



**CYBER DEFENSE**  
MAGAZINE

**eMAGAZINE**

**MAY**  
**2021**

## In This Edition

*Addressing the Growing Cybersecurity Risks of  
Cyber-Physical Systems*

*Boosting Morale During Tough Times Will Also  
Boost Your Security Resilience*

*COVID-19 Pushes the Introduction of Secure  
Digital Government Solutions*

*Current Cybersecurity Weaknesses Will Result  
in Continued Data Breaches*

*...and much more...*

**MORE INSIDE!**

# CONTENTS

Welcome to CDM's May 2021 Issue-----	6
<b><i>Addressing the Growing Cybersecurity Risks of Cyber-Physical Systems -----</i></b>	<b>21</b>
By Michael Welch, Managing Director, MorganFranklin Cyber	
<b><i>Boosting Morale During Tough Times Will Also Boost Your Security Resilience -----</i></b>	<b>25</b>
By Nir Polak, CEO, Exabeam	
<b><i>COVID-19 Pushes the Introduction of Secure Digital Government Solutions-----</i></b>	<b>29</b>
By Andreas Räscheimer, CEO at Veridos	
<b><i>Current Cybersecurity Weaknesses Will Result in Continued Data Breaches -----</i></b>	<b>32</b>
By Randy Reiter CEO of Don't Be Breached	
<b><i>The Internet of Things Ongoing Directions -----</i></b>	<b>35</b>
By Milica D. Djekic	
<b><i>The Importance Of Protecting Your App's Source Code -----</i></b>	<b>38</b>
By Rui Ribeiro, CEO and Co-founder, Jscrambler	
<b><i>How Various Flavors of PKI Can Protect and Secure Financial Services Data -----</i></b>	<b>41</b>
By Abul Salek, Director of Product Management, Sectigo	
<b><i>Five Steps for Safely Migrating your Workloads to the Cloud -----</i></b>	<b>45</b>
By Paul Farrall, CISO at Skytap	
<b><i>Cybersecurity in Healthcare: Benefits, Examples, and Usage Tips Healthcare cybersecurity framework -----</i></b>	<b>48</b>
By Kate Orekhova, Cleveroad company	
<b><i>All the User Experience, None of The Security?-----</i></b>	<b>56</b>
By Deepika Gajaria, Vice President of Product, Tala Security	
<b><i>In the Midst of COVID-19, We're Seeing a Pandemic of Cyber Attacks -----</i></b>	<b>58</b>
By Babur Khan, Technical Marketing Engineer - Enterprise Security at A10 Networks	
<b><i>Why A 'Layers and Lists' Approach to Cybersecurity Is Doomed to Fail -----</i></b>	<b>62</b>
By Gary Fischer, VP Americas, XM Cyber	

---

<b><i>New Report Shows Over Two Million Secrets Detected on Public GitHub in 2020 and a 20% growing trend Year-Over-Year.</i></b> -----	<b>65</b>
By Jeremy Thomas, GitGuardian CEO	
<b><i>Securing Patient Private Information in The Age of Shared Information</i></b> -----	<b>69</b>
By Christian Gitersonke, CEO, Health Insurance Answers	
<b><i>Overcoming Security as a Barrier to Cloud Adoption</i></b> -----	<b>73</b>
By Ron Newman, SVP at NTT Ltd. Security Division	
<b><i>Three things’ organizations must do to secure “passwordless”</i></b> -----	<b>75</b>
By Jerome Becquart, COO, Axiad	
<b><i>Time Is Money: How to Minimize Data Breach Damages with Early Detection</i></b> -----	<b>78</b>
By Karl Swannie, Founder, Echosec Systems	
<b><i>Why We Care About Cybersecurity Hygiene</i></b> -----	<b>81</b>
By James Opiyo, Senior Consultant Security Strategy, Kinetic By Windstream	

@MILIEFSKY

From the  
**Publisher...**



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

**Dear Friends,**

We're now only weeks away from RSAC 2021 with the theme "RESILIENCE". We're so grateful to be part of this event and continue in our 9<sup>th</sup> year of partnering and promoting this event with the awesome team at the RSA Conference. Even though we're all under tremendous pressure in this remote worker transition, we will succeed!

"Grace Under Pressure" is a long-standing commendatory phrase often used to celebrate success under difficult circumstances. Based on my broad view of the collective response of individuals in our cybersecurity industry, it is clear that these professionals have demonstrated this sought-after acclamation.

Let me be clear, the cybersecurity threats are nowhere near over; they will continue as long as digital data and storage facilities exist. But at this moment, with more than 3200 companies, and untold numbers of free-lancers, in the marketplace, the home team has admirably risen to the challenge.

This May issue of Cyber Defense Magazine is replete with examples of cybersecurity professionals who have submitted articles based on their own experiences and expertise. In turn, this information and interpretation will help our readers in the industry to grow their own successes.

As you review the topics in our Table of Contents and focus on the articles of relevance to your own endeavours, please know that you are among millions of other professionals who depend on Cyber Defense Magazine and the other affiliates of Cyber Defense Media Group to support these important functions of protecting our cyber assets from attacks by criminals and state actors.

Wishing you all success in your own cyber endeavours.

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...

The international implications for cybersecurity during the pandemic are intensified by the widely divergent impacts of COVID-19 and its variants on our various nations and international organizations.

More and more, we see conflicting vectors pulling us in different directions, and challenging our ability to maintain a healthy coordination between national interests and international, even global, responses to the disruption of “business as usual” and the so-called “new normal.”

Even with the guidance of the World Health Organization, individual nations are responding to physical threats in divergent ways, which results in disparate outcomes in health, the ability to function normally, and ultimately the way digital work gets done.

Both individually and organizationally, our resilience in overcoming these challenges makes the difference between success and something less. Although the concept may now verge on becoming a cliché, the threat is truly “existential” in its potential impact.

As always, we encourage cooperation and compatibility among nations and international organizations in responding to these cybersecurity and privacy matters.

**To our faithful readers, we thank you,**  
**Pierluigi Paganini**  
International 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](mailto:stevinv@cyberdefensemagazine.com)

### INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER

Pierluigi Paganini, CEH

[Pierluigi.paganini@cyberdefensemagazine.com](mailto:Pierluigi.paganini@cyberdefensemagazine.com)

### US EDITOR-IN-CHIEF

Yan Ross, JD

[Yan.Ross@cyberdefensemediagroup.com](mailto:Yan.Ross@cyberdefensemediagroup.com)

### ADVERTISING

[marketing@cyberdefensemagazine.com](mailto: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 © 2021, 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/>

## 9 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:

**CDMG   B2C MAGAZINE**

**B2B/B2G MAGAZINE   TV   RADIO   AWARDS**

**PROFESSIONALS   WEBINARS**

---

## Welcome to CDM's May 2021 Issue

### From the U.S. Editor-in-Chief

We find ourselves another month into the COVID-19 pandemic with no end in sight. It is no wonder our pages for the May issue of Cyber Defense Magazine reflect continued and growing developments in dispersal of the digital workforce as well as the migration to cloud facilities for the storage and access of data.

No doubt remains that the digital effects of this health emergency are going to be with us well into the foreseeable future. But there are also diverging trends.

For example, the continuation and institutionalization of work-from-home (WFH) appears to be divided into two camps: those organizations providing incentives for workers to return to a more controlled central environment on one hand, and those working to harden the WFH structure to resist cyber-attacks.

We are fortunate to count on a broad diversity of perspectives among our contributors this month, providing informative and actionable information on the various trends and developments.

We strive to make our publication most valuable to our readers by keeping current on emerging trends and solutions in the world of cybersecurity. To this end, we commend your attention to the valuable guidance provided by our expert contributors.

Wishing you all success in your cybersecurity endeavors,

Yan Ross

U.S. Editor-in-Chief

Cyber Defense Magazine

### About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at [yan.ross@cyberdefensemediagroup.com](mailto:yan.ross@cyberdefensemediagroup.com)





# SPONSORS



## Prepare Against Cyber Attacks!

With Dynamically Defined Defense™ (3D).

[See If I Need Cyber Defense](#)

### Cyber Defense

Best-in-Class Cyber Defense Services, operated 24 / 7 by Industry-Leading Professionals from around the world.

### IRAAS + TRU-A™

Incident Response as a Service provided by our dedicated world class Threat Operation Center.

### Digital Forensics

You need answers into what happened and how to fix it. You want to know who accessed what, when and how.

### Remote Monitoring

Our Threat Operation Center Provides Remote Monitoring and Response Services with dedicated Analysts at your side.

As seen in

THE WALL  
STREET  
JOURNAL.



CIOReview

I.R.I.S.™  
INCIDENT RESPONSE INVESTIGATION SYSTEMS

TRU-A  
THREAT RESEARCH UNIT ALPHA

AI acquisition  
international  
*the voice of modern business - est. 2010*



THETA432™  
BEYOND VISIBILITY™

**Next Gen**  
Managed Prevention, Detection  
And Response Services (MPDRS)



THETA432™  
BEYOND VISIBILITY™

**Cutting Edge**  
Cyber Defense Services



THETA432™  
BEYOND VISIBILITY™

**Hot Company**  
Cyber Security Services



THETA432™  
BEYOND VISIBILITY™

**Publisher's Choice**  
Cyber Threat Services



# THE SECRETS OF HARDENING ACTIVE DIRECTORY

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

**GET YOUR FREE eBook**

Get <https://cionsystems.com/>




# Passwordless Anywhere with **SMARTidentity**

Secure digital interactions for users  
and machines to keep your business  
moving forward



[axiad.com](https://axiad.com)



A man with dark hair and glasses, wearing large black headphones, is seated at a wooden desk. He is looking down at a laptop, with his right hand on the trackpad. The desk is cluttered with various items, including a smartphone and some papers. The background is slightly blurred, showing a wooden floor and a chair.

# FOCUS ON YOUR BUSINESS, NOT YOUR EMPLOYEES' CYBER HABITS.

---

CYBERSECURITY DONE RIGHT.

[FluencySecurity.com](https://FluencySecurity.com)



# Do you check the boxes with your cybersecurity?

## ☒ Leadership Prioritizes Cybersecurity

☐ Assessments

☐ Plans

☐ Policies

☐ Procedures

☐ Training

☐ Education

☐ Testing

☐ Scanning

☐ Monitoring

☐ Response



### Antivirus

*Protects devices  
against known  
infections*



### Firewalls

*Protects  
networks against  
unauthorized access*



**DEFENDIFY**

*Cybersecurity. Simplified.*

*Protects organizations against  
diverse threat landscape*

What's Your Cybersecurity Strength?

A+ A A- B+ B B- **C+** C C- D+ D D- F

Find out in 3 minutes

[www.defendify.io/mygrade](http://www.defendify.io/mygrade)



# Predictive Cyber Defense

**Lucio Frega, Threat Researcher**

Deutsche Telekom - Cyber Threat Intelligence

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.

## About the Author/Disclosure



Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.

  
MALWARE  
YARA  
HUNT

PREDICT

# 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](http://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](https://attivonetworks.com/ebook)

# 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



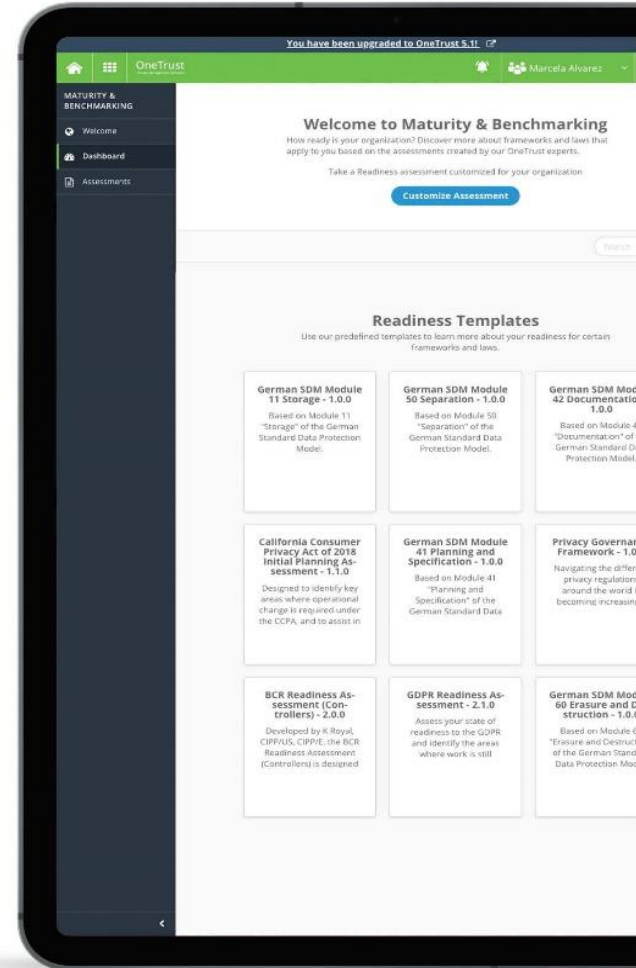
#### Third-Party Risk Management

- **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](https://onetrust.com/request-a-demo) | [ONETRUST.COM](https://onetrust.com)



# STRATEGIC COMMUNICATIONS

## Now More Than Ever, You Need To Be Connecting With



Customers



Influencers



Media

**At Vrge Strategies,** we've been making connections that businesses build around for more than a decade.

Cybersecurity companies (from VC-funded startups to the Fortune 500) and global nonprofits count on us every day to deliver results that lead, influence, as well as spark conversations and new business.

Isn't it time you maximized the value of your **strategic communications?**

**Come talk to us,  
we'd love to connect.**

Email Adam Benson  
adam@vrge.us  
or visit us at  
[www.vrge.us/cybersecurity](http://www.vrge.us/cybersecurity)

**vrge**

Navigate the Politics  
of Disruption

# Database Cyber Security Guard

**Don't be the next data breach. Equifax paid \$575 million, British Airways \$230 million and Marriott \$124 million in fines.**

**Prevents confidential data theft by Hackers, Rogue Insiders, Phishing Emails, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks.**

## Product Features

- **Detects Informix, MariaDB, MySQL, Oracle, SQL Server and Sybase data theft within milliseconds and shuts down Hackers immediately.**
- **Advanced SQL Behavioral Analysis of the database query activity learns the normal query patterns and detects database data theft.**
- **View all suspicious database activity and attempted data theft.**
- **Supports key GDPR compliance requirements. Non-intrusive detection of data theft. Runs on a network tap or proxy server.**

**Get a FREE COPY now.**

[www.DontBeBreached.com/Free](http://www.DontBeBreached.com/Free)



**"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](http://www.nightdragon.com)

A hand holding a black pen is positioned over a spiral-bound notebook on a wooden desk. To the left of the notebook is a white computer keyboard. The background is a blurred image of a building with a blue-tinted network overlay consisting of white lines and dots. A semi-transparent horizontal band across the middle of the image contains the word "ARTICLES" in large, bold, black capital letters.

# ARTICLES



# Addressing the Growing Cybersecurity Risks of Cyber-Physical Systems

By Michael Welch, Managing Director, MorganFranklin Cyber

Cyberattacks against critical infrastructure and other cyber-physical systems have increased for years. These attacks are particularly concerning because they pose a realistic threat to peoples' lives, health, and safety.

As the Internet of Things (IoT) continues to expand, society also becomes increasingly dependent on cyber-physical systems. Properly securing these systems is essential to managing the risks that they pose to owners, managers, and the general community.

## Cyber-Physical Attacks Are Not Theoretical

Cyber threat actors have had the capabilities to access critical infrastructure for a long time. However, in recent years, security incidents in power grids and other infrastructure have moved from proof of concept to actually harnessing this access.

Some examples of high-profile cyber-physical attacks include:

- Stuxnet, one of the most famous cyberattacks to date, used malware to disrupt and damage centrifuges.
- Multiple cyberattacks against the Ukrainian power grid caused a loss of power to hundreds of thousands of residents.

- 
- A ransomware attack in February 2020 caused a two-day shutdown of a US-based natural gas operator.
  - The recent cyberattack against a water treatment plant in Oldsmar Florida could have resulted in a poisoned water supply if not detected and reversed in time.

However, while critical infrastructure threats result in some of the most visible and wide-reaching cyber-physical attacks, they are not the only area to consider. Research has demonstrated numerous potential attack vectors against pacemakers and other personal health devices, which could be exploited to cause personal harm or used for ransomware attacks. The increased use of IoT devices in manufacturing, transportation, and similar sectors make it possible for cyberattacks to cause industrial accidents, train derailments, and similar incidents.

## Addressing Cyber-Physical Security Challenges

Cyber-physical systems have many of the same cybersecurity challenges as their traditional IT counterparts. Although, these systems also pose additional enterprise cybersecurity risks for several different reasons.

## Operational Technology

Operational technology (OT) systems include all of the cyber-physical systems that make up critical infrastructure. This includes both specialized components (like power generation equipment) and the computers that control them.

OT cybersecurity is challenging because of the industry's unique situation. Previously, most OT devices were physically separated from IT networks, making them more difficult to access and attack. In recent years, a push for increased efficiency and centralization has eroded this air gap, suddenly connecting many devices to the internet that were not designed for external access.

These security challenges are exacerbated by the high availability requirements of OT environments. It is not feasible to shut down a power grid for a couple weeks to perform widespread updates. As such, critical infrastructure components are also only updated during tight maintenance windows, leaving systems largely out-of-date and lacking adequate protection against modern threats.

## Internet of Things Devices

IoT devices are extremely convenient for personal and professional use. The ability to centrally monitor and manage remote sites offers substantial cost-savings for organizations, and employees commonly deploy "smart" solutions in the office. This trend has only accelerated with the transition to remote work.

However, IoT devices also create significant security risks for organizations. IoT security is notoriously poor, which prompted the creation of the California Internet of Things Security Law to help ensure a baseline level of device security. Unfortunately, this regulation is not enough to ensure the devices are actually secure against exploitation.

While IoT devices create widespread digital security risks to organizations, they hold physical security risks as well. Many "smart" devices are given positions of trust within the home or office, such as controlling the temperature, managing access to doors, detecting smoke and carbon monoxide in

---

buildings, and similar functions. A cyberattack against these devices could easily cause property damage or harm to a building's residents.

### Personal Healthcare Devices

Personal healthcare devices like “smart” pacemakers and similar systems provide a higher level of patient care than was previously available. The ability to continually monitor and manage these devices allows them to be better tuned to a patient's needs.

However, the numerous ransomware attacks against healthcare providers in 2020 demonstrated that cybercriminals have no reluctance for targeting healthcare systems. These same attacks could also be aimed at personal healthcare devices. Security researchers have already demonstrated that pacemaker vulnerabilities could be exploited to deliver painful electric shocks. Similar vulnerabilities could install ransomware on these devices – forcing victims to pay for medical treatment – or performing additional attacks.

Personal healthcare devices are a specialized type of IoT device and carry many of the same security challenges. A lack of security research and investment by manufacturers, combined with the difficulty of installing updates on these devices, leaves patients vulnerable to attack.

### Inconsistent Regulation and Enforcement

For critical infrastructure, cybersecurity regulations come from the government agency responsible for that utility, but the agencies responsible differ from one to another. For example, water distribution falls under the EPA, the power grid is under the Department of Energy, and transportation is regulated by DHS and the Department of Transportation.

With different organizations directing cybersecurity needs across the sectors, cybersecurity regulations and enforcement differ as well. This can result in vulnerabilities when a particular utility lacks stringent cybersecurity regulations, or the requirements are not effectively audited or enforced.

### Best Practices for Securing Cyber-Physical Systems

Most cyber-physical attacks take advantage of lacking security sophistication. The targets of these attacks have often not gained the same level of cybersecurity research and development as traditional IT systems. Some cyber-physical systems (like parts of the power grid) predate the Internet, while others (such as IoT devices) are manufactured by companies that do not have backgrounds in IT system design and cybersecurity.

Managing these types of cybersecurity risks requires taking proactive security measures. Some best practices for protecting cyber-physical systems include:

- **Perform a Risk Assessment:** Adding IoT and other internet-connected devices to an organization's network can increase convenience at the expense of security. Before deploying these devices, perform a risk assessment to determine if the cost to organizational security outweighs the benefits.
- **Implement Network Segmentation:** IoT devices, OT systems, and other cyber-physical systems should be located on a separate segment of an organization's network. This helps protect the organization against compromise via IT networks and from being used as an entry vector into its environments.

- **Enforce Access Controls:** Cyberattacks like the Oldsmar water treatment plant hack take advantage of poor access controls. Access to these systems should be restricted based on the principle of least privilege and use multi-factor authentication (MFA) to help prevent unauthorized access.
- **Apply Updates Promptly:** Many cyberattacks against cyber-physical systems also take advantage of unpatched vulnerabilities in these devices. Regularly testing and applying updates can help mitigate the impact of security issues in these devices.
- **Use Real-Time Protection:** Real-time protection solutions run on a device and attempt to identify and block attacks against it. This approach can also help lessen the impact of unpatched devices on enterprise cybersecurity.

As the world becomes ever more connected, cyber-physical threats will increase in tandem. It is vital to understand how to incorporate these systems with sound cybersecurity strategies to minimize their cyber risks.

### About the Author

Michael Welch is responsible for supporting new business relationships and spearheading cybersecurity consulting initiatives for MorganFranklin. A leader in cybersecurity and technology with over 20 years of experience in risk management, compliance, and critical infrastructure. Mike previously served as global chief information security officer for OSI Group, a privately-owned food processing holding company that services some of the world's best-known brands throughout 17 countries. In addition, he has worked with Burns & McDonnell, Duke Energy Corp. and Florida Power & Light, among other companies. He is an accomplished CISO, senior manager, and security consultant, leading teams of InfoSec engineers, architects, and analysts to deliver complex cybersecurity transformations.



Michael can be reached online at <https://www.linkedin.com/in/michael-welch-93375a4/> and at our company website <https://www.morganfranklin.com/cybersecurity/>



## Boosting Morale During Tough Times Will Also Boost Your Security Resilience

By Nir Polak, CEO, Exabeam

While 2020 impacted nearly every business, the pandemic was not the only obstacle leaders faced last year. As we begin 2021, it's important to remember the factors that shape company morale can also play a role in determining potential security risks for your business. Changes made to teams, uncertainties around the economy and job security, employee wellness, shifting to remote work, and rising cyberthreats are just a handful of the issues leaders must combat to avoid the negative impacts on company culture.

Whether we look around the room or analyze statistical data, it's clear that job satisfaction and company culture play a vital role in navigating tough times. A survey of 351 international security professionals showed that despite high-stress levels, [cybersecurity professionals are satisfied and feel secure in their](#)

---

[jobs](#). While this is good news, business leaders must constantly consider the different ways that a negative company culture may lead to frequent employee turnover, less loyalty or even disgruntled employees, which may result in [increased security risks](#) due to negligence and/or malicious insider threats.

There are many ways organizations can improve company morale and top leadership must be behind it. Great morale will help companies get through any storm, whether unexpected turnover, data breaches, the challenges of not seeing each other in-person, Zoom fatigue that comes with 100% remote work, and the initial and ongoing shock of living through a pandemic. **Constant communication is key.**

As the effects of the pandemic and remote work carry over into 2021, managers can be empathetic in their endeavor to understand and address factors contributing to any high stress levels on their teams.

Check in on your employees through regular team meetings and encourage opportunities to unwind. At Exabeam, we've implemented a mix of offerings, from virtual meditation and yoga, to online trivia and happy hour sessions. To further lift morale, you can also:

- Build new communities that encourage frequent meetings between employees from different departments.
- Establish or resume mentorship programs that provide employees with a safe space to discuss their professional life goals and any obstacles, personal or professional, that stand in the way of achieving them.
- Ensure all managers and employees are working towards transparent and shared business objectives. This will improve performance, increase trust in leadership, build confidence and increase engagement. And most importantly, drive loyalty, commitment and passion for the work.

## Manage Stress and Recognize Employee Needs

The survey of international security professionals also revealed that despite an increase in cyberthreats in the early days of the pandemic, [three-quarters of organizations had to furlough members from the SOC team](#). Combating new and familiar threats with fewer people on staff to help naturally leads to added stress. The 2008 recession saw higher rates of unemployment and increased anxiety for those who kept their jobs. Just over a decade later, those who kept their jobs in cybersecurity are facing a larger threatscape. Compounding the issue, remote work has made it more difficult to mitigate growing threats, hindered communication with IT departments and led to more mistakes due to distractions at home.

The blurred lines between work and home also mean employees both within and outside of the SOC are working longer hours and finding it difficult to completely shut down every day. As our employees juggle the need to work with the distractions that come along with home life -- taking care of aging parents or helping children with virtual learning, for instance -- burnout should be on every business leader's radar. While the idea of vacation might mean stepping away from your desk for a few days rather than traveling to new locations or visiting loved ones, encourage your employees to take that time off and truly unplug.

Set boundaries with work schedules and offer flexible hours to those who would benefit from them. In short -- listen to your employees' needs. Fatigue across departments can lead to more mistakes, such

---

as falling for phishing emails, and on the security side, burnout can lead to SOC employees missing key attack indicators. Paying attention to employees' mental health will help them, their teams and the company's security posture.

### Keep Cybersecurity Training and Education Top of Mind

Reminding employees of basic security hygiene will also go a long way in mitigating risk and reducing the impact of negligent insider threats, such as forgetting to log out of a work computer or utilizing weak passwords. This also serves as an opportunity to remind administrators to change default passwords and apply security patches. Another useful tactic with remote work is continuing to conduct regular anti-phishing training across the organization. Regularly sending phishing emails and identifying users who do not recognize the email as phishing attempts will help reduce the number of employees and contractors who may become compromised insiders. Investing in training can also help employees develop advanced skills, open up new job opportunities, and enable organizations to deal more effectively with new, emerging threats.

### Provide Employees with Tools for Success

For organizations operating with a smaller team or fewer SOC staff, automation tools are essential in mitigating security threats. Automation provides security professionals with an opportunity to transition from lower-valued activities to other high profile, strategic projects. User and entity behavior analytics (UEBA), which tracks, collects and analyzes user and machine data to detect threats within an organization, is one such tool. Using various analytical techniques, UEBA determines anomalous from normal behaviors. This is typically done by collecting data over a period of time to understand what normal user behavior looks like, then flagging behavior that does not fit that pattern.

UEBA can often spot unusual online behaviors – credential abuse, unusual access patterns, large data uploads – that are telltale signs of insider threats. More importantly, UEBA can often spot these unusual behaviors among compromised insiders long before criminals have gained access to critical systems.

Unsettling [recent SOC research](#) shows that the pandemic has forced 60% of companies to defer investments in security technology, which were previously planned. While it's tempting to cut corners for the sake of budget, investing in automation tools now will not only assist with minimizing security team exhaustion and increasing productivity. Paradoxically, doing so could help save thousands or even millions of dollars in breach and legal costs down the line as well as the immeasurable cost of the toll on company morale.

Working in technology means your employees are tasked with difficult work that needs constant protection to keep up with the fast-paced nature of the industry. For many of us, we were able to continue that work remotely once lockdowns spread throughout the world, but as we look towards maintaining business continuity and resilience throughout this new year, we must prioritize company culture and understand the important role it plays in ensuring both employee and security wellness.

Committing to the health of our company culture will continue to ensure customer and security wellness, too.

---

### About the Author

As CEO and Co-Founder of next-gen SIEM company, Exabeam, Nir Polak is an experienced entrepreneur and successful leader in the cybersecurity market. Nir can be reached online at [www.exabeam.com](http://www.exabeam.com)





# COVID-19 Pushes the Introduction of Secure Digital Government Solutions

*The Secure Digital Authentication of Official Documents Plays an Important Role in Times of Pandemic*

By Andreas Räschmeier, CEO at Veridos

In the wake of the pandemic, governments and public authorities need smart solutions to manage the situation efficiently. Digital government solutions that enable the authentication of official documents and provide a high level of IT security have an important role to play.

The ongoing coronavirus pandemic has presented a host of challenges for governments and citizens alike. The implementation of necessary health precautions has greatly affected working environments and the ways people interact with one another, meaning many government services can no longer be carried out without digital alternatives.

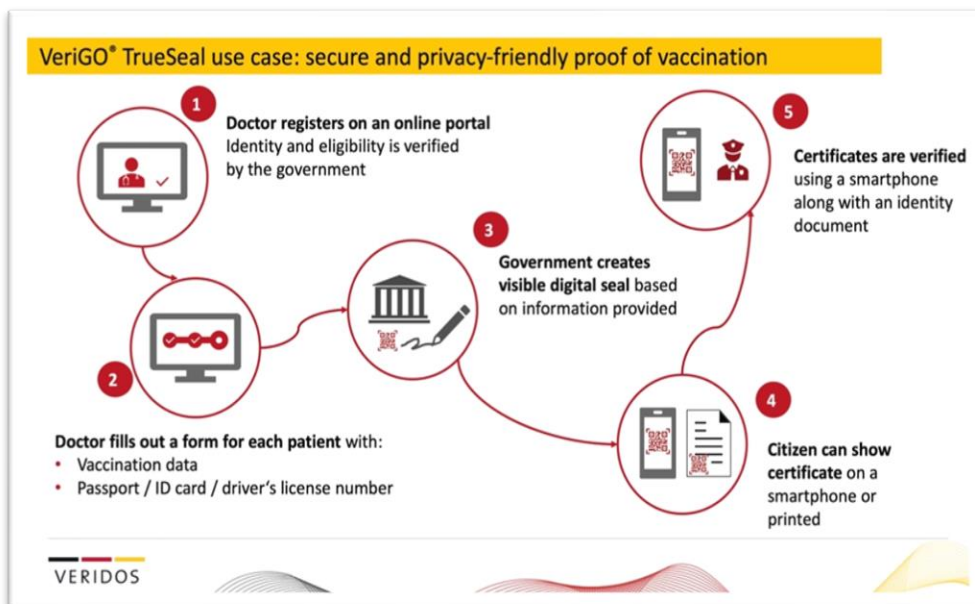
While minimizing human contact helps to contain the virus, citizens are in need to gain access to authenticated sensitive documents, including health and vaccination documents. In addition, public authorities want to ensure that those documents are genuine in order to manage the crisis efficiently.

Ultimately, we believe that the only valid answer to this problem is the development of digital government services that enable secure and user-friendly issuing and verification procedures. The outcome: highly secure certificates with a visible digital seal. This allows key users, e.g. doctors or vaccination centers, to issue universally accepted, state-authorised and recognised certificates. Such services enable citizens

to obtain digital documents from medical practitioners, insurance companies or authorities responsible for medical certificates, vaccination certificates or travel permits.

The use of a visible digital seal guarantees that the documents remain secure and in turn allows for a simple verification process. Since the seals are cryptographically secured, their content cannot be changed. Additionally, a visible digital seal helps governments and authorities to combat fraud, as government agencies can check who issued each seal and void seals that were issued in error. The visible digital seal is displayed in the form of a 2D barcode on a smartphone and can be scanned with another mobile device, or if preferred by the citizen, the seal can be printed and used in hard copy.

Veridos, a joint venture of the international technology group Giesecke+Devrient and the Federal Printing Office of Germany, offers such a digital solution with VeriGO® TrueSeal. Based on tried-and-tested technology, the easy-to-use platform can be rolled out quickly and customized for use. It represents a fast and secure solution for generating officially certified sensitive documents and provides a high level of security in these challenging pandemic times. The solution is great proof of the positive impact that smart digital government services can have.



While innovations in technology are the foundation of the development of digital government use cases, these new solutions must not only enable high-quality, user-friendly services, but must also guarantee the privacy and security of citizens. Liu Zhenmin, Under-Secretary-General of the Department of Economic and Social Affairs at the United Nations, has rightly stated that progress in the implementation of digital government services "is accompanied by existing and new challenges and risks, such as cybersecurity and data protection" (1).

Nowadays, there exist tools that drastically reduce security threats. Companies such as Veridos specialize in providing end-to-end solutions and services that meet all requirements for the secure collection and storage of data and information and the preservation of citizens' privacy. As citizens will get used to digital government services in the future, it is essential that they can trust the infrastructure behind these services – especially when it comes to sensitive documents like vaccination certificates.

In short, digital advancements along with a new normal have not only emphasized the importance for remote access of services but also the potential to integrate secure eGovernment services to existing trusted infrastructure and processes.

## About the Author

Andreas Räschmeier is CEO of Veridos GmbH, a joint venture between Giesecke+Devrient and Bundesdruckerei (Berlin). The company supplies governments and authorities with tailor-made complete solutions for secure identification. Räschmeier began his professional career at G+D in 2004, when he took over as Head of Business Development in the area of chip card security. Since then, he has held several management positions in various business sectors, including Group Vice President Sales & Marketing for the former payment division. Most recently, he was Global Vice President Operations & Global Support at the subgroup Currency Technology. He has been CEO of Veridos since November 1, 2019. Before joining G+D, the industrial engineer worked for Siemens and STMicroelectronics in France.



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

## Data Breach Statistics



## Current Cybersecurity Weaknesses Will Result in Continued Data Breaches

By Randy Reiter CEO of Don't Be Breached

Problems in cybersecurity resulted in the successful hacking campaign that foreign state hacking groups used leveraging product updates from the IT software company SolarWinds. The foreign state hacking groups' hack of SolarWinds allowed them to access important systems at nine US federal agencies, Microsoft, cybersecurity companies and 100+ private companies.

Was it the lack of cyber security funding, available security personnel, problems in existing cybersecurity solutions, management recognition of what's required to protect confidential data or the lack of security standards for protection of confidential data? Perhaps all of the above.

---

A recent Bitdefender study found that many organizations have not applied security patches issued two years ago. They found in 2020 that 64% of the security patches released in 2018 had not been applied. This is a Hackers dream come true for implementing successful Data Breach and Malware Attacks.

Some of this lag is due to not applying critical security patches on a timely basis since the patches may have a negative impact on running systems. Applying security patches can also be time-consuming and not the most exciting work for time strapped IT professionals to perform. This is perfect storm for Hackers, Rogue Insiders and Supply Chain Attacks to steal confidential data.

Confidential data includes: credit card, tax ID, medical, social media, corporate, manufacturing, trade secrets, law enforcement, defense, homeland security, power grid and public utility data. This data is almost always stored in DB2, Informix, MySQL, Oracle, SAP ASE and SQL Server databases. Once inside the security perimeter (via a Supply Chain or Zero Day Attack) a Hacker or Rogue Insider can use commonly installed database utilities to steal confidential database data. If a Hacker gains privileged access to confidential data conventional security software may not detect their presence until it is too late

### How to Stop the Theft of Confidential Database Data

Protecting encrypted (and unencrypted) confidential database data is much more than securing databases, operating systems, applications and the network perimeter against Hackers, Rogue Insiders and Supply Chain Attacks.

Non-intrusive network sniffing technology can perform a real-time full packet capture and analyze in real-time 100% the database query and SQL activity from a network tap or proxy server with no impact on the database server. This SQL activity is very predictable. Database servers servicing 1,000 to 10,000 end-users typically process daily 2,000 to 10,000 unique query or SQL commands that run millions of times a day. SQL packet sniffing does not require logging into the monitored networks, servers or databases. This approach can provide CISOs with what they can rarely achieve. Total visibility into the database activity 24x7 and protection of confidential database data.

In 2020 the DHS, Department of State, U.S. Marine Corps and the Missile Defense Agency all issued requests for proposals (RFP) for network full packet data capture for analysis of network traffic. This is an important step forward for both cybersecurity and protecting confidential database data.

### Advanced SQL Behavioral Analysis of Database SQL Activity Prevents Data Breaches

Advanced SQL Behavioral Analysis of 100% of the real-time database SQL packets can learn what the normal database activity is. Now the database query and SQL activity can be non-intrusively monitored in real-time and non-normal SQL activity immediately identified. This approach is inexpensive to setup, has a low cost of operation and low disk space usage. Now non-normal database SQL activity from Hackers or Rogue Insiders can be detected in a few milli seconds. The Security Team can be immediately notified and the Hacker database session terminated so that confidential database data is not stolen, ransomed or sold on the Dark Web.

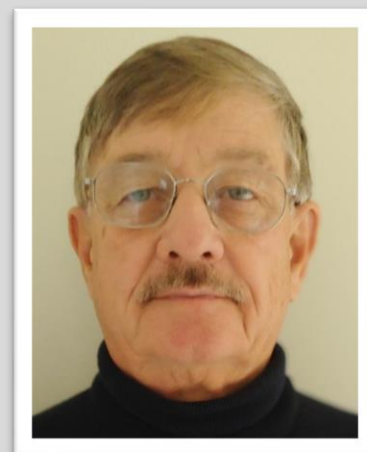
Advanced SQL Behavioral Analysis of the query activity can go even further and learn the maximum amount of data queried plus the IP addresses all queries were submitted from for each of the 2,000 to 10,000 unique SQL queries that run on a database server.

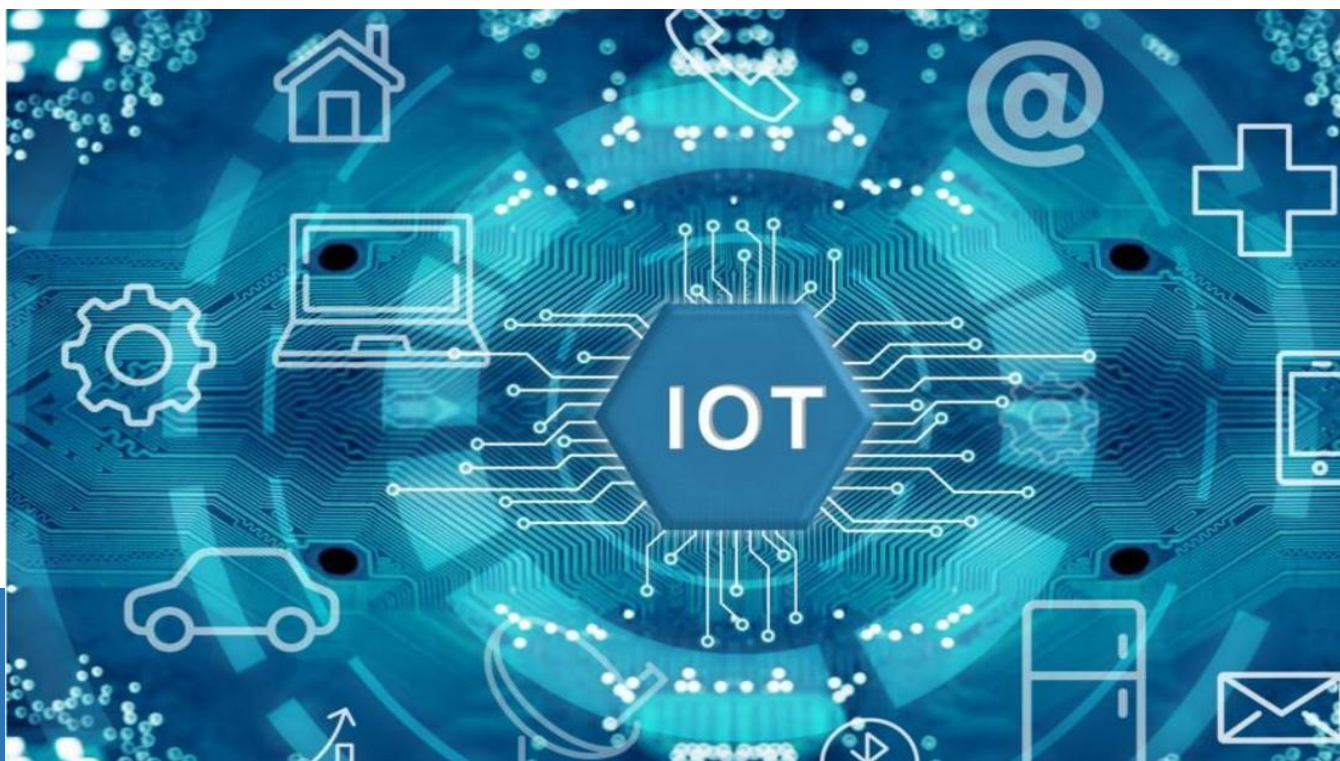
---

This type of Data Breach Protection can detect never before observed Hacker query activity, queries sent from a never observed IP address and queries sending more data to an IP address than the respective query has ever sent before. This allows real-time detection of Hackers and Rogue Insiders attempting to steal confidential database data. Now an embarrassing and costly Data Breach may be prevented.

### About the Author

Randy Reiter is the CEO of **Don't Be Breached** a Sql Power Tools company. He is the architect of the Database Cyber Security Guard product, a database Data Breach prevention product for Informix, MariaDB, Microsoft SQL Server, MySQL, Oracle and SAP Sybase databases. He has a Master's Degree in Computer Science and has worked extensively over the past 25 years with real-time network sniffing and database security. Randy can be reached online at [rreiter@DontBeBreached.com](mailto:rreiter@DontBeBreached.com), [www.DontBeBreached.com](http://www.DontBeBreached.com) and [www.SqlPower.com/Cyber-Attacks](http://www.SqlPower.com/Cyber-Attacks).





## The Internet of Things Ongoing Directions

By Milica D. Djekic

It takes time to get through the journey. Several decades back the global technological landscape has been less developed and different than it is today. In the meantime, our societies have become overwhelmed with the cutting-edge stuffs such as the Internet of Things, artificial intelligence, machine learning and much more. Indeed, all of those technologies have the strong root in the past and they are only the part of the historical wheel that impacts our lives and businesses. The primary accent of the modern emerging world is on the sub-second communication that can make both – people and machines exchanging the information at much faster level.

It appears we are connected better than ever and in that interconnected surrounding we can deal much quicker. Also, the good question in such a case is if the humans are capable to process that information that fast. Maybe the machines can proceed with those findings much better than people as they cope with the powerful processing capacities. In other words, it seems that this novel time can make us move at much prompter scale not only physically, but also virtually.

The shift from ordinary to smart landscape is not the surprise as the generations before us have prepared the condition for such a community's boom. So, our journey is long-term, and it is not over yet. Apparently,

---

it seems it is getting ready for the new and new rounds that are waiting for us in the closer or more distant future. In the modern time, when we think about the things such as virtual reality, renewable energy and much more we can notice all of those advancements are common for the technologically developed economies and as well they are doing their knock, knock at the doors of developing world.

At this stage, it appears that we live in the Internet of Things era and that technology is dealing with its everyday changes and innovations. The crucially important thing for that improvement is the web connectivity that provides an opportunity to interconnected devices to exchange the information relying on the internet signal. On the other hand, anything coping with the internet communication has its IP address and from that perspective it's clear that such a protocol is from the vital significance to that communication and also, it's the biggest weakness to such a system. From this point of view, it looks like that the security of such a communication can be the imperative for the coming times and indeed, such an innovation can run the entire breakthrough of the new industrial revolutions. The high-tech defense is something that is ongoing in this age and maybe some of the directions of the Internet of Things technology are as so. In addition, the Internet of Things is the non-separated part of the industry 4.0 that is the leading engine for the economic growth and development. The Internet of Things is gaining its popularity everywhere in the world and as the technology is getting cheaper and cheaper the industry leaders are opening the new and new marketplaces across the globe.

Basically, it's the trick that will transform the digital endeavors in the way that is so simple and probably not that revolutionary. In the essence, everyone will talk about the 4<sup>th</sup> industrial revolution and maybe they are right, but in our opinion, it is something branding new and still not the discovery on its own. So many Asian countries will take part into this competition and obviously they will not manufacture anything new but rather rely on their contractors and suppliers that will produce the semi-products, so some industry 4.0 factory will just do the assembly of the finalized parts. Anyhow, no one will care, and many industries will see the convenient chance to make the profit as well as the breakthrough to the always evolving marketplace, so far.

As we have suggested – the 4<sup>th</sup> industrial revolution is not something that will deal with any discovery, but it is the phenomenon that will impact our economies, societies, and businesses at the same glance. So, maybe we will not deal with the discovery of the alternating current as it was the case in the industry 2.0, but we will cope with the entire new environment of opportunities that will change many of so with us. Indeed, maybe this revolution if we can call it like so is not purely technological one, but more economical, business, and social by its nature. Everything is so simple and the Internet of Things by itself is becoming the outcome of the golden outlets to industry as we know it from the past. In other words, this new wave will shake and move everyone in the world and that change being revolutionary or not will impact the non-returnable process giving the chance to everyone following that tendency to make a profit for their efforts.

Some prognoses will suggest that the future directions in such a sense will seek from us to take care about our safety and security in the technological manner and indeed, maybe those courses will define our further development. From this perspective, we can notice a plenty of similarities between the 3<sup>rd</sup> and 4<sup>th</sup> technological revolution as the both occurrences will cope with the digital systems. Therefore, the

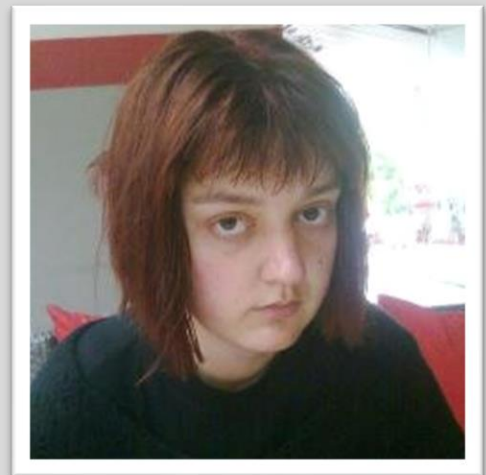
---

industry 2.0 will cope with the analog environment, while the industry 3.0 will also be dependable on electricity but it will make a shift to digital surrounding. Finally, the industry 4.0 is relying on the electricity as well, but it will be so like the 3<sup>rd</sup> industrial revolution as it will also correspond with the digital systems. The entire new trend will suggest that the next epoch will bring the revolutionary new paradigm such as quantum computing.

It's up to us to see what the future will bring, but at this stage we need to think hard how to protect our lives and assets from the harm. The things are not always as they seem.

### About The Author

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





# The Importance Of Protecting Your App's Source Code

By Rui Ribeiro, CEO and Co-founder, Jscrambler

If your business operations involve any type of web or mobile app, it's likely that the source code of these apps represents a very important part of your company's intellectual property. As a result of the ongoing digital transformation, these apps have often become key pieces of a company's competitive advantage and thus a strategic business asset. It's no wonder then that unwarranted access to this source code could put this competitive advantage at risk. However, this is just the tip of the iceberg, as unprotected source code can lead to critical security issues such as automated abuse, piracy, and data exfiltration.

When we take a look at the development scheme, we see that JavaScript, for instance, has grown immensely over the years, and now it powers around 97% of modern web applications. Every Fortune 500 company relies on this thriving open-source ecosystem with thousands of frameworks available that speed up the development process. But, despite the many benefits and business value associated with JavaScript, organizations need to consider the changes to their threat model when using JavaScript-based web and mobile applications. Especially when it comes to applications in sectors such as banking, healthcare, broadcasting, and e-commerce.

The tricky part about JavaScript is that it needs to be interpreted by a browser for it to work, therefore becoming exposed in a way that anyone can access, read, and change. And although the general recommendation is to keep sensitive code on trusted environments such as the backend, this is often

---

infeasible due to the inherent performance issues. The result is that companies end up running proprietary algorithms and important business logic on the exposed client-side.

Regulations and standards such as NIST and ISO 27001 also mention the risks of unprotected source code, recommending that organizations put in place strict control procedures to keep them from experiencing the consequences of attacks to the source code.

## Security Risks: Automated Abuse, Piracy and Data Exfiltration

As [OWASP mentions](#), potential attackers can take advantage of the exposed code to modify the application's data and resources, change the system APIs, or change the contents of memory dynamically. This way, they can hijack the intended use of the code for personal or monetary gain.

One of the hijacking routes attackers can take is relying on **automated abuse** attacks by exploiting the web application's functionalities to gain access or privileges through the use of bots. Typically, these types of attacks need some sort of source code manipulation, which is possible when JavaScript is unprotected. The target for this type of attack is often cloud providers that offer free benefits in new accounts. Attackers will abuse the system to automate new trial account creation and use the benefits without ever having to pay for the services. Automated attacks are especially troublesome because they can target new versions of the code with minimal cost, which means that they can scale up and target more and more systems.

When it comes to **piracy**, attackers typically target the growing OTT industry, leaking premium content which naturally ends up causing a loss of revenue for legitimate businesses. Aware of the problem, providers are using multiple techniques to fight pirates and trace the leaked content, but they must ensure that attackers can't easily bypass these techniques, namely by protecting their source code. Other examples of piracy are also commonly seen in the gaming and gambling industry where counterfeit apps pose a threat to the business integrity.

Now, one of the most important risks is **Data Exfiltration** which probably resonates with everyone who has had to submit data such as email, name, address, credit card number, or even medical information on a website using a form. Because the logic behind these forms is handled by JavaScript and all the sensitive data passes through the client-side, the safety of the data is potentially at risk. By leaving their JavaScript exposed, organizations make it easier for attackers to understand how their web applications work and facilitate the planning/ automation of data exfiltration or scraping attacks. This class of attacks is known for generating severe losses, both from the business standpoint and from the breach of compliance with data privacy regulations.

By leaving their source code exposed, organizations make it easier for attackers to understand how their web applications work and increase their attack surface. To secure their web and mobile applications, the best approach is to start securing them during the development stage.

This includes protecting the application's source code with multiple layers, to ensure that any code sent to production can actively prevent tampering and reverse-engineering attempts. Plus, with the ongoing digital transformation showing no signs of slowing down, this approach can be crucial to ensure that companies' intellectual property and user data are protected.

---

### About the Author

CEO and Co-Founder of Jscrambler, Rui Ribeiro has led the company from bootstrapping to global expansion. Currently, he executes the company's growth strategy and manages its vision and culture. With over 15 years of experience in IT, Rui has co-authored several application security patents and has extensive expertise in the financial sector, namely in international banking.

Our company website is <https://jscrambler.com>.





## How Various Flavors of PKI Can Protect and Secure Financial Services Data

By Abul Salek, Director of Product Management, Sectigo

How much time and budget does your company allocate to cybersecurity to protect you and your customers' critical data and private information? Is your organization doing enough, or is your information at risk?

In many ways, data constitutes the essential lifeblood of the financial services industry. From providing real-time account and trading information to automating risk management processes, forecasting, and fraud detection, to managing real-time transaction details, data is your business's most important resource to protect.

According to a [recent study by Deloitte](#), financial firms spend an average of 10% of their IT budget on cybersecurity. In addition, they reported that CISOs rank keeping up with rapid IT changes and rising complexities in tech systems as top challenges, regardless of company size or maturity level.

Despite these budget and time expenditures, most financial firms are not sufficiently protected because they lack data security.

Financial institutions leveraging emerging business models are not recognizing the significant security risk represented by connected devices. Given the insurance, banking, and brokerage sectors' growing

---

reliance on data and the increasing digitization of financial services, financial institutions must continually fortify their security capabilities and eliminate potential vulnerabilities to stay ahead of threats.

### Threats Come from Many Directions

Any device, system, or organization that holds or transmits sensitive financial or customer information is at risk. These cyber-threats, which can originate from both internal and external sources, run the gamut from phishing attempts, large-scale data breaches, malware and credit/debit card theft, Business Email Compromise (BEC), to ransomware-based extortion.

The consequences are far-reaching, such as the Equifax data breach in 2017 that compromised the personally identifiable information (PII) of nearly 150 million consumers, exposing them to identity theft and other potentially serious consequences. [According to the U.S. Government Accountability Office \(GAO\)](#), Equifax had installed a tool to inspect network traffic for evidence of malicious activity, but an expired certificate prevented that tool from working correctly. As a result, cybercriminals could launch attacks and gather sensitive consumer information without being detected for 76 days. News of the breach led to federal investigations and a nationwide consumer class-action lawsuit, which the company is now reportedly paying \$700 million to resolve.

### So, how can the financial services sector ensure the security, privacy, and integrity of their data?

Public-Key Infrastructure (PKI), the gold standard in digital privacy, identity, and security, offers an excellent security foundation for every device, server, user, and application in the enterprise, whether on-premise or in the cloud. PKI guards data against theft or tampering and guarantees secure authentication of users and applications to protect against fraud. By leveraging digital certificates, an organization can roll out passwordless authentication which is experiencing an increasing adoption rate in the enterprises.

While nearly every financial services firm has incorporated PKI into its web and device security in some way, not all are fully or appropriately leveraging its power.

Unfortunately, organizations are often overwhelmed when it comes to managing security certificates and secret keys throughout the enterprise, as it can be challenging to issue, manage, and revoke/renew/replace certificates and keys numbering in the thousands or even tens of thousands. Think of the number of the Secure Shell (SSH) keys floating around in your enterprise that you may not even be aware of.

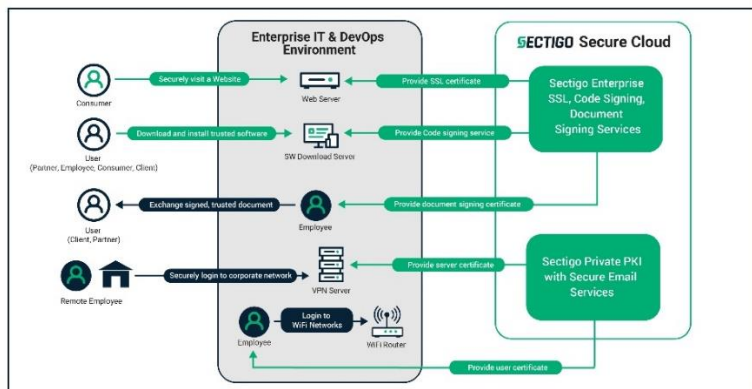
Many financial institutions fail to see the broad range of digital assets and use cases that PKI can protect. Outside of using Secure Sockets Layer (SSL) PKI certificates to protect public-facing websites, enterprise PKI solutions can address the large-scale requirements of SSL for internal-facing servers, private Certificate Authority (CA), S/MIME email encryption, code signing, and document signing.

### Five ways PKI can be used to protect and secure critical financial data

- ✓ Enterprise SSL
- ✓ Private Certificate Authority
- ✓ S/MIME Email Encryption
- ✓ Code Signing
- ✓ Document Signing

There are at least five ways that PKI can be used to protect and secure financial services data:

1. [Enterprise SSL](#), which enables administrators to easily manage certificates through a single-pane-of-glass interface, is ideal for secure online banking and transaction sites, customer information site, market analysis and forecasting sites, tax filing, insurance, securities trading, and data gathering sites.
2. [Private CA](#), which allows financial institutions to secure users and devices, and automates the management of internal devices and applications regardless of which internal protocols an enterprise has in place, is useful for supplementing Microsoft Active Directory Certificate Services, mobile devices, IoT, DevOps, cloud/multi-cloud, web servers, SSH Key management, Private S/MIME for secure email, intranet services, Wi-Fi access, VPN access, POS systems, networking devices, and Windows Hello for Business.
3. Using Zero-touch [S/MIME](#) for email enables both the sender and recipient to use their existing S/MIME-capable email applications on multiple devices – mobile or desktop; a welcome improvement to other approaches that disrupt the user experience by requiring users to use multiple certificate credentials. Zero-touch S/MIME is suited for email signing, email encryption, mobile email encryption and signing, mobile Wi-Fi access, and mobile website authentication.
4. [Code signing](#) supports all file types, from drivers and firmware to scripts and applications. With enterprise-scale issuance, management, and renewal/revocation/replacement features, development teams have greater cryptographic flexibility and improved time to market for new financial services and products. Code signing allows your software to be trusted by users and helps with a wider adoption of it. It is optimal for application development, DevOps, mobile devices, and IoT. With the higher assurance EV code signing, your application can achieve instant reputation with many Operating Systems which helps with users trusting and using it instantly.
5. [Document signing](#) allows financial institutions to maintain compliance with the strictest electronic signature/digital signature regulations, such as U.S. FDA CFR 21 Part 11 requirements. Digital signatures leverage PKI certificates to offer the highest levels of security for regulated and sensitive document use cases such as account openings, loan applications, investment/private banking, and insurance documents and agreements. If the document signing certificate is issued from a CA that is in the Adobe Approved Trust List (AATL), the signed document can be universally exchanged with trust.



*Sectigo provides a platform for financial services companies to authenticate and secure users, devices, and data.*

Because of the financial, reputational, and business consequences of failing to protect data, banks, insurers, and other financial institutions should leverage the powerful capabilities of PKI to protect against increasingly sophisticated threats and avoid costly attacks.

By adopting a suite of enterprise PKI solutions, the financial sector can future-proof security, protect customer information, gain greater peace of mind, and maximize the value of data.

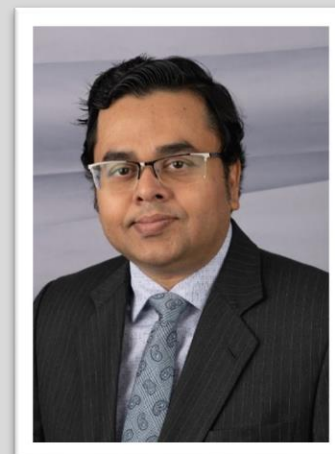
## All About Sectigo

Sectigo is a global cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As a leading Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit [www.sectigo.com](http://www.sectigo.com) and follow @SectigoHQ.

## About the Author

Abul Salek, MSc, PMC, is Director of Product Management at Sectigo, a leading provider of automated digital identity management and web security solutions. With 20 years of experience in software engineering and managing cybersecurity products, Abul leads innovations around PKI, quantum security, and IoT. He holds an M.S. degree in Computer Science from the University of Alberta, Canada.

Abul can be reached online at [abul.salek@sectigo.com](mailto:abul.salek@sectigo.com) and at our company website <https://sectigo.com/>





## Five Steps for Safely Migrating your Workloads to the Cloud

Why security in the cloud is a shared responsibility relationship between the infrastructure provider and the customer

**By Paul Farrall, CISO at Skytap**

Organizations moving workloads to the cloud must make sure that those workloads remain secure, especially organizations that handle sensitive customer data (such as financial or health records) and must comply with regulatory requirements as well as security frameworks like the Payment Card Industry Data Security Standard ([PCI DSS](#)). Security in the cloud is a shared responsibility relationship between the cloud infrastructure provider and the customer purchasing computing resources, however many organizations get confused about who is responsible for what. These misunderstandings can lead to insecure systems, data breaches and the loss of sensitive data with all the negative consequences that go along with them.

To help simplify, here are five steps organizations should take before and during a cloud migration to make sure their data remains secure.

---

## 1. Conduct a risk assessment of existing systems

The first step is determining which of your organization's systems need the most protection. For example, HR data on employees and financial information is very sensitive and needs to be well-protected. Marketing documents that are publicly available don't need as much protection, so your time is probably better spent focused on other systems. Conducting a risk assessment will help you understand your current security posture and vulnerabilities. With this information, you can prioritize which systems and data need the most protection. This will be helpful when you start evaluating cloud providers. Are you looking for a cloud provider to host your marketing brochures? Security assessment of the cloud provider can be relatively lightweight. Are you migrating HR data to the cloud? Then you need to do a more careful evaluation of the provider's security to ensure they meet your security control requirements.

## 2. Interview cloud infrastructure providers and ask about their certifications and infosec program

Certifications like PCI DSS and ISO 27001 indicate that a cloud infrastructure vendor offers a safe, secure and standards-compliant foundation for business-critical applications. At a minimum, any cloud provider should allow customers to view their annual SOC 2 Type 2 audit report (which should be prepared by an independent third-party audit firm). Beyond SOC 2, ask the vendor if they are compliant with other security standards that are applicable to your business. This will depend on the high-priority systems that you identified in Step 1 along with any regulatory and contractual requirements you are subject to (for example, if you are an ecommerce company, you may need to be compliant with PCI DSS and should look for a cloud provider that possesses PCI certification; if you are a U.S. government agency, you may be restricted to only cloud providers who possess FedRAMP certification). Remember that vendors may be working towards compliance with a standard and meet most requirements even if they're not fully compliant. Depending on your needs, this may be good enough for your purposes.

Also, ensure that the cloud vendor has a documented information security program led by an experienced security professional (the most common title for this is Chief Information Security Officer). These are indicators that the vendor takes security seriously. Again, remember to prioritize and scrutinize vendors that will be storing sensitive information more closely than ones that will be storing non-critical information.

## 3. Understand the Shared Responsibility Model

This step is critical. Cloud infrastructure providers will specify which aspects of the overall security framework they are responsible for and the aspects that the customer must manage on their own. Generally speaking, infrastructure providers are responsible for protecting the infrastructure itself, including the people, hardware, software, networking and physical facilities that comprise the hosting platform. Customers are typically responsible for securing their own environments, including the guest OS, applications and data. The vendors should provide you with a copy of their shared responsibility matrix if you ask. Make sure you understand this thoroughly so you don't assume the vendor will secure something that is actually your responsibility.

For example, cloud infrastructure providers do not typically patch servers running in customer VMs or prevent weak passwords from being used on those servers – these are customer responsibilities.

---

Similarly, don't assume data backups are a service that cloud infrastructure providers include by default. Depending on the type of cloud service offered, backup of customer data might be included as a standard service or it might require custom contract terms. Make sure you understand these nuances and don't just assume that the vendor will secure everything for you in the cloud.

#### 4. Secure Your Own Virtual Machines

Now that you understand what the vendor will secure, you need to step in and secure the rest. As stated above, cloud infrastructure providers protect their platform and protect customers from each other. You, the customer, are responsible for application security and for configuring your cloud environment correctly. IaaS providers won't fix your coding mistakes for you! If you introduce a security flaw into a virtual machine that leads to a breach, there may be nothing that the infrastructure provider can do about it.

#### 5. Find Out What's Exposed to the Internet

If you do not implement strong configuration management and server hardening procedures, you may find that you have accidentally exposed your virtual machines and cloud services to the internet. This is the root cause behind most of the Amazon [S3 buckets breaches](#) you may have read about over the past few years. There are even [search engines](#) to find exposed S3 buckets. The risk from configuration errors is magnified in the cloud because the pool of attackers on the public internet is larger by orders of magnitude than what a server in a data center behind a firewall would normally face. An unpatched server with a weak password exposed to the public internet will be hacked in minutes.

To make sure this doesn't happen to you, spend the time and effort needed to determine exactly which services are exposed to the public internet, cut off any that do not need to be exposed, and harden those that do.

Moving workloads to the cloud can produce solid benefits like reductions in cost and potential for application modernization. But misunderstandings around cloud security can leave your data exposed and open your organization up to serious consequences. Make sure to follow these steps to reduce your risk, and don't be afraid to use a consultant if your team doesn't have the necessary expertise.

#### About the Author

Paul Farrall is the CISO at Skytap. He has spent the past fifteen years in executive cybersecurity roles at Skytap, Big Fish Games and Intelius and serves on the IT Advisory Board at the University of Washington. He holds CISSP and CISA certifications. Paul can be reached online at @paulfarrall and our company website <https://www.skytap.com/>.





# Cybersecurity in Healthcare: Benefits, Examples, and Usage Tips Healthcare cybersecurity framework

By Kate Orekhova, Cleveroad company

Health organizations deal with a large amount of sensitive personal information. That's why they face challenges complying with tightening regulations, and they're constantly combating increased cyber risks and adapting to digital transformation.

The healthcare institutions have to prove that technologies and methods they adopted keep patients' personal information secure and bring no risks. And using recognized standards and frameworks is a great decision.

In this guide, we discuss how to apply security frameworks in healthcare, along with recognizing well-known cybersecurity frameworks.

## What Does Cybersecurity Framework Mean?

Cybersecurity framework (CSF) is a mix of processes, technologies, and practices designed to reduce cybersecurity risks in different fields, including healthcare. Moreover, the framework helps organizations operate sensitive data and predict security risks due to its adaptive and practical approach.

---

In short, the frameworks are the guidelines to secure IT systems.

But a framework isn't a panacea from all misfortunes. It offers a common language and methods for combating cybersecurity-related threats but isn't the only way to secure sensitive data.

CFS is updated depending on each organization. That's why CFS is based on questions healthcare institutions should ask themselves to manage their risks effectively and in the right direction. And while technologies and standards may transform – the principals stay.

The primary goals of cybersecurity frameworks:

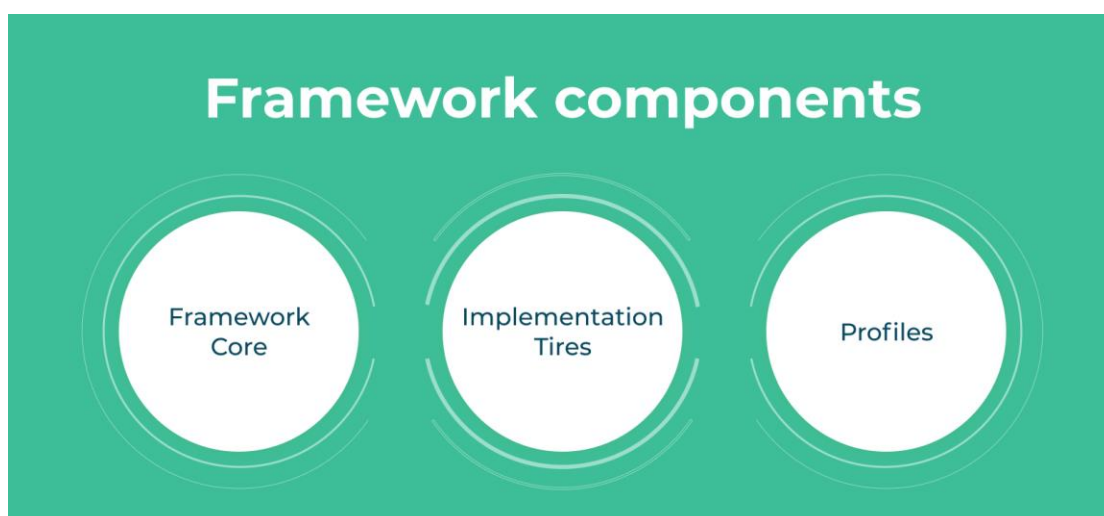
- Defining the current security situation
- Outlining target security position
- Constant improvement
- Analyze progress towards the target position
- Communication risk

#### But what is the structure of these frameworks?

There are three fundamental pillars of a CSF:

1. The core
2. Implementation layers
3. Profiles

Let's



consider each of them in detail.

- **Framework core** is based on cybersecurity activities and rules designed to reach a particular result. Its function is to inform about cybersecurity risks across an organization
- **Implementation layers** help associations by determining how they understand cybersecurity management. They help to reveal the right level of thoroughness for a security program and warn about cyber risks across an organization
- **Profiles** are a set of organizational objectives and premises, and assets against the framework's primary outcome. They reconcile industry standards and common practices, support priority settings and measurement according to the business goals

## Why Use CSF in Healthcare?

Hospitals and other healthcare are vulnerable to security threats.

That's why they need safeguards that private data will be secured within an organization and meet industry and federal requirements.

Besides, healthcare is one of the industries where internal cybersecurity threats are more dangerous than external ones. According to the Verison [report](#), 59% of all cybersecurity threats are internal compared to 42% of external incidents.

Most often, it happens because of human errors. Hospital employees may misuse their power and access to the internal systems and information they store. In this case, it's better to [build your own CRM](#) compliance with ISO 27001 standards to reduce frequent cyber-attacks and data breaches. For example, it happens when the hospital staff wants to know what procedures celebrities take. No surprise that 6% of breach incidents happen because of "just for fun."

## So how exactly do CFS resolve these matters?

Let's take the example of the most popular health cybersecurity framework – NIST.

**First**, CSF is used to detect, react, protect and recover from the influences of security threats and their consequences. It's not a rule book for healthcare institutions, but an experience of best practices of IT security. And hospitals use these guidelines to strengthen their existing cybersecurity policies.

**Second**, the NIST healthcare cybersecurity framework provides security implementing its core elements, implementation layers, and a profile that coordinates them with business requirements, financial capabilities, and resilience to risk.

CSF helps both external and internal stakeholders understand and handle cybersecurity together as a team. It's a tool that lets healthcare entities coordinate business policy with a tech one.

---

It improves security risk management across the whole organization. And, thus, it leads to better outcomes. It's crucial when it comes to providing healthcare services to patients or enhanced operational efficiency with personnel.

## Health CSF Adoption

Finally, it's time to provide medical cybersecurity and work on CSF implementation. Let's consider what steps most organization take when it comes to framework adoption:

- Step 1: Determine core tasks and organizational components
- Step 2: Define current risk management approaches
- Step 3: Make a risk management profile
- Step 4: Assess the risks
- Step 5: Create a risk management profile based on the evaluation results
- Step 6: Create an action plan
- Step 7: Implement the plan

Now, let's take a closer look at framework adoption steps.

### 1. Prioritize and make the scope

Before starting cybersecurity action, hospitals need to determine the primary goals and priorities. Thus, they can make strategic decisions regarding the security standards and find the systems and tools that hold the selected process.

And CSF implementation starts with creating a strategy for framing, estimating, analyzing, and responding to risks. This way, a healthcare institution understands how and where to utilize the framework and analyze threats and impacts.

### 2. Orient

First, the organizations check what resources they have (tools, technologies, data, personnel). They also choose the appropriate regulatory agency and look for authoritative sources (security standards, methods, risk management rules, and so on).

Second, they carefully weigh the overall risk approach and determine the system's weak points.

### 3. Work on a Target Profile

The organization determines its own risk factors and does an overlay of the healthcare framework. After, the entity sets the overlay to block any threats and breaches. Moreover, organizations may also build

---

their own Categories and Subcategories to report for unique risks. They identify the category and subcategory of the results they are dealing with from the framework core.

#### 4. Estimate the risks

At this stage, healthcare organizations figure out the level of risk to the information system. They analyze possible security risks and the consequences they may cause.

#### 5. Create a Current Profile

The healthcare institutions make a detailed risk evaluation and determine their current posture. It's better to conduct an assessment from both the functional area and independently across the organization.

Risk assessment aims at understanding current cybersecurity risks in the healthcare industry. Thus, all the breaches and vulnerabilities should be found and documented.

#### 6. Define, analyze and prioritize the gaps

After finding all the risks and impacts they cause, healthcare entities should provide a gap analysis to compare the actual results with the target ones. For instance, they may design a heat map showing the results clearly. With this approach, it'll be easy to find the areas that need to be improved. Then, organizations brainstorm to understand what they should do to fill the gaps between current and target outcomes.

#### 7. Realization step

Finally, by understanding possible cybersecurity challenges in healthcare and having a list of necessary actions, medical organizations can adopt the framework.

Indeed, it doesn't end just with implementing the action plan. Companies should structure and analyze metrics to ensure their efficiency and that their CSF is meeting the company's expectations. The major purpose of this process is to get the maximum benefit and customize the framework to meet business needs.

### Best Framework Examples in Healthcare

In 2018, HIMSS conducted a "[Cybersecurity Survey](#)" to know what medical cybersecurity frameworks are in demand in the healthcare sector. Let's take a look at five popular cybersecurity frameworks and the reasons why healthcare entities implement them.

## Which security frameworks does your organization use?

Framework	Percent
NIST	57,9%
HITRUST	26,4%
Critical Security Controls	24,7%
ISO	18,5%
COBIT	7,3%
Other	5,1%
No framework	16,9%

### 1. NIST Healthcare Framework

NIST CFS is the commonly used security framework in many industries, including healthcare. It's a USA-based company that develops lots of tech standards and rules, data security included.

The best-known NIST documents are:

[NIST Framework](#) for Improving Critical Infrastructure Cybersecurity

[NIST SP 800-53](#) for Security and Privacy Controls for Federal Information Systems and Organizations

[NIST SP 800-171](#): Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST CSF is based on threat modeling, intelligence, and collaboration. By using it, healthcare organizations not just execute a required analysis of future risks, but remove emerging threats and collaborate with other institutions.

### 2. HITRUST

[HITRUST framework](#) ranks second in cybersecurity frameworks: 26,4% of frameworks users use the Health Information Trust Alliance guidelines.

HITRUST is a private organization working with the best specialists in the healthcare industry. Their major goal is to make data security the foundation of information systems. That's why their CSF strives to satisfy organizations' needs by offering specific guidance.

The programs involve standard risk establishment, an estimation and assurance methodology, awareness, and so on. Moreover, the framework uses the ISO/IEC 27001:2005 Information Security Management system and supports business associates worldwide.

---

### 3. Critical Security Controls

Critical Security Controls, created by the Center for Internet Security, is a set of practices aimed to prevent healthcare cyber attacks. In CSC, all the controls are started from the most important ones like operating vulnerabilities or providing an inventory of assets.

Generally, CIS Controls is used with other CFS, for example, NIST.

### 4. ISO 27000 Series

ISO stands for International Organization for Standardization. It's a non-governmental company that creates standards to uphold world trade. ISO follows measures to create and maintain an information security management system – [ISO/IEC 27000](#).

This framework can be used in the healthcare sphere to manage complex and changing requirements of data security.

### 5. COBIT CFS

COBIT CFS is an IT governance tool. It lets healthcare institutions fill the gap between control requirements and helps with policy development.

COBIT is aimed at the effectiveness of the IT sphere more than at the security of business processes. However, many companies utilize the CSF to adopt practices developed by other security standards, for example, the NIST healthcare cybersecurity framework and ISO 27001/2.

Hospitals and insurance companies join other organizations (financial institutions, private corporations, governments) in implementing COBIT.

## Wrapping Up

Cybersecurity framework implementation can be a difficult task due to its constantly changing rules and requirements. However, it's vital to apply these frameworks in the healthcare sphere to prevent cybersecurity-related threats on time.

---

### About the Author

Kate Orekhova is a content writer at Cleveroad. It's a mobile and web development company in Ukraine. Alina enjoys writing about cybersecurity technology and AI innovations.





## All the User Experience, None of The Security?

*EU telcos gather a lot of highly sensitive customer information. New research suggests it's not as well protected as you might think.*

By Deepika Gajaria, Vice President of Product, Tala Security

Mobile service providers are known for their content-rich user experience. But how good are they at securing it?

Few sectors collect as much sensitive information: from national ID/passport numbers and scans to payslips, bank details and payment card information, the amount of data the average customer enters to sign up for a contract or buy services online is significant. But what happens when the same applications and integrations that deliver that rich user experience inadvertently expose this sensitive information to over-sharing and theft?

[New research](#) that we recently completed indicates that data exposure is a significant, unaddressed problem for Europe's top mobile providers - and the more than 253 million customers who sign up for their services and share sensitive personal data. At the heart of the problem: insecure website supply chains.

## Unlimited calls, texts, data (sharing)...

We analyzed 13 of the top Mobile Service Providers in 7 EU countries and found that *none* had effective web security in place. On a ten point scale where a score of 50 indicates limited control, the average score was 4.5. This weak security is underscored by vulnerable site architecture:

- **Sensitive data is at significant risk via form data exposure** - Forms used to capture credentials, banking details, passport numbers, etc. are exposed to an average of 19 third parties. Without control, this sensitive data is at risk. This level of exposure, combined with the high value of the data captured make this an attractive target for Magecart attacks.
- **100% of the websites are vulnerable to cross-site scripting (XSS)** - the most widespread website attack, which frequently results in significant sensitive data leakage
- **The highest number of third party JavaScript integrations** found on a single site was 735; the average was 162.

## Why it matters

Unintentional data exposure is a significant, unaddressed risk for all of the telcos analyzed. Without controls, every piece of JavaScript code running on websites - from every vendor included in the website owner's website supply chain - can modify, steal or leak information through client-side attacks enabled by JavaScript. Telcos amongst this sample group averaged 31 third-party integrations.

In many cases, data sharing or exposure takes place via trusted, legitimate applications on the allowlist - often without the website owners' knowledge. While most online businesses do a great job protecting data *after* the user has entered it, few seem to be aware of data leakage as an unintended consequence of the dynamic, rich website experience telcos are known for. This has potentially far-reaching implications for user privacy and, by extension, GDPR. With the lack of awareness of this very real risk its time for website owners to start caring about oversharing.

## About the Author

Deepika Gajaria is the Vice President of Products at Tala Security. An experienced product leader and technologist, Deepika is responsible for product strategy and delivery at Tala. Working closely with customers, she drives product direction and shapes the product roadmap to address their core needs.

Prior to Tala, Deepika was part of Cisco Jasper where she led the launch of IoT smart city applications. Her career in product management began at EMC, in the new product introduction team, working on key initiatives across the Storage and the Data protection divisions.

Deepika is a longhorn, holding undergraduate and graduate degrees from the University of Texas at Austin, in Natural Sciences and the McCombs School of Business.





## In the Midst of COVID-19, We're Seeing a Pandemic of Cyber Attacks

By Babur Khan, Technical Marketing Engineer - Enterprise Security at A10 Networks

In the first quarter of 2021, the COVID-19 pandemic is still wreaking havoc around the globe. The coronavirus is continuously evolving and presenting new challenges.

In addition to the direct effects of the COVID-19 pandemic, we also saw a sharp rise in cybercriminal activity. From simple phishing attacks to one of the largest DDoS attacks ever recorded, we saw the cyber threat landscape evolve and grow.

At the same time, we also saw a rapid growth in the tech and cyber security industry. From the roll out of 5G in many parts of the world to exponential growth in the SaaS industry, we saw the pandemic put many positive changes into full gear as well.

We believe that these challenges, and the changes that they brought about, will not stop. The effects of this pandemic on the tech industry will be long lasting. Moreover, some of the challenges introduced in 2020 will affect cybersecurity well into 2021, and even beyond. As we move deeper into 2021, here are some of the cyber security trends that we see:

---

## Cybercrimes Will Experience a Surge

Last year was a busy year for both attackers and hackers as well as cybersecurity personnel defending against the plethora of attacks to which they were subjected. With an election year in the United States in 2020, we saw a rise in anti-government cyber activities, a prominent example of which was the attack on FireEye, allegedly by a foreign nation state sponsored entity, where multiple tools were stolen for use in attacks later on.

In 2021, such attacks will not just be more frequent, but they will also be very specific regarding who they target. International cyber espionage will be one of the main motivators for cyber attacks and we will see security vendors being attacked and compromised at an even greater pace. Even the attacks that happened in 2020, like the FireEye attack or the Sunburst attack, that targeted the SolarWinds supply chain, will have long lasting effects. We have only seen the beginning of these attacks. Investigators suspect, for example, that up to 250 organizations may have been compromised in the SolarWinds attack. Actual results are yet to come.

Such attacks will not only create opportunities for newer attacks, or variants/branches of the existing ones, but will also drive cybersecurity innovation in 2021.

## The Intelligent Edge will be Weaponized

One of the major innovations driven by 5G is the implementation of multi-access edge computing (MEC). Building intelligence into the edge will boost the availability and efficiency of 5G networks. However, keeping the global cybersecurity trends in mind, we can see that the intelligent edge might be hijacked by attackers for launching different kinds of attacks, both on the mobile core networks as well as on victims outside of the realm of the service provider that has been compromised. If nothing else, MEC can be used for propagating malware into different networks for drone recruitment in IoT botnets.

## Low-volume DDoS Attacks will be More Frequent

In 2020, even though we saw one of the largest DDoS attacks ever recorded target one of the biggest names in the tech industry, we also saw that a large number of DDoS attacks went unnoticed because, even though the frequency of these attacks was very high, their size was not. These high-frequency, low-volume attacks will keep the security industry busy in 2021 and may be instrumental to disabling security infrastructures or just acting as smokescreens for larger malware attacks such as the recent Sunburst attack.

## Five Million DDoS Weapons will be Added to the Global DDoS Arsenal

The A10 Networks security research team observed that the number of DDoS weapons doubled from around six million at the end of 2019 to 12.5 million in 2020. This trend will remain the same in 2021 as more IoT devices come online with each passing day, with an expected addition of at least five million weapons.

---

The large number of DDoS weapons will also enable attackers to launch another record-breaking DDoS attack in 2021. We will have to wait and see whether it will be made public by the victims or not.

### 2021 will be the Year of Zero Trust Implementation

2020 was the year of understanding what the Zero Trust model is in a practical sense. Throughout the year, we saw security vendors align their solutions with the Zero Trust model, adjust the model as we got more clarity on what it means to be a Zero Trust user, device, or network, and explore the policy changes necessary to a successful implementation of the Zero Trust model. As the COVID-19 pandemic fast-tracked the move to SaaS and made the “work from home” model mainstream, the importance of Zero Trust security has gained critical importance.

Organizations now understand that Zero Trust is not a specific device or vendor, but rather a series of strategic policy and practical changes that help enable better security. A successful implementation requires good understanding of what the Zero Trust model is as well as the many diverse solutions that have to work in unison to enable its implementation.

We believe that the concept of Zero Trust has reached a level of maturity and clarity where it will be effectively adopted and implemented by many organizations in 2021, and that it will become the go-to security model for all types and sizes of organizations. Sophisticated attacks like Sunburst will also drive the need for effective Zero Trust implementation.

### SASE Adoption will Accelerate

Since 2020 forced most of the workforce to work remotely, attackers have been experimenting with new ways of exploiting security loopholes or shortcomings exposed by these rapid changes. This accelerated and will continue to accelerate the development and adoption of Secure Access Service Edge (SASE) solutions.

However, since the move to the cloud does not happen overnight, many organizations still have most of their resources hosted on-premises. They will keep on struggling with maintaining the remote work model and will revert back to business as it was once a vaccine for COVID-19 becomes readily available and things go back to normal.

This, however, might be temporary as the world has now experienced a pandemic and many organizations have already started moving their businesses from on-premises to the SaaS-based model, with the trend only being accelerated by COVID-19. In summary, SASE will be an essential part of the enterprise security infrastructure in 2021 and beyond.

---

## 2021 will the Year TLS 1.3 Shines

TLS 1.3 will finally start seeing widespread adoption, in part, driven by the adoption of QUIC/HTTP3 given that TLS 1.3 is built into it. Many vendors support TLS 1.3 already and that will help drive the protocol into mainstream use. Changes will also be made to the TLS 1.3 standard as the demand for encrypted SNIs rise.

That said, TLS 1.2 will still remain the more widely used choice as an encryption protocol over the internet since moving to the newer version may prove to be expensive for many organizations. But as QUIC/HTTP3 becomes more widely used by the end of the year, we may see this change.

In conclusion, we are facing new, persistent threats of all shapes and sizes, and we have to make sure that, going forward, we face these threats with the best of our collective abilities. 2021 will be the year of cybercriminal activities, but it will also drive innovations in cybersecurity like never before.

### About the Author

Babur Nawaz Khan is a technical marketing engineer at A10 Networks. He primarily focuses on the company's enterprise security solutions, including Thunder® SSL Insight for TLS inspection and Cloud Access Proxy, which is a SaaS access security and optimization solution. Prior to his current role, he was a member of A10 Networks' corporate systems engineering team, working on application delivery controllers. Babur holds a master's degree in computer science from the University of Maryland, Baltimore County.

Babur can be reached online at (bkhan@a10networks.com) and at our company website <https://www.a10networks.com/>





## Why A 'Layers and Lists' Approach to Cybersecurity Is Doomed to Fail

By Gary Fischer, VP Americas, XM Cyber

Why is cyber-defense such an asymmetrical war? Hackers can launch a barrage of attacks on a single target and keep going until they find one overlooked weakness. Defenders, meanwhile, are often overwhelmed with alerts, unsure what to patch first and have little real visibility into the weaknesses of their ever-changing environments.

In a battle between active adversaries who only need to land a single blow to win -- and passive defenders who aren't even sure where they are truly vulnerable -- the outcome is almost pre-ordained.

Fortunately, there is something IT teams can do right now to flip the odds: Drop the old approach of siloed security products and disconnected lists and build a cybersecurity defense that mimics the attacking mindset of adversaries -- and turns it against them.

---

## Layers and Lists vs. Risk-Based Vulnerability Management: Why It's No Competition

Piling security controls on top of security controls and working with endless streams of poorly prioritized Common Vulnerabilities and Exposures (CVEs) is no way to protect your assets. Unfortunately, that's the status quo for many enterprises.

While firewalls, standard Vulnerability Management (VM) and endpoint tools have their uses, all of them can be defeated by a simple human error. They don't always play nice with each other. Additionally, server misconfigurations, credential mismanagement and other mistakes are a perpetual problem.

Larger organizations are often deluged with alerts, and the amount of time security teams spend chasing down patches for relatively low risk vulnerabilities is enormous. Without key risk context, defenders often spend precious hours addressing the wrong set of problems at the wrong time. Not only does it place your most valued assets at risk, it's also a massive waste of time and energy.

Fortunately, there is a better way: Constant, attack-centric analysis of exposures caused by exploitable vulnerabilities and human error paired with effective prioritization. Integrating these concepts into an existing security posture allows you to achieve continuous, risk-based vulnerability management -- and provides the best tool we have against Advanced Persistent Threats and other sophisticated attackers.

### Beat Them at Their Own Game

To adopt an attacker's mindset, defenders need to stop thinking "lists" and start thinking "attack graphs." In practical terms, this means incorporating risk-based VM software that can continuously scan a network and identify exposures from exploitable vulnerabilities and errors. Then, such software can launch simulated attacks against critical assets seeking to illuminate paths that can be exploited.

The outcome of all of this continuous scanning and attack modeling is a targeted and ranked list of exposures that put your business-critical assets at the most risk. Factor in context-sensitive and least effort remediation advice, and SecOps teams can begin quickly patching exposures. The entire process of identifying, classifying and addressing vulnerabilities can be profoundly streamlined and made vastly more effective.

Now let's contrast this sort of tool with the conventional approach.

You've got a slew of siloed security controls, but no real visibility into evolving vulnerabilities in complex hybrid environments -- places where even the smallest change can create new security gaps.

You've got vulnerability scanners, but you're missing key risk context. Without understanding how exposures can be exploited and which vulnerabilities are truly exploitable, you can't efficiently prioritize your patches. Without a risk-based VM tool to point you to the most accurate vendor patch or update, you may waste untold hours of research time. Larger enterprises may deal with thousands of CVEs, each of which must be researched and prioritized. In many cases the issues are low risk or require a patch that has been superseded by another patch. Without all the needed context, defenders are often struggling to make the right decisions.

---

## The Takeaway

Ultimately, relying on layers and lists alone is a recipe for subpar security and wasted resources. Attack-focused, risk-based VM solutions represent the next wave of risk quantification for cloud and on-premises environments. Using a tool that allows you to think like an attacker -- and helps you understand potential impact, asset criticality, related connections and choke points -- is essential for meeting today's cybersecurity challenges.

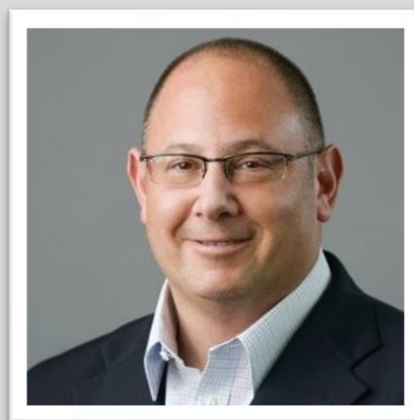
The right risk-based VM tool should be able to help identify vulnerabilities that allow attack paths leading to business-critical assets and prioritize based on risk to those key assets. This then allows you to immediately perform the right remediation work to close the attack chain.

By working smarter, you not only lower your risk but save your team a substantial amount of time and effort. An attack-centric, risk-based VM tool can help you focus on the most critical patches, which can reduce workloads by up to 90-percent -- because you are only working on the 10-percent of CVEs that pose the gravest risk.

Less wasted time for defenders and better security for your crown jewel assets. Everybody wins -- except for the adversaries trying to steal your data.

### About the Author

Gary Fischer is the VP Americas for [XM Cyber](http://www.xmcyber.com). He has been in the cybersecurity software arena for over 20 years. Prior to joining XM Cyber, Gary served as Vice President of Sales for the Americas at Skybox Security for close to 10 years. Before that, he held other senior sales leadership roles in the cybersecurity field. He has a proven track record of taking startup companies from early stage to acquisition. Gary can be reached online at <https://www.linkedin.com/in/gsfischer/> and at our company website <http://www.xmcyber.com>





## New Report Shows Over Two Million Secrets Detected on Public GitHub in 2020 and a 20% growing trend Year-Over-Year.

By Jeremy Thomas, GitGuardian CEO

When we started working on GitGuardian's detection algorithm and got the first detection results, we could not believe it. We were facing a very counterintuitive reality. Secrets were actually hard coded in source code and available for all to see on public GitHub. And not just developers' personal secrets but also corporate secrets ending up on developers' personal repositories outside of corporate control.

After scanning billions of commits each year on public GitHub, we wanted to share our findings and we issued our first [State of Secrets Sprawl on public GitHub report](#). The report, which is based on GitGuardian's constant monitoring of every single commit pushed to public GitHub, indicates an alarming

---

growth of 20% year-over-year in the number of secrets found. A growing volume of sensitive data, or secrets, like API keys, private keys, certificates, username and passwords end up publicly exposed on GitHub, putting corporate security at risk as the vast majority of organizations are either ignoring the problem or poorly equipped to cope with it.

### A major blind spot in application security

What companies ignore most of the time is that only 15% of leaks on GitHub occur within public repositories owned by organizations. 85% of the leaks occur on developers' personal repositories. Secrets present in all these repositories can be either personal or corporate and this is where the risk lies for organizations as some of their corporate secrets are exposed publicly through their current or former developer's personal repositories.

GitHub is more than ever "The Place to Be" for developers when it comes to innovating, collaborating and networking. GitHub gathers more than 50 million developers working on their personal and/or professional projects. When 60 million repositories are created in a year and nearly two billion contributions added, some risks arise for companies even if they don't use GitHub or open source their code, because their developers do.

### A growing issue linked to componentization of applications

As architectures move to the cloud and rely more on components and applications, the growth of commits occurring and the use of digital authentication credentials has increased the number of secrets detected. To compound the problem companies are pushing for shorter release cycles, developers have many technologies to master, and the complexity of enforcing good security practices increases with the size of the organization, the number of repositories, the number of developer teams and their geographical spread.

As Anne Hardy CISO of Talend states it, *"We launched an audit using GitGuardian, and several leaked secrets were brought to our attention. What was very interesting and what we didn't anticipate was that most of the alerts came from the personal code repositories of our developers."*

Using our secrets detection engine, we have found over 2 million secrets on public GitHub in 2020 which is about 20% more compared to previous year. The type of secrets found include google keys, keys from development tools, data storage, payment systems, cloud providers and so on.

### Why is this happening?

Usually these leaks are unintentional, not malevolent. They happen because developers typically have one GitHub account that they use both for personal and professional purposes, sometimes mixing the repositories. It is also easy to misconfigure git and push wrong data and it is easy to forget that the entire git history is still publicly visible even if sensitive data has since been deleted from the actual version of source code.

---

## A need for automated secrets detection

Companies can't avoid the risk of secrets exposure even if they put in place centralized secrets management systems. These systems are typically not deployed on the whole perimeter and are not coercitive as they do not prevent developers from hardcoding credentials stored

in the vault.

Solutions are available for them to automate secrets detection and put in place the proper remediation, but the market is far from mature on this subject. The reality is most organizations are operating blind. Most leaks of organization's credentials on public GitHub occur on developers' personal repositories, where organizations often have no visibility, let alone the authority to enforce any kind of preventive security measures. Companies need to scan not only public repositories but also private repositories to prevent lateral movements

of malicious actors.

Some [best practices](#) can be followed to limit the risk of secrets exposure or the impact of a leaked credential:

- Never store unencrypted secrets in .git repositories
- Don't share your secrets unencrypted in messaging systems like slack
- Store secrets safely
- Restrict API access and permissions

Developers training programs should be put in place although these do not eradicate the risk of leaked credentials.

Following best practices is not sufficient and companies need to secure the SDLC with automated secrets detection.

Choosing a secrets detection solution they need to take into account:

- Monitoring developers' personal repositories capacities
- [Secrets detection performance](#) - Accuracy, precision & recall
- Real-time alerting
- Integration with remediation workflows
- Easy collaboration between Developers, Threat Response and Ops teams.

## To conclude

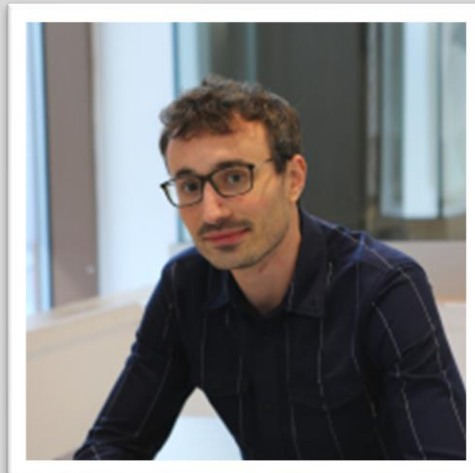
There are millions of commits per day on public GitHub, how can organizations look through the noise and focus exclusively on the information that is of direct interest to them? How can they make sure their secrets are not ending on their developers' personal repositories

---

on GitHub? They can't avoid that developers have personal repositories, they need automated detection and efficient remediation tools. In this state of secrets sprawl on GitHub analysis we focused on secrets although this is not the only sensitive information that can end up being publicly exposed: Intellectual Property, personal and medical data are also at risk.

### About the Author

Jérémy Thomas, co-founder of GitGuardian, is an engineer & an entrepreneur. He graduated from Ecole Centrale in Paris. He first worked in finance and then began his entrepreneurial journey by first founding Quantiops, a consulting company specializing in the analysis of large amounts of data, then GitGuardian in 2017. GitGuardian, a cybersecurity start-up co-founded with Eric Fourrier, has been pursuing a strong growth trajectory since 2017, supported by investors such as Balderton Capital, BPI France or Scott Chacon, co-founder of GitHub and Solomon Hykes, founder of Docker.



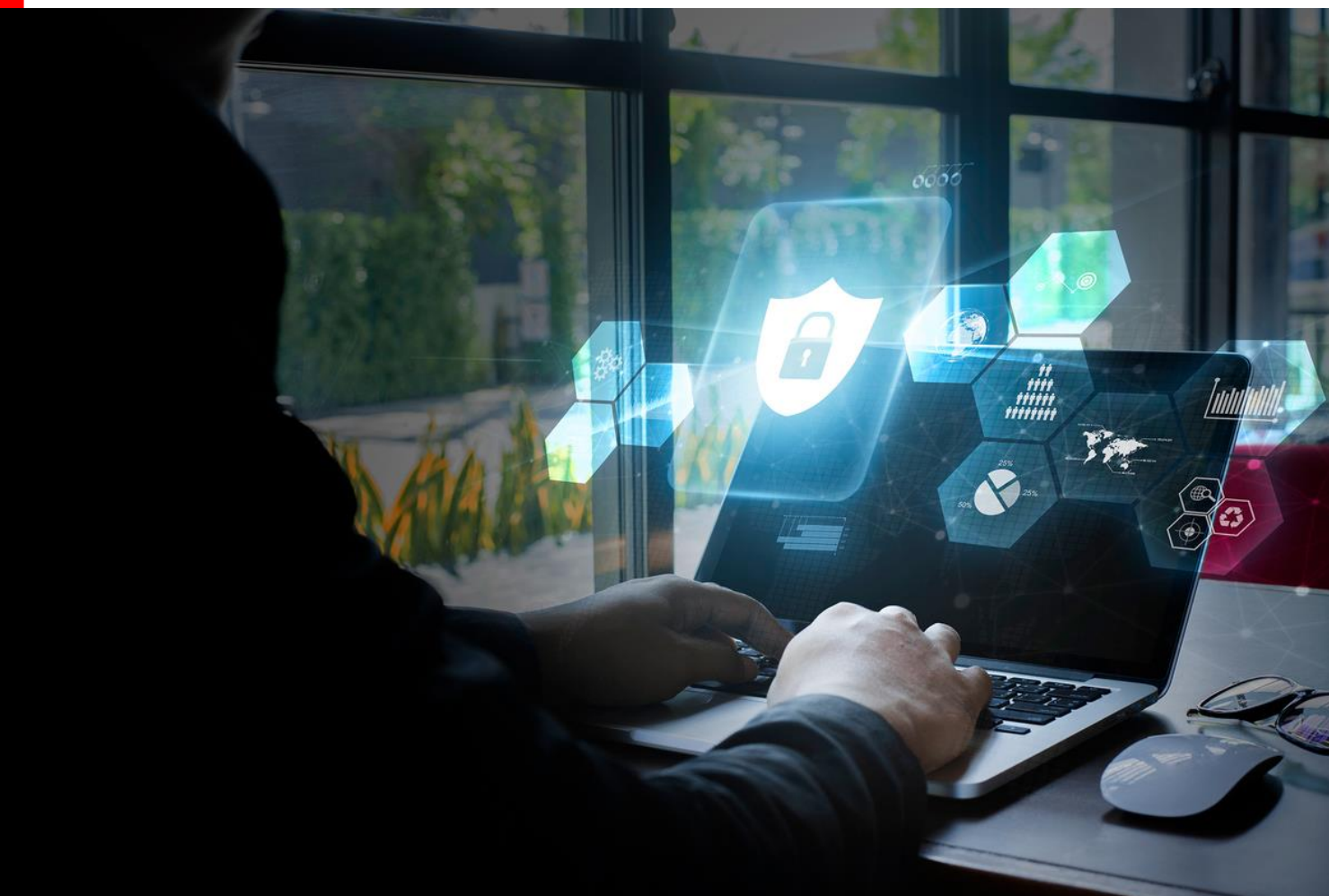
<https://www.linkedin.com/in/jeremy-thomas-gitguardian>

@GitGuardian

<https://www.gitguardian.com/>

Holly Hagerman is the Contact

Hollyh@Connectmarketing.com



# Securing Patient Private Information in The Age of Shared Information

By Christian Gitersonke, CEO, Health Insurance Answers

## The Problem

Theft of Private Health Information (PHI) has been around almost as long as healthcare in this country. As technology has evolved and safeguards continue to be put in place to protect it, criminals have found ways to exploit the often times inadequate and sloppy protection of our personal health data.

Regardless of the technological safeguards in place, one of the greatest exposures we see are employees writing down PHI on a note pad or post it note and throwing that in a trash can at a desk or purposely walking out with the information to sell on the dark web. Another glaring problem is that many times employees do not realize the data they are exposing is considered a breach and inadvertently release it to those who may do harm.

---

Many low-level healthcare crimes start at the most basic level. A disgruntled employee in a clinic or a biller looks to make extra money and the gate is open. Dealing in stolen PHI is also a lot less risky for many would-be identity thieves. The process for starting a Medicare approved service, Durable Medical Equipment (DME) company or home health agency has traditionally been an easy one. Once established, all the would-be thieves need to do is secure a few, readily available facts about a patient and then go to work billing for services and products without the patient being the wiser for a long period of time.

With little to no regulation on medical billers, front office staff, and even certain clