upfront

planning to build a disciplined process. Recent studies confirm this prediction is coming true. If arguments about lifecycle, hygiene and security aren't convincing, arguing for greater plans and governance to ensure savings may yet win the day.

To large degree, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), bring the same promise, but hide the same concerns. Obsolescence and hygiene aren't issues for SaaS, but security and compliance certainly do. SaaS administrators, tasked with rapidly enabling the business, rarely understand cybersecurity or receive adequate security training before taking responsibility for an internet-facing application. PaaS platforms partially mitigate risks of obsolescence and hygiene by wrapping the lower tiers of an application into a service but do nothing to manage the health of the custom code itself. An unpatched, unmonitored Ruby on Rails installation running on overprovisioned workloads, could easily bring the house down upon you.

Like Dorothy, Lion, Scarecrow and Tin Man learned (the hard way), you can't wish your way to a better world. It takes a strong will, uncommon courage, pragmatic intelligence to successfully walk the road, learning lessons along the way. Migrating to the cloud holds tremendous promise - speed, agility, strategic enablement - but only if you take the time to understand the trade-offs and take full advantage of the opportunity.

About the Author

Craig Burland is the 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 Globhttp://www.inversion6.comal Security, and Oracle Web Center. Craig can be reached online at LinkedIn and at our company website http://www.inversion6.com.

Operationalizing Zero Trust Architecture

By Chaim Mazal, Chief Security Officer, Gigamon

Over the last few years, organizations have been hearing about a Zero Trust architecture (ZTA) as a means for IT leaders to take a more proactive approach to security. Yet various ZTA documentation, guidance and roadmaps are not one-size-fits-all. Each organization's mission, environment, staffing and unique needs vary. This is why organizations should not only think about the ZTA guidance from a compliance perspective, but also from an operational perspective.

And this couldn't come at a more critical time; 95% of organizations reported experiencing a ransomware attack in 2022.

So, how does an IT leader effectively implement and operationalize ZTA within their organization? Start by laying a solid foundation that will enable the three core building blocks: adaptability, data normalization, and visibility.

- **Adaptability** – IT environments will adapt and change as business, mission, and environmental requirements evolve. Organizations need to have constant and consistent end-to-end visibility into the environment as computing evolves and shifts between on-premises physical and virtual compute resources and multiple cloud service providers. The dynamic nature of software-defined networks (SDN) also requires that the visibility fabric be easily adaptable.

- **Data normalization** – Data normalization is a core component of building robust, accurate, and broad-based analytics across various data sources for on-premises networks, containers, and multiple cloud providers. This is an important step because artificial intelligence/machine learning-based (AI/ML) detection is only as good as the data used to train the classifiers. It is crucial to standardize and normalize data sources (such as logs) across all components of the environment so AI/ML-based detection engines can be used to help drive policy-based decisions on user and system behaviors. Wide variations of data and sources will make detection classifiers unreliable and inconsistent across an organization's environment.

- **Visibility** – End-to-end visibility is another core component of ZTA that should be consistent and unified across the enterprise. I believe there are five critical areas where visibility is necessary:

    - **Cloud** – Most organizations do or will leverage multiple cloud providers, and each may offer its own native, unique, and mutable log generation tools. Being able to standardize network and application visibility across networks on-premises and in the cloud will allow unified monitoring.
    - **Containers** – The rapid adoption and flexibility of containers create gaps in visibility for security teams and gaps in an organization's ZTA. The ability to monitor and extract communication from containers will help prevent them from being a haven for cyber threat actors in your environment.
    - **Hybrid** – Mixed on-premises and cloud compute environments make it challenging to gain single-pane visibility that is standardized across various and disparate environments. As organizations continue to migrate to hybrid and multi-cloud environments, leveraging the power of network-derived intelligence is more important than ever. In fact, research confirms that 75 percent of enterprises consider deep observability critical to mitigating threats quickly and effectively.
    - **Endpoints** – Visibility at the endpoint level offers a wealth of data and information. It is good to cross-reference other data sources to better identify advanced persistent threats, a good practice to get into, especially since data obtained from endpoints could be mutable if a device is compromised.
    - **IoT** – Endpoints that can't be covered by monitoring software, such as printers, IoT devices, appliances, and other operational technology (OT) devices, create blind spots unless a deep observability solution is in place.

It's not a matter of if an attack will occur, but when. Taking proactive steps to implement a ZTA by leveraging these three building blocks (adaptability, data normalization, and visibility) enables IT leaders to more effectively avoid common implementation challenges while finding a solution that works best

within their existing infrastructure. A bonus? The organization is able to fend off cyberattacks before it's too late.

About the Author

Chaim Mazal, the Chief Security Officer of Gigamon. He is responsible for global security, information technology, network operations, governance, risk, compliance, internal business systems, as well as the security of Gigamon product offerings. Prior to joining Gigamon he held similar roles with several industry leaders, most recently at Kandi, where he was the SVP of Technology and CISO. Chaim is a lifetime member of the Open Web Application Security Project (OWASP) Foundation and currently sits on several advisory boards, including Cloudflare, Gitlab, and Lacework. Chaim holds a bachelor's degree from the Rabbinical College of America.

Chaim can be reached on linked in at linkedin.com/in/cmazal and at our company website www.gigamon.com/.

Phishing Kit: New Frontier of Hacker Attacks within Everyone's Reach

By Lorenzo Asuni, CMO, Ermes Cyber Security

The Phishing phenomenon is growing exponentially, and unlike the most common forms of scam, it is much more dangerous, because it is more democratized and accessible. The latest quarterly report of the Anti-Phishing Working Group (APWG) reported that over 611,000 phishing attacks were detected in January-March 2021 alone, marking a record for the month of January which recorded around 245,711 attacks. But why? What is the anatomy of a Phishing Kit? Generally, it consists of a set of ready-to-deploy files that can easily be copied to a web server and used almost as is with little configuration. The composition of a typical phishing kit can be broken down into resources and documentation, primary files and scripts, basic/advanced features, and detection avoidance.

These off-the-shelf kits usually provide a complete package of manuals, documentation, and detailed instructions located in the root folder of the phishing kit, to help hackers effectively use the files to execute phishing attacks. The instructions are very clear and easy to understand: they will explain to a potential phisher how to set up a virtual private server (VPS) and obtain a transport layer security (TLS) certificate. There will also be an explanation on how to install the phishing kit, default login credentials, and

references to the creator of the kit. This new fraudulent system is therefore very dangerous, on one hand because it allows less experienced scammers to purchase a complex code from a cyber-criminal, while on the other because both parties receive the victim's data at the time of the attack. For many of these kits, in fact, the only thing that a bad actor needs to do is to configure the drop email address to an account controlled by the phisher.

The kits typically use PHP as the back-end programming language to ensure it will work consistently on most servers. The files also contain all the CSS, HTML, JavaScript, and images necessary to create the phishing front-end web pages that will ultimately be presented to potential victims. These front-end pages typically impersonate the original login screens for targeted brands, banks, and other institutions. Phishing kits also provide scripts that automate the process for exfiltrating the sensitive data gathered. In the vast majority of cases, the data provided will simply be sent by email to a “drop address” or saved to some local text file.

Phishing kits have also become sophisticated enough to include anti-detection systems that can be configured to prevent detection by law enforcement agencies or independent researchers. They also include code that can be slightly or heavily obfuscated to avoid detection by automated anti-phishing solutions. They may even be configured to refuse connections from known bots belonging to security, anti-phishing companies, or search engines to avoid being indexed. Some kits may even use countermeasures that leverage geolocation. These kits also have the ability to encrypt data before exfiltration, or even send the collected data to a secondary location as a precaution or as a way for some phishers to secretly collect other phisher’s loot.

But there is good news in all of this: the Kit is actually a great source of data, as it provides information on the techniques that are used for phishing attacks and Phishing Kit analysis can therefore also lead to the identification of criminals. However, the kits are not recognizable by the user: for the more attentive ones it is possible to recognize the Phishing page itself, but to identify the kit hidden behind the page, special tools are needed.

