

eMAGAZINE

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

IN THIS EDITION

Seven Security Predictions for 2020

2020 Industry Predictions

Data Privacy in A Device-Driven World

Industrial Control System Vulnerabilities

The Growing Importance of API Security

*Conquering the Cyber Security Challenges of
The Cloud*

*Cybersecurity Talent Shortage and Ways to
Address the Gap*

...and much more...

FEBRUARY 2020

MORE INSIDE!

EXPLORE THE HUMAN ELEMENT OF CYBERSECURITY.



What's the most important weapon in the fight against cyberthreats? New software? Faster equipment? Smarter computers? At RSA Conference, we believe it's people.

Attend RSA Conference 2020, February 24-28, and join thousands of security professionals, forward-thinking innovators and solution providers for five days of actionable learning, inspiring conversation and breakthrough ideas.

Register today to save your spot at the world's most comprehensive cybersecurity event.

rsaconference.com/cyberdefense-us20

#RSAC



FOLLOW US

CONTENTS

Welcome to CDM's February 2020	7
Seven Security Predictions for 2020	21
By Corey Nachreiner	
2020 Industry Predictions	26
By Peter Goldstein, CTO and co-founder, Valimail	
Balbix 2020 Predictions	29
By Gaurav Banga, CEO and founder, Balbix	
ForgeRock 2020 Predictions	31
By Eve Maler, Interim CTO, ForgeRock	
DivvyCloud 2020 Predictions	34
By Chris DeRamus, CTO and co-founder, DivvyCloud	
ForgeRock 2020 Predictions	37
By Ben Goodman, SVP at ForgeRock and CISSP	
Bitglass 2020 Predictions	40
By Anurag Kahol, CTO and co-founder, Bitglass	
AttackIQ 2020 Predictions	43
By Christopher Kennedy, CISO and VP of Customer Success, AttackIQ	
AttackIQ Report On Ponemon Survey: Despite Spending An Average Of \$18.4 Million On Cybersecurity Solutions, Organizations Still Get Breached	46
By Stephan Chenette, co-founder and CTO, AttackIQ	
Data Privacy in A Device-Driven World: Navigating the Impact Of California's 2020 IOT Security Legislation	48
By Brian Murray	
Conquering the Cyber Security Challenges of The Cloud	51
By Steve Durbin, Managing Director, Information Security Forum	
How to Address Multi-Cloud Security	55
By William Klusovsky, CISSP, CISM	

<i>5 Key Steps to Secure IOT Product Development</i> -----	59
By Kateryna Boiko, Marketing Manager, Mobilunity	
<i>The Struggle of Updating Government Cybersecurity Measures</i> -----	64
By Kayla Matthews	
<i>Accelerating the Pace of Government IT Modernization</i> -----	67
By Jeff Elliott	
<i>Cybersecurity Talent Shortage and Ways to Address the Gap</i> -----	71
By Blake Tinsley, Founder and CEO, Prosyntix	
<i>5 Recruitment Predictions in Cybersecurity For 2020</i> -----	74
By Karl Sharman	
<i>Cross Domain Solutions – Quo Vadis</i> -----	76
By Alexander Schellong, VP Global Business, INFODAS	
<i>Industrial Control System Vulnerabilities: A Prime Target of Our Critical Infrastructure by Adversaries</i> -----	80
By Dr. Daniel Osafo Harrison, DCS, C CISO, CISM, CISA, CRISC, Security+	
<i>The Growing Importance of API Security</i> -----	84
By Ameya Talwalker, Co-founder and CPO, Cequence Security	
<i>A Single Security Recommendation to Solve an Age-Old Problem</i> -----	88
By Morey Haber, CTO & CISO, BeyondTrust	
<i>Not All Hackers Are Criminals, And Some of The Good Guys Can Earn A Million Dollars</i> -----	92
Dr. Roberto Di Pietro	



@MILIEFSKY

From the Publisher...



New [CyberDefenseMagazine.com](https://www.cyberdefensemagazine.com) website, plus updates at [CyberDefenseTV.com](https://www.cyberdefensetv.com) & [CyberDefenseRadio.com](https://www.cyberdefenseradio.com)

Dear Friends,

We're delighted to present the February 2020 issue, featuring a broad spectrum of knowledgeable contributors on what's coming down the pike as we face a new year of cybersecurity challenges and responses.

We are excited to be preparing to expand our role in the RSA Conference 2020, held once again in San Francisco, CA, USA. More than a dozen of our team members will head to the biggest infosec show on earth in late February – detailed information is posted online at <https://www.rsaconference.com>. By the time we head for the City by the Bay, we will also be publishing the RSA Conference edition of Cyber Defense Magazine, building on the firm foundation of the current issue.

Our vision for 2020 is already becoming a reality as the activities of our Black Unicorn Award winners converge with the prognostications of challenges and responses in the world of cybersecurity. Likewise, we are delighted to see our InfoSec Awards for 2020 projected to include market leaders, innovators, and others offering some of the best solutions for cyber security in the global marketplace.

We'd like to remind those women who did not make our Top 25 Women in Cybersecurity for last year or missed out on the deadline, we have now added Women in Cybersecurity as a new category this year. Also, we encourage you to ask our judges if they will create a new category for your unique product or service. Be creative and assertive!

If you're an infosec innovator, please consider applying at: <https://www.cyberdefenseawards.com/> Your participation in our programs will support your efforts and help integrate you into our growing community of vendors, decision-makers, and others active in cybersecurity pursuits. Remember that we offer our own statistics that you are free to access and use anytime, from this page: <http://www.cyberdefensemagazine.com/quotables/>.

During the month of February, we will have more new interviews going live on <https://www.cyberdefensetv.com> and <https://www.cyberdefenseradio.com>, so please check them out and share links to them with your friends and co-workers.

We've started out the new year with well over 5m views on [Cyber Defense Magazine](https://www.cyberdefensemagazine.com) expected as we measure results for the month of January. We expect big improvements and changes to how we handle growth and respond to customer and partner needs as we all work together to continue to learn new and better ways to respond to known and (so far) unknown threats!

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.





InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE InfoSec information.

From the International Editor-in-Chief...

So many changes are in play in the international theatre of cybersecurity! As they always tell us at the matches, "You can't tell the players without a program!"

From one perspective, the growth of legal and regulatory requirements has created a playing field with so many rules, it's hard to keep track of who is winning and who isn't. One complicating factor is the pattern of jurisdictional conflicts, largely among international, national, and individual State requirements. We face a constantly moving set of compliance targets – some of which overlap and others which leave gaps. Even if we make our corporate home in one place, will we need to comply with the rules of the jurisdiction where our clients and customers are located? Can we claim compliance with GDPR as the standard if we have operations or distributors in California? And what will the effect of Brexit be? Will this be the year that the U.S. federal government enacts a national privacy law – and who will be covered?

These are just a few of the questions we at Cyber Defense Magazine must address, and we are grateful for our contributors for sharing their expertise with our staff and readers.

We invite you to read in this issue the perspectives of others, and then send us comments on your own experiences in dealing with the growing complications in international cybersecurity practice.

To our faithful readers, we thank you,

Pierluigi Paganini

Editor-in-Chief



@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.

PRESIDENT & CO-FOUNDER

Stevin Miliefsky

stevinv@cyberdefensemagazine.com

INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER

Pierluigi Paganini, CEH

Pierluigi.paganini@cyberdefensemagazine.com

US EDITOR-IN-CHIEF

Yan Ross, JD

Yan.Ross@cyberdefensemediagroup.com

ADVERTISING

Marketing Team

marketing@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

Toll Free: 1-833-844-9468

International: +1-603-280-4451

SKYPE: cyber.defense

<http://www.cyberdefensemagazine.com>

Copyright © 2019, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (a Steven G. Samuels LLC d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.

PUBLISHER

Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:

<http://www.cyberdefensemagazine.com/about-our-founder/>

WE'RE TURNING A CORNER INTO 8 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

Welcome to CDM's February 2020

In this edition, we are pleased to include Predictions for 2020 from several different perspectives. The points of view range from industry experts to vendors to market sector commentators, and even include 2 divergent articles by authors from the same company!

Cyber Defense Magazine provides a forum for theoreticians and practitioners alike, as we welcome readers to draw your own conclusions from your own experience and knowledge bases. Overall, we present thoughtful and actionable information for readers to make informed decisions and implement the best offerings in the marketplace.

Looking ahead this year, our broad research shows a marked interest in the 2020 election cycle in the U.S. Starting in the March issue, we will be looking for and publishing an array of articles on the "Countdown to the 2020 Elections," and we expect to provide feature articles on topics related to the integrity of the electoral process.

There are many challenges facing the various organizations in the elections process, as demonstrated by numerous announcements from the media, government and private sources. They range from denial to reasoned approaches to "Chicken Little" responses.

We've chosen just one to highlight now, and it's from an official source, the Federal Bureau of Investigation. In this recent announcement, the FBI vows to warn county-level election officials if the agency becomes aware of more cyber attacks. This enhanced notification process supports the designation of the electoral process by the Department of Homeland Security as one of the elements of critical infrastructure.

Going forward, Cyber Defense Media Group has added to our corporate capacity to provide editing and writing services to our readership, including feature articles based on interviews on topics of current interest to all.

We continue to add to the value proposition of Cyber Defense Magazine: keeping our audience informed and ahead of the curve of these important developments.

Wishing you all success in your cyber security endeavors,

Yan Ross
US Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief



Yan Ross, J.D., is a Cybersecurity Journalist & US Editor-in-Chief for 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 via his e-mail address at yan.ross@cyberdefensemediagroup.com



SPONSORS



CYBER DEFENSE MEDIA GROUP

WHERE INFOSEC KNOWLEDGE IS POWER

**Rise above the noise,
take your Infosec story to the moon and back!
Only with Cyber Defense Media Group**



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

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011



Founder & Managing Partner

SEAN DRAKE



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

Sean Drake

Managing Partner

Stony Lonesome Group LLC

203-247-2479

www.stonylonesomegroupllc.com



By the time an attacker tastes the difference, their presence is known.



"Attacker mistakes are made when they cannot distinguish real from fake."

Tony Cole, CTO Attivo Networks

DECEPTION-BASED THREAT DETECTION

Detecting threats needs to be comprehensive, however it doesn't have to be complicated. Designed for simplicity, Attivo Networks brings uncertainty to the mind of the attacker, redirecting them away from the target assets and providing defenders with high-fidelity alerting that is backed with actionable attack and forensic data on malicious activity and insider policy violations.

Attivo
NETWORKS.
Deceive. Detect. Defend.

Learn more at attivonetworks.com/ebook

Setting the Standard

in Cyber Defense Training & Education

Transform your cyber defense capabilities with customized training. Regent's Institute for Cybersecurity will help you develop your workforce credentials, manage your cyber risks and defend your assets.

CORPORATE | GOVERNMENT | MILITARY | EDUCATION



Powerful Hyper-Realistic
Range Simulation



Industry Certifications



Executive & Senior Leadership
Cyber Workshops



Associate, Bachelor's &
Master's Programs



Regent's B.S. in Cybersecurity has
received NSA and DHS designation.

Learn More

regent.edu/cyber | 757.352.4590



REGENT
UNIVERSITY

Institute for
Cybersecurity

OneTrust

Privacy Management Software

World's #1 Most Widely Used Privacy Management Software

For Privacy, Security & Third-Party Compliance

Solutions to Comply with the CCPA, GDPR & Global Privacy Laws & Security Frameworks



Privacy Program Management:

- **Maturity & Planning:** Compliance Reporting Scorecard
- **Program Benchmarking:** Comparison Against Peers
- **DataGuidance Research:** Regulatory Tracking Portal
- **Assessment Automation:** PIAs, DPIAs & Info Security



Marketing & Privacy UX

- **Cookie Compliance:** Website Scanning & Consent
- **Mobile App Compliance:** App Scanning & Consent
- **Universal Consent:** Consent Receipts & Analytics
- **Preference Management:** End User Preference Center
- **Consumer & Subject Requests:** Intake to Fulfillment
- **Policy & Notice:** Centrally Host, Track & Update



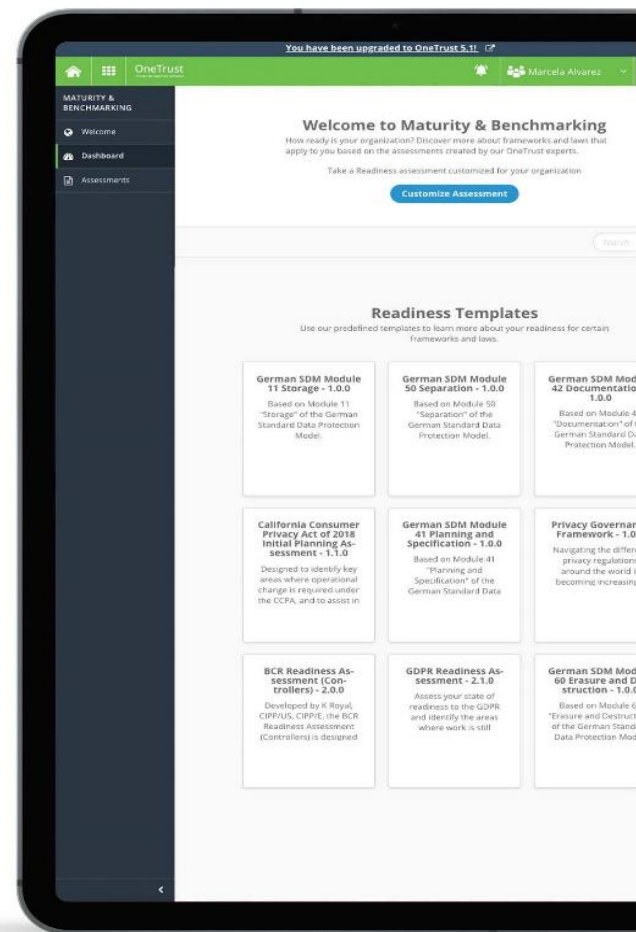
Third-Party Risk Management

- **Vendorpedia Management:** Assessment & Lifecycle
- **Vendorpedia Risk Exchange:** Security & Privacy Risks
- **Vendorpedia Contracts:** Contract Scanning & Analytics
- **Vendorpedia Monitoring:** Privacy & Security Threats
- **Vendor Chasing Services:** Managed Chasing Services



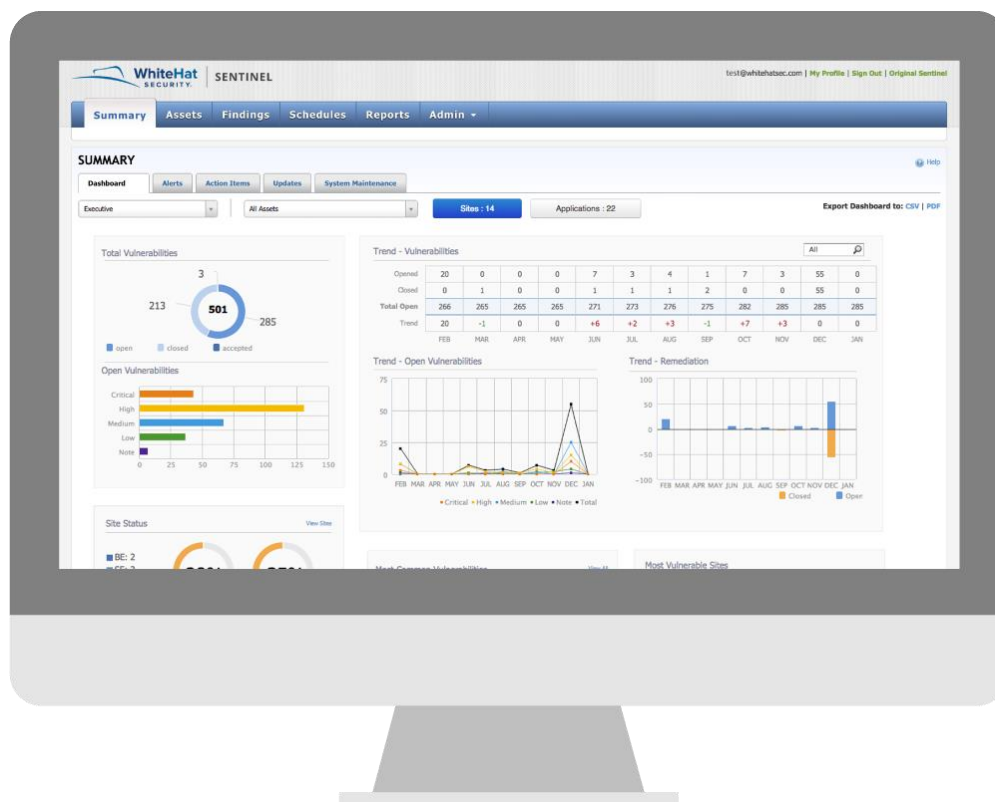
Incident & Breach Response

- **Incident & Breach Response:** Intake & Lifecycle Management
- **DatabreachPedia Guidance:** Built-in guidance from 300 laws



GET STARTED TODAY | [ONETRUST.COM/FREE-EDITION](https://onetrust.com/free-edition)

LEARN MORE ABOUT ONETRUST | [REQUEST A DEMO | ONETRUST.COM](https://onetrust.com)



Your website could be vulnerable to outside attacks. Wouldn't you like to know where those vulnerabilities lie? Sign up today for your free trial of WhiteHat Sentinel Dynamic and gain a deep understanding of your web application vulnerabilities, how to prioritize them, and what to do about them. With this trial you will get:

An evaluation of the security of one of your organization's websites

Application security guidance from security engineers in WhiteHat's Threat Research Center

Full access to Sentinel's web-based interface, offering the ability to review and generate reports as well as share findings with internal developers and security management

A customized review and complimentary final executive and technical report

[Click here](https://www.whitehatsec.com/info/security-check/) to sign up at this URL: <https://www.whitehatsec.com/info/security-check/>

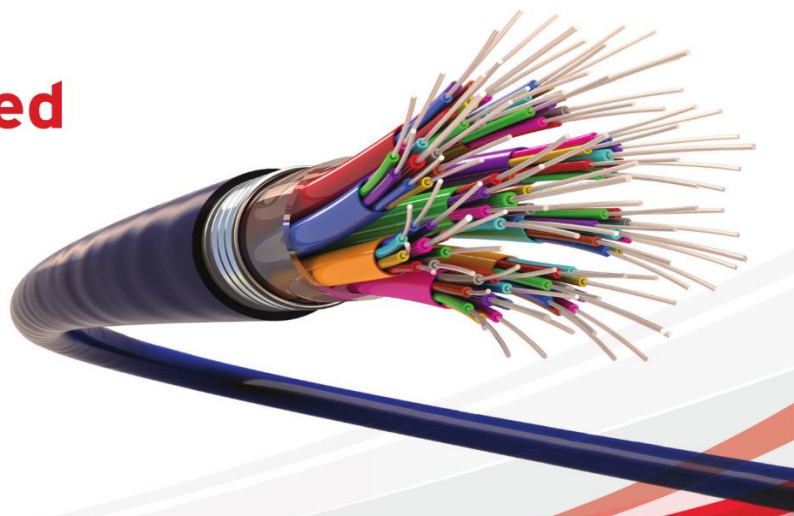
PLEASE NOTE: Trial participation is subject to qualification.

Detect and prevent breaches at wire speed

Your enterprise is in the crosshairs of the increasingly complex array of ransomware, advanced threats, targeted attacks, vulnerabilities, and exploits.

Only complete visibility into all network traffic and activity will keep your network security ahead of today's purpose-built attacks which bypass traditional controls, exploit network vulnerabilities, and either ransom or steal sensitive data, communications, and intellectual property.

Trend Micro Network Defence detects and prevents breaches at wire speed anywhere on your network to protect your critical data and reputation.



Proven capability

Trend Micro TippingPoint:
"Recommended" Next-Generation Intrusion Prevention System and 99.6% security effectiveness.

Trend Micro Deep Discovery:
"Recommended" Breach Detection System 4 years in a row and 100% detection rate

Industry leading threat intelligence



Please get in touch:

Bharat Mistry, Principal Security Strategist
Bharat_mistry@trendmicro.co.uk

www.trendmicro.co.uk/xgen-cyber

©2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

Database Cyber Security Guard

Prevents data theft by Hackers, Rogue Insiders, Phishing Email Attacks, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks when the security perimeter has been penetrated.

Average data breach costs \$7.3 million dollars. Would have immediately shutdown the Equifax and Marriott hackers.

Product Features

- Prevents WordPress, Drupal, Joomla and non content management system (CMS) web site confidential data theft.
- Detects Infromix, MariaDB, MySQL, Oracle, SQL Server and Sybase potential data theft within a second and immediately shuts hackers down.
- View all suspicious hacker SQL activity and attempted data theft.
- Dashboard summary of hacker activity over any time period.
- Runs from a network tap or proxy server for non-intrusive detection of data breaches. Has no impact on database servers.

Advanced SQL Behavioral Analysis of the query activity learns the normal query patterns and stops the theft of database data.

www.DontBeBreached.com and www.Sqlpower.com/Cyber-Attacks



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

Two Years Later

NotPetya's Game-Changing Lessons for Cybersecurity and Collective Defense

In early Summer 2017, the highly destructive NotPetya malware appeared and spread with devastating efficiency across data systems and architectures worldwide. The attack not only shattered records for speed and destruction, but also served as a wake up call for security professionals to up their game on cyberdefense. Here are key lessons learned from NotPetya, and how those lessons continue to shape today's leading practices in cybersecurity.

LESSON 1

Malware is increasingly designed to disrupt business operations in the physical world.

NOTPETYA CREATED AN UNPRECEDENTED

\$10 billion
IN DAMAGE WORLDWIDE¹



How NotPetya changed the game — Unlike ransomware and other profit-driven attacks, NotPetya was built simply to destroy.



How the cybersecurity industry is adapting — NotPetya has taught today's security teams to assume destruction is a potential goal, appreciate the elevated risk and then act accordingly.

LESSON 2

NotPetya raised the speed limit for modern cyber attacks.

NOTPETYA SPREAD TO MORE THAN

64 countries
IN JUST THE FIRST
24 hours²



How NotPetya changed the game — NotPetya was built for speed, with code designed to proliferate automatically, rapidly and indiscriminately.



How the cybersecurity industry is adapting — Cyberdefenses today should ideally use near-real time network traffic analysis and behavioral analytics to rapidly catch new forms of attacks that perpetually outdated signature-based systems would miss.

LESSON 3

The worst attacks take lateral movement to the extreme — across all organizational and industry barriers.

THE FAR-FLUNG INDUSTRIES AFFECTED BY NOTPETYA INCLUDE shipping, pharmaceuticals, banking, advertising, energy AND OTHER MAJOR SECTORS³



How NotPetya changed the game — NotPetya's spread was not only fast, but also far and wide — with cross-sector damage at major organizations like Maersk, FedEx and others. NotPetya was also patch-resistant, vacuuming up credentials on infected targets for use later as workarounds on protected servers.



How the cybersecurity industry is adapting — Companies must assume the when, not if, mindset to penetration and lateral movement, and embrace collective defense and threat information sharing — across entire industries and even between many different sectors.

LESSON 4

NotPetya shows the limits of attribution.

CYBERATTACK ATTRIBUTION IS GETTING MORE COMPLEX, WITH AT LEAST 10 variations OF NATION-STATE RESPONSIBILITY⁴



How NotPetya changed the game — While Russia is generally blamed for NotPetya,⁴ the attribution is less critical, given the indiscriminate nature of the attack and increased “collective offense” between criminal groups and nation-states sharing tactics and targets.⁵



How the cybersecurity industry is adapting — Security teams must meet threat actor's collective offense approach with collective defense — working with peers to share threat information and identified attack techniques.

¹ <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

² <https://www.securityweek.com/petyanotpetya-what-we-know-first-24-hours>

³ <https://www.securityweek.com/notpetya-attack-costs-big-companies-millions>

⁴ <https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/>

⁵ <https://ironnet.com/white-paper-survey-download/>

⁶ https://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF



ARTICLES



2020

Seven Security Predictions for 2020

By Corey Nachreiner

Each year, the [WatchGuard Threat Lab](#) research team examines the top emerging threats and trends across the information security landscape to develop predictions for the coming year. Even though the threats coming at you won't be any less intense, complicated, or difficult to manage moving forward, 2020 will be the year of simplified security. This year, we believe there are seven key security trends to watch, and have provided actionable tips for simplifying your approach to handling each of them:

1) Ransomware Targets the Cloud

Ransomware is now a billion-dollar industry for hackers, and over the last decade we've seen extremely virulent strains of this malware wreak havoc across every industry. As with any big-money industry, ransomware will continue to evolve in order to maximize profits. In 2020, we believe ransomware will focus on the cloud.

Recently, untargeted "shotgun blast" ransomware has plateaued with attackers showing preference for targeted attacks against industries whose businesses cannot function with any downtime. These include healthcare, state and local governments, and industrial control systems.

Despite its far-reaching damages and soaring revenues, ransomware has largely left the cloud untouched. As businesses of every size move both their servers and data to the cloud, it has become a one-stop shop for all of our most important data. In 2020, we expect to see this safe haven crumble as ransomware begins targeting cloud-based assets including file stores, S3 buckets, and virtual environments.

Do you have cloud security? Virtual or cloud UTM? Asking these questions is where to start. Use advanced malware protection to detect evasive malware. More importantly, consider new security paradigms that allow you to implement security controls, like advanced malware protection, in cloud use cases. Finally, the cloud can be secured, but it requires work. Make sure you've hardened your cloud workloads. For instance, investigate resources for properly securing S3 buckets.

2) GDPR Comes to the United States

Two years ago, the General Data Protection Regulation (GDPR) came into force, protecting the data and privacy rights of European Union citizens. As of yet, few places outside the EU have similar laws in place, but we expect to see the United States (U.S.) come closer to matching it in 2020.

GDPR boils down to placing restrictions on how organizations can process personal data, and what rights individuals have in limiting who may access that data, and it has already shown teeth. To date, companies have been fined millions of euros for GDPR violations, including massive €50 million and £99 million judgements in 2019 against Google and Marriott respectively. While the burden placed on companies can be intense, the protections provided to individuals are massively popular.

Meanwhile, the U.S. has suffered a social media privacy plague the last few years, with no real GDPR equivalent to protect local consumers. As organizations like Facebook leak more and more of our personal data, which bad actors have used in everything from targeted election manipulation to unethical bounty hunting, U.S. citizens are starting to clamor for privacy protections like those enjoyed by our European brothers and sisters. So far, only one state, California, has responded by passing their California Consumer Privacy Act (CCPA), which goes in effect in early 2020.

Though the same senator who passed CCPA in California has proposed a Federal Consumer Data Privacy Act (CDPA) bill, we don't think it will gain enough support to pass nationwide in 2020. However, we do expect more and more states to jump onto California's bandwagon, and pass state-level consumer privacy acts of their own. In 2020, we anticipate that 10 or more states will enact similar laws to California's CCPA.

There isn't a specific security tip for this prediction, but you can still take action. Contact your local congressperson to share your opinion on regulations to protect your privacy. Meanwhile, consider the lack of regulation here when sharing your private information online and with social networks.

3) Voter Registration Systems Targeted During the 2020 Elections

Election hacking has been a hot topic ever since the 2016 U.S. elections. Over the last four years, news cycles have covered everything from misinformation spread across social media to alleged breaches of state voter systems. During the 2020 U.S. presidential elections, we predict that external threat actors

will target state and local voter databases with a goal of creating voting havoc and triggering voter fraud-alerts during the 2020 elections.

Security experts have already shown that many of the systems we rely on for voter registration and election day voting suffer from significant digital vulnerabilities. In fact, attackers even probed some of these weaknesses during the 2016 election, stealing voter registration data from various states. While these state-sponsored attackers seemed to draw the line by avoiding altering voting results, we suspect their previous success will embolden them during the 2020 election, and they will target and manipulate our voter registration systems to make it harder for legitimate voters to submit their votes, and to call into question the validity of vote counts.

While there isn't a specific cyber security tip for this prediction, we do have some voter preparedness tips in the event this prediction comes true. First, double-check the status of your voter registration a few days before the election. Also, monitor the news for any updates about voter registration database hacks, and be sure to contact your local state voter authority if you are concerned. Be sure to print out the result of a successful voter registration, and bring you ID on election day, even if technically unnecessary.

4) 25% of All Breaches Will Happen Outside the Perimeter

Mobile device usage and remote employees have been on the rise for several years now. A recent survey by WatchGuard and CITE Research found 90% of mid-market businesses have employees working half their week outside the office. While remote working can increase productivity and reduce burnout, it comes with its own set of security risks. Mobile employees often work without any network perimeter security, missing out on an important part of a layered security defense. Additionally, mobile devices can often mask telltale signs of phishing attacks and other security threats. We predict that in 2020, one quarter of all data breaches will involve telecommuters, mobile devices, and off-premises assets.

Make sure you're as diligent implementing off-network protection for your employees as you are perimeter protection. Any laptop or device that leaves the office needs a full suite of security services, including a local firewall, advanced malware protection, DNS filtering, disk encryption, and multi-factor authentication, among other protections.

5) The Cyber Security Skills Gap Widens

Cyber security, or the lack of it, has gone mainstream. A day doesn't seem to go by where the general public doesn't hear of some new data breach, ransomware attack, company network compromise, or state-sponsored cyber attack. Meanwhile, consumers have also become intimately aware of how their own personal data privacy contributes to their own security (thanks, Facebook). As a result, it's no surprise that the demand for cyber security expertise is at an all-time high.

The problem is, we don't have the skilled professionals to fill this demand. According to the latest studies, almost three million cyber security jobs remained unfilled during 2018. Universities and cyber security trade organizations are not graduating qualified candidates fast enough to fill the demand for new information security employees. Three-fourths of companies claim this shortage in cyber security skills has affected them and lessened their security.

Unfortunately, we don't see this cyber security skills gap lessening in 2020. Demand for skilled cyber security professionals keeps growing, yet we haven't seen any recruiting and educational changes that will increase the supply. Whether it be from a lack of proper formal education courses on cyber security or an aversion to the often-thankless job of working on the frontlines, we predict the cyber security skills gap to increase an additional 15% next year. Let's hope this scarcity of expertise doesn't result in an increase in successful attacks.

While the available cyber security workforce won't appear immediately, you do have options to help create and manage a strong cyber defense. Taking a long-term view, you can work with your local educational institutes to identify future cyber security professionals so that you might fill your open roles first. In the short term, focus on solutions that provide layered security in one solution, or work with a managed services provider (MSP) or managed security services provider (MSSP) to whom you can outsource your security needs.

6) Multi-Factor Authentication (MFA) Becomes Standard for Midsized Companies

We predict that multi-factor authentication (MFA) will become a standard security control for mid-market companies in 2020. Whether it's due to billions of emails and passwords having leaked onto the dark web, or the many database and password compromises online businesses suffer each year, or the fact that users still use silly and insecure passwords, the industry has finally realized that we are terrible at validating online identities.

Previously, MFA solutions were too cumbersome for midmarket organizations, but recently three things have paved the way for pervasive MFA, both SMS one-time password (OTP) and app-based models, among even SMBs. First, MFA solutions have become much simpler with cloud-only options. Second, mobile phones have removed the expensive requirement of hardware tokens, which were cost-prohibitive for mid-market companies. And finally, the deluge of password problems has proven the absolute requirement for a better authentication solution. While SMS OTP is now falling out of favor for legitimate security concerns, app-based MFA is here to stay.

The ease of use both for the end user and the IT administrator managing these MFA tools will finally enable organizations of all sizes to recognize the security benefits of additional authentication factors. That's why we believe enterprise-wide MFA will become a de-facto standard among all midsized companies next year.

This tip is simple – implement MFA throughout your organization. Everything from logging in to your laptop each day to accessing corporate cloud resources should have some sort of multi-factor authentication tied to it. Products like [AuthPoint](#) can do this for your company.

7) Attackers Will Find New Vulnerabilities in the 5G/Wi-Fi Handover to Access the Voice and/or Data of 5G Mobile Phones

The newest cellular standard, 5G, is rolling out across the world and promises big improvements in speed and reliability. Unknown to most people, in large public areas like hotels, shopping centers, and airports, your voice and data information of your cellular-enabled device is communicated to both cell towers and to Wi-Fi access points located throughout these public areas. Large mobile carriers do this to save network bandwidth in high-density areas. Your devices have intelligence built into them to automatically and silently switch between cellular and Wi-Fi. Security researches have exposed some flaws in this cellular-to-Wi-Fi handover process and it's very likely that we will see a large 5G-to-Wi-Fi security vulnerability be exposed in 2020 that could allow attackers to access the voice and/or data of 5G mobile phones.

Most mobile devices don't allow the users to disable cellular to Wi-Fi handover (also known as Hotspot 2.0). Windows 10 currently does, however. If unsure, individuals should utilize a VPN on their cellular devices so that attackers who are eavesdropping on cellular to Wi-Fi connections won't be able to access your data. For businesses looking to enable Hotspot 2.0, make sure your Wi-Fi access points (APs) have been tested independently to stop the six known Wi-Fi threat categories detailed at <http://trustedwirelessenvironment.com>. If the APs block these threats, attackers cannot eavesdrop on the cellular to Wi-Fi handoff.



About the Author

Corey Nachreiner, CTO of [WatchGuard Technologies](#) Recognized as a thought leader in IT security, Nachreiner spearheads WatchGuard's technology vision and direction. Previously, he was the director of strategy and research at WatchGuard. Nachreiner has operated at the frontline of cyber security for 16 years, and for nearly a decade has been evaluating and making accurate predictions about information security trends. As an authority on network security and internationally quoted commentator, Nachreiner's expertise and ability to dissect complex security topics make

him a sought-after speaker at forums such as Gartner, Infosec and RSA. He is also regularly contributes to leading industry publications and delivers WatchGuard's "Daily Security Byte" video [Secplicity](#).



2020 Industry Predictions

By Peter Goldstein, CTO and co-founder, [Valimail](#)

1. Email security will prove to be the weakest link in election security. Email is implicated in more than 90 percent of all cybersecurity attacks, and election infrastructure is also vulnerable to email-based attacks. This means email security must be a priority for thwarting interference with the 2020 presidential election. But research shows the majority of U.S. states are overlooking this vulnerability. Only 5% of email domains associated with local election officials across the U.S. have implemented and enforced DMARC.

DMARC is a widely accepted open standard that ensures only authorized senders can send emails from a particular domain – it's one of the most basic and highly effective means of stopping phishing attacks, which is why the Department of Homeland Security mandated its use for federal agencies in 2017. Yet below the federal level, governments remain vulnerable. In May 2019 we learned Russian hackers breached two county election systems in Florida via a spear-phishing campaign, and in November we learned of a phishing-based ransomware attack on Louisiana during an election cycle.

Because only a tiny percentage of counties and states have DMARC configured at enforcement, email is an easy way in for malicious actors looking to disrupt our elections.

2. Identity validation will be a major challenge across the entire security sector. Most companies think about cybersecurity in terms of encryption, sandboxing, network segmentation, etc., and overlook the core role of identity. In 2019 we saw enterprises and security vendors increasingly wake up to the importance of identity and access management (IAM) as an integral component of enterprise security, and for good reason. But granting access is just one slice of the cybersecurity "identity crisis." Every person, phone, computer, and IoT device has an identity that must be authenticated in order to establish trusted communication. And validating identity is no easy task. Over Labor Day weekend we saw Twitter CEO Jack Dorsey's Twitter account get hacked via SIM swapping (which was most likely initiated by an impersonation of Dorsey himself), and incidents of business email compromise (BEC) attacks and social

media disinformation campaigns executed by bots are all examples of havoc wreaked when identity is not authenticated.

3. Deepfake technology will be leveraged in more cyber attacks. In 2020, we'll see deepfake technologies migrate from proof of concept and occasional attack tool to a more common tactic. Deepfake audio and video can make cyberattacks against individuals and organizations far more sophisticated and convincing, and therefore, more effective. In 2019, a fraudster used AI voice technology to impersonate the CEO of a German company, convincing an employee to transfer more than \$200,000 to the bank of a Hungarian supplier – which was then immediately transferred to another bank in Mexico. It would be foolish to think cyber criminals all over the world didn't take notice of this incident, and start exploring how they too could leverage this type of technology to reap similar payouts (i.e. delivering messages via Google Voice). Scammers will add deepfakes to their toolkits, combining them with already proven successful techniques, such as phone number spoofing and email impersonation, to advance phishing and BEC techniques and propel increasingly targeted attacks. We predict losses from impersonation-based attacks could be in the billions of dollars in 2020, spurred by an increase in the use of deepfake tech.

4. DMARC adoption will grow across industries. We'll see a continued increase in Domain-based Message Authentication, Reporting and Conformance (DMARC) adoption. DMARC is a vendor-neutral authentication protocol that allows email domain owners to protect their domain from spoofing, and the number of domains using it has grown 5x in the last 3 years. We'll see increased growth across several verticals in 2020 - especially healthcare and government. Following the lead of the federal government's civilian branches, the Department of Defense will soon be requiring all of its domains to enforce DMARC, resulting in an increase in the number of military domains protected. H-ISAC, global nonprofit organization serving the health care sector, [has urged](#) health care companies to adopt DMARC as part of best practices for securing email, and as a result we've already seen a rise in adoption rates in this vertical. This growth will continue throughout 2020.

5. Major brands will lead the way with BIMl. Brand Indicators for Message Identification (BIMI) is an email standard that will change the way people interact with their favorite brands via email. BIMI provides a framework through which an organization can provide an authorized logo for display in the recipients' inboxes alongside authenticated email from that organization. We predict BIMI will grow in popularity, especially among large enterprises and prominent brands that rely heavily on the trust and engagement of their customers. In fact, Google will be launching a BIMI pilot in 2020, which will help spur adoption. Research by Verizon Media has shown that BIMI can increase open rates and boost customer engagement, giving marketers a big incentive to support the email authentication that is a prerequisite for BIMI.

6. AMP for email is lifting off in 2020. AMP, a Google-backed technology for accelerating web page load time, will take off in 2020. With AMP for Email, users will have expanded interactive capabilities within email messages, such as scheduling appointments, taking surveys and completing purchases – all without needing to open a browser. Retailers will likely be early adopters of this technology, and we can expect to see personalized emails leveraging previous purchases and items in shopping carts to be used to accelerate purchases and increase customer engagement. Customer satisfaction surveys will

also likely be early use cases of this technology – consumers will receive a short survey after visiting their favorite coffee shop and be able to complete and submit the survey, all within their email.

7. IoT/smart city security will continue to grow as a target for attackers. Securing cities must begin with preventing phishers from gaining access to computers where they could push out commands to IoT devices remotely. There are many challenges with IoT security, least of which is authenticating device-server communications. Additionally, using default passwords and outdated encryption makes these systems easy to hack. In 2019 we read about some annoying and spooky incidents based on IoT hacking – but heading into the new year what we really need to be concerned about is hackers targeting energy grids and other major infrastructure to cause serious economic and social disruption.

8. Use of AI will become more specialized. 2019 saw a lot of enterprises experimenting with artificial intelligence. Many of these experiments led to the realization that it requires a lot of time and expertise to implement AI successfully. In 2020, we will see some of those experiments start to pay off, as enterprises refocus their AI efforts on areas where it saves time and money — such as examining x-rays, automating customer service with chatbots, and simplifying driving via semi-autonomous vehicles. But other AI projects will be abandoned, as it becomes clear that AI is not the most effective approach — such as email security, where AI-powered security systems often miss phishing attacks and BEC scams; and identifying fake news, where AI-powered tools have also missed the mark thus far.



About the Author

Peter is an MIT and Stanford trained technologist who has worked in a variety of software verticals including security, enterprise, email, and video. He has built products and teams at a number of large technology companies such as RSA Security and Perot Systems, as well as at small startups like Tout, Securant, and Swapt.

2020

Balbix 2020 Predictions

By Gaurav Banga, CEO and founder, [Balbix](#)

- 1) In light of the ever growing [cybersecurity skills gap](#), and an exploding attack surface, infosec leaders will shift their focus from increasing headcount to increasing efficiency. By prioritizing tasks based on risk, solving the most impactful issues first, CISOs can ensure that even a small team can have maximum possible impact.
- 2) The accepted definition of a vulnerability will broaden. Typically associated with flaws in software that must be patched, infosec leaders will redefine the term to anything that is open to attack or damage. The impact will be systematic processes, similar to those commonly applied to patching, extended to weak or shared passwords, phishing and social engineering, risk of physical theft, third party vendor risk, and more.
- 3) In recent years, CISOs have gotten much desired access to the board of directors, yet have struggled to speak in a language that resonates. This has limited the value of their exposure to the board, with many struggling to achieve the appropriate backing for their initiatives. In 2020, CISOs will recognize that business leaders will never understand technical security details such as threats and vulnerabilities, and will begin to leverage education and new tools to communicate business risk and economic exposure to the board.
- 4) Unfortunately, poor understanding of the massive enterprise attack surface will continue to be the root cause of much cybersecurity-related frustration and anxiety. Discussions with BoD members and C-suite execs on security posture will still be based on gut instinct and incomplete data. Vulnerability management tools will continue to report 1000s of issues, and BU owners will still

not be able to keep up, leaving thousands of assets unpatched. Senior executives will still fall for phishing attacks, with embarrassing and expensive consequences. Security teams will still not fully understand the risk of breach of sensitive data like intellectual property. CFOs will once again approve bigger security budgets, and the organization will continue to have no idea whether that was money well spent. Infosec leaders will still not be able to tell curious execs whether the company is vulnerable to the next Wannacry. Business unit teams will still surprise the security team with new soon-to-go-live product offerings that just need to be “blessed.” And by the end of 2020, most organizations will still be one bad click, a single reused password, or one unpatched system away from a major cybersecurity incident. The others will use risk-based tools to transform their cybersecurity posture.



About the Author

Gaurav Banga is the Founder and CEO of Balbix, and serves on the boards of several companies. Before Balbix, Gaurav was the Co-founder & CEO of Bromium and led the company from inception for over 5 years. Earlier in his career, he served in various executive roles at Phoenix Technologies and Intellisync Corporation, and was Co-founder and CEO of PDAapps, acquired by Intellisync in 2005. Dr. Banga started his industry career at NetApp. Gaurav has a PhD in CS from Rice University, and a B.Tech. in CS from IIT Delhi. He is a prolific inventor with over 60 patents.



ForgeRock 2020 Predictions

By Eve Maler, Interim CTO, [ForgeRock](#)

1. Healthcare patients will be able to share and redact their data in 2020.

2020 will be the year healthcare IT moves from data privacy 1.0, which focuses primarily on data protection, to data privacy 2.0, which fully includes data transparency and data control. The consumer experience of health plan members will be a huge focus in the coming year, along with building superior experiences in connected health, IoT and patient control of data sharing. In today's digital world, it is essential for organizations to provide consumers with access to a consolidated view of their health-related data, while giving them the ability to leverage their valuable data across multiple platforms.

As consumers move toward both a personalized experience while seeking a real measure of privacy, health providers and plans must go beyond keeping their patients' and members' personal health data safe and provide meaningful options for control. We will see the intersection of healthcare identity management and data security come to a head as providers seek to build trust with members. Providing patients with the ability to share, unshare, and withhold from sharing data will become a reality in 2020.

2. The impact of Open APIs will broaden and deepen in financial services, healthcare, and telco.

What is an Open API? It's a sector-specific set of application programming interfaces designed to enhance security, privacy, consent, data portability, and interoperability, to address regulatory

imperatives and stimulate service provider and app ecosystems for the mutual benefit of people and businesses.

Open APIs in financial services were said to have lost steam; instead, they will globalize in 2020 with a regulatory scope that is now global, including Open Banking in the UK, PSD2 in the EU, the Australian Consumer Data Standards, the US Financial Data Exchange, financial bodies in Japan and Hong Kong, and more. Every region of the world is seeking to benefit and is cycling fast on the latest standards.

The Fast Healthcare Interoperability Resources (FHIR) API has been around for a longer time than Open Banking, but adoption is only now truly accelerating. With healthcare spending accounting for [18% of US GDP](#) and with payers under pressure to manage costs along with all ecosystem participants urged to open up [data access](#), it will be the next industry to take advantage of Open APIs in 2020. Adopting Open APIs enables offering more consumer journeys, such as smartphone access to and sharing of health data, at lower cost and with greater security and privacy because elements such as consent, encryption, and stronger authentication can be required or built in so that they work cross-system.

3. Tech giants will start to be regulated as “dark patterns” in 2020.

In 2020, governments are going to continue to put pressure on the tech giants, which will respond by trying to self-regulate to overcome increasing laws that threaten their business models. The privacy hits are going to continue for social and tech giants and they are going to continue to prove that they don't deserve consumers' trust.

In 2019, Facebook received a \$5B fine for prior violations of user privacy. [The Federal Trade Commission and the Department of Justice](#) are already investigating Facebook as part of a broader federal review of tech giants and leaning towards more robust action this time around. A unified federal-level push to regulate privacy is coming, essentially a U.S.-wide version of the Digital Single Market goal of GDPR, extending outward from the California Consumer Privacy Act (CCPA).

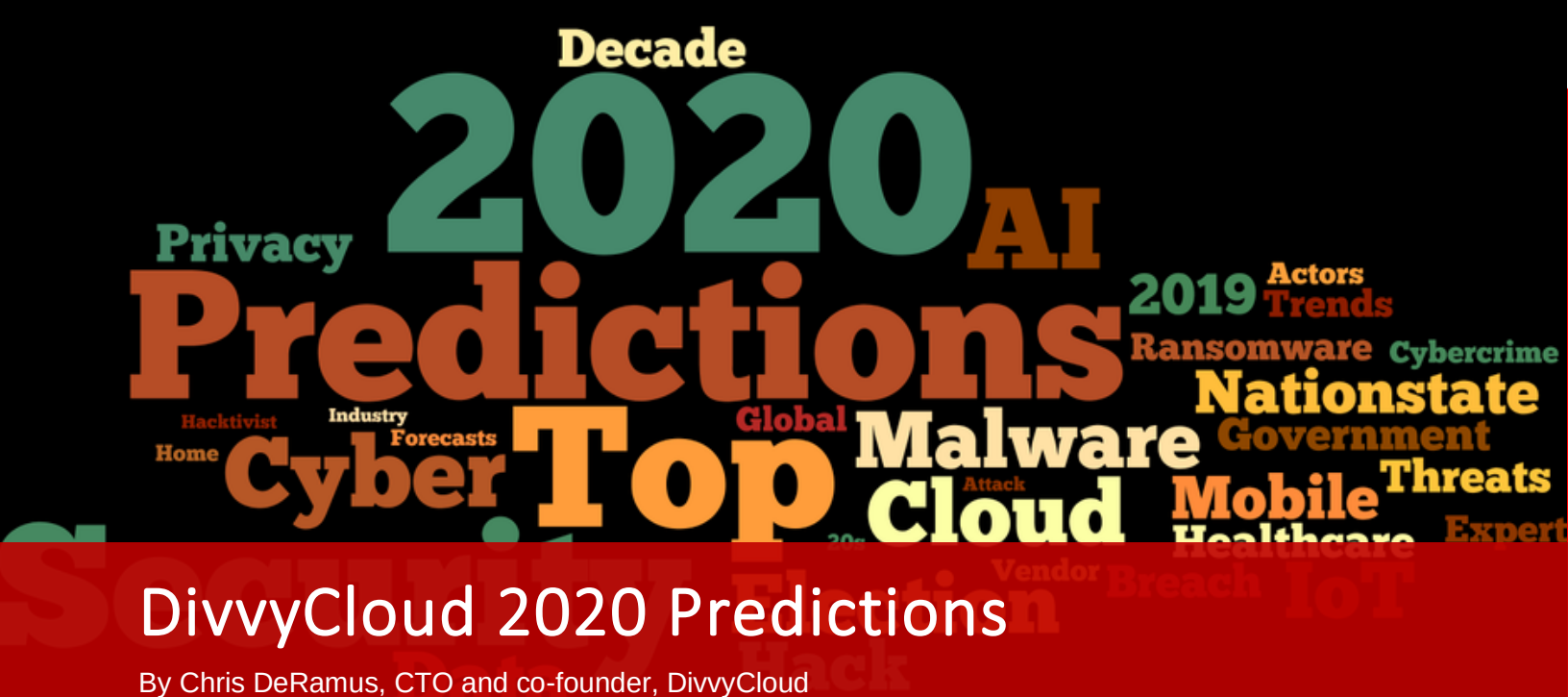
The big social networks have more to fear than privacy laws. Greater attention will be paid to [dark patterns](#) in 2020, which will encourage legislators and regulators likewise to pay broader attention to antitrust and consumer protection threats. Consumers will not leave their social networks in 2020, but we'll see increased consumer protection laws as a result.



About the Author

[Eve Maler](#) is ForgeRock's Interim CTO. She is a globally recognized strategist, innovator, and communicator on digital identity, security, privacy, and consent, with a focus on fostering successful ecosystems and individual empowerment. She founded and leads the [User-](#)

[Managed Access](#) (UMA) standards effort and provides expert advice to forums such as [Open Banking](#). Previously Eve co-invented the [SAML](#) and [XML](#) standards.



DivvyCloud 2020 Predictions

By Chris DeRamus, CTO and co-founder, DivvyCloud

1. **Cloud misconfigurations will continue to cause massive data breaches.** As enterprises continue to adopt cloud services across multiple cloud service providers in 2020, we will see a slew of data breaches caused by misconfigurations. Due to the pressure to go big and go fast, developers often bypass security in the name of innovation. All too often this leads to data exposure on a massive scale such as the [First American Financial Corporation's breach](#) of over 885 million mortgage records in May. Companies believe they are faced with a lose-lose choice: either innovate in the cloud and accept the risk of suffering a data breach, or play it safe with existing on-premise infrastructure and lose out to more agile and modern competitors. In reality, companies can accelerate innovation without loss of control in the cloud. They can do this by leveraging automated security tools that give organizations the ability to detect misconfigurations and alert the appropriate personnel to correct the issue, or even trigger automated remediation in real-time. Automation also grants enterprises the ability to enforce policy, provide governance, impose compliance, and provide a framework for the processes everyone in the organization should follow—all on a continuous, consistent basis. Companies can innovate while maintaining security, they simply must adopt the proper cloud strategies and solutions.
2. **New Year, New Threats.** As companies continue to invest in new technology, we will see the introduction of new and advanced tactics, techniques, and procedures from malicious third-parties that seek to either exfiltrate critical customer, company, and partner data or even interrupt or disable business operations. Companies often make the costly assumption that they will be safe from threats just by investing in additional security tools for every new technology or service that they adopt. This piecemeal approach to security is both extremely expensive and inefficient. In fact, since we don't know what the most pertinent threats will be in a year from now, the best approach is for companies to invest in holistic security solutions that can evolve and scale with a company over time.

3. **IAM is the new perimeter, and it is harder than you think.** Everything in the cloud has an identity, and the relationships are complex, so scoping to least privilege or adopting zero trust sounds great, but is really difficult to do. In 2020, security professionals are going to realize that identity and access management (IAM) is an area where they can lose control rapidly, and it is very hard to take back. Approaches and strategies from the datacenter world don't transfer, and companies need to rapidly invest in the process and in supporting tools (including automation) to stay ahead in this complex landscape. The repercussions of poor IAM governance are substantial and sometimes unpredictable. For example, a former AWS employee was able to access [over 100 million Capital One customers'](#) records by bypassing a misconfigured web application firewall, performing privilege escalation and as a result, obtained access to a swathe of customer information.
4. **There will be increased caution around M&A deals.** Learning from the mistakes of Marriott, companies going through M&A deals in 2020 will prioritize comprehensive evaluations of cybersecurity and risk. Before Marriott acquired Starwood in 2016, it was reported that [Starwood suffered a breach of North American customers' credit and debit card data](#) after threat actors implanted malware on the company's point-of-sale registers. Eventually, Marriott became aware of its breach of about 383 million Starwood guests' data when a security tool flagged a database query from an unauthorized user whom had admin privileges. The company later found out that the intrusion went undetected for four years before Marriott even acquired Starwood, however, Marriott still had to pay more than \$120 million to the UK's Information Commissioner's Office (ICO) for violating GDPR, and the hotel giant can even face additional punishments from other data privacy mandates, including the soon-to-be-enforced CCPA. While M&A is an important part of many companies' growth plans, organizations will become increasingly wary of suffering a similar fate as Marriott. In 2020, organizations will place cloud security at the forefront of the M&A process including thorough audits of how the acquisition or merger target is operating cloud services. In a multi-cloud world, companies will need solutions that provide complete visibility across all clouds and cloud services, and an approach to bringing these into their security and compliance posture via automation.
5. **Federal data privacy law on the horizon.** With the enactment of CCPA and the introduction of [additional ideas for state-regulated data privacy laws](#) across the U.S., all roads point towards the creation of a federal data privacy law. It is highly unlikely that a federal law will be passed in 2020, but it will be likely that Congress prioritizes the idea and begins discussing criteria for such a law. A patchwork of slightly differing data privacy laws in each state would discourage businesses (especially SMBs) from operating across state borders. Multiple, varying data privacy laws is a thorn in the side for large companies, but devastating for SMBs, and is a turn off for international corporations that have to comply with other mandates such as GDPR as well. CEOs of Amazon, AT&T, Dell, IBM and other companies that comprise the Business Roundtable have already sent an open-letter to Congress asking for a federal data privacy law, and the Internet Association, which boasts Dropbox, Facebook, Reddit, Snap and Uber as members, has also [made a push toward a federal law](#).



About the Author

Chris DeRamus is the co-founder and CTO of DivvyCloud where he leads product development and the technology team. He is dedicated to building the most robust, scalable, high-quality software possible to meet DivvyCloud's customers' demanding requirements. Before co-founding DivvyCloud, Chris was the online operations manager at Electronic Arts for the Mythic Studio where he helped design, build and operate large scale cloud infrastructure spanning public and private clouds to run Electronic Art's largest online games



ForgeRock 2020 Predictions

By Ben Goodman, SVP at [ForgeRock](#) and CISSP

1. **2020 Will be the Beginning of the End of Passwords.**

Consumers already log in to dozens of protected resources everyday: from email, banking and financial accounts, social media, healthcare, government accounts, and beyond. Even when tools like TouchID are leveraged each of these resources currently still have an associated username and password that can be attacked. To save time and remember their credentials for all these sites, consumers reuse the same username and password across several sites. As a result, the user's exposure from any one security breach on one of those profiles dramatically increases the odds that additional accounts can be compromised as well, allowing attackers to access far more sensitive information.

Users can also put their employer at risk of being breached if they use the same login credentials across personal and professional accounts. Organizations have reacted to this risk by increasing their password policies and requiring more and diversified characters, as well as more frequent password changes; however, this still allows users to reuse usernames and passwords across different accounts.

To eliminate this issue, passwordless authentication methods, such as using out-of-band steps on smartphones that leverage push notifications, will become widely adopted. In fact, [Gartner estimates](#) that 60% of large and global enterprises, as well as 90% of midsize organizations, will leverage passwordless methods in over 50% of use cases by 2022. Companies that properly implement passwordless authentication will not only be more secure, but they subsequently improve the overall user experience by reducing friction in the login process.

2. Unified, third-party identity providers become the gold standard to streamline and secure the user experience.

Consumers already validate their identities by leveraging single sign-on (SSO) and registration with Facebook, Google, Apple and more. However, similarly to how a NASCAR car is covered with logos, the practice of using too many third-party identity providers creates a “NASCAR” condition which can hinder the user experience. The truth is that with even more market entrants coming in 2020 none of these providers will likely get enough critical mass in order to be recognized as the de facto provider for all US consumers.

To combat this problem, the U.S. will balance the need for security with the importance of a seamless user experience. The U.K. Postal Service currently uses [Digidentity](#) as a method for consumers to quickly and securely obtain access to postal services, and it would not be surprising to see similar concepts take off in the US.

The benefits of leveraging digital identity speak for themselves, as a [recent Deloitte Insights article referenced](#) how:

- [Nigeria saved \\$1 billion](#) on civil service staff by using digital identity and removing 62,000 ghost workers.
- [24 of the 28 European Union member countries](#) that have implemented the Once-Only initiative are [expected to save](#) nearly 855,000 hours for their citizens and 11 billion euros for businesses annually.
- [Estonia's use of digital signatures](#) saved the country 2% in annual gross domestic product (GDP).

3. By assigning identities to connected things to secure and manage them, they will become first-class citizens in 2020.

To reduce IoT security incidents, device providers will cease to prioritize connectivity over security in their projects. In fact, security will be integrated at an earlier phase of the development cycle, and devices will have identities assigned to them from square one in order to effectively and efficiently secure and manage them.

Recently, [it was reported](#) that hackers have created dedicated software for breaking into Amazon Ring's security cameras, and there have already been successful attacks in Florida and Tennessee. To get IoT security right, companies must be secure at multiple levels: the transportation of data, access to that data and access to connected devices. As a result, organizations will define unique and secure identities for the devices they are trying to secure and manage. This can be done by working with vendors that understand the identity and access management (IAM) issues companies will be dealing with.

4. **There will be an AI arms race to defeat deepfakes and other counterfeit media.**

The [heinous use of AI](#) to create convincing deepfake videos is becoming more publicly known, and they represent a massive threat with potential to spread misinformation and slander individuals on a grand scale. The industry will respond to this threat by fighting fire with fire, and using AI ethically to discern whether a video is a deepfake or legitimate.

For the most part, individuals that are public figures, such as politicians and celebrities, will be targeted by threat actors with deepfake campaigns as there are usually plethoras of content available to aid with modeling the movements, speech and appearance displayed in these videos.

However, the AI for the “Good Guys” can get an advantage in combating these convincing videos and content via the intersection of three techniques: implementing behavioral biometrics that look at unconscious actions of users to transparently authenticate users and their content, leveraging digital identity to help create a subset of real, validated and tamper-evident content, and considering whether that content is digitally signed by the individual displayed or not. These capabilities will allow good AI to apply a certainty score to a piece of content to display the chances of whether it is legitimate or not.

With this AI arms race, ethical uses of AI will have an advantage by leveraging digital identity as its secret weapon.



About the Author

Ben Goodman is a CISSP and the senior vice president of global business and corporate development at ForgeRock. He has over 20 years of experience in the sale, design and implementation of IT. Prior to joining ForgeRock, Goodman was the lead evangelist of VMware end-user computing for VMware.



Bitglass 2020 Predictions

By Anurag Kahol, CTO and co-founder, [Bitglass](#)

1. We will see an increase in the number of M&A deals in 2020. In fact, 79 percent of respondents to [Deloitte's M&A trends 2019 report](#) expect the number of deals they close to rise in the next 12 months – up from 70 percent last year. Consequently, companies need to learn from the headaches faced by [Marriott in 2018 when it acquired Starwood and inherited a breach of guest data](#). Security needs to be a key component of any M&A strategy. If companies lack solutions that provide adequate visibility into their own systems as well as those of the companies that they are acquiring, we will see similar breaches take place in 2020.
2. Ambiguity around CCPA will cause a slow start to enforcement in early 2020; this is made more likely by the fact that [several groups are still suggesting changes to the original version of](#) the regulation. In other words, California legislators are not prepared to adequately and consistently enforce the new law. Additionally, many businesses are still unsure about its specific requirements, and are not ready to be in compliance when the regulation goes into effect in January. This is particularly true of small and medium sized businesses that don't have the same amount of resources as larger corporations – it is more challenging for them to discern what they need to do in order to be in compliance. As a result, we will most likely need to wait some extended period of time before we see the first significant fine under the new law; much like GDPR. In fact, it took nearly a year for British Airways to be fined \$250 million under GDPR – its breach was reported in [September 2018](#) and the company was not fined until [July 2019](#). Similarly, once the initial lull period that will follow the enactment of CCPA comes to a close, we will see similar, significant fines being given to companies that fail to meet the requirements demanded by the new law.
3. In 2020, we will see a U.S. federal data privacy law be drafted and considered. This is needed to avoid a patchwork of differing data privacy laws from each state, to facilitate more nationwide

business, and to enable international commerce – facing numerous regulations can be a barrier that keeps foreign businesses from entering a market. Complying with data privacy laws can be a top challenge, particularly for small and medium-sized businesses that lack the same resources as larger companies that are better equipped to navigate all of the regulations with which they are faced. [Some of the largest tech firms in the U.S.](#) as well as a [group of 51 CEOs](#) have already asked U.S. lawmakers for a federal privacy law.

4. Threat actors are always enhancing their current tactics, techniques, and procedures (TTPs) as well as creating new ones in order to infiltrate businesses and steal data, implant ransomware, and more. One technique that will continue to gain traction in 2020 is lateral phishing. This scheme involves a threat actor launching a phishing attack from a corporate email address that was already previously compromised. Even the savviest security-minded folks can be lulled into a false sense of security when they receive an email asking for sensitive information from an internal source – particularly from a C-level executive. As we will continue to see cybercriminals refining their attack methods in 2020, companies must be prepared.
5. Misconfigurations of cloud databases will continue to plague enterprises around the world and will be a leading cause of data breaches in 2020. [Gartner forecasts](#) that global public cloud revenue will reach \$249.8 billion in 2020, a 16.6% increase from 2019. This rapid rise in revenue is spurred by continued growth in cloud adoption. However, cloud adoption is clearly outpacing the adoption of the tools and expertise needed to properly protect data in cloud environments; this is supported by the fact that 99% of cloud security failures will be the customer's fault through 2025, [according to Gartner](#). Consequently, misconfigurations will continue to be a leading cause of data leakage across all verticals.

In addition to the above, highly niche cloud tools provided by second-tier cloud service providers are making their way into enterprises. While services that cater specifically to individual industries or company departments are gaining traction, they do not typically have the same native security measures that mainstream cloud services do. Regardless, companies are gaining confidence - even if it's a false sense of confidence - in their ability to utilize the cloud and are adopting these second-tier and long-tail cloud apps without considering all of the security ramifications. Enterprises will need visibility and control into all of their cloud footprint, including niche services, in order to proactively mitigate any vulnerabilities and properly secure data in the cloud.

6. Foreign meddling will occur in the 2020 presidential election. The [Mueller Report found that Russians have and will continue](#) to interfere in U.S. elections (which is backed by the [Senate](#)

[Intelligence Committee's findings](#)), while [Twitter has already shut down](#) thousands of Iranian-backed disinformation accounts. It has also been [proven](#) that voting machines contain security flaws from decades ago, but that we've run out of time to find and correct the bugs in these machines before the 2020 election. Due to foreign interference, the hacking of voter registration databases, and the exploitation of flaws in voting machines, there will be even more controversy and concern over the integrity of the 2020 election than there was in 2016. However, this widespread concern should serve as a catalyst for change moving forward – even if it's too late to make these changes for 2020. There is simply too much at stake to neglect these issues indefinitely. Voters, legislators, and tech providers will need to come together to ensure greater cybersecurity throughout election processes – thereby strengthening the integrity of our democratic system.



About the Author

Anurag Kahol is the CTO and co-founder of Bitglass. His mission is to expedite the technology direction and architecture of Bitglass. Prior to co-founding Bitglass, Kahol served as the director of engineering in Juniper Networks' security business unit. He received a global education, earning an M.S. in computer science from Colorado State University, and a B.S. in computer science from the Motilal Nehru National Institute Of Technology.



AttackIQ 2020 Predictions

By Christopher Kennedy, CISO and VP of Customer Success, AttackIQ

- 1) **2020 Election Security Insecurity:** Election security will be an open wound that can't be healed in time for the 2020 election. There is still bad blood from the 2016 election which has created a social distrust of technology and there is not enough time to strengthen the integrity of the election system in such a way that the electorate can be confident in the outcome. This begs the question, will there be public faith and acceptance of the outcome of the 2020 election, and if not, what will happen? Public concern will serve as a springboard for the federal government as well as state/county election officials to enact real change and significant improvements to cybersecurity of election infrastructure before the 2024 election.
- 2) **Fight The Power Against Technology:** We are just beginning to recognize the social dangers of rapidly-advancing and broadly-used technology in a highly connected society. Take new biometric technologies, as just one example. Advanced facial recognition capabilities are being used by governments around the world, and in response, consumers have begun to revolt by creating and donning an "opt out" cap that obstructs the wearer from being identified by facial recognition scanners to avoid physical tracking. In 2020 we'll see a continued rejectionist movement, particularly among young people; further exploitation of various technologies; and a growing trend of avoiding social media. We will witness a strong movement of distrusting the government's use of technology in the processes that put them in power, and in services intended to protect and support the public.
- 3) **Defense Wins Championships:** New unfolding laws like the [Hack Back Bill](#) allow organizations to take a more proactive and near-offensive strategy in their incident response and defensive approaches. However, companies need to be careful to strike a delicate balance in investing in hack back techniques and understand there is unproven case law and legal ambiguity surrounding this approach. Companies must be aware of the full implications of this complicated bill and understand that having the right security policies, programs and tools in place to properly protect data is still the best line of defense. As Paul Bear Bryant says, "defense wins championships." It is more important to have a thorough and measured security program in place

that adequately protects your organization than it is to take advantage of now-potentially-legal offensive security concepts.

- 4) **The Emergence Of MITRE ATT&CK:** As cybercriminals are always evolving and creating new attack methods, organizations will be at even greater risk in 2020. To keep up with new threats, MITRE ATT&CK will emerge as one of the most beneficial tools for organizations as it allows them to predict the next steps of an attack based on known threats and focus resources on thwarting specific phases of a likely attack. MITRE ATT&CK also recently partnered with several enterprises to create the Center for Threat-Informed Defense, a research group dedicated to advancing a shared understanding of adversary behavior. No one can predict what new attack methods will come in 2020, but companies will increasingly lean heavily on the MITRE ATT&CK framework to inform their cybersecurity programs and identify gaps in coverage or configurations in need of remediation.
- 5) **Keep Your Coins, We Want Change:** In 2019, over 50 tech CEOs [came together](#) urging U.S. lawmakers to create a federal data privacy legislation. Why? Because of the continued regulatory sprawl across international, national and state standards. Managing cybersecurity should not be as complicated as adhering to the IRS tax code. Breaches continue to be a pervasive problem, and the complexities of applying various and overlapping regulations in a globally-connected world are not helping. To this end, we'll see some consolidation of regulatory requirements and standards in 2020.
- 6) **More Money Doesn't Mean Less Problems:** Enterprise spending on cybersecurity will reach an all-time high in 2020. Today, companies spend [an average](#) of \$18.4M on cybersecurity each year, and 58% plan on increasing their IT security budget in 2020. This increased spending is due to emerging cybersecurity threats, the need to support enterprise technical transformation, and C-suite and boards becoming more involved in their company's cybersecurity strategy. What's truly alarming is that 53% of IT experts admit they don't know how well the cybersecurity tools they've deployed are working. Enterprises must have full visibility into their environments and be able to identify if tools are working as expected, if there are gaps and if any tools overlap or are misconfigured. British Airways and Marriot are both examples of why having visibility at all times is important with the companies receiving hefty fines of \$230 million and \$123 million, respectively for their data breaches. While cybersecurity insurance can help, it is not always enough. Companies should invest in a programmatic approach that includes automation which continues to validate that security is working as expected, at all times.
- 7) **Rise of Mid-tier MSSPs:** In 2020, we will see a rise of the mid-tier MSSPs, as they are more focused on identifying the best tools to address specific cybersecurity challenges. The big channel partners on the other hand, are too focused on chasing money associated the sale of large, legacy providers that claim to "do it all." Enterprises are increasingly frustrated with this approach and prefer partners with expertise on the latest, most effective security practices and solutions.



About the Author

Chris Kennedy is the CISO and vice president of customer success at AttackIQ. Kennedy joined AttackIQ from Bridgewater Associates where he was head of security for infrastructure technology and controls engineering and brings more than 20 years of cybersecurity risk and operations practitioner experience. Previously, Kennedy led the development of the U.S. Department of Treasury's and the U.S. Marine Corps' Cybersecurity Operations Programs, defense and

federal contracting for Northrop Grumman, and is a former Marine Corps Officer and Operation Iraqi Freedom veteran.

AttackIQ Report On Ponemon Survey: Despite Spending An Average Of \$18.4 Million On Cybersecurity Solutions, Organizations Still Get Breached

Enterprises plan on increasing their security budgets in the next year too. However, the key to preventing breaches relies upon accurately identifying and remediating gaps in current security defenses.

By Stephan Chenette, co-founder and CTO, AttackIQ

Based on a survey of 577 IT and IT security practitioners in the United States from the Ponemon Institute, AttackIQ has released a new report, [The Cybersecurity Illusion: The Emperor Has No Clothes](#). The report's title is inspired by Hans Christian Andersen's short tale, [The Emperor's New Clothes](#), since the findings demonstrate many IT professionals simply don't know whether the security tools they have in place are actually effective. Findings also show that enterprises across industries are spending an annual average of \$18.4 million to support cybersecurity efforts, yet data breaches persist. In fact, there were reportedly 110 total breaches affecting organizations across all industries in July 2019 alone that exposed over 104.5 million records, according to [findings from the Identity Theft Resource Center](#). Much like the emperor in Andersen's tale, companies are willing to spend top dollar on advanced security solutions, but don't have visibility into them, leaving them "naked" and vulnerable to breaches.

Enterprises spend far too much money on an average of 47 different cybersecurity solutions without knowing if they are effective. In fact, 58 percent of organizations plan to increase the budget allocated toward cybersecurity by an average of 14 percent in the next year even though over half of the experts surveyed admit they are in the dark about how well the technologies they have are working, which is disturbing considering these organizations rely on these solutions to protect sensitive data including customers' personally identifiable information (PII).

Organizations must be certain their security measures can effectively prevent critical infrastructure disruption. In order for enterprises to prevent data breaches, they must be able to accurately identify and

remediate gaps in their security defenses. This is best accomplished by leveraging continuous security validation (CSV) platforms. With CSV technologies, enterprises can identify gaps, protection failures like misconfigurations, and validate the capabilities of current security solutions they employ are actually working as intended.

Premier CSV platforms operationalize the industry standard MITRE ATT&CK framework to systematically test the efficacy of companies' security programs. MITRE ATT&CK is a globally-accessible knowledge base of threat actor tactics, techniques and procedures (TTPs) that have been assembled for use as a foundation for the development of specific threat models.

In addition, CSV technologies help consolidate and streamline security technologies within a security program by finding redundant technologies. CSV helps optimize each technology to make sure a security program is operating at its highest potential, providing visibility and helping strategic leaders a decision framework. By taking the guesswork out of measuring the effectiveness of their cybersecurity strategy, enterprises can save money, maximize ROI from their security tools and gain peace of mind that they are, in fact, protected.



About the Author

Stephan Chenette is the Founder and CTO of AttackIQ. Chenette is a 20 year information security veteran, servicing clients that range from startups to multinational corporations as a pentester, security and risk consultant, solutions architect and head of research and development. Chenette has presented at numerous conferences

including RSA, Blackhat, ToorCon, BSides, CanSecWest, RECon, AusCERT, SecTor, SOURCE and PacSec.



Data Privacy in A Device-Driven World: Navigating the Impact Of California's 2020 IoT Security Legislation

A call for consumer education on device security vulnerabilities in light of the increasing push for IoT security regulation

By Brian Murray

Throughout the past few decades, the Internet of Things and connected devices have become more and more ingrained in our everyday lives at an increasingly rapid pace. Concurrently, these smart devices, which hold massive amounts of our private data, have become synonymous with vulnerability.

While the notion that IoT devices are susceptible to security threats and attacks is nothing new within the cybersecurity industry, government regulation, such as California's SB-327 which is set to start on January 1, 2020, consumers are starting to take notice.

Yet, after 30+ years of rapid IoT growth, the question remains: Is smart device security regulation too little, too late?

IoT devices have fundamentally shifted the way consumers live, work and play. Consumers of all ages are empowered by the endless possibilities that a simple touch of a button or swipe of their finger can grant them access to. It has created what many believe to be a modern-day Pandora's Box situation. What has been perceived to be an evolution of technological advancements to streamline every day activities have opened the flood gates personal data to be digitally downloaded by criminals throughout the globe.

At the core of the matter rests the fact that many IoT device vendors had, at best, subpar background in building internet-connected devices. Their expertise was rooted in constructing devices to be functional, not necessarily secure—and hackers took note.

The year-over-year reports show that the number of [IoT threats](#) have nearly doubled with weak or default credentials and unpatched vulnerabilities driving the majority of observed threats. What's more, the

[American Consumer Institute](#) found that more than 80 percent of home and office routers were vulnerable to hacking.

This uptick may be the result of more sophisticated hackers. It could also be consumers' lack of ability to make security assessments on their own when purchasing devices, leading to a greater proliferation of insecure routers and digital recording devices. Some believe the rise in IoT attacks are the result of undocumented standards for common security issues to serve as a guiding principle for manufacturers lacking the capital funding such as Google and Amazon, who have been able to advance their smart home devices as a result.

Regardless of the reason, change is on the horizon.

Regulation: Hindsight in 2020

At the start of the new year, the state of California's SB-327 Information privacy: connected devices went into effect with the intent to eliminate a common security vulnerability among IoT devices. Under this law, each device manufactured in the state must be equipped with a unique password.

History has shown that many IoT threats—most notably, those born from the Mirai malware's leaked source code—target default and known passwords. While the effectiveness of SB-327 is not yet known, it has been championed as a solution for this decade's old headache of leveraging default or weak credentials.

However, it has also created further confusion among cybersecurity experts and manufacturers alike with its vague language of "reasonable security features" for "any device, or other physical object that's capable of connecting to the internet, directly or indirectly." The ambiguity of the law leaves room for interpretation that can vary from entity-to-entity and can make enforcing this law a challenge across the board. It can also make compliance a moving target for manufacturers saddled with navigating the implementation and adoption of the law.

The true impact of SB-327 is bound to take time and its success hinges on deep collaboration and open communication across all parties. The hope is that in hindsight, 2020 will prove to be a teaching milestone for how to better equip consumers with the knowledge to secure their data on all IoT devices.

Smart Education

It has been said that great power can come from simply being more informed. Cybersecurity professionals have a duty to consumer to keep them informed and educated to make intelligent decisions about their smart devices used in their homes and offices.

For example, routers pose a significant threat to consumers, and should be an IoT device that is heavily researched prior to purchasing. The router is the gatekeeper for all information, including passwords, emails and credit card information, coming in and out of your home or business. As such, it is critical

consumers understand ways to safeguard their routers, including updating the firmware and turning on automatic updates.

More so than legislation regulating manufacturers, IoT device vendors and cybersecurity experts should plan to place a greater emphasis on arming consumers with a portal of information that not only makes understanding IoT security easy, but makes implementing security procedures seamless.

For years, IoT devices were left hanging in the balance open to ongoing threats and attacks before talks of standardized processes and procedures were ever broached. As the line between IoT devices and devices used to get online increasingly blur together, educating consumers on securing IoT devices is not just a *nice to have* piece of information, it is a *need to know* piece of information, and it is up to cybersecurity industry leaders, experts, and professionals to help guide the way.



About the Author

Brian Murray is Leader North America Operator Business for F-Secure, a global cybersecurity firm driving innovations in the industry with experience in endpoint protection as well as detection and response. Brian can be reached at

brian.murray@f-secure.com.



Conquering the Cyber Security Challenges of The Cloud

By Steve Durbin, Managing Director, [Information Security Forum](#)

Cloud computing has become a prevalent force, bringing economies of scale and breakthrough technological advances to modern organizations, but it is more than just a trend. Cloud computing has evolved at an incredible speed and, in many organizations, is now entwined with the complex technological landscape that supports critical daily operations.

This ever-expanding cloud environment gives rise to new types of risk. Business and security leaders already face many challenges in protecting their existing IT environment. They must now also find ways to securely use multiple cloud services, supported applications and underlying technical infrastructure.

The Need to Use Cloud Services Securely

The surge in business processes supported by cloud services has been well evidenced by organizations using cloud services store confidential data in the cloud environment. But when using cloud services, organizations are still unsure whether to entrust cloud service providers (CSPs) with their data. CSPs generally provide a certain level of security as substantiated by multiple surveys, but cloud-related security incidents do occur.

CSPs cannot be solely responsible for the security of their customers' critical information assets. Cloud security relies equally on the customer's ability to implement the right level of information security controls. Nevertheless, the cloud environment is complex and diverse, which hinders a consistent approach to deploying and maintaining core security controls. It is vital that organizations are aware of and fulfill their share of the responsibility for securing cloud services to successfully address the cyber threats that increasingly target the cloud environment.

The Rise of the Multi-Cloud Environment

As organizations acquire new cloud services, they typically choose these from a selection of multiple CSPs and therefore need to deal with a multi-cloud environment, which is characterized using two or more CSPs.

Organizations favor a multi-cloud environment because it allows them to pick and choose their preferred cloud services across different CSPs (e.g. AWS, Microsoft Azure, Google Cloud, Salesforce). However, each individual CSP adopts its own jargon, its own specific technologies and approaches to security management. The cloud customer therefore needs to acquire a wide range of skills and knowledge to use different cloud services from multiple CSPs securely.

Organizations require a range of different users to securely access cloud services from within the organization's network perimeter through secure network connections (e.g. via a gateway). However, organizations also need their cloud services to be accessed from outside the internal perimeter by business partners and users travelling off-site or working remotely, all connecting through a selection of secure network connections as dictated by the organization.

Overcoming Cloud Security Challenges

While CSPs provide a certain level of security for their cloud services, organizations need to be aware of their security obligations and deploy the necessary security controls. This requires organizations to understand and address the many security challenges presented by the complex and heterogeneous aspects of the cloud environment.

Our ISF members have identified several obstacles to operating securely in the cloud environment. The main challenges include:

- Identifying and maintaining the appropriate security controls
- Balancing the shared responsibility for security between the CSP and the cloud customer
- Meeting regulatory requirements to protect sensitive data in the cloud environment

The rapid explosion of cloud usage has accentuated these challenges and, in some instances, left organizations insufficiently prepared to tackle the security concerns associated with using cloud services.

Balancing the Shared Responsibility for Security Between the CSP and the Cloud Customer

Securing the use of cloud services is a shared responsibility between the CSP and the cloud customer. The security obligations incumbent on the CSP are to protect the multi-tenant cloud environment, including the backend services and physical infrastructure, as well as to prevent the commingling of data between different customers.

While the CSP maintains much of the underlying cloud infrastructure, the cloud customer is responsible for securing its data and user management. Whether the customer's responsibility extends to performing security configurations for applications, operating systems and networking will depend on the cloud service model selected.

This shared responsibility for security can create confusion and lead to over-reliance on the CSP to mitigate threats and prevent security incidents. It is essential that the cloud customer does not depend wholly on the CSP to deploy the appropriate security measures, but clearly understands how responsibility for security is shared with each CSP in order to identify and deploy the requisite security controls to protect the cloud environment.

Meeting Regulatory Requirements to Protect Sensitive Data in the Cloud Environment

An organization using an on-premises IT data center will know exactly where its critical and sensitive data resides and can exert full control over the movement of its data. This helps considerably when implementing security controls, whereas in the cloud environment, data moves in and out of an organization's perimeter more freely. This can obscure where critical and sensitive data is located, and how it can be protected, which can hinder an organization's ability to effectively enforce the requisite security controls across all of its cloud services in line with compliance requirements.

While it is the cloud customer's responsibility to ensure the security of its data in the cloud environment, the customer's control over its data is intrinsically limited since the data is stored by an external party – the CSP – in an off-site location, often in a different country. Moreover, the CSPs will often leverage several data centers in geographically distinct locations to ensure the organization's data is stored on more than one server for reasons of resilience. This creates additional complexity in terms of managing data across borders, understanding where it is located at a given moment in time, determining the applicable legal jurisdiction and ensuring compliance with relevant laws and regulations – an obligation that rests fully with the cloud customer, not the CSP.

Maximize Potential and Take Responsibility

Modern organizations must operate at a fast pace, delivering new products and services to stay ahead of the competition. Many are therefore choosing to move ever further towards cloud computing, as the elasticity and scalability offered by cloud services provide the desired flexibility needed to compete. For an organization to have confidence that it can move to the cloud whilst ensuring that vital technological infrastructure is secure, a robust strategy is required.

The cloud environment has become an attractive target for cyber attackers, highlighting the pressing need for organizations to enhance their existing security practices. Yet consistently implementing the fundamentals of cloud security can be a complicated task due to the diverse and expanding nature of the cloud environment.

This is but one of many challenges that organizations need to overcome to use cloud services securely. Organizations cannot rely purely on CSPs to secure their critical information assets but must accept their own share of responsibility. This responsibility calls for a combination of good governance, deployment of core controls and adoption of effective security products and services. Controls that cover network security, access management, data protection, secure configuration and security monitoring are not new to information security practitioners, but they are critical to using cloud services securely.

Moving forward, organizations can select from a variety of trends and technologies that will enable them to use cloud services securely – from the adoption of new products to the embedding of improved processes, such as a focus on secure containers, where security is given greater emphasis during development.

Assuring that services are used securely will provide business leaders with the confidence they need to fully embrace the cloud, maximizing its potential and driving the organization forward into the future.



About the Author

Steve Durbin is Managing Director of the [Information Security Forum](https://www.securityforum.org) (ISF). His main areas of focus include strategy, information technology, cyber security, digitalization and the emerging security threat landscape across both the corporate and personal environments. Previously, he was senior vice president at Gartner.

Steve can be reached online at (@stevedurbin) and at our company

website www.securityforum.org



How to Address Multi-Cloud Security

By William Klusovsky, CISSP, CISM

NTT Ltd.

Networks for our businesses are not as simple as they used to be. With the evolution of cloud environments and the multitude of “everything ‘as a service’” offerings, we are faced with a gauntlet of additional security challenges.

Dealing with multi-cloud presents many security challenges, one being simply the sheer quantity. Working with one cloud provider is an endeavor, but many organizations today are dealing with four or more providers, and this creates an expanding array of tasks. At the “1’s and 0’s level”, your security engineers are probably already addressing plenty of issues, but there are additional risks to the business you may not have remediated or even identified yet. As the following illustrates, managing multi-cloud security also calls for competence in policy, negotiation, organizational alignment, budgets, business processes and partnerships.

Responsibility

One of the largest and most difficult challenges we face with the plethora of cloud solutions is understanding exactly which party is responsible for what aspects of security and to what degree. Is the service provider on board with your company’s compliance requirements? Will you be able to audit them or conduct pentesting? In the event of a breach or loss, how does the incident response play out and who has liability?

At the end of the day, this requires a lot of diving into contracts and working with lawyers. That may not be what you signed up for, but as security leaders we have to understand how our controls and policies will – or will not – be applied. As an example, your hardening standards may exceed the capabilities or willingness of a provider. If that’s the case, how will you address the additional risk? And from your own compliance standpoint, how do you account for an exception? Many times, cloud services may push back on requirements, making their link in your chain of security a weak point. When that happens, you’ll need to address the issue both technically and contractually.

Access Controls

In the multi-cloud world it's likely you are using some form of Identity and Access Management (IAM). Even with these robust solutions, you have to understand how to restrict access. Will you leverage least privileged or a role-based solution? And will all of your cloud vendors accept and apply those rules? What about data shared between multiple providers? This area of concern is complex, and the right solution will vary based on the services you are consuming and your business, but it will require very detailed evaluation. The key here is understanding your data and processes, something many businesses struggle with. Multiple business lines will need to be on the same page as to how to access data, what those processes will be and how to maintain security while enabling the business. You will need to talk to these business lines and understand them.

Data Protection

Now that we know who is responsible for what and how we'll access "the clouds," how are we going to protect the data? Service providers are likely encrypting your data in transit, but not at rest, and many will charge a lot more to do so. Does your data protection solution extend or work with your provider, or are they offering their own solution?

You also have to translate how your requirements impact costs. As business leaders, we are challenged to keep the business secure, without negative impacts and within budget. Selection of the right vendor is key, as is partnering with the right vendors to deliver what is needed. Notice I said "partnering," often just buying the cheapest solution can end up costing more than the right (more costly) one. This is even more critical in multi-cloud environments, where you could have data residing in multiple locations with different levels of protection. Here we need to understand the business processes and then apply the necessary controls at all steps of data flow and across the multi-cloud design. If gaps exist, you'll have to address them with a compensating control or possibly some acceptance of risk to the business.

Shadow IT

Even if you are not officially living in the multi-cloud world, you're likely already dealing with Shadow IT, which includes a multitude of cloud-based apps and services that individual users or departments employ because it just makes their jobs easier. The solution here is again to understand the business process and identify how the data is used, why those services are in place and what data is really required. Some business lines send excessive data outbound because "it's easy." Automating or streamlining a process to send only relevant data can reduce risk and improve the operation. With existing Shadow IT, start by identifying what the risk is, relevant to the services being used. Once the risk is understood, take measures to reduce it through redaction, masking, encryption, new processes or other approved solution.

Tracking Shadow IT is a continual challenge. Having a great asset management program in place can help reduce the risk, as can documenting data, data flow and business processes. Couple those steps with strong integration of information security into systems development and acquisition processes and you further reduce risk by getting involved early in the process. Moreover, you do so as an enabler to the

business. Often security is seen as a roadblock; working with business lines to improve their processes in a secure manner helps position the CISO organization as a valuable partner.

Monitoring & Response

This is a culmination of areas. You'll need to look into what traffic you can actually monitor within the multi-cloud, as well as what services for this are available, who allows you to use your own solutions, where all of the monitoring data is originating from and where it is going. Ideally, you want this all managed in your own SoC or MSSP, but there is a chance you'll have multiple feeds for different services. The goal is to be as efficient as possible and leaving any crucial areas un-checked. This may take time, and a long term planning. Take the time to analyze this out and incorporate it into your risk management program.

Getting It All Done

How many organizations finish 100 percent of their security projects every year? The simple fact is there are more needs than there are individuals to address them. In order to realize more progress in multi-cloud security, you may want to bring on someone who has relevant experience, or else contract-out some projects to help with the stepping-stones.

Create a plan of your current and desired state, identify high-level tasks you need to do and then realistically assess what steps you can and can't do. Be honest. Data discovery, business process documentation and asset management may be areas you can't tackle alone. Or if those tasks are well in hand, maybe it's the complexity around deploying and managing access controls across the multi-cloud. Seeking knowledge, training or aid will reduce the headaches and boost your probability of success, leading to earlier completion dates and overall better management of the challenging, multi-cloud security environment.



About the Author

William Klusovsky has 20 years in the InfoSec and IT industries, is a US Marine Veteran, and held multiple positions in retail and consulting. He is currently the Sr. Director of Client Strategy with NTT; his team advises security leadership across the industry spectrum. He maintains CISSP and CISM certifications and holds an MS in Information Security Management, as well as business coursework from The Wharton School and Univ. of Notre Dame.

Wil can be reached online at www.linkedin.com/in/wilklu and at our company website hello.global.ntt.



5 Key Steps to Secure IOT Product Development

By Kateryna Boiko, Marketing Manager, Mobilunity

A new concept that has taken the world by storm is the so-called "Internet of Things" (IoT). IoT refers to systems designed to transfer data over a network of traditionally non-internet-connected devices without the interaction between humans or between humans and computers. These devices are embedded with technology, can communicate via the internet and can be controlled remotely. IoT has simplified a large range of tasks, including business processes, home and business automation by enabling devices to communicate data to humans and other devices. Though IoT has many benefits, there is a range of pitfalls that need to be addressed. The most concerning obstacle is the **IoT security risk**. With the increase in the use of data through IoT devices, the probability of security breaches and privacy issues rises. Therefore, it is important to iron out any security issues during the first [IoT product development](#) stages.

The Categorization of IoT Device Types

IoT devices are usually used to simplify processes in the home, in the industrial sector and business world. Therefore, devices are usually categorized into three groups: industrial, enterprise and consumer.

Consumer devices

These days many modern homes are designed with [IoT devices](#) already installed. These devices are referred to as consumer devices. IoT consumer devices are specifically used for home automation and can include smart appliances, smart TVs, smart lighting and smart security systems. In homes, these

types of devices are all excellent additions to automate certain tasks. Not only does it simplify life, but it also saves time. While smart devices in and around the home have multiple benefits, security is a major concern. If these systems are designed with poor security measures anyone can access or hack these systems and retrieve highly personal data.

Enterprise devices

In the business world, IoT devices and systems offer even more benefits than in the home. Devices used in businesses can include automation devices that can streamline day-to-day tasks. These can include smart screens, security systems, alarm clocks, smart lights and vending machines, as well as smart electronic devices. In a business environment, these types of devices can not only save a lot of valuable time but can also save money in the long run. It is important to note, however, that IoT systems used in business are especially vulnerable to data hacking and other privacy issues that may, in turn, lead to major loss of information and profits. Difficulties in updating systems and lack of cybersecurity knowledge are the major obstacles observed while using IoT in businesses.

Industrial devices

In the industrial sector, many establishments are already making use of complex IoT systems. These systems can speed up operating processes by providing information for when parts on machines need to be replaced, predicting downtime, productivity and profits, diagnosing issues. In the industrial sector, IoT systems are excellent additions to standardized processes in order to increase productivity, however, there are a few stumbling blocks that need to be kept in mind. These include loss of jobs and total reliance on technology.

5 Key Steps in IoT Product Security Development

There have been numerous debates on the internet about the lack of security in IoT. Since the development of IoT, security risks have been a major concern and many experts in the field are working on solutions to this issue.

Security in IoT should start at the development phase, including the **IoT development tools** used. Now that most security concerns have been identified, developers have to implement solutions to ensure IoT devices are completely secure and that consumers' data is protected.

Here are five steps [IoT developers](#) should keep in mind when developing systems and devices:

1) Design secure network architecture

Ensuring watertight security right from the development stage of IoT product design will guarantee secure processes for end-users. IoT developers, therefore, need to make sure that the basic framework or network architecture is reliable, secure and can accommodate the traffic they carry. The first step at this

stage is to get physical devices in the network to securely connect by means of sensors that carry information safely to IoT gateways.

Robust network architecture sets the basis on which an IoT system will function. Once the basic structure is designed, it should also be evaluated according to specific evaluation methodologies to iron out any issues before the next step in the development process. Securing this right from the beginning of the development process will avoid complex **Internet of Things security issues** that are difficult to solve once an IoT system operates.

2) Authentication is needed

Authentication is the process of verifying users' identities. This process is foundational and one of the main factors that need to be in place with IoT systems and devices. Strong authentication requires that each IoT device in a system has a unique identity (ID) that can be verified when the device wants to connect to, for example, a central server. With this unique ID in place, any entity wanting to use a system has to prove their identity first. With this ID, system administrators can also manage devices securely and prevent it from performing unsecure actions.

If developers do not add strong authentication to IoT devices, anyone can use or hack a system which can lead to major security breaches.

Encrypt all data

Encryption is a vital step in security when **IoT application platforms** are developed. Encryption involves the process of taking information that humans communicate via an IoT system, mixing it up through complex formulas and producing a special key to unlock the data. Only those users that have the special key can unlock information or data. Currently there are a variety of IoT encryption standards with their own encryption methods and algorithms, that developers can use depending on product and user needs. When it comes to encryption, developers have to comply with certain standards to protect end-users. Some of the most widespread encryption methods include the Triple Data Encryption Standard (DES) and Twofish Encryption Algorithm.

Any IoT system that makes use of the internet to transmit data needs to be encrypted to avoid hacking of intelligence data. Therefore, IoT devices, no matter how small, must be designed with their own solid encryption.

1. Update and manage open-source software

As with so many other technologies used these days, open-source software is included in IoT devices. Open-source software's source code is accessible and can be distributed to anyone and for any purpose. With the rise of IoT development, a wide range of open-source libraries and platforms has been created for this purpose. Open-source software is preferred when it comes to IoT product development because the developer has more control over it and can modify it to match specific development needs. However, if this software is left unmanaged, anyone can exploit security vulnerabilities through weak spots. It is, therefore, incredibly important to make sure all open-source software used in IoT devices is always updated and carefully managed. If this step is left incomplete, **Internet of Things hacking** becomes a big possibility.

2. Add extra layers of security

When it comes to data, the **IoT developer community** will agree that no amount of security layers is ever enough; the more layers you add, the more secure your IoT system will be. These layers will add extra protection when top layers such as authentication and data encryption are cracked. Additional security layers should include a rock-solid interface or API security to allow only authorized devices and users to access devices, shielded storage and backups for data in a secure cloud environment, and device lifecycle management which includes automatic device monitoring and security layer updates.

Security Checklist for Engineers to Follow During the IoT Development Process

With **IoT application development**, it is incredibly important to follow a checklist to ensure all the boxes are ticked.

- Identify security issues
- Design secure network architecture
- Add authentication
- Encrypt of all data
- Update and manage open-source data
- Add extra layers of security
- Troubleshoot and fix all **Internet of Things security issues** in the first design steps
- Test, upgrade and update
- Have a recovery plan

The Bottom Line

As the IoT industry grows, the amount of data used with these systems also expands. Therefore, it is vital to have top-security in place, from the product design stage, to guarantee absolute privacy and security. No longer can devices and systems be designed without following a comprehensive security checklist. IoT product developers need to identify security issues before the development process starts, design secure network frameworks, ensure multiple watertight layers of security, including authentication and encryption, troubleshoot, and update IoT products often. Only by ticking all the security boxes IoT products can be used with confidence. **Internet of Things** security is a major concern, but luckily, with the right steps in place it can be solved and can be a major asset to IT business owners.



About the Author

Kateryna Boiko is a Marketing Manager at Mobilunity, Provider of Dedicated Development Teams with 9 years of hands-on experience in digital marketing. Kateryna managed to work with diverse industries and markets and now is keen on sharing unique cases with the world and coach on topics relevant to Web Analytics and Search Engine Optimization. Kateryna can be reached online at pr@mobilunity.com and at our company website <http://www.mobilunity.com/>



The Struggle of Updating Government Cybersecurity Measures

By Kayla Matthews

The cybersecurity landscape is ever-changing, and staying on top of developments often requires promptness. Unfortunately, government bodies typically aren't known for taking quick action. That's because they can't.

Making any update in government requires the proposed alteration to go through a long process of agreement and approval that involves numerous government authorities.

Input From Multiple People or Organizations May Slow the Decision-Making Process

The Government Accountability Office (GAO) is a watchdog organization that monitors the evolution of federal buildings to ensure they are adequate reflections of taxpayers' dollars.

The GAO recently released recommendations, some of which involve cybersecurity. The body advised partnering [with several federal authorities](#) to make critical improvements to cybersecurity infrastructure by adopting a national framework. That sounds good, in theory, and such collaboration could lead to more accurate and relevant insights.

However, as multiple organizations decide when and how to make cybersecurity improvements, the back-and-forth communications could mean it's virtually impossible to make rapid changes.

A Lack of Accountability Could Delay the Necessary Changes

What's more, these issues of outdated cybersecurity plans and the updates not happening fast enough are not merely problematic for governments in the U.S. A recent report about the cybersecurity readiness of the Australian government drew some worrisome conclusions. It showed that [nearly 40% of government agencies](#) had yet to implement mandatory information security measures rolled out in 2017-2018.

In Australia, one of the likely problems is that cybersecurity strategies for the government are mandated, but they are not enforced. Moreover, a 2017 cybersecurity audit found that some agencies self-reported being compliant in some areas, even though they still did not meet minimum standards.

However, these problems could affect any nation if a person does not know if they are the responsible party for raising awareness about the need for newer cybersecurity measures. For example, an individual may notice a cybersecurity weak point and report it to an immediate supervisor.

But, if that person fails to take action because they don't agree that the problem is as severe as the person who initially reported it indicated, they may fail to keep the matter flowing along the chain of command.

Governments Often Lack the Budgets Necessary to Make Improvements

Both physical security and cybersecurity are extremely important in government settings. Domestic and international security risks continue to [rise at an alarming rate](#), which means members of the government with decision-making authority face constant challenges. They have to decide how much money to devote to each aspect of security, and that often means the budget gets stretched thin.

Margaret Byrnes, Executive Director of the New Hampshire Municipal Association, [recently took part in an interview](#) where she explained why hackers often target municipal governments. Byrnes clarified that one of the reasons municipalities are seen as an easy target is because they often have budget constraints that prevent them from bolstering their security infrastructure. Hackers know this, and they know these municipalities may not be as well protected.

It's not difficult to envision a scenario where some members of a town or local government's approval chain heartily agree to expand the budget for cybersecurity, and others are not as eager to spend money that way. Then, the reluctant parties need more convincing, and crafting a more compelling argument could take a lot of precious time.

Strong Leadership Helps Cybersecurity Changes Happen

It might seem that if the GAO consistently makes recommendations for cybersecurity improvements, such feedback would make them occur. However, the Department of Veterans Affairs proves that assumption wrong. The GAO has, [for the last 17 years](#), cited cybersecurity issues with that agency's financial systems. The majority of the GAO's concerns mentioned most recently also came up previously.

If leaders are willing to take responsibility for facilitating progress with government-related cybersecurity, that could help. However, a 2018 Accenture study of government leadership showed that's more difficult than some people may think.

Only 39 percent of respondents [gave themselves high performance ratings](#) for both the ability to relate mission and business requirements to reasons for making new IT investments and to collaborate with stakeholders to agree on IT priorities. Those findings could mean that even if people intend to act as cybersecurity leaders that drive decision-making, success is harder to achieve than expected.

A Complex Problem

Slow government processes are largely to blame for cybersecurity downfalls. However, remedying the problem will not come quickly, and many bodies must collaborate to make progress occur.



About the Author

Kayla Matthews, a cybersecurity journalist, has written for sites like Security Boulevard, the National Cyber Security Alliance, Information Age and more. Matthews can be reached via Twitter @KayleEMatthews or on ProductivityBytes.com.



Accelerating the Pace of Government IT Modernization

By Jeff Elliott

For decades, the federal government has been hamstrung in its efforts to adopt new IT systems by the glacial pace of RMF accreditation and the manual processes required to secure any system connected to the outside world from security risks and inherent vulnerabilities.

Streamlining this process, however, could dramatically reshape government operations and allow for shorter-duration projects that advance the cause of government IT modernization much more quickly – including moves to the Cloud.

With government IT modernization initiatives stimulating new legislation and increasing funding opportunities, it is even more critical to address a significant and continuous drag on the system: the painstaking process of securing the system to the specifications of the Defense Information Systems Agency, a support agency for the Department of Defense (DoD)

As part of this process, systems must be hardened to standard Security Technical Implementation Guide (STIG) benchmarks. The STIGs provide configuration specifications for operating systems, database management systems, web servers and weapon system used by government agencies.

The problem is STIGs are long and detailed. Often containing hundreds of pages, adhering to or upgrading software or systems to a particular STIG has been a highly specialized manual process that can take many months to accomplish. In addition to the significant time involved, it requires well-trained engineers that are skilled in the technical system, operating system policies and security guidance.

This task adds to implementation costs and can add years before an Authorization to Operate (ATO) is issued. The task is so tedious and painstaking, and there is such a shortage of STIG experts, that it often prevents agencies from pursuing modernization projects.

“With modernization, the government is spending a lot of money upfront, but they don’t get any benefit until someone can actually use the new technology in production,” says Brian Hajost, president of SteelCloud and an expert in automated STIG compliance. “One of the things that must get done is the system must be ‘hardened’ and it has to be accredited through the RMF process before an ATO is possible.”

IT modernization projects for government agencies comes in many forms. Information may be consolidated into a single, shared data center or new applications moved to a different infrastructure. Increasingly, due to the government’s Cloud Smart program as well as security guidelines outlined by FedRAMP, modernization projects involve moving to the commercial cloud. The advantages for government are moving to a more agile and accessible system that can be accessed anywhere and does not require complex on-premise networks.

According to Hajost, however, the difference between deploying an application in the Cloud and a traditional data center is insignificant, at least as it relates to security hardening.

“Moving to the cloud is supposed to be relatively quick and easy, but addressing system security in the cloud is no faster or easier than it is for an on-premise environment,” explains Hajost. “In our world, it isn’t much different than if an application moved from one data center to another, or the application is moved from a data center to the Cloud.”

Hajost says that even considering the slow pace of it, most still underestimate the expertise and time required, particularly when moving to the Cloud. A shortage of trained personnel impacts the ability to modernize, a shortage that is even more acute in classified environments.

“In a classified environment you need to hire someone with five years of information assurance (IA) that has a TS/SCI security clearance,” says Hajost. “If you put out an ad, you wouldn’t get one person applying for that job in six months. There just aren’t many around.”

Instead, settle for staff that are multi-tasking from other disciplines and specialties that have little to no STIG experience.

“Even with competent, trained people, [manually handling the STIGs] is a slow process,” says Hajost. “If you use people that know nothing about the STIGs, it goes *really, really* slowly.”

Fortunately, new automated software tools are eliminating months from the RMF accreditation process by virtually eliminating the time of the initial hardening effort while also providing the required documentation for RMF accreditation.

“With a software tool that can automate the process, you can take someone that is competent in some other aspect of IT and re-skill them to handle the STIGs in a few weeks and shave months off your project time,” explains Hajost.

Fortunately, there are new STIG automations tools that can quickly identify any conflicts that an application will run into in a hardened environment.

Products such as ConfigOS from SteelCloud identify and harden all controls considered a potential security risk. As outlined in the STIGs, risks are categorized into three levels (1/2/3) with Category 1 being the most severe and having the highest priority.

The software then produces a domain-independent comprehensive policy “signature” including user-defined documentation and STIG policy waivers. In this step alone, weeks, or months of manual work can be completed in an hour.

The signature and documentation are included in a secure, encrypted signature that is used to scan endpoints (laptops, desktops, physical/cloud servers) without being installed on any of them. The time it takes to remediate hundreds of STIG controls on each endpoint is typically under 90 seconds and ConfigOS executes multiple remediations at a time.

The encrypted signature can then be transported across large and small networks, classified environments, labs, disconnected networks, and tactical environments with connected and disconnected endpoints. No other changes are required to the network, security and no software is installed on any endpoints.

To date, ConfigOS has been licensed by just about every branch of the Department of Defense, as well as parts of DHS, HHS, and Department of Energy. The product is also used by large defense contractors and in programs for all branches of the military.

In addition to resolving issues proactively at much less cost and time, the software also provides the required documentation for RMF accreditation. This can eliminate months from what is typically a 6 to 12-month process to further speed time to production.

The STIGs are updated and evolve as well. With a new update every 90 days, automated STIG remediation software accommodates for changes in the requirements. Two business days after DISA publishes a new version of the STIGs, new production signatures are tested and made available to customers.

“New security updates are introduced periodically to account for newly discovered vulnerabilities as well as changes and updates to by the vendors supplying the major operating environment components,” explains Hajost.

According to Hajost, removing this significant impediment to project completion has a greater benefit than just allowing for modernization.

“The greater benefit is the capacity to modernize is greatly expanded,” explains Hajost. “Modernization shouldn’t be once every 10 years – it should be a continual process. So, if automating security compliance allows you to move faster, you might be able to move more than a few systems to the cloud in the next year, maybe it can be seven or eight,” says Hajost.

“Then once you can modernize more, then you get reap the benefits, which includes greater agility, more consolidated information, better access to information – with better security overall,” adds Hajost.

For more information about ConfigOS from SteelCloud please contact them at (703) 674-5500; or visit them online at www.steelcloud.com.



About the Author

Jeff Elliott is a Torrance, Calif.-based technical writer. He has researched and written about industrial technologies and issues for the past 20 years. For more information about ConfigOS from SteelCloud please contact them at 703-674-5500; or visit them online at www.steelcloud.com.



Cybersecurity Talent Shortage and Ways to Address the Gap

By Blake Tinsley, Founder and CEO, Prosyntix

The cyber threat landscape is ever evolving. From rapid deployment of new code for application usage, the Internet of Things (IoT) pushing for billions of connected devices, to entire architecture being transformed by the cloud. Going into the new decade is going to present new forms of threats but also new ways of getting work done. The exciting thing to see is the transformation of how organizations look at security needs. It's gone from the uncomfortable unknowns to proactive adoption of the right security measures as the primary foundation to grow.

With that being said, the current supply of talent does not meet the demand for businesses. The data is all over the internet showing how immense the shortfall is today and going into the future. According to The US Department of Commerce there was around 350,000 unfilled jobs in 2018 and growing to a predicted 3.5 million open jobs by 2021. This is a staggering number to try and comprehend considering how much investment and time is going into Cybersecurity initiatives.

I spent time with many decision makers on ways to address this issue. The commonalities of our discussion primarily hit on Practical Education Programs, Training, Changing Traditional Requirements for Hiring, and Lengthy Hiring Processes.

The needs of the hiring manager and Cybersecurity programs taught at the collegiate level seems to have a very wide gap. Due to the business needs, hiring managers are searching for specific abilities to fill an immediate gap, including key non-technical "soft" skills and business acumen. This is part of the reason why recent college graduates are often overlooked or have a tough time getting into the field. Ultimately, it boils down to professors looking at theory-based education as more intellectually appealing which is why it has been the common form of practice since the beginning of time. Cybersecurity, however, is one of those fields that needs practical ability right out of the gate. We're already starting to see it on a very small scale but outside entities or local businesses around these institutions need to work together to build out labs where students can touch relevant tools and learn typical processes prior to graduating. NICE and NIST help influence the curriculum but we need to expand further to better align

with business needs. This adoption is critical for young professionals to be equipped with applicable skillsets hiring managers can use.

Training is also a hot button we always hear about. My company is one of the very few startup firms only focused on Cybersecurity and Engineering Talent Services in the nation. This is what we do, and I like to think we do it well. However, I can tell you right now, the WELL FEELS VERY DRY. Decision makers need to focus on developing their existing team and not depend entirely on adding headcount to address a gap. Not only does this give your team broader knowledge that is more tailored to the organization's specific needs but, in some cases, it expedites your gap coverage. I have had the pleasure of partnering with an amazing ISACA Cybersecurity Consulting firm. Their focus is working with existing teams to cross train needed skillsets all while providing a flexible training program so that employees can keep up with daily business demands. Companies like these need to be used everywhere across all industries.

One of the things I see on a consistent basis is red tape disqualification of talent. Good, very capable candidates are being disqualified due to lack of education standards and years of experience. In the past 4 years, I have seen 13 candidates not get the job because they were 1 or 2 years shy of the minimum years of experience. I've seen 3 cases where candidates did not get the job because they didn't have a bachelor's degree. Just recently I had a client rave on the abilities of a candidate but passed on him because his 6 years of experience didn't align with their definition of a "lead". Companies need to focus more on ability rather than formality. The idea of someone not getting a job because they lack the required education is beyond belief considering our current state. The youngest hacker in the world is a 9 year old kid that was accredited for exploiting a vulnerability. I have a close friend who taught himself how to code, never earned a college degree, was overlooked for several jobs, and is now the Lead Application Security Engineer for a well-known financial firm. Loosening up on red tape standards is a must when trying to creatively attract talent. Talent shortage, aggressive company growth, and red tape requirements don't go together.

A well-defined hiring process is important but can also work against you. Every time I find a top not security professional, they have 4 other interviews going by the time I send them over to the client. Times have drastically changed since the recession. The talent pool was abundant, there was a high probability the candidate would commit to a lengthy hiring process, and they would do anything the company needs to get the job. Now days, professionals are leaving companies without a contingency plan because they know they have a marketable skillset and will land a job in a matter of days or weeks. Companies must have an expedited hiring process because TIME IS THE ENEMY. On top of that, companies need to have 5 to 10 selling points on why that candidate should join the firm. Don't just sell benefits and flexibility but focus on collaboration, meaningful projects, culture, etc. Without these things, you will have trouble finding top talent. The hiring process is not a one-way assessment anymore. Candidates are evaluating you just as much as you are evaluating them.

As we all know, cybersecurity is the leading job of the future. We are at a point now where data is the most important asset to an organization. How well you use and safeguard that data all depends on the type of people you can attract, how you sell the company story, and the time you invest in those people.



About the Author

Blake founded Prosyntix as one of the few startup Cybersecurity Talent Services firm in the nation where they help clients find experienced professionals within Risk Management and InfoSec. Prior to starting Prosyntix, he was a Partner at a risk management consulting firm. In this role he helped clients enhance their security posture by focusing on Critical Security Controls and architecting secure data centers using DISA STIGS. He graduated from The Citadel, The Military College of South Carolina with a bachelor's degree in Business Administration



5 Recruitment Predictions in Cybersecurity For 2020

By Karl Sharman

As we prepare for more figures to be produced saying the amount of jobs unfilled has increased by another 20%, I want to challenge every person in a hiring capacity to really ask yourself – am I doing enough to ensure this role is filled?

The industry is crying out for change within workforce management and maybe improving your processes or your job descriptions will be your change for 2020. What if you could decrease your fill time to 2 weeks? What if you could fill these positions without it damaging your bottom line? What if you can increase your talent pool by 20%? All of this is possible and that's the great part of working in cybersecurity.

If I was a betting person, most companies won't change or will change for the month of January and go back to their old habits (I didn't say change was easy). So, I am going to predict the following and provide alternatives:

1. Hiring a candidate will take on average over 3 months

Alternative: Hire people that have a network you can gain from, while also partnering with specialised recruiters to supplement and grow your talent pool. During the process, remove unnecessary interview stages or even do it all in one day, to decrease time taken. I predict this will decrease your fill time to 2-3 weeks.

2. You will replace as much as you grow

Alternative: Accept you will lose people; our salary reports states that 86% are open to moving. The two things you need to ensure you do this year, is constantly grow your talent pool to provide depth and hire the right managers who can create a safe and ambitious environment for people to thrive.

3. You will still use the same "wish list" job descriptions

Alternative: I challenge you to cut the job description to 3 key functions within the role and 3 “must have” criteria. This will increase more women and neurodiversity candidates applying as our data proves.

4. You will still make decisions on technical skills over soft skills

Alternative: Prioritize hiring on company and manager values. Set up a process which allows multiple voices to focus on values and behaviors within interviewing. Remember, technical skills can always be trained.

5. You will still make education mandatory over talent and people skills

Alternative: Remove education. You can still have it as a benefit but in this industry, it will limit your talent pool if you make it mandatory. Many people transfer from different industries where it hasn't been required or they train their self from a young age.

Now I am sure this is a lot to take in, but it is all possible if you want to achieve your hiring goals this year. We speak to many candidates who want to be a manager and hiring is a huge part of that role. My prediction in cybersecurity for 2020 is that people will hire managers who are successful at hiring including retaining talent. Poor recruitment will damage your organizations bottom line, while great recruitment will lead to managerial success. Which one do you want to be this year?



About the Author

Karl Sharman is a Cyber Security specialist recruiter & talent advisor leading the US operations for BeecherMadden. After graduating from University, he was a lead recruiter of talent for football clubs including Crystal Palace, AFC Wimbledon & Southampton FC. In his time, he produced and supported over £1 million worth of talent for football clubs before moving into Cyber Security in 2017. In the cyber security industry, Karl has become a contributor, writer and a podcast host alongside his full-time

recruitment focus. Karl can be reached online at karl.sharman@beechermadden.com, on LinkedIn and at our company website <http://www.beecher-madden.com>



Cross Domain Solutions – Quo Vadis

By Alexander Schellong, VP Global Business, INFODAS

Highly sensitive systems and data assets (domains) are often separated from the Internet or less critical systems. Separation is achieved through isolation, commonly referenced as an air gap. While isolation significantly increases the barrier for data exfiltration or malware infection, Cyberattacks can still happen in various ways. The Stuxnet attack of the Iranian nuclear program is a prominent case in point. However, keeping isolated systems updated with patches or important data and sharing selected data from those systems with others, requires time and manual labor (“swivel chair” or “sneaker” networks). In other words, system and data silos— isolation—contradicts the benefits and needs of digitization such as real-time data sharing in geographically dispersed operating and IT environments.

Accordingly, cross domain solutions (CDS) were developed over the past 10-15 years that allow manual or automatic transfer, access or exchange of data across segmented domains of different classification level. Data can only be shared when necessary and sharing is combined with redaction or validation requirements. CDS are not Firewalls or about encryption.

Outside of military, intelligence, homeland security and some critical infrastructure industry circles many IT professionals are not aware of CDS which also have to adapt to new end-user requirements and technology trends.

What makes Cross Domain Solutions unique?

Most cross domain solutions are accredited by government information security authorities through rigorous multi-year testing. They need to fulfill a complex set of requirements as highly trusted components for the most sensitive environments. This includes security cleared development resources and component supply chain transparency. Moreover, hardware and software security architecture elements such as a hardened operating system, hardware level separation, tamper proof enclosure or enhanced secure logging. CDS functionalities include manual or automatic control of the flow of

information between domains, the possibility to add customized filters (parsers) for certain data types or the capability to operate in complex environments (e.g. heat, shock, dust, humidity). Consequently, very few companies have developed CDS and CDS products tend to be higher priced.

Cross Domain Solutions at a glance

Within the Cybersecurity solution market, CDS represent a niche within the data security, DLP and network security space. Currently, CDS are always hardware based solutions (security appliances). Classically CDS are boundary devices that are combined with Firewalls to protect two domains. The domain that needs to be protected or holds more sensitive data is usually referred to as HIGH while the other domain of lesser sensitivity is referred to as LOW.

The most common solution are **data diodes**. They ensure data flow is only possible in one direction which is mostly achieved through the use of hardware or software. To achieve this functionality, the majority of vendors uses a fiber optic cable which leads to galvanic separation between domains similar to the semiconductor of the same name. Within the public sector, data diodes are utilized to provide data to a classified network. In critical infrastructure (e.g. power plants, oil refineries, manufacturing) data diodes are used to send data out of an industrial control network to safeguard its integrity and availability while taking advantage of it for predictive maintenance. Hardware based diodes come in different form factors but many of them are limited in transmission speed or the protocols they support. Some may include pre-defined data filters or malware protection but usually they don't. There are around 30-40 vendors worldwide that offer data diodes.

High Assurance Data Guards (HAG / HADG), Information Exchange Gateways (IEG) or Security Gateways are commonly used terms for security appliances that allow for controlled bi-directional data exchange between two domains. Their main purpose is to protect any accidental or purposeful leakage of classified data from a HIGH to a LOW domain. Filters check all data transfers down to the binary level. Some Security Gateways are combined with Firewalls features, optimized for streaming or emailing. There are around 10 vendors worldwide that offer these types of CDS.

Finally, CDS are complemented by solutions to securely **classify data objects**. These can be security appliances, virtual machines or applications. Many applications allow to tag or classify data manually or automatically. Some labels are markings inside documents, some happen through other labels are small external files. Classifications can follow regulatory compliance or a government's classification guidelines (e.g. Confidential, Secret, Top Secret). However, when the label becomes the critical element for downstream release decisions, it needs to be protected against manipulation. In these cases labels are cryptographically bound. There are around 5-6 vendors worldwide that offer government level data classification with secure labels.

Next steps in Cross Domain Solutions

Due to the government accreditation requirements and testing cycles, CDS tend to trail behind technology trends. These government accreditations also create market entry barriers so that vendors can ask for higher prices, even when the technology might already be outdated or offering reduced functionality. Among the areas of CDS that will require improvements are:

- Higher data volumes and lower latency
- Virtual CDS instance (Cloud CDS)
- Improved data discovery and classification (e.g. via Artificial Intelligence)
- Easier deployment
- Easier filters / parsers / Out-of-the-box filters of structured data formats
- Multi-asset management (Dashboard)
- Formfactor miniaturization

Future use-cases might be expanded to other industries within critical infrastructure (e.g. Financial Services) and mobility (e.g. Connected Car, Planes) as the struggle of data custodians and security architects for the right balance between zero trust, protection (“Need to Know”) and sharing continues (“Need to Share”)

The infodas approach to Cross Domain Solutions

Over 10 years ago infodas was asked by the German military to develop a bi-directional CDS for an IT-service management use-case. Machine data had to be shared from a classified environment with IT service providers such as IBM so that they could monitor and manage the machines without having access to classified data. infodas worked and continues to work closely with the German Federal Office for Information Security BSI to maintain the accreditation status for its products. Now infodas is one of the few vendors in the world that offers products for all CDS scenarios for unidirectional transfer, bi-directional exchange and data classification between HIGH and LOW domains in the SDoT Product Family (Secure Domain Transition). All of the SDoT products feature a unique hardware and software architecture with a microkernel OS following the security by design principle. Fully evaluated and with only 15,000 lines of code the SDoT Microkernel OS differs significantly from secure Linux OS currently used in most trusted CDS on the market.

The SDoT Diode is also the only software based data diode in the world with 9.1 Gbit/s with a NATO, EU and German Secret accreditations. The bi-directional SDoT Security Gateway and Security Gateway Express also gained NATO, EU and German Secret accreditations. UDP, TCP, SMTP/S and HTTP/S can be used for transmission in each 1U 19” rack space appliance without additional proxies. The SDoT Labelling Service can be integrated into most applications to create tamper proof NATO Stanag 4774/8 compliant XML security labels. This makes it easy to integrate the manual classification process in the workflow of whitelisted personnel. The security appliances are used in Navy vessels, weapon systems, data centers or containers around the world.



About the Author

Dr Alexander Schellong, VP Global Business, INFODAS. As a member of the infodas management board, Alexander leads all international activities. He has extensive experience in strategic consulting, business development, general management, business unit leadership and mission critical international project and operations management in Europe, Middle East, Africa and Asia for the U.S. government, German government and other commercial clients. His domain expertise covers among others eGovernment, Cybersecurity, Cloud, BPO or digital transformation. He has authored one book on CRM in the public sector

and over 60 articles on a variety of topics at the intersection of technology, society and organizations. He holds a Masters and Phd. He studied and taught at Goethe-University Frankfurt am Main, Harvard Kennedy School, The University of Tokyo and Stanford University.

Alexander can be reached online at a.schellong@infodas.de and @schellong. More information about INFODAS Cybersecurity services and products can be found at <http://www.infodas.de>



Industrial Control System Vulnerabilities: A Prime Target of Our Critical Infrastructure by Adversaries

By Dr. Daniel Osafo Harrison, DCS, C|CISO, CISM, CISA, CRISC, Security+

Industrial control system (ICS) is a dynamic technological system with subsystems such as programmable logic controllers (PLCs), Remote Terminal Units (RTUs), Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Human Machine Interface (HMI) and others such as Engineering Workstations and Operator workstations. ICS consists of a dynamically complex network of several interconnected and interactive control systems and other network devices working together to supply valuable information about instrumentations, sensors and measurements, gauges, and alerts from several industrial control network devices.

Introduction

The industrial control system plays a pivotal role in our livelihood, supporting critical infrastructures such as electricity, water supply, transportation, oil, gas, communication, and manufacturing, to mention the least. We depend on ICS for economic sustainability, wealth creation, and national security. These systems function by monitoring complex industrial processes that provide us with abundance of water supply to our homes, electricity and natural gas, extraction of crude oil, development of our weapon systems, railways transportation, traffic control systems, air control systems, manufacturing processes, and other essential services across the globe. As such industrial control systems are a prime target of nation-state attacks, advanced persistent threats attacks, and industrial espionage attacks.

Industrial Control Systems Vulnerabilities

The demand for an Industrial Control System uptime compounded by the fact that most of the Industrial Control Systems is a legacy system that is near their end of life and have a limited integrated microprocessors chips, low system memories and uses an outdated operating system which often lacks the support for vendor's patch updates. Unfortunately, fieldbus protocols which connect devices such as PLCs and Sensors have little to no security, backend protocols which enable systems to systems communication are also ridden with vulnerabilities. This phenomenon is a weakness that can be exploited by a determined attacker. In fact, in today's world, most of these systems are connected to the internet, which also increases the attack surface and present uber threat to ICS network (Paganini, 2013).

Suffice it to say, ICS premier support to our infrastructure, economy, and well-being makes them a target by industrial espionage aimed at stealing proprietary information or a nation-state attack like the Stuxnet and Night Dragon attacks to disrupt operations. Imagine the entire state of New York without electricity for a few days or the City of Chicago without water supply, think about the impact on society and businesses. I hope you get the picture!

Furthermore, the constant demand for the availability of the system also means we limit security protection because extreme cybersecurity safeguards such as intrusion prevention system (IPS) and packet inspection technologies can put enormous burden on these systems and networks which can completely deplete the network into a grinding halt (Stopping plant operations) as such the vulnerabilities outline below:

Lack of Patching and hardware failures:

Most ICS systems run on Windows XP operating system with zero patch releases available, which makes them susceptible to all forms of Trojan and Worms attacks. Additionally, hardware failure and inability to obtain replacement parts for these systems are common problems for end of life system. It cost vendors more money to support the end of life products. Vendors are forward thinkers and would rather invest their money on the most current and future products for profit maximization instead.

Lack of encryption:

The absence of encryption on the ICS network or devices means that all activities or transactions performed on the network are in a plain text format, which makes it susceptible to all forms of cyber-attacks. Encryptions convert plain text into a cipher-text that prevents unauthorized disclosure of sensitive information such as proprietary information, user identity and passwords, SQL transactions, protocol communications, setpoints, gauges, and so forth. Encryption protects confidentiality by keeping sensitive information private. Digital signatures used to encrypt the sender's private key to validate the integrity of information from the sender (Systems) and non-repudiation. This way, the sender is unable to deny sending sensitive information across a network to another device. However, encryption is known to create several issues on the ICS network; hence due care and due diligence must be considered before deploying encryption.

Human Error:

Systems misconfiguration and inadequate firewall rules can create a huge vulnerability that can be exploited by adversaries. All it takes is for a well-intended automation engineer or cognizant engineer to unknowingly insert malware-infected USB into a workstation or a server to cause havoc on the network. Once upon a time, an automation engineer forgot to properly save a configuration changes he made to a cisco 2960 switches because he failed to “copy running-configuration and startup-configuration.” Running-config is volatile, and startup-config is nonvolatile RAM (NVRAM), his actions created a self-inflicted denial of service disrupting production. Imagine how much productivity and money lost.

Inadequate Access Control Management:

Often, ICS systems require little to no identification, authentication, and authorization process to restrict user access, and this action presents a vulnerability that can be exploited by both external attackers and disgruntle insider. A successful attacker may gain full access to critical systems on the network, thereby disrupting production operations.

Mitigating ICS Vulnerabilities

According to the NIST SP 800-82 Revision 2 publication, the following steps can mitigate a lot of the vulnerabilities associated with ICS networks and systems.

- Employ application whitelisting to protect infrastructure from potentially harmful programming. For instance, PLCs don't need Microsoft office install on them.
- Implement configuration management and patch management controls to keep control systems secure. Establishing a Security Configuration Management Board that reviews all system configuration and approve them before deployment to production will mitigate risks.
- Reduce attack surface areas by segmenting networks into logical parts by functional groups such as cognizant engineering, automation engineering, control room operators, historian, business network, and so forth and restricting host-to-host communications paths.
- Require multi-factor authentication and enforce the principle of least privilege (POLP) wherever possible, use expert judgment.
- Require remote access to be operator controlled and time-limited.
- Monitor traffic within the control network and on ICS perimeters (enclave). For example, deploying Security Information and Event Management (SIEM) for continuous monitoring will help identify issues on the network as well monitor implemented security controls
- Analyze access logs and verify all anomalies.
- Employ a robust back and recovery program for the ICS network.

Conclusion

In a nutshell, the ICS network is vulnerable and attractive to APT, Nation-State, and other forms of attacks that aim at stealing sensitive information and proprietary information. There are many issues to take into consideration when creating a risk assessment for the industrial control systems. The organization must

first analyze what they are going to look for and then evaluate the process. Stakeholders should be part of the internal evaluation process because the people within an organization understand their organization the best. Conduct assessments using regulations from the local, state, or federal programs/standards, and implement security controls to reduce risks on the ICS network to a level the organization is willing to accept.

References

Pierluigi Paganini (2013, Dec). Two Million Social Media Credentials Stolen by Cybercriminals. Retrieved from <http://securityaffairs.co/wordpress/20219/cyber-crime/two-million-credentials-stolen.html>

NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security. (2015) NIST. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>



About the Author

Dr. Daniel Osafo Harrison, DCS, C|CISO, CISM, CISA, CRISC, Security+

Dr. Harrison is a Doctor of Computer Science in Information Assurance and Head of Cybersecurity. Background in Industrial Control System Cybersecurity, DoD Information Assurance, Artificial Intelligence, Enterprise Network Architecture Security, Computer Programming, and Laboratory Information Systems.

Contact me at daniel@docharrison.org, and <https://www.linkedin.com/in/dr-daniel-harrison-dcs-cciso-ciscism-sec-38459015/>



The Growing Importance of API Security

APIs are everywhere, and they are ripe targets for malicious attacks

By Ameya Talwalker, Co-founder and CPO, Cequence Security

Earlier this year I wrote a [blog](#) about key trends in application security. One of those trends – the explosion of APIs and endpoints – has come to fruition. In conjunction with the explosive use of APIs, bad actors are now using to execute a wide range of attacks.

The result – the API security market is crowded with new offerings from startups to large security vendors, all claiming they have API security. To us, API security is nothing new – we’ve watched for years as bad actors execute automated attacks against our customer’s APIs supporting mobile login or web form registration or login applications. But it’s clear from my customer conversations that while API security is top of mind, the topic itself is vague, leading to indecision as to what they are looking for. Yet, their application teams are deploying API based applications at a faster rate than ever. Given the confusion around API security and the fact that we have been protecting APIs from day one, I thought I would share my perspective on API security.

API Security: Why the Hype?

The API explosion is driven by several business factors. Enterprises are moving away from large monolithic apps that are updated annually at best. Legacy applications are being broken into smaller independently functional components, oftentimes, rolling them out as container-based microservices. These application components and microservices work together to deliver the same functionality as the monolithic applications.

Key API Growth Drivers:

- Rapid adoption of iterative development methodologies (DevOps, DevSecOps, Agile, etc.) enable teams to quickly push incremental changes to application components directly to customers instead of following the long development and quality assurance cycles of legacy applications. The result is increased competitive differentiation and customer satisfaction.

- Ability to scale up and down to handle seasonality-based demand leads to more efficient infrastructure use and associated cost savings.
- Technology adoption trends such as public/private cloud adoption, containers and orchestration (Kubernetes), management frameworks (Istio) make it easier to develop and deploy API based microservices at scale.
- Partner ecosystem expansion, enabled by API based microservices that partners, aggregators, suppliers and 3rd party developers use to grow their business without replicating functionality. These APIs are well documented and publicly available – as evidenced by the directory of more than [23,000 APIs here found on programmableweb.com](https://programmableweb.com)

The adoption of APIs is great for business but it's a nightmare for security professionals. The same understaffed security team tasked with protecting a handful of applications is now suddenly responsible for protecting hundreds if not thousands of public-facing APIs from a range of security risks. Therefore, API Security is top of mind for most CISOs.

API Security Requirements

Based on our recent customer conversations, here are the five problems security teams are trying to solve when it comes to API Security.

1. **Visibility:** The old adage of Knowledge is Power is appropriate when it comes to API visibility. Customers are concerned with the lack visibility into which APIs are published, how and when they are updated, who is accessing them, and how are they being accessed. Understanding the full scope of your API usage is the first step towards securing them.
2. **Access Control:** Often times, API access is loosely controlled which can lead to unwanted exposure. Ensuring the right set of users have the right set of access permissions for each API is a critical security requirement often addressed through Identity and Access Management.
3. **Traffic Management:** Bot traffic is here to stay. In some customer environments, as much as 90% of their traffic is automated – both good and bad – traffic. Understanding the traffic profile and controlling good bots while preventing bad ones that may lead to network and application layer DDoS attacks, implementing IP policies (whitelist, blacklists and rate-limits) and geo-fencing specific to use-cases and corresponding API endpoints.
4. **Threat Prevention:** APIs simplify the process of an attack by eliminating the web form or the mobile app itself, allowing a bad actor to easily execute their attacks. Protecting API endpoints from automated bot attacks, business logic abuse and vulnerability exploits is a key API security requirement.
5. **Data Security:** Preventing data loss over exposed APIs, either due to programming errors or security control gaps, for appropriately privileged users or otherwise is a critical API security requirement.

Alternative Approaches to API Security

Researching API security will show that there are four distinct solution groups, each addressing specific challenges.

- API Gateways: the most mature and heavily populated category, these solutions focus heavily on visibility and control.
- API Security: largely populated with startups that find your APIs and protect them from vulnerabilities or data leakage.
- Web Application Firewalls: apply traditional web-based vulnerability exploit protection to APIs.
- First Generation Bot Mitigation vendors: prevent automated attacks against web and mobile apps using JavaScript instrumentation and mobile SDKs to collect attack telemetry. Adding API security as an afterthought through a variety of approaches.

None of these solutions solve all five of the requirements outlined above. In many cases, customers will use multiple offerings from the mix of API security providers.

How Cequence Security Addresses API Security

When we talk about API security, it is with a focus on automated bot attacks that can be executed against an API as easily as they can against a web form. The same flexibility and efficiency benefits that APIs bring to the application development team are leveraged by bad actors to execute automated attacks. Cequence Security addresses three of the five requirements listed above and we are working to address the remaining requirements soon.

- **Visibility:** Our agentless, intelligence-based approach allows us to continuously monitor and build a site-map of all the APIs in use including those accessed by users, partners, aggregators, IoT devices etc. Since we are typically deployed at a choke-point in the application layer, we can see and aggregate data across the entire API fabric and give a unified and real-time view of API usage to security teams. That enables them to decide the security posture for the entire API fabric. New APIs and periodic updates are automatically discovered, without injecting security delays into the development lifecycle. For example, we were able to alert the security team at a large retailer about a new version of an existing API application being rolled out and live, which the security team was completely unaware of.
- **Traffic Management:** CQ botDefense and CQ appFirewall combine to provide high precision traffic management based on the visibility generated by CQAI. Driven through policies, we can enforce a positive security model that precisely allows what you want and while denying all else. As the application fabric scales based on seasonal demands, we also scale with the fabric to provide continuous protection. For example, a regional bank in the US was experiencing a burst of OFX (Open Financial Exchange) transactions from east Asia, where they have virtually no customers. With the Cequence Security solution, they were able to divert those potentially fraudulent transactions from east Asia to an alternate server, while not impacting legitimate transactions.
- **Threat Prevention:** APIs are subject to same set of threats that can be executed against web applications – automated business logic abuse and vulnerability exploits. Business logic abuse at scale can be driven through large automated or human bot farms, leading up to fraud and financial loss. For example, immediately following the disclosure by Facebook that they had leaked close to 50 million OAuth tokens used for Facebook logins on other platforms, one of our social media customers experienced a high-volume credential stuffing attack on their Facebook login application API. We were able to thwart that attack with CQ botDefense.

Public API documentation makes it easier to target API-based applications when compared to traditional web applications that require a certain level of analysis along with trial and error. Just like a web application, APIs are subject to application vulnerability exploits to gain unauthorized access, steal sensitive data and launch even more damaging attacks. Our CQ botDefense solution protects APIs from automated business logic abuse. Our CQ appFirewall prevents these APIs from being exploited by motivated and well-resourced attackers.

API Security is “trending” now and it can be confusing. We are helping enterprise security teams navigate a path towards securing their API applications while not standing in the way of rapid development and deployment cycles. Look for more exciting announcements in this space from us in 2020.



About the Author

Over the last 10 years, Ameya Talwalkar has built strong engineering teams specializing in enterprise and consumer security in Silicon Valley, Los Angeles, Madrid, Pune, and Chengdu. Before co-founding Cequence Security, he was Director of Engineering at Symantec. He was responsible for its anti-malware software stack that leverages network Intrusion prevention and behavior and reputation technologies, and anti-virus engines. Under his leadership, Symantec developed an advanced version of network intrusion prevention technology that blocks more than two billion threats a year. Prior to Symantec, Ameya worked in various engineering roles at Valicert, focused on PKI-based security solutions for finance and government. He led the first commercial implementation of RFC 5055 and contributed to its progress at IETF. Ameya holds a Bachelor of Engineering in Electrical Engineering from the University of Mumbai's Sardar Patel College of Engineering (SPCE). Ameya can be reached on LinkedIn at <https://www.linkedin.com/in/ameya-talwalkar-910b8/>



A Single Security Recommendation to Solve an Age-Old Problem

By Morey Haber, CTO & CISO, BeyondTrust

In the cyber world, we're exposed to an onslaught of recommendations and top lists for improving IT security. They may have some universal characteristics, but are infrequently not relevant for adoption by everyone, everywhere, and at every time. In fact, can you guess what the number one, universal, and best security recommendation is for everyone to embrace? Here's a hint, it is related to passwords.

To further set the stage for this recommendation, let's consider all the infosec recommendations we experience on a daily basis. These include everything from security skills and cyber awareness training to patch management. They target problems from phishing to vulnerability management, but are not necessarily relevant to every employee within an organisation, nor are they necessarily relevant to each person on their personal devices at home.

While it is common knowledge to avoid email spam, and employees are often trained on how to identify suspicious emails and advised not to click on suspicious links, it is interesting that younger generations are far less likely to embrace email outside of the corporate enterprise. Instant messaging and other forms of social media are their tools of choice, which suggests that traditional email may slowly fade away like postal correspondence, or the fax machine. The demise of email may take a few more decades to transpire, but this downshift is well underway.

All of this helps further refine the single best recommendation. Remember, we need to consider a universal security recommendation that translates to everyone.

Fixing an Age-Old Security Issue

Regardless of persona at home or at work, the one thing everyone uses are passwords. We use passwords for work, for resources on the Internet, for social media and for our applications. We use them in the form of passcodes and PINs for banking, mobile devices, and for office and home alarm systems. Passwords are ubiquitous, and we use them constantly — even on newer systems that ironically claim to be “password-less.” In these instances, a mechanism under the hood is still identifying your access rights and storing that “somehow”.

The most common storage of any password is within a single human brain. We assign a password to a system or application, recall it when it needs to be used, and hopefully remember it each time we change it. Our brains are full of passwords, and often, we forget them, reuse them, need to share them, and are forced to document them on post-it notes, spreadsheets, and even communicate them via email or SMS text messages (a very poor security practice!).

These insecure methods for creating, sharing, and reusing passwords are responsible for the types of data breaches that routinely make the front-page news, serving as cautionary tales of what is at high-risk of happening when good password management strategies are not adhered to. The ramifications crisscross both our professional and personal lives.

Passwords literally can be found everywhere, and we need at least one basic tenant to help fix a thousand-year old problem. Therefore, the most important security recommendation for everyone is:

Ensure that every password you use is unique and not shared with any other resource (including people) at any other time.

While there is no denying that remembering an already considerable and ever-expanding list of passwords (an average of 120 for the modern-day corporate user) is improbable for most humans, there are password management tools, solutions, and techniques for making this a reality, thereby going a long way toward reducing password-related threats.

Modern operating systems, browsers, and applications can help create unique passwords for every resource, and securely store them for retrieval in lieu of a human having to remember every single one. The passwords are basically stored behind one unique “master” password (it may also be referred to as a “key” or “secret”) that only the individual knows. While this is good solution for home and small business users (to a limited degree), it does not scale to most businesses that need to share accounts (due to technology limitations) and automatically generate unique passwords, such as to keep up with employee changes or to meet regulatory compliance guidelines.

Another security best practice to be mindful of — a password alone should never be the only authentication mechanism for critical data, sensitive systems, and potentially daily operations into those resources. Multi-factor authentication (MFA) or two-factor authentication (2FA) should be layered on top to ensure a unique password, per account, is actually being used by the correct identity when authentication is required.

One key merit of this universal security recommendation is that it ensures that if your password is stolen, leaked, or inappropriately used, it can only be leveraged against the corresponding resource assigned (if MFA or 2FA is not present). If passwords are unique, a threat actor cannot use one compromised account and password to attack other resources. The attacker's options and movement are significantly limited, though they could try to leverage advanced techniques to steal other credentials from the system they have compromised, such as by scraping passwords from memory. In that case, not only generating unique passwords, but also rotating passwords frequently will help mitigate the attack.

Solutions for privileged password management across an organisation's entire information and security infrastructure can help. Advanced tools provide automated management for sensitive accounts and passwords (including SSH key management), such as shared administrative accounts, application accounts, local administrative accounts, and service accounts, across nearly all IP-enabled devices.

This helps ensure this top security recommendation can be implemented across any organisation to enforce strong enterprise password security.



About the Author

With more than 20 years of IT industry experience and author of Privileged Attack Vectors and Asset Attack Vectors, Mr. Haber joined BeyondTrust in 2012 as a part of the eEye Digital Security acquisition. He currently oversees the vision for BeyondTrust technology encompassing privileged access management, remote access, and vulnerability management solutions, and BeyondTrust's own internal information security strategies. In

2004, Mr. Haber joined eEye as the Director of Security Engineering and was responsible for strategic business discussions and vulnerability management architectures in Fortune 500 clients. Prior to eEye, he was a Development Manager for Computer Associates, Inc. (CA), responsible for new product beta cycles and named customer accounts. Mr. Haber began his career as a Reliability and Maintainability Engineer for a government contractor building flight and training simulators. He earned a Bachelors of Science in Electrical Engineering from the State University of New York at Stony Brook.



Not All Hackers Are Criminals, And Some of The Good Guys Can Earn A Million Dollars

Dr. Roberto Di Pietro, a full professor of cybersecurity at Hamad Bin Khalifa University's College of Science and Engineering, explains why there is a misconception about the term 'hackers'.

The term 'hacking' generally has a negative connotation as many people assume that all hackers are bad, and they treat them with suspicion in the belief they have criminal intentions.

It is important to understand, though, that not all hackers are bad. Indeed, many hackers are helping to protect us from the untrustworthy ones.

In our context, a hacker is simply someone who enjoys the intellectual challenge of using computer, networking or other skills to overcome a technical problem. For example, if you have turned your vegetable mixer into a fan, or used your Arduino platform to control the watering of your garden, you could be described as a hacker.

To most people, though, the term 'hacker' is associated with just one thing: cyber criminals who gain unauthorized access to a computer system, or elements of it, for malicious purposes.

These hackers are known as black hat hackers. They look to exploit companies or individuals by bypassing security protocols to break into computer networks, generally for financial gain. These are the ones who make the news and give hackers a bad name, notably by gaining unlawful access to information from banks (such as that experienced by Qatar National Bank in 2016, when they suffered a serious breach) or other businesses.

Typically, black hat hackers steal personal data to be used for identity theft, or credit card information or IP data, such as industrial secrets.

Their actions are, of course, illegal but there is undoubtedly a black market for such data that makes their efforts hugely rewarding, and some believe the bad guys are winning the war against the good guys.

The trustworthy guys in this instance are known as white hat hackers, and they engage in what is known as ethical hacking. White hat hackers seek to identify vulnerabilities in current systems (be they computers, networks, or even Internet of Things elements), and possibly proposing fixes.

These names come from the old western movies of the 1960s, where the bad guys traditionally wore a black cowboy hat while the good guys tended to wear a white hat.

Although white hat hackers use many of the same skills as black hat hackers, they have to abide by several rules, such as obtaining preventive permission to force an access to a network; respecting a signed Statement of Work; observing good security practices; and following responsible disclosure; that is, reporting the identified vulnerabilities to software and hardware vendors first.

White hackers play a major role in both society and industry, since they enable organizations to address the vulnerability in current and future products released to the public. For instance, a few of the Microsoft or Apple iOS security updates available to install include patches that are developed based on the security vulnerabilities found by ethical hackers.

Some will argue that hacking is hacking, and that there is no such thing as ethical hacking, but reality tells a different story. Moreover, white hat hacking is growing in importance due to the increase in phishing and cybercrime.

The cost of being a victim of cybercrime is so high that a growing number of organizations are now paying big money to hackers who can identify and exclusively share with them security vulnerabilities. It was recently reported that six ethical hackers, one of whom was just a teenager from South America, each received \$1 million for their security-critical findings.

Many ethical hackers claim they do so as a hobby, rather than for financial gain, but for those who do want to make a career of out this there are an increasing number of companies employing the skills of such people. Therefore, the rewards can be huge, as Santiago Lopez – a 19-year-old from Argentina who became the world's first ethical hacker to earn \$1 million – will testify.

Hamad Bin Khalifa University's College of Science and Engineering offers an MS in Cybersecurity and also one in in Data Science. The former is conceived to allow our students to be able to reason about the fundamental properties of security, to design security solutions, and to improve the security of complex critical systems, just to cite some of the high qualifying learning objectives of our MS.

A lateral pay-off of this two-year process is for some students to discover the white hat hacker within them, while others already at that level can refine their skills and move to a superior level of knowledge and ability.



About the Author

Dr. Roberto Di Pietro, ACM Distinguished Scientist, is a full professor of cybersecurity at Hamad Bin Khalifa University's College of Science and Engineering, leading the effort to establish a world-class research and innovation center in

cybersecurity. He is an expert on FinTech services such as bitcoin, and holds eight patents/provisional patents on security topics, such as blockchain technology.

The Communications Directorate at Hamad Bin Khalifa University (HBKU) submitted this article on behalf of Dr. Roberto Di Pietro. The views expressed are that of the author's and do not necessarily reflect the university's official stance.

First Name can be reached online at (EMAIL, TWITTER, etc..) and at our company website www.HBKU.edu.qa



EVENTS

ADECS

ASIA DEFENCE EXPO &
CONFERENCE SERIES 2020

REGISTER
NOW



📍 Marina Bay Sands, Singapore

📅 4-5 February 2020



THREE TECHNICAL CONFERENCE STREAMS ONE REGIONAL MEETING PLACE



Organised by



For more information please contact us:

✉ team@asia-decs.com

🌐 www.asia-decs.com

☎ +44 (0)20 7384 8092

25 – 26 FEBRUARY 2020 | LAGOS CONTINENTAL HOTEL

Focused on the theme, "Accelerating Cyber Security for a Safer Africa", Cyber Africa Summit (CyFrica 2020) will bring together 300+ pre-qualified CISOs, CIOs, CTOs, CEOs, senior information security, risk, forensics, compliance, cyber law and law enforcement professionals from all over West Africa on to one exclusive platform.

300+

**CYBER SECURITY
EXPERTS**

40+

**ELITE
SPEAKERS**

150+

**TOP
ORGANIZATIONS**

16+

**HOURS OF
NETWORKING**

30+

**SOLUTION
PROVIDERS**

A glimpse of the stellar speaker line-up



Daniel Adaramola
CISO
Unity Bank



Olawumi Babalola
Country CISO
Standard Chartered Bank Nigeria



Igboa Abumere
CISO
Stanbic Bank



Tunde Dada
Head of IT/BCM
Vodacom Nigeria



Fene Osakwe
Group Head - IT Security
IHS Towers



Victor Idonor
Director General
Cyber Security Challenge Nigeria(CYSEC NG)



Prasanna Kumar Burri
Group CIO
Dangote Group



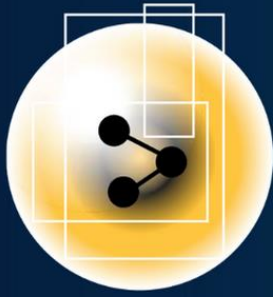
Tobe Nnadozie
Group CIO
Wapic Insurance



Indranuj Choudhury
CIO
Sterling Oil Exploration & Energy Production Co. Ltd.



Steve Isitua Obiabo
CIO/Group Head Information Technology
Chicason Group



14th Annual

BIOMETRICS FOR GOVERNMENT & LAW ENFORCEMENT

February 26-28, 2020 | Washington D.C.

**Meet Top Level
Government Security,
Biometric Officials, Heads
of Biometrics, and CTO's**

**VIEW THE
ATTENDEE LIST!**



#SaudiIoT



CYBER DEFENCE
SUMMIT

8 - 10 March

2020

Riyadh International
Convention &
Exhibition Center

Organized by



مدينة الملك عبدالعزيز
للعلوم والتقنية KACST

Government Sponsor



وزارة الاتصالات
وتقنية المعلومات
MINISTRY OF COMMUNICATIONS
AND INFORMATION TECHNOLOGY

Executed by



New Horizon
For Conferences & Exhibitions

Kingdom of Saudi Arabia is emerging as a formative leader in the adoption of Technologies...

Saudi Arabia is successful in its quest to becoming a global leader in technology and innovation. Digital transformation is one of the most significant value drivers unlocking major economic value and enabling the diversification to the Saudi Arabian economy under the rulebook of Vision 2030. Saudi Arabia was quick to commit to the transition with the adoption of Emerging Technologies.



Saudi IoT is MENA region's BIGGEST and the Most awaited event, organized by **King Abdulaziz City for Science and Technology (KACST)** and **sponsored** by Saudi Arabia's **Ministry of Communications & Information Technology**. The event will showcase new and innovative concepts, offering opportunities for tech entrepreneurs and business people to build partnerships with international firms. Saudi IoT's profuse objective is to bring the complete digital ecosystem under one unique platform to embark the Digital Transformation journey in the Kingdom & promote Technological Evolution in the region. This event is the only bridge of its kind between regional and international technology players.

Eng. Fahad Algarni, Managing Director of New Horizon expresses "I take pride in welcoming the International organizations to the Kingdom of Saudi Arabia, the land with a treasure of Immense & lucrative opportunities, Saudi IoT is a distinctive marketing platform which provides a valuable manifesto to the Sponsors & Exhibitors to benefit from. An exceptional roundup of topics covering emerging technologies, application and implications on organizations and people"

CYBER

3rd

2020

www.cypber.com



CyberSecurity4 Maritime - Oil & Gas - Energy

CYPRUS, 10 March 2020

We look forward to receive your interest on awareness of **CyberSecurity** and to explore together new approaches towards the security and risk assessment for the **Maritime, Oil & Gas** and **Energy** sectors in the Eastern Mediterranean.

More details at www.cypber.com

SUPPORT



Media Partners



Organizer

ZOMIDEA design & services ltd
T: +357 22 515561
E: zomidea@cytanet.com.cy
W: www.zomidea.com



BAPCO 2020

The Annual Event



10 - 11 MARCH 2020 | RICOH ARENA, COVENTRY

WWW.BAPCO-SHOW.CO.UK

REGISTRATION NOW OPEN

THE UK'S LEADING PUBLIC SAFETY TECHNOLOGY EVENT

**"NO EVENT IS BIGGER OR MORE
IMPORTANT IN THE UK FOR PUBLIC
SAFETY PROFESSIONALS"**

Chris Fleckney – ESN Business Change, Metropolitan Police



2000+ PUBLIC SAFETY
PROFESSIONALS



INNOVATIVE TECHNOLOGY
FROM LEADING SUPPLIERS



EXPERT-LED CONFERENCE
SESSIONS



INTERACTIVE BAPCO
DRONE ZONE



Platinum Sponsor



Silver Sponsors



CAPITA



AUTOMOTIVE CYBERSECURITY

DETROIT

March 30 – April 1, 2020
Detroit, MI

Meet Automotive
OEMs, Tier 1
Manufacturers,
and Solution
Providers

DOWNLOAD THE
EVENT GUIDE!





WE ARE ALL IN THE RACE TO PROTECT THE GRID!

MARCH 30 – APRIL 1, 2020
ANAHEIM CONVENTION CENTER | ANAHEIM, CA

CYBERCON 2020 IS THE NEW, SOLUTIONS-BASED CONFERENCE that gives power and utility executives unprecedented access to the cybersecurity experts who are as invested as you are in the race to protect the grid.

Discover the latest strategies, solutions and technologies to protect your infrastructure from what's next in a rapidly evolving industrial cyber risk landscape.

Industry Leaders

Cybersecurity Experts

Cybersecurity Workforce Development

We are all racing to protect our nation's power grid from cyber-physical threats by educating and growing the global cybersecurity workforce. It's never been more essential to be on the leading edge and prepared for the future.

LEARN MORE AND REGISTER TODAY AT

www.CyberConConference.com



EXPOSEC INTERNATIONAL SECURITY FAIR

14 to 16

APRIL | 2020

SÃO PAULO EXPO

SÃO PAULO - BRAZIL
FROM 1PM TO 8PM

THE NEW ERA
OF SECURITY

CONNECTED.



Anticipate your Accreditation!
Visit the Site:

www.exposec.com.br

 [exposecbrasil](https://www.facebook.com/exposecbrasil)

 [feirainternacionaldeseguranca](https://www.instagram.com/feirainternacionaldeseguranca)

 [@feiraexposec](https://twitter.com/feiraexposec)

 [exposec](https://www.linkedin.com/company/exposec)

 [Cipa Fiera Milano](https://www.youtube.com/CipaFieraMilano)

Or Catch the Smartcode



Affiliated:



Member of:



International Network:



Realization:



Official Magazine:



Venue:



Organization and Promotion:



CYDES 2020

THE WORLD'S FIRST INTEGRATED CYBER DEFENCE, CYBER SECURITY & FUTURE TECHNOLOGY GOVERNMENT AND TRADE EVENT FOR THE GLOBAL NATIONAL SECURITY LANDSCAPE

24-26 MARCH 2020

MAHSURI INTERNATIONAL EXHIBITION CENTRE
LANGKAWI ISLAND, MALAYSIA

"EMBEDDING RESILIENCE WITHIN OUR CYBERSPACE"

CYDES 2020 will be a showcase of advanced expertise, solutions and technologies to combating present and future cyber threats especially for government, military and law enforcement with one common objective of protecting each nation's critical infrastructure networks including:

- ▶ Banking & finance
- ▶ Emergency services
- ▶ Energy
- ▶ Food & agriculture
- ▶ Government
- ▶ Health services
- ▶ Information & communications
- ▶ National defence and security
- ▶ Water
- ▶ Transportation

FEATURE EVENTS

AI & ROBOTIC
DRONE & SATELLITE
NXT SECURITY



PLEASE CONTACT OUR SALES TEAM LOCATED NEAREST TO YOUR BASE:

For Local (Malaysian)

Mohd Hadhri
Tel : +60125379019
Email : hn@aisgroup.biz

Syarifuddin Shahrin
Tel : +60135989497
Email : ss@aisgroup.biz

For Asia & Russia

T.Devadas
Tel : +6581136515
Email : td@aisgroup.biz

Adeline Cheah
Tel : +6598247920
Email : ac@aisgroup.biz

For United States,
Middle East, Europe & Africa

Randy Wright
UK : (+44) 7510371883
UAE : (+971) 501043458
Malaysia : (+60)125684804

Supported by :



Organiser :



ISAF | CyberSecurity

9th International Cyber Security, Information & Network Security Exhibition

OCTOBER 08th-11th, 2020

Istanbul Expo Center (İFM) - Türkiye



www.isaffuari.com

T. +90 212 503 32 32 - marmara@marmarafuar.com.tr

MARMARA
TANITIM FUARCILIK
www.marmarafuar.com.tr

 /marmarafuar

 /isafexhibition

 /company/marmara-fuar

CCPA

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

VS

GDPR

GENERAL DATA PROTECTION REGULATION

1 When Do You Need to Comply?

GDPR

May 25, 2018

CCPA

Jan 1, 2020



GDPR

Any business that collects or processes the data of EU citizens or residents

CCPA

Any company conducting business with California citizens that:

- Has an annual revenue of \$25M+
- Collects, shares, buys, or sells the data of >50,000 Californian consumers
- Makes at least 50% of its revenue from the sale of Californian consumer data

2 Who Needs to Comply?



3 What Are the Penalties for Noncompliance?

GDPR

Up to 4% of the company's annual gross revenue or 20M euros

CCPA

\$750 per person, per violation



www.egyptdefenceexpo.com

[@egyptdefenceexpo](https://www.instagram.com/egyptdefenceexpo)

[/egyptdefenceexpo](https://www.facebook.com/egyptdefenceexpo)

[@visitedex](https://www.tiktok.com/@visitedex)

[#edex2020](https://twitter.com/visitedex)

THE 2ND EDITION OF EGYPT'S ONLY INTERNATIONAL DEFENCE EXHIBITION

EGYPT INTERNATIONAL EXHIBITION CENTRE
7-10 DECEMBER 2020

 **400 +**
EXHIBITORS

 **30,000 +**
VISITORS

 **FULLY-HOSTED VIP**
DELEGATION PROGRAMME

Media Partner

Supported by

Organised by



The only security event you need to be a part of

IFSEC International returns to ExCeL London on 19-21 May 2020

IFSEC International, Europe's leading integrated security event, is critical to today's changing landscape. Running for the first time alongside *Counter Terror Expo* and *Smart Buildings Expo*, IFSEC is your unmatched opportunity to showcase your security technologies to a global network of installers, integrators, end-users, consultants, distributors and government officials.

"IFSEC has been transforming over the years. It is a must attend show for any stakeholder in physical and converged security."

CTI/CISO
Virtually Informed

"It was our first time exhibiting in the UK and Europe, as we wanted to expand our markets. There was a good quality of visitors and foot traffic – we would definitely exhibit again."

Business Development
Manager, **Telaeris Inc**

"We came to broaden our security portfolio, we wanted to explore the markets and understand ROI. It has been a really successful show with excellent networking opportunities."

Business Manager
Siklu

For more reasons to exhibit and to book your stand visit: www.ifsec.events/international

Co-located with:

FIREX
INTERNATIONAL

SAFETY & HEALTH EXPO

FACILITIES
SHOW

SMART BUILDINGS
EXPO

CTX
COUNTER
TERROR EXPO
19-21 May 2020
ExCeL, London

FORENSICS
EUROPE EXPO
19-21 May 2020
ExCeL, London

AMBITION
THE EPRR EXPO
19-21 May 2020
ExCeL, London

Plus:

EXPLORE THE HUMAN ELEMENT OF CYBERSECURITY.



What's the most important weapon in the fight against cyberthreats? New software? Faster equipment? Smarter computers? At RSA Conference, we believe it's people.

Attend RSA Conference 2020, February 24-28, and join thousands of security professionals, forward-thinking innovators and solution providers for five days of actionable learning, inspiring conversation and breakthrough ideas.

Register today to save your spot at the world's most comprehensive cybersecurity event.

rsaconference.com/cyberdefense-us20

#RSAC



FOLLOW US

You don't need to be next in line for a data breach.

Put on your thinking hat and step into the shoes of a hacker.

Cyber incidents are on the rise. While most organizations play defense--creating plans that tell them what to secure and how to react if their security settings fail--it's not enough to respond to a data breach.

What if you looked at cybersecurity from a different point of view?

In our guide, "How to Think Like a Hacker and Secure Your Data," you'll discover how to go on offense with your data by:

- Diving into modern data breach statistics
- Exploring hacking terminology and techniques
- Walking through seven strategies for data protection

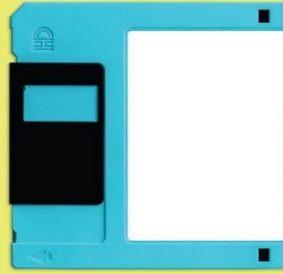
Are you ready to put yourself in the shoes of a hacker?

Visit [**https://www.goanywhere.com/think-like-a-hacker**](https://www.goanywhere.com/think-like-a-hacker) to get a free copy of our cybersecurity guide.



GO ANYWHERE®
Managed File Transfer





File Transfer – Done the Right Way

Graduate to the Better Method

There are currently numerous ways to transfer files. Even if some of the methods are old-school and not as highly recommended as others, they are options available to you.

The good news is that newer, better, and faster methods now exist. For instance – the Grade A method itself, secure managed file transfer.

Along with offering IT teams multiple options for users and partners to securely exchange data, managed file transfer can also:

- Be deployed on-premises or to cloud computing platforms (i.e. AWS and Azure)
- Exchange files via batch, collaboration, and ad-hoc methods
- Use workflows to execute tasks before and/or after transfer

Graduate to the BEST method! Our guide, “How to Do File Transfer the Right Way” is a great way to see what else this dynamic secure file transfer solution can do.

Visit www.goanywhere.com/openpgp-studio for a free copy!



GO ANYWHERE®
A HelpSystems Solution



DATA PROTECTION WORLD FORUM

PRIVACY | TRUST | RISK | SECURITY

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Rowena Fell

Global and EMEA Risk Assurance
Operations Leader - Ernst & Young

Flavius Plesu

Head of Information Security
Bank of Ireland UK

Steve Wright

Data Privacy and Information
Security Officer - John Lewis

Marloes Pomp

Head of Blockchain Projects
Dutch Government



SEE THESE SPEAKERS FOR FREE

Use our code 'CYBERMAGFREE'

#CYBERBYTE
@ROSSOWESQ



Meet Our Publisher: Gary S. Miliefsky, CISSP, fmDHS

“Amazing Keynote”

“Best Speaker on the Hacking Stage”

“Most Entertaining and Engaging”



Gary has been keynoting cyber security events throughout the year. He's also been a moderator, a panelist and has numerous upcoming events throughout the year.

If you are looking for a cybersecurity expert who can make the difference from a nice event to a stellar conference, look no further email marketing@cyberdefensemagazine.com



CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here...we've launched CyberDefense.TV

At least a dozen exceptional interviews rolling out each month starting this summer...

Market leaders, innovators, CEO hot seat interviews and much more.

A new division of Cyber Defense Media Group and sister to Cyber Defense Magazine.

The Interviews

These anticipated "CEO Hotseat" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by **Gary Miliefsky**. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense eMagazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. [Click here](#) to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

[By signing up, you'll always be in the loop with CDM.](#)

Copyright (C) 2020, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com

All rights reserved worldwide. Copyright © 2020, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

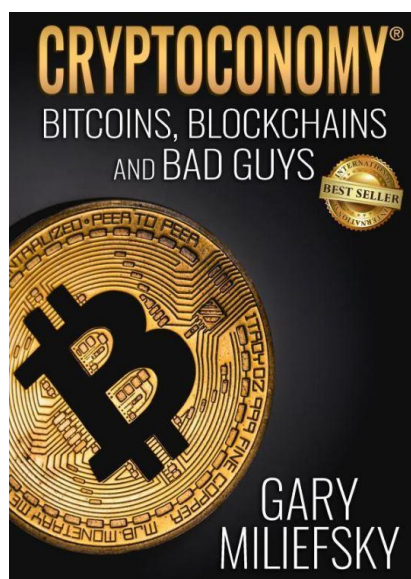
NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 01/03/2020

TRILLIONS ARE AT STAKE

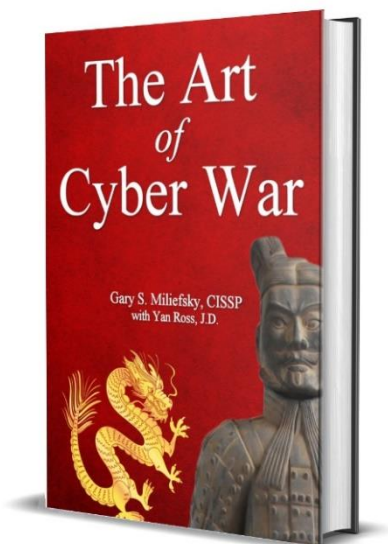
No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES

Released:



<https://www.amazon.com/Cryptoeconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH>

In Development:





Do your file transfers meet the right compliance requirements?



GDPR. DTRP. PCI DSS. HIPAA.

There are so many data compliance laws and regulations impacting file transfer that you might not have noticed **we completely made one of these acronyms up.**

Data handling requirements exist to protect sensitive information, from consumer credit card details, to electronic health records (EHR), and personally identifiable information (PII). Be confident that you not only pass the latest audit standards but are responsibly protecting the data of those who trust your organization.

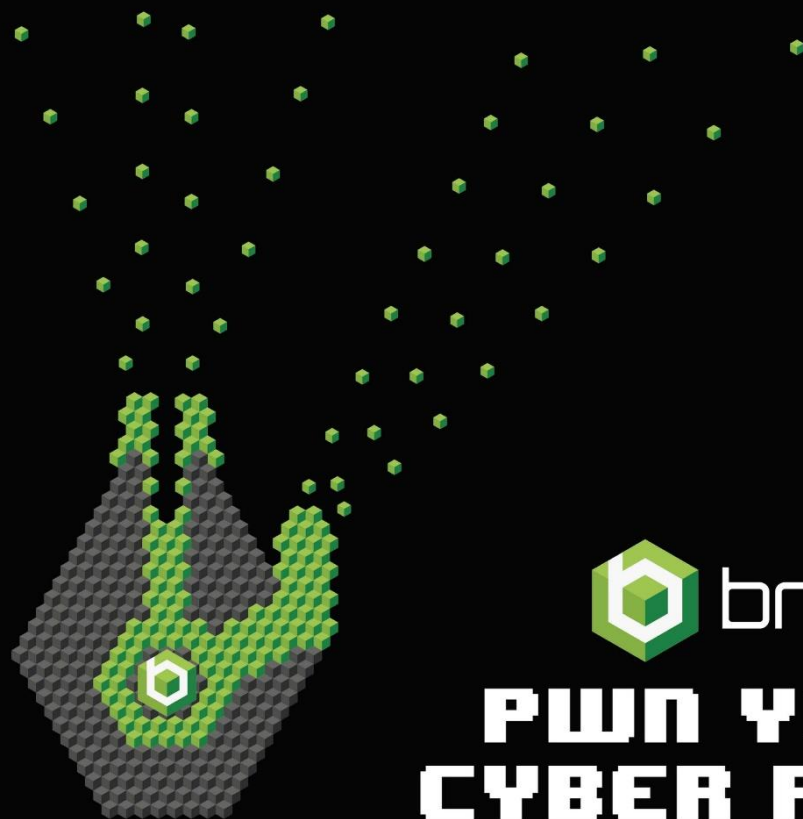
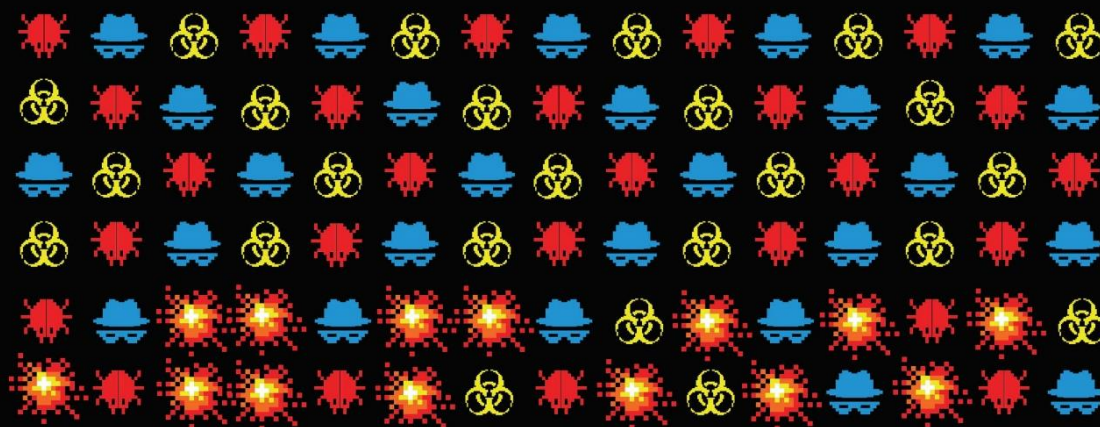
GoAnywhere Managed File Transfer makes securing data easy with tools such as:

- Full end-to-end encryption
- Detailed audit logs and reporting
- Stringent security controls
- And more



GO ANYWHERE®
Managed File Transfer

Learn how GoAnywhere helps meet security requirements for organizations worldwide at:
www.goanywhere.com/ga-compliance-ds



**PWN YOUR
CYBER RISK**

GROUNDBREAKING
COMPANY
APPLICATION SECURITY

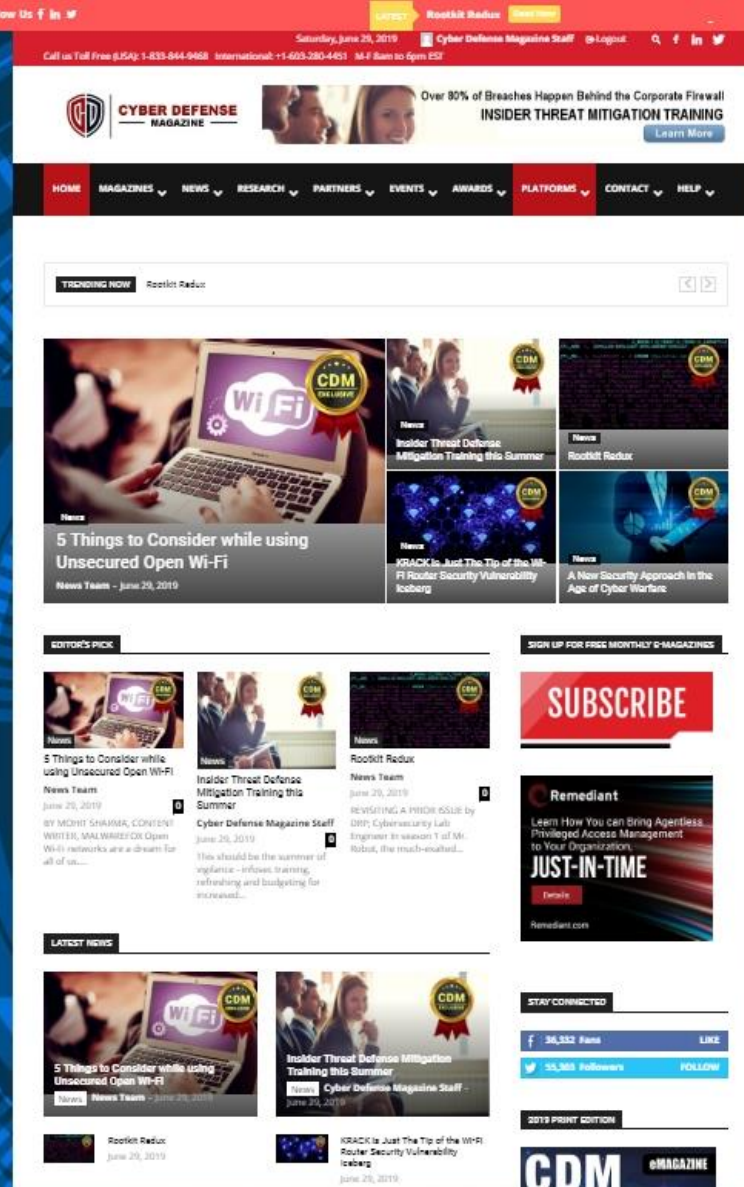
CYBER DEFENSE MAGAZINE

2019

**BEST
PRODUCT**
VULNERABILITY
MANAGEMENT

CYBER DEFENSE MAGAZINE

2019



Nearly 8 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 shooting for 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 CyberDefenseMagazineBackup.com up and running as an array of live mirror sites.

5m+ DNS queries monthly, 2m+ annual readers and new platforms coming...

JUNE 2-4, 2020

David L. Lawrence Convention Center | Pittsburgh, PA

SMART MANUFACTURING EXPERIENCE

the path to the connected world of manufacturing

Greater Connectivity = Greater Need for Cybersecurity Solutions

- **Thousands of buyers.** Engage with qualified attendees searching for the best ways to secure their data and their business
- **Exclusive opportunity.** Only open to companies that can demonstrate a connection/application to smart manufacturing
- **Active participants.** Demonstrate your solutions and educate manufacturers on the most effective methods to safeguard their valuable data

The Event is Focused on These Transformative Technologies:

- | | |
|---|---------------------------------------|
| • Cybersecurity | • Automation & Robotics |
| • Additive Manufacturing (AM) & 3D Printing | • Data Analytics |
| • Artificial Intelligence/Machine Learning | • Industrial IoT (Internet of Things) |
| • Augmented Reality (AR) and Virtual Reality (VR) | • Workforce Transformation |



Be Part of the Experience!

Call **800.733.3976** or visit smartmanufacturingexperience.com



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
Star of ABC's Shark Tank
Founder & CEO of Herjavec Group

Recognized Industry-Wide

**MOST INNOVATIVE
IAM PROVIDER**



**SECURITY SERVICES
LEADER**



**LEADER IN MANAGED
SECURITY SERVICES**



**SECURITY COMPANY
OF THE YEAR**



**#1
ON THE**



**TOP 10
ON THE**



CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefenseemagazine.com

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

Gary S. Miliefsky, Publisher & Cybersecurity Expert



**ALWAYS FREE
NO STRINGS ATTACHED**

EXPLORE THE HUMAN ELEMENT OF CYBERSECURITY.



What's the most important weapon in the fight against cyberthreats? New software? Faster equipment? Smarter computers? At RSA Conference, we believe it's people.

Attend RSA Conference 2020, February 24-28, and join thousands of security professionals, forward-thinking innovators and solution providers for five days of actionable learning, inspiring conversation and breakthrough ideas.

Register today to save your spot at the world's most comprehensive cybersecurity event.

rsaconference.com/cyberdefense-us20

#RSAC



FOLLOW US