The researchers’ analysis led by Ermes - Cybersecurity, the Italian Cybersecurity excellence, highlights how, in the evolution of writing Kits, it happens that attackers copy and paste parts of code from others Kits, adapting them to their own needs. Therefore, there are very few original kits, and this means that entire Clusters of correlated kits can be identified. Ermes analyzed a set of tens of thousands of phishing kits to identify around 6,000 kits targeting well-known brands. Ermes has significantly prioritized intelligence gathering and detection for phishing attacks, especially those making use of phishing kits. To combat phishing threats, Ermes has built a unique and proprietary dataset containing tens of thousands of phishing kits, which are continuously augmented by downloading phishing kits left by attackers on phishing sites that have been identified. Ermes routinely leverages this valuable resource to conduct research and map newly discovered phishing sites to a phishing kit family for the purpose of providing customers with critical insights and intelligence.

About the Author

Lorenzo Asuni graduated in Management at the University of Cagliari and at the Universidad Complutense de Madrid. He has over 10 years of experience in startup and scaleup filed as Marketing & Sales Director. In the past he launched AirHelp, YCombinator startup included among the top 100 global startups in 2016 Lunii, a French scaleup and led the growth of the Italian Enuan. He has an international experience between the USA and Europe, specialized in Growth Hacking and Digital Marketing. It has also recently launched two projects in the field of sport marketing and health-tech: respectively Teda and Healthy Virtuoso, a rapidly expanding reality in recent years.

In February 2022 he joined the Ermes team as Chief Marketing Officer leading the company's initiatives aimed at disseminating knowledge and awareness of its innovative security system and will promote the large-scale expansion of corporate marketing to respond to the direction of international growth recently undertaken by the company.

https://www.linkedin.com/in/lorenzo-asuni/?originalSubdomain=it

https://www.ermes.company/

Securing Communications for Operational Military Success

By Nicole Allen, Senior Marketing Executive at Salt Communications.

The significance in having Secure Communications for Military Operations.

Thanks to expertly planned operational communications, military duties can be carried out in a successful manner to avoid crisis situations.

To preserve the highest level of security for military communications a method of secure communication technology should be deployed. This should protect and facilitate communications for operational actions in response to crucial events while troops are on the ground and engaged in missions.

Why Secure Communications is important for Military teams.

The use of mobile devices for communication has become so widespread in modern society that it has even impacted the military and defence sectors. On these mobile devices soldiers regularly use consumer messaging systems to share and discuss sensitive events. Thanks to soldiers now being able to utilise mobile devices on the battlefield, combatants can now discuss and assess complex and dynamic situations in a way that was previously not feasible. Imagine two fire squads going toward an object in a

steep location in arrowhead formation when they are hit by effective enemy fire and are compelled to retire to hostile territory. In the case that the terrain limits line-of-sight contact between the two teams, mobile technology can ensure that they can analyse the situation collaboratively and react more effectively. But surely these conversations should be being had in a secure manner?

A secure communications system can ensure that the two teams can jointly assess the situation and take more effective action if the terrain prevents line-of-site contact between them, while reporting key information back to HQ for effective and secure decision making.

Communication is key

The capacity to communicate clearly on the battlefield has been crucial since the beginning of warfare. The ability of commanders to communicate instructions to soldiers in reaction to a shifting tactical environment has always been an essential component of military endeavour, from the trumpets and cornets of ancient Rome to the carrier pigeons and runners of World War I to modern software-defined radios. Military operations today depend on this continual information transfer between troops and base stations, including messages, calls and media sharing. There are greater risks in today's military operations with the advanced technology in place to intercept these communications.

Portable mobile devices for team communication within a squad or section have only recently been made available to troops. For the kinds of operations carried out by a dismounted infantry squad within the relatively confined geographic region, shouting and gestures were previously thought to be sufficient. The use of devices on the field soon demonstrated their advantages, particularly in enabling precise movement coordination when screened or behind cover. As expected, unfortunately, many of these operations and processes are being performed on insecure communications channels, like WhatsApp and Signal and even GSM channels.

High-performance secure communications technologies are a MUST for these conversations. According to estimates, the market for tactical communication would be valued at USD $147.8 billion by 2029. Over the next ten years, it is anticipated that demand for communications equipment with ever-sophisticated capabilities will continue to soar.

With over 75% of these engagements focusing on cyber security, military networks, and secure communications networks as a focal point and obvious strategic driver, military IT and C4ISR contracts are expected to be worth a total of USD 100 billion by this period.

Dependability when it matters

In order to ensure that crucial information can be exchanged when it counts most, military secure communications networks must be dependable and private under all circumstances, especially in deteriorated and denied network environments. Since satellite network bandwidths are frequently limited in conflict zones, communication integrity is threatened by high latency and tough operating features, soldiers must be able to function even in locations with poor connectivity infrastructure, and often in areas that rely on satellite networks.

When it comes to the official communications of the military and in the institutions of the defence sector, the safety and security of data are of utmost importance. Every military leader is in charge of making sure that their comrades are safe and secure.

The degree of security, encryption, and compartmentalisation of the connection closely correlates with the success rate of properly protecting sensitive and private information. Countries frequently have multiple national military networks as well as distinct networks for various tasks. To enable information sharing across different teams, an efficient communications system must be able to operate across these networks in an efficient and most importantly, secure manner.

The dependability, integrity, and compatibility of the underlying software is becoming more and more important as military operations call for ever-sophisticated secure communication capabilities. Implementing, maintaining, and managing conventional military message handling systems (MMHS) can be challenging and expensive. By using a system such as Salt Communications can quickly and simply implement a secure military messaging system to ensure your force has confidence in the security of your communications.

In a number of military and civilian scenarios, having that additional security can offer life-saving early warning of otherwise invisible threats, therefore the ability to share information in the moment is vital. Salt has been deployed in these environments across the globe leveraging low latency networks to share sensitive information to and from troops on the ground. Being able to generate structured and secure reports allows military organisations to access and act upon key events in seconds, with the security required for fast moving and time sensitive environments.

Secure your military communications today - sign up for a free trial of Salt Communications contact us on info@saltcommunications.com or visit our website at https://saltcommunications.com/military/.

About Salt Communications

Salt Communications is a multi-award-winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. Salt Communications offers 'Peace of Mind' for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. Salt Communications is headquartered in Belfast, N. Ireland, for more information visit Salt Communications.

References:

https://www.britannica.com/technology/military-communication

https://www.britannica.com/technology/military-communication/World-War-II-and-after

https://www.acs.psu.edu/drussell/Asterix/02-RomanBrass.html

https://blog.bliley.com/10-popular-software-defined-radios-sdr

https://blog.sciencemuseum.org.uk/exciting-tales-and-top-secret-work-of-pigeons-in-the-first-world-war/#:~:text=as%20messenger%20pigeons.-,In%20the%20First%20World%20War%2C%20carrier%20pigeons%20were%20used%20to,was%20about%20to%20take%20place.

https://www.mymobileworkers.com/blog/military-smartphones#:~:text=Mobile%20America&text=On%20a%20battlefield%2C%20it%20allows,paper%20maps%20and%20intelligence%20reports.

https://www.restore.co.uk/Digital/Insights/Blogs/why-is-data-so-important-to-the-defence-industry

https://thestrategybridge.org/the-bridge/2016/4/7/on-joint-leadership-the-importance-of-communication#:~:text=Leadership%20is%20demanding%2C%20and%20effective,in%20combat%20or%20on%20staff.

https://www.csis.org/analysis/battle-networks-and-future-force

https://www.linkedin.com/pulse/role-technology-war-professor-andy-pardoe/?trk=pulse-article_more-articles_related-content-card

https://www.militaryaerospace.com/computers/article/16710872/wearable-computers-help-make-individual-soldiers-part-of-the-digital-battlefield

https://www.army-technology.com/buyers-guide/army-command-and-control-systems/

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/.

Three Things Corporate Board Members Need to Know to Protect Their Companies from Cyberattacks

By Sami Mäkiniemelä, Chief Security Officer, Miradore

Last year, the U.S. saw a 57% increase in the number of cyberattacks — that's nearly double the 38% increase that was reported worldwide. This rising threat of cyberattacks comes at a time when many companies are cutting costs and reducing staff in response to economic uncertainty. While these cost savings may help a company in the short term, they could be opening the door to catastrophic, long-term consequences associated with data breaches and cyberattacks.

Recent data shows that each of these cyberattacks — whether it's a malware, ransomware, data breach, or DDoS attack — had a median cost of $18,000 in 2022. That's nearly double the amount from the year before, up from $10,000 in 2021. The study also showed that nearly half of all American businesses suffered a cyberattack in some way during the last year.

However, as the risks and costs of cyberattacks are growing, concern at the corporate level is not matching the threat. New research shows just 23% of corporate board directors think the risk of a cyberattack is very likely — even more alarming is that 47% believe their company is unprepared to handle a cyberattack if it did come. This could be a serious problem as the costs of these attacks continue to grow, posing a threat to the very businesses these boards are overseeing. That's why those in the C-suite positions and their board members need to be more proactive about protecting their businesses from this complex and costly threat.

This disconnect between the disinterest of corporate boards and the reality of the threat landscape is especially disconcerting considering the fiduciary and oversight responsibilities these bodies are entrusted with. Boards and their members have a duty to educate themselves about the risks and strategies for cyber resilience in order to take the proper precautions against these attacks.

Here are three essential things board members need to know about cybersecurity today to help protect their companies from future fiscal disaster.

Understanding the importance and impact of cybersecurity is the first and most important step in safeguarding your business.

Cybersecurity can seem very complicated to someone without deep IT or technological knowledge. However, your entire board doesn't have to understand everything about computer networks and how to protect them against potential attack. They just need to be committed from the top down to enhancing cybersecurity. If not, employees who see their board dismissing cybersecurity concerns are likely to do the same.

Also, cybersecurity considerations need to be part of a company's overall business strategy. When reviewing corporate financials, board members need to ensure that there's a robust budget to support regular maintenance and upgrades to company infrastructure that will defend against cyberattacks. Even with the current economic uncertainty and cost-cutting mandates, cybersecurity spending is expected to rise by more than 10% this year compared to 2022. This underscores the importance of this issue for organizations of all sizes.

Poorly managed cybersecurity can risk the entire business.

It's easy to ignore cybersecurity when nothing happens. But when things go wrong, fixing it after the fact can be problematic and very expensive. Cyberattacks can have significant consequences for a company, such as financial loss and reputational risk. IBM estimated the average cost of an American data breach in 2022 to be $9.44M. But there's also the reputational damages of lost public trust that are harder to measure and can have a significant negative impact on the business too.

Years after Facebook's Cambridge Analytica data breach, 44% of social media users still have a negative opinion of Facebook — 41% of millennials use Facebook less because of the data breach, compared to 37% of Generation Xers and 24% of baby boomers. According to a recent study, the average financial

losses for this particular type of damage are $8,653 for SMBs and $204,750 for larger companies when you combine consultancy expenses, lost opportunities due to damaged corporate image, and marketing and PR activities aimed at reducing the impact to reputation.

That's why it's cheaper and easier to make sure in advance that your business is fully protected against cyber-crimes before they even happen. With the increasing frequency of state-sponsored and other highly sophisticated cyberattacks, the threat of cybercrime is growing more serious. Fortunately, while cybercrimes are getting more sophisticated so is the technology that helps prevent them. Towards this end, there are a variety of available resources to help stay on top of cybersecurity trends and issues. Government agencies like CISA and the SBA provide essential guidance, while companies like Miradore offer MDM, and cyber intelligence firms like Google's Mandiant can help companies mitigate risks before, during, or after an attack.

It's helpful to think about cybersecurity like your home — it's easier to deter a burglar with cameras, an alarm system, and proper outdoor lighting than it is to recover stolen property after the break-in. By being proactive about cyberdefense before an attack, board members can save their companies money on the bottom line.

Management needs to be an active participant in the company's larger cybersecurity efforts.

Companies of all sizes should set up an information security management strategy and management committee. Members of the board of directors and senior management team should be on this committee to signal the importance of this issue to the company and its customers. Also, having a presence in that space means the board will be informed of and able to act on any potential cybersecurity incidents in a timely manner, ensuring a more efficient response.

Additionally, board members should push to establish metrics and reports to measure the business impact of cybersecurity. To quote American author and entrepreneur H. James Harrington, "Measurement is the first step that leads to control and eventually to improvement. If you can't measure something, you can't understand it." Boards should keep track of all cybersecurity incidents and how much money and time is spent fixing these, while also looking into how they can prevent similar incidents in the future. Measuring the impact of cyberattacks and progress towards preventing them is a critical step in managing a company's cyber risk profile.

As the cybersecurity landscape continues to evolve and expand, the threat of cyberattacks will continue to grow more pernicious. Members of a company's board of directors have an obligation to understand the basics about cyberattacks and how to prevent them in order to exercise their oversight responsibilities and protect their business from untold monetary and reputational losses.

While there is no one perfect solution or silver bullet for all cybersecurity issues, boards who are committed to this issue should experiment with the available resources until they find a combination of tools that works for them. The right mix of actions and intentions about cybersecurity from the board will ensure the company is in the best position to prevent cyberattacks and respond to any attacks that do come quickly and efficiently.

About the Author

Sami Mäkiniemelä is the Chief Security Officer at Miradore, a software company that offers MDM services. Sami can be reached online via LinkedIn. You can learn more about the cybersecurity benefits of mobile device management on Miradore's website.

An Interview with Sarah Armstrong-Smith

By Megan Lupton, Senior Content Executive, Champions Speakers

Sarah Armstrong-Smith is a globally revered voice in the cyberspace. She is regularly booked for corporate conference and as a Cyber Security Awareness Month speaker, where she uses the event to share the importance of data privacy. In this exciting interview, Sarah reflects on her career in cyber security and what she learned from working on the Millenium Bug.

Why did you embark on a career in cyber security?

“I've been working in the technology sector for over 20 years, and I chase this back to 1999 – all those many years ago! I was actually working for a water utility company on the Millennium Bug or Year 2000 programme, and many companies were on really large transformation programmes to recode a lot of their computers and servers.

“The theory was, at the stroke of midnight, a number of computers and servers would melt down, because of the way that the year ‘2000’ was actually coded into a number of different systems. And really, for me, from a young age, I've always been driven to keep asking ‘why’ and ask abundant questions: ‘what if the systems go down?’, ‘what if we can't get people to work?’, ‘what if what if’ - all these types of things.

“I didn't really understand at the time, but what I was looking at was business continuity. For me, it just felt like common sense to keep asking these ‘what if’ questions. I always look at that as the point where I started my career.”

What did you learn from your experience of working on the Millenium Bug?

“I think having a background in business continuity has really enabled me to think about the big picture, those worst-case scenarios – ‘what’s the worst thing that could happen?’. We need to think wider, we need to think about incidents that are not just relevant to our own company, but issues that go cross sector and even across the world. That scope and scale is really important, and some of these major events have also triggered global changes, as well.

“I would say 9/11 was a really good example of a major incident, at massive scale, that we probably never seen before, how that was televised and the shock that came with it. It really brought home the impact of terrorism, and again, how important business continuity is at that scale.

“When we're thinking about these threats, it's not just about business continuity but cyber security attacks as well. It's about thinking holistically, thinking much, much, much wider. It's about having resilience to all of these types of attacks and types of threats.”

What is the biggest cyber threat faced by UK businesses?

“We think about cyber criminals and they're inherently opportunistic, they absolutely love a crisis. We've seen a massive increase of phishing attacks, or really preying on people's fears and emotions. So, they pretend to be your bank, they might pretend to be just offering support. They might pretend to be a charity and those types of things. It's really trying to fool you into a false sense of security, to get you to give up credentials or click on links.

“We've also seen a massive increase with regards to ransomware, specifically targeting healthcare or other critical infrastructure. I think what's interesting is that almost no company is out of bounds, they're small, large enterprises, these frontline services.

“I think there's a real psychology behind the way that cyber criminals act and the way they take advantage of the situation. It’s important that we're mindful with regards to what's going on and how these changing tactics and techniques are going to continue to evolve.

“It really comes back to that, kind of, business continuity, which means constantly asking questions: ‘what if somebody could get access to our systems? What if somebody could disrupt our services? What if someone could get access to our data? If that data is leaked, what's the impact of that? And therefore,

where do I put my priorities?' We're no longer just talking about cyber security; we must think again and have more of a holistic response."

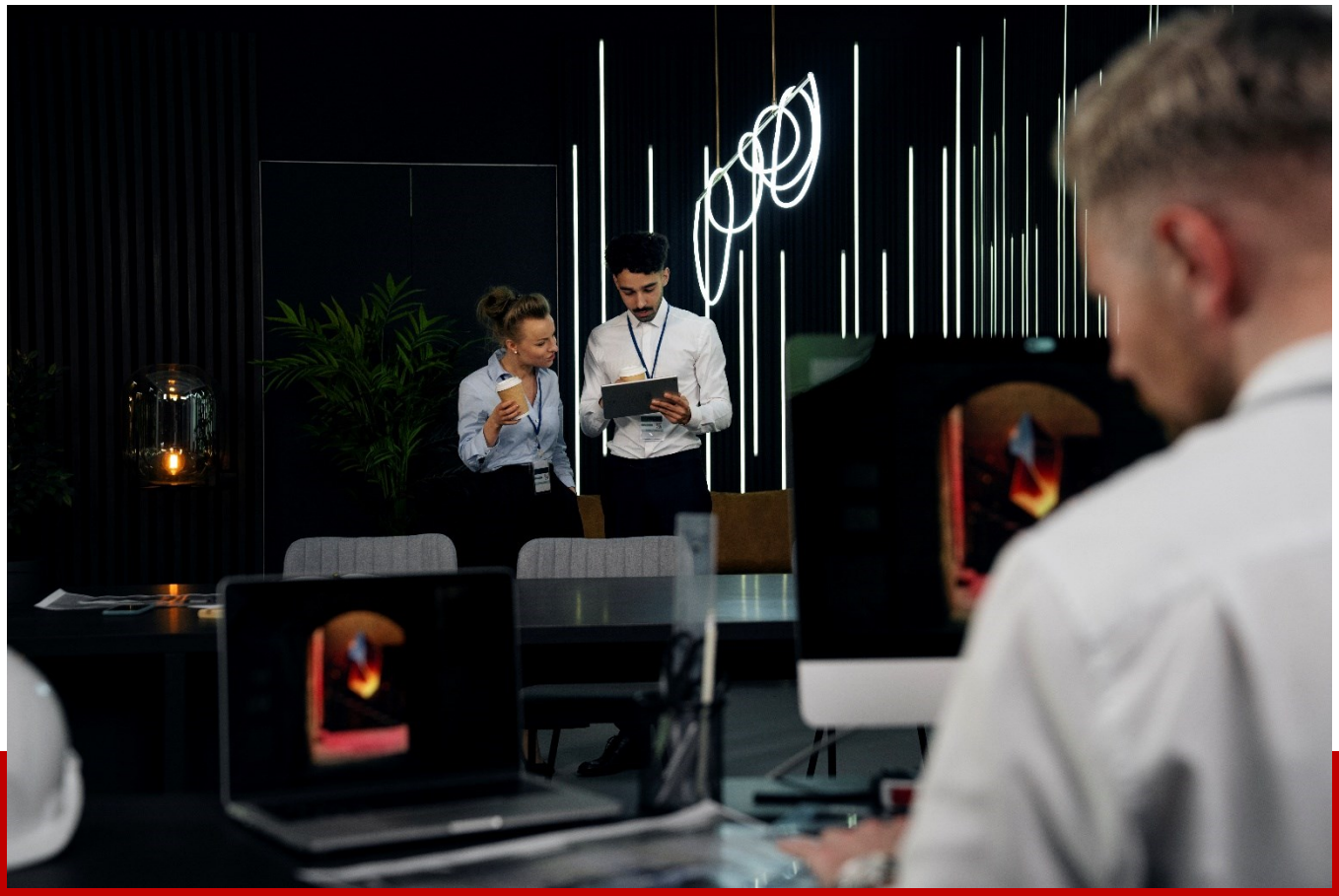
This exclusive interview with Sarah Armstrong-Smith was conducted by Mark Matthews.

About the Author

Megan has managed the internal content for Champions Speakers since 2019 when she joined the company as a Digital Copywriter. In 2020, she progressed to Content Executive and only a year later, Megan was promoted to Senior Content Executive, where she now manages the Champions Speakers YouTube channel and PR outreach.

Continuing her passion for writing, Megan started a PhD at De Montfort University in October 2021. She previously earned her Bachelor of Arts in Film & Creative Writing at the University of Essex and her Masters of Arts in Creative Writing from Teesside University. In her current course, Megan is studying the ethics of such digital forms as podcasts and is conducting metafictional research on the creative process.

In her role, Megan has interviewed several exciting names including Dr Alex George and Sir Mo Farah. She is particularly passionate about LGBTQ+ pride and female empowerment, digital media and journalism – topics Megan enjoys writing about at Champions and researching for her PhD.



Why Should Everyone in Your Workplace Know About Cybersecurity?

The Importance of Strengthening Your Organization's Human Firewall By Involving All Business Levels And Functional Areas.

By Sara Velásquez, Growth Lead, Seccuri

What exactly is cybersecurity? Is it a matter that should only be addressed by people in IT or, as we are seeing today in the industrial domain, the Industrial Internet of things (IIoT)?

All of us who are involved in the practices of cybersecurity are well aware of how important this subject has come to be in the present world, where our daily life in both our organizations and at home are immensely dependent on technology, electronic devices, and the sharing of information.

We have learned through constant news headlines and even our own practical work that cyber threats are becoming increasingly sophisticated and complex, and that they will continue to evolve to become

even more threatening and damaging, just as the people behind them keep getting better at their malicious production.

No matter the threats we face, our role in cybersecurity will continue to rely on safeguarding our organizations' crown jewels (whether these are information, services, or systems). But as we focus on determining the best way to secure these assets, we need to start counting today, more than ever, with the rest of our organization to become part of the cybersecurity army we are today part of. According to CompTIA, the cost of cybercrime has risen 10% in the past year, expecting to cost over $10.5 trillion annually by 2025. What's worse, we currently face a cybersecurity talent workforce gap of 3.4M people… In case you are wondering what these indicators translate into, try guessing whether they might indicate the lack of professionals in cyber supporting our inhouse organizational efforts, or even possible burnouts from the amount of work we'll be tackling in our day-to-day basis, as a result of more complex cyber threats but the same – or even less members in our cybersecurity workforce (as we have been seeing big companies such as Amazon conducting major layoffs).

Whichever case it might be, having the rest of our organization jump on board in our cybersecurity matters seems to be one of the best strategies to tackle these challenges. To do so, building a cyber awareness culture throughout our entire organization becomes critical. Training all business levels, from C-Level executives and Board Members to our colleagues in other functional areas (such as Finance, HHRR, Marketing and Operations) on topics such as cybersecurity fundamentals, and keeping them constantly aware of not only the cyber threats the organization is most susceptible to face, but also the mitigation and defensive actions that must be taken each time, are some of the key points that must be addressed to build this cyber awareness culture.

All people in our organization need to be aware of which are their responsibilities when it comes to cybersecurity, and actively own up to them. Yes, working directly in our IT or cybersecurity teams means being part of the first line of defense, but remember there exists a about a 95% of becoming victim of a cyber-attack due to human error. Today, 52% of global company employees still work remotely, of which 80% have claimed to have encountered more cyber threats. What's more, about 76% of worldwide employees are having inappropriate access to sensible information. There's for sure work to be done on better defining access controls, but making sure everyone knows what the best practices are for information management is a fine measure to prevent cyber-attacks from materializing or at least having an enormous impact on our operations.

People at our organization need to know the risks associated with sharing information with third party entities (including all those that directly and indirectly involved in our supply chain), keep a record of best practices for rutinary activities such as safe password management, ensuring secure remote work, and safely using online applications (such as email and collaborative apps such as Google Drive or Zoom).

Keeping our entire organization updated on the latest cyber risks and cybersecurity trends, and making sure this information is clear and easy to be assimilated by any other team (regardless of their nature) will for sure enable your organization to have a strong human firewall that relies not only on IT and cybersecurity teams, but on every single individual who makes up the entire organizational ecosystem.

Cybersecurity is a matter that should be addressed by everyone, not only us!

About the Author

Sara Velásquez is part of Seccuri, the Global Cybersecurity Talent Platform, where she works as a Growth Lead helping cybersecurity professionals upscale their career paths through job opportunities and training. By focusing on closing the cybersecurity talent gap that exists worldwide, she helps companies find the professionals they require and supports the growth of the cybersecurity talent pool.

Sara can be reached online at sara.velasquez@seccuri.com and at our company website www.seccuri.com/.

The Brick Wall of Identity Security: Five Parts for a Rock-Solid Defense

By Raj Gopalakrishna, Co-Founder and Chief Product Architect, Acalvio Technologies

The use of stolen credentials and resulting identity compromises have become a top attack trajectory. In the past year, 84% of organizations experienced an identity related breach, and 61% of all cyberattacks are based on stolen credentials, which is a number that should make organizations everywhere sit up and pay attention. Like other cybersecurity threats, threats to identities are ever evolving, so identity security and management must evolve ahead of the techniques and strategies of attackers. The cyber defenses that worked in the past might not work in the future, as attackers continually experiment and innovate to find new footholds in identity compromise and credential misuse. Often, just when an organization thinks they have a handle on their identity security, that's when an attacker figures out how to break in from a new and unexpected direction. Staying on top of identity security is key for that reason, and to understand the best defense option for your organization, you must understand all of the parts.

The identity security landscape has five notable parts that can link together to form a defense. The first three, Identity Provisioning Governance and Administration (IGA), IAM & PAM, and Directory Service,

are all well-established identity components that are widely deployed by organizations everywhere. The other two parts are Attack Surface Management (ASM) and Identity Threat Detection & Response (ITDR), which have recently come into focus as strides have been made in their efficacy. Think of these pieces like a brick wall, with each part being an important brick to create the whole wall.

That wall is built on a foundation that we know as "Zero Trust", meaning that all users or devices, whether previously known or not, must be authenticated over and over again every time they wish to gain access. This approach is coined Zero Trust because that's the foundational value: to not trust anyone, no matter what, even if they've been trusted in the network before. By definition, Zero Trust continually authenticates access and constantly monitors user activity in order to properly govern access and user privileges within the network. Think of Zero Trust as the mortar supporting the bricks. Having a foundation of Zero Trust is critical, as Identity Management in hybrid and cloud work environments continues to be an issue that plagues organizations. As remote work environments are set to remain popular, building on that foundation is necessary for the health and security of organizations everywhere. Let's get into the nitty gritty of the five parts of identity security.

Identity Provisioning Governance and Administration (IGA)

IGA is the part of the wall most commonly known as simply "identity security". In 2012, identity governance was recognized by Gartner as the fastest-growing sector of the identity management market. The "governance and administration" portion refers to quite literally governing and administering identities for all users and applications on a given organization's network. Ideally, it provides easy and automated access for those users while also defending against unauthorized users attempting to access the network.

Identity Access Management (IAM) and Privileged Access Management (PAM)

IAM and PAM are frameworks that hold different policies and technologies in order to manage digital identities within an organization. The main difference between the two is the focus; IAM is focused on identity management and validates credentials, while PAM validates access to specific resources based on attributes. In essence, IAM deals with validating everyone who wishes to join the network, while PAM serves as a gate-keeper for important information that shouldn't be accessible to everyone on the network, and directs only "privileged" users to the VIP section, and only after they prove that they're VIP's who belong there.

Directory Service (DS)

The Directory Service portion of our cybersecurity brick wall is like an identity database. This is the part of the identity security strategy where information about users, applications, and resources is stored. This is all the small information like usernames, passwords, device locations, and other minutiae that make up the difference between a real user and an attacker. These directory services exist both in on-prem

servers and in cloud environments in order to support the growing hybrid working environment. Without this key info being stored somewhere, there isn't a common framework for all other parts of identity management to work off of.

Attack Surface Management (ASM)

The ASM part of identity security focuses on the perspective of the attacker rather than the perspective of the defender, which is a newer approach to cybersecurity. ASM identifies attack surfaces on endpoints, privileged identities, Identity Stores, and hypervisors where an attacker could potentially get a foothold and then attempts to remediate those weaknesses. ASM is becoming more crucial as the attack surface itself grows. Just like IAM, PAM, and Directory Services have been impacted by hybrid work, remote work also means that the attack surface of a network is larger. In 2022, 67% of organizations saw their attack surfaces grow significantly. Attack surfaces are also a fluid and changing thing, so ASM must function continuously to keep up. Especially as digital transformation continues to take hold of all industries, networks everywhere can't make attack surfaces smaller, they can just manage what they now have to work with.

Identity Threat Detection & Response (ITDR)

The newest player in the identity security game, ITDR fills a critical role. Instead of focusing on authentication and authorization by focusing on the users (or fake users) and their devices, ITDR protects the identities themselves. The "R" part of ITDR is another step further, where instead of remediation like we see with ASM, we can see attackers actually being caught instead of just fixing what they've left behind. With ITDR, attackers are caught based on their behavior. Deception technology plays an important part here by luring potential attackers into interacting with fake assets, and thus detecting them. This throws up an immediate red flag for the organization that shows exactly what has been compromised. In addition, deception technology can detect threats other technologies like Behavior Analytics and Log Analytics are blind to, creating a more holistic view of cybersecurity.

If we return to our image of a brick wall, ITDR is the barbed trip wire on top, and deception technology is what gives it the barbs. An attacker may think they've "breached" the network by making it to the top of the wall, when really, they'll just find themselves trapped in barbed wire. Individually, all parts of the identity security landscape are important, and they come together to form a strong defense. ITDR is the additional piece of security a plain wall is missing.

Building our Brick Wall

On their own, each part of identity security is still a solid brick, but when combined, they form a rock-solid defense. Combine that with Zero Trust as a steadfast foundation, and ITDR as the barbed wire on top, attackers have their work cut out for them trying to breach an organization's defenses. ITDR and ASM are the advantages that organizations have been looking for, and with deception technology,

cybersecurity has a new edge that attackers aren't prepared for. With the current chaotic and malicious cyberattack environment, any advantage could mean the difference between a breach or stopping an attacker before they can do damage.

About the Author

Raj Gopalakrishna is a Co-Founder and Chief Product Architect at Acalvio Technologies. Raj brings 30+ years of R&D experience and holds over 20 patents. Prior to joining Acalvio, Raj was SVP and Distinguished Engineer at CA Technologies (acquired by Broadcom in 2018) and the VP of R&D at Arcot Systems. Raj can be reached online on LinkedIn and at our company website www.acalvio.com/.

The Next Evolution of Devsecops for the Defense Department

By Jonas Lazo, Vice President of Digital Engineering, Sev1Tech

The White House recently proposed an $842 billion budget for the Department of Defense (DOD) for 2024, emphasizing the Administration's commitment to continue the DOD's IT modernization momentum. IT modernization initiatives will be especially crucial in reaching the Department's goal of fully adopting a Joint All-Domain Command and Control (JADC2) posture, a concept that aims to unite all the armed forces and their networks.

JADC2 is necessary for the future of American defense, but it cannot be achieved unless legacy software and vendor lock-in are eliminated and an interoperable system is established. For many years, a posture of secrecy was leveraged to keep the country and its warfighters safe. Unfortunately, this mentality has created a level of disconnect between the service branches and formed a culture of mistrust regarding sharing information about ideal modernization initiatives and technology.

To overcome these challenges and make JADC2 a reality, the DOD will need to implement a new approach toward deploying robust technology to support mission success and adopt policies that ensure technology is used to its fullest extent and can evolve as needed without sacrificing security. A "software factory of the future" approach can enable DOD to achieve these key goals. This DevSecOps-based mindset creates a software foundation with built-in security that can be modified and tailored to the organization with a common pipeline and basic connectivity. This mindset will allow the DOD to become more agile and evolve quickly.

The challenges of a multi-service organization

One of the most well-known challenges facing the DOD is legacy technology. In addition to being expensive to maintain, legacy technology is often more difficult to operate, especially when integrating with newer, modern technologies. These outdated systems that are extensive and complex to integrate also make adding advanced security or incorporating holistic network security more challenging, creating an open door for vulnerabilities.

Another obstacle to modernization is vendor lock-in. Vendor lock-in hinders the ability to easily transition to a new service provider due to financial or technical complexity. It prevents the DOD from removing technology that no longer serves its mission or acquiring tools that can meet evolving threats, often restricting its path forward toward modernization.

While these two obstacles are gradually becoming less common, the DOD continues to struggle with a mentality of distrust. The service branches often only trust technology that is specifically developed for them. While there are admittedly some security concerns to consider, this frequently prevents the service branches from sharing valuable learnings and knowledge with each other. To accelerate the IT production pipeline, service branches should communicate with each other and share best practices so that technology and processes can evolve.

Cultural transformation enables digital transformation

One of the keys to overcoming roadblocks to digital modernization is encouraging a cultural evolution in the organization and adopting mentalities that will support modernization progress over the long term.

This cultural evolution includes prioritizing warfighter-centric design. Warfighter-centric design includes and consults these end users throughout the development, testing and implementation process. This approach allows the warfighter to become familiar with the technology before ever using it in the field and gives them the opportunity to share concerns and perspectives as it is being developed. Warfighter-centric design is a key component of modern DevSecOps, which aims to allow warfighters to focus more on their mission and less on cyber concerns when on a battlefield. A software factory of the future approach can overcome all these challenges, and an excellent example of it being put into practice is the U.S. Coast Guard's digital modernization efforts.

Laying the Foundation for DOD Modernization

Recently, the Coast Guard has begun to develop its own software factory of the future based on previous work by the Navy. Through a collaborative approach, the Coast Guard is building upon the Navy's initial modernization work and advancing its own more rapidly by learning from the Navy's previous experiences. Conversely, the Navy also stands to reap the benefits because of the foundational nature of software factory of the future, which can enable the Navy to use the technology developed by the Coast Guard to fit future needs it may have.

Service branches working together and creating a collaborative ecosystem via a software factory of the future approach will be essential for the DOD's digital modernization efforts and our nation's future defense capabilities. It will require defense leaders and warfighters to adopt an agile mindset and workflow so that everyone can work together cohesively — with open lines of communication — to achieve mission success. While legacy software, a self-reliant mindset and vendor lock-in are challenges, they can be overcome by shifting long-held mindsets, prioritizing warfighter-centric design and adopting a software factory of the future approach.

About the Author

Jonas Lazo is Vice President of Digital Engineering at Sev1Tech. He has deployed enterprise-level applications for Navy and Marine Corps operations and led DevSecOps design-thinking workshops with the Navy, USMC, Army and USCG. A cleared IT/Software Engineer and registered Agile Coach, he was formerly the Navy Technical Warrant Holder for Cloud Computing as a Navy civilian, where he authored the Naval Cloud Playbook and Cloud Reference Architecture engineering/cybersecurity standards for cloud migration.

What Can We Learn by Analyzing 197 Years of Cumulative Cybersecurity Testing?

By Carolyn Crandall, Chief Security Advocate, Cymulate

Each year, Cymulate releases a Cybersecurity Effectiveness Report that summarizes and analyzes the findings from customers' security assessments throughout the year. Unlike other cybersecurity research, this report does not focus on the security incidents detected by security controls but rather on those gaps and events that were *not* detected. The report covers attack surface exposures, vulnerabilities, and attack paths to provide a more holistic view of the threat landscape and the effectiveness of today's security solutions. It's no longer enough to know which attacks were detected – organizations need to understand where vulnerabilities remain.

The 2022 State of Cybersecurity Effectiveness report analyzes the equivalent of 197 years of anonymized offensive cybersecurity testing within customer product environments during 2022. Those customers span various locations, sizes, and industries, providing a comprehensive view of cybersecurity resilience. While the full report contains a more thorough analysis of the findings, below, you can find a selection of the most compelling findings included in the study.

Organizations Still Haven't Mastered the Fundamentals

One of the most concerning findings in the report was that 40% of organizations have vulnerabilities within their environments that have had patches available for more than two years. Of course, this isn't a new threat—exploiting known vulnerabilities is just about the oldest tactic in the book. But too many organizations lag in basic cyber hygiene, failing to improve their patching cadence. The result is that many organizations have unpatched CVEs, poorly configured Identity and Access Management (IAM) solutions, and other dangerous vulnerabilities just waiting to be taken advantage of.

Part of the reason for this is that headlines too often dictate an organization's remediation priorities. This is understandable—when a major attack makes the news, it's only natural to want to protect your network against it. But the State of Cybersecurity Effectiveness report finds that this often leads to tactics seen in media coverage receiving attention vastly disproportionate to their actual risk level—often at the expense of more pressing threats. This is further driven home by the fact that 92% of detected exposures fall within domain security and email security. Rather than focusing on headline-grabbing threats, most organizations would find their efforts better spent doubling down on fundamentals like domain and email security.

Preventing Exfiltration Remains a Challenge

The effectiveness of data protection measures is declining, with data exfiltration risk scores worsening over the past year. This can be partially attributed to the complexity of Data Loss Prevention (DLP) and Cloud Security Access Broker (CSAB) solutions, and the cost associated with their implementation, but also to the simple fact that today's businesses rely heavily on access to certain cloud storage platforms. Unfortunately, restricting access to those platforms without hampering business operations can be extremely difficult. As a result, cloud service-related assessments received a significantly higher risk score in 2022 than in 2021.

It isn't all bad news, though: the report's findings indicate that email restrictions have effectively prevented data exfiltration. A growing share of organizations are now taking advantage of native and third-party solutions to restrict what data can be shared outside the organization via email. While cybercriminals can use other exfiltration methods, this makes their job more difficult—which is always a good thing.

Although email restrictions have helped, Cymulate's research found that social engineering remains problematic, and Business Email Compromise (BEC) attacks remain popular among adversaries.

Tactics include CEO fraud, where the attacker impersonates a company's CEO or other high-ranking executives to request funds or information, false invoice schemes, in which the attacker impersonates a supplier asking for payment. PII misappropriation is another tactic in which the attacker impersonates an employee from another department to gain access to protected data, continue to find success. Email protections can help, but training employees to recognize the signs of these scams will improve the security of your organization.

The Impact of Breach and Attack Simulation on Risk

By comparing data over time, the report reveals that measures like Breach and Attack Simulation (BAS) are highly successful at reducing an organization's overall risk. By comparing the data between a customer's first endpoint security assessment and their most recent assessment, it becomes clear that there is a significant improvement in risk reduction over time when BAS testing is performed regularly. Moreover, those results are consistent across all industries and businesses, indicating a strong correlation between BAS implementation and reduced risk.

The initial average risk score for Windows signature-based antivirus scanning was extremely high for most customers but dropped to only moderate risk following BAS implementation. The risk fell from moderate to low for Windows behavioral-based detection (EDR and XDR solutions). MacOS anti-malware defenses and Linux anti-malware defenses both fell from high risk to moderate risk. While this shows that there is still room for improvement, it also serves as a clear indicator that attack simulation has a positive impact on risk across the board.

Making Informed Cybersecurity Decisions

The 2022 State of Cybersecurity Effectiveness report makes it clear that the most dangerous threats organizations face aren't necessarily the newest or most innovative but the same risky behaviors and poor hygiene practices that have plagued them for years. In order to address and remediate those threats, organizations need to double down on the fundamentals, training employees to recognize the signs of social engineering attacks and implementing stronger password and patching policies. But policies and training aren't enough—continuous security validation is also needed. As organizations look for ways to reduce risk across the board, running continuous assessments can help ensure that their security solutions work as intended against today's most pressing threats.

About the Author

Carolyn is the Chief Security Advocate and CMO at Cymulate, a leader in cybersecurity risk validation and exposure management solutions. She is a high-impact technology executive with over 30 years of experience in building new markets and successful enterprise infrastructure companies. She has a demonstrated track record of effectively taking companies from pre-IPO through to multi-billion-dollar sales and has held leadership positions at Attivo Networks, Cisco, Juniper Networks, Nimble Storage, Riverbed, and Seagate.

Why Dwell Time is the Biggest Threat to Security Operations Center (SOC) Teams in 2023

By Sanjay Raja, VP of Product, Gurucul

Dwell time, or the length of time a cyber attacker remains hidden within an organization's environment, is a major threat plaguing Security Operations Center (SOC) teams today. Reducing dwell time is critical for organizations because the longer attackers remain undetected, the longer they have to steal sensitive data or plant ransomware. According to the latest Cost of a Data Breach Report published by IBM, in 2021 it took a mind-boggling average of 287 days before attackers were discovered and kicked out. Despite the best efforts of organizations, that number doesn't seem to be going down substantially. So, why is this happening? And what can these organizations do to defend themselves?

How Hackers Get into Your Network:

Oftentimes, hackers get initial access to a network by exploiting employees of a company. In recent years, hackers have achieved this through social engineering or via phishing attacks through a person's cell phone or email address. Once they achieve access to a network and obtain the structure of usernames for a particular enterprise, they try to hack in using brute force passwords or by using guesswork depending on what they know about the user. Additionally, if hackers have obtained legitimate credentials, it's much harder for SOC teams to detect and block them.

In addition to employees being exploited, software and system exploits remain a huge issue for organizations. Both zero-day exploits (which are vulnerabilities in software, hardware or firmware that are unknown to the organization) or vulnerabilities that haven't yet been patched, represent common ways into a network. It's critical that IT teams be in regular contact with their software vendors and internal software architects to be up to date on the latest vulnerabilities and patches. If a patch exists, IT staff should apply it as soon as it is tested in their environment.

Another way hackers can gain access to a network is through smaller organizations that can't afford to hire dedicated security staff. When organizations don't have a dedicated security staff, cybersecurity often becomes just one more additional duty for IT. Oftentimes IT professionals aren't equipped with the proper security software, tools or skills to prevent cyber-attacks, let alone detect dwellers on their network. This lack in a security infrastructure makes them a prime target for hackers and hacking groups. Attacks can sometimes use this access to breach larger organization's networks in a supply chain attack.

Despite hackers finding ways to exploit employees and loopholes in software, organizations can defend themselves against dwell time. By utilizing unified SOC views, true machine learning and establishing a cost-efficient data model, organizations can prepare themselves for attacks against these hackers and other threats that come their way.

A unified SOC view to streamline investigations: By automating initial responses to threats and the gathering of actionable intelligence, SOC teams can investigate threats more quickly. This lets them not only detect dwellers, but also take actions to remove them from the network. Additionally, SOC teams that are stuck using static, legacy threat detection products aren't optimizing their systems to their full potential either. These legacy products produce too many false positive alerts that can make dwell time worse because real threats are drowned out. The solution here is to use machine learning threat detection that adapts and can detect different variants of threats, ensuring that SOC teams are getting true threat detection.

Machine learning software that can adapt: Many products that advertise as having machine learning really don't. They have limited, rules-based ML that can't adapt to situations or threats it's not programmed to respond to. By using true machine learning, modern cybersecurity software can create models of normal activities that learn and adapt based on incoming data. This lets them more readily flag true positives, saving time and effort for SOC teams and security analysts. This allows SOC teams to detect new and emerging threats that are not yet in the threat intelligence feeds.

Establishing a cost-efficient, data ingestion model: An unfiltered approach to data analysis will generate many false positive results. These are usually activities that are unusual but legitimate. SOC analysts could well be overwhelmed by seemingly real threats that turn out to be spurious. Using an unlimited data model allows a full field of view into what's happening on the network by giving the security software the context it needs to generate more accurate responses. Limiting analytics to save on cost makes threat detection less accurate and puts more work on SOC teams. Paying based on data volume can run also up the bill quickly.

Dwell time is a critical threat facing organizations today that continues to worsen every year. However, organizations can reduce dwell time by taking a unified SOC approach, using machine learning software, and establishing a cost-efficient model that allows for unlimited data ingestion for full analytics. By doing so, SOC teams can reduce the damage caused by attackers and mitigate the cost of a data breach. Today, organizations must modernize their security systems and software and take proactive steps to defend themselves against dwellers on their network.

About the Author

Sanjay Raja is the VP of Product of Gurucul. Sanjay brings over 20 years of experience in building, marketing, and selling cyber security and networking solutions to enterprises, medium-to-small business, and managed service providers. Previously, Sanjay was VP of Marketing at Prevailion, a cyber intelligence startup. Sanjay has also several successful leadership roles in Marketing, Product Strategy, Alliances and Engineering at Digital Defense (acquired by Help Systems), Lumeta (acquired by Firemon), RSA (Netwitness), Cisco Systems, HP Enterprise Security, Crossbeam Systems, Arbor Networks, Top Layer Networks, Caw Networks (acquired by Spirent Communications), Nexsi Systems, 3Com, and Cabletron Systems. Sanjay holds a B.S.EE and an MBA from Worcester Polytechnic Institute. Sanjay is also a CISSP as well as Pragmatic Marketing certified.


EVENTS

agora
Bridging Value

6th Edition

The Gulf Congress on Cybersecurity

May 9th, 2023 | Conrad Hotel - Dubai, UAE

ICDSS

EVENT BY

P2B SERVICES

INDIA

CLOUD & DATA SECURITY SUMMIT - 2023

"Consolidating the future of Cloud & Data security opportunities in India"

11 - 12 MAY 2023

Chennai, India , In Person Event

REGISTER

www.clouddatasecuritysummit.com

CONATCT DETAILS

Point To Business Services Private Limited

Phone : +91 98804 42379 / +91 77089 97535

Email : info@pointtobusinessservice.com

info@clouddatasecuritysummit.com

MEDIA PARTNER

CYBER DEFENSE MAGAZINE

IFSEC 50 YEARS

THE SUSTAINABLE SECURITY EVENT

SUPPORTING THE GLOBAL SECURITY COMMUNITY FOR 50 YEARS

16-18 MAY 2023 | EXCEL LONDON

Fueling security leaders with the expertise and innovation to keep people and assets safe

Connect face-to-face with the entire security supply chain and network with global security companies across access control, video surveillance, perimeter protection, cyber security and more.

> The best exhibition for networking with professionals in the field, due to its privileged location. Add the chance to observe the trends and novelties in the security field, and then a prospective visit becomes worthwhile.
>
> Advancis Software and Services

FIND US ON STAND IF.3046

ISJ INTERNATIONAL SECURITY JOURNAL

ENQUIRE ABOUT EXHIBITING AT | WWW. IFSEC.EVENTS

Setting new industry standards for quality and sustainability

JOIN EUROPE'S BIGGEST EVENT
ON INTELLIGENT TRANSPORT SYSTEMS AND SERVICES

EUROPEAN CONGRESS

LISBON, PORTUGAL
22-24 MAY 2023

ITS: The Game Changer.

22-24 May 2023

CALL FOR CONTRIBUTIONS IS OPEN!

WHAT TO EXPECT

800 delegates

120 Exhibitors

2500 Attendees

100 Programme Sessions

50+ countries represented

Government, state and city representatives

Private sector representatives from multiple industries

A UNIQUE EXPERIENCE TO:

- Network with 3200+ smart mobility stakeholders
- Discover the latest mobility solutions and services
- Share experiences through lessons learnt
- Monitor progress and measure results
- Exhibit and experience innovative technologies
- Benefit from first-hand experience through demonstrations

ORGANISED BY ERTICO ITS EUROPE

HOSTED BY LISBOA CÂMARA MUNICIPAL · ITS PORTUGAL

SUPPORTED BY Turismo de Lisboa · TURISMO DE PORTUGAL

www.itseuropeancongress.com/call-for-contributions/

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

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

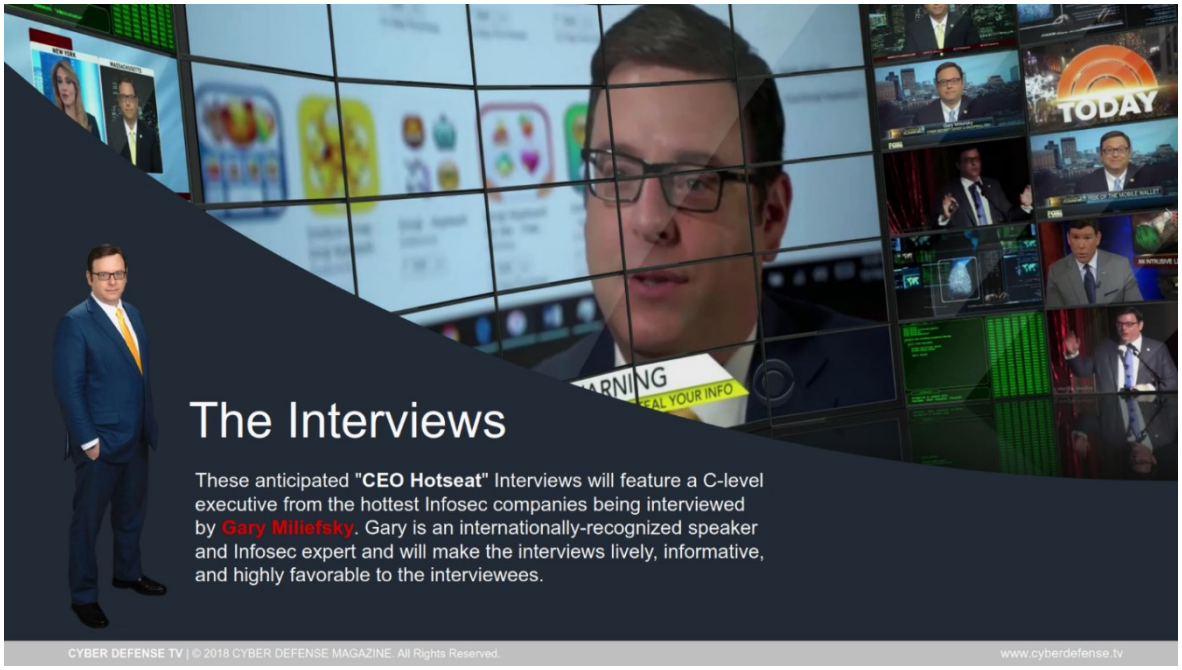
CYBER DEFENSE TV

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.

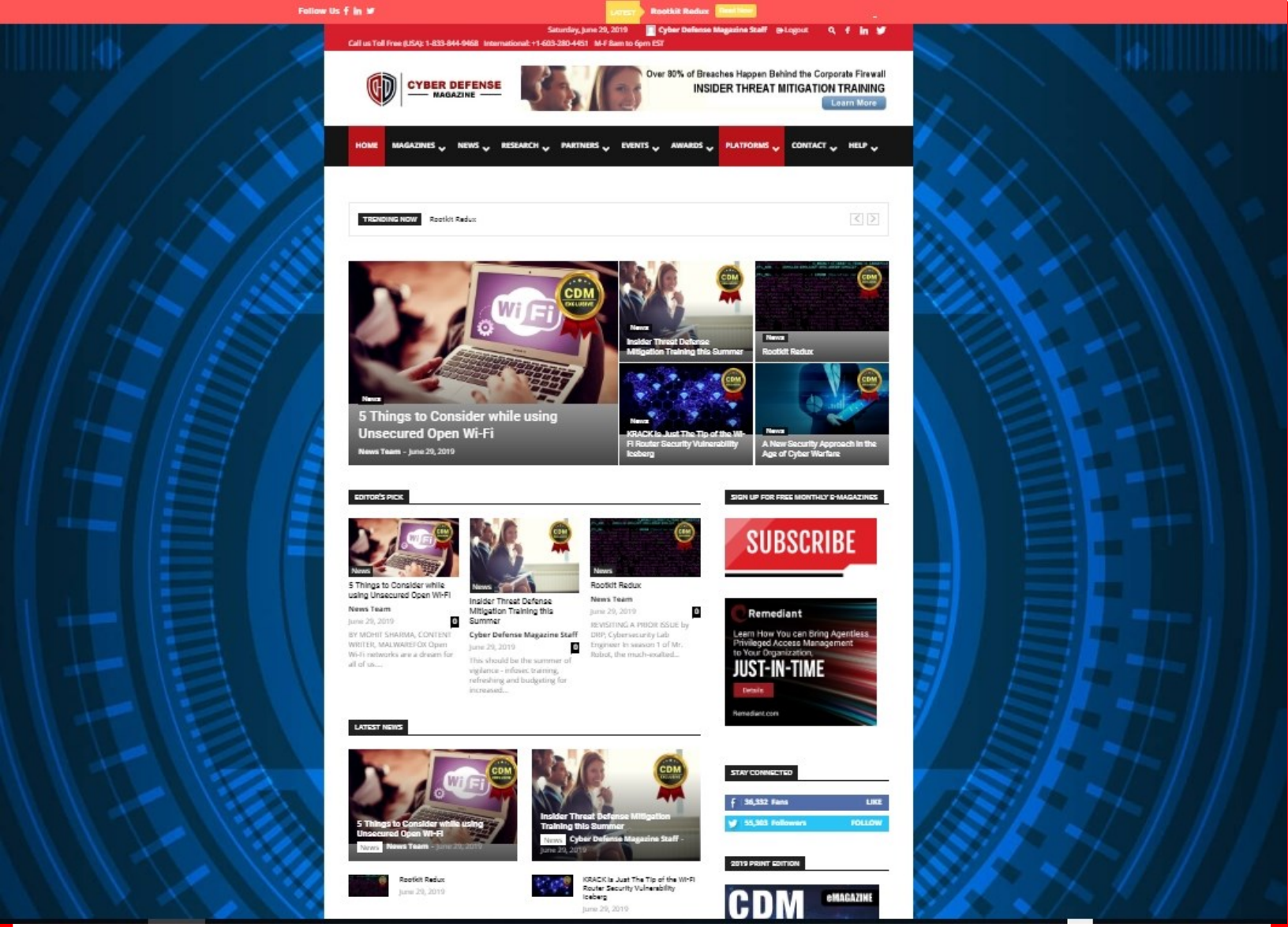
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 05/03/2023



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 www.cyberdefenseconferences.com and have another amazing platform coming soon.

UNKNOWN CYBER

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

Not by us. We detect the unknowns.

www.unknowncyber.com

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

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

RSA Conference 2023 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From April 24 – 27, 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.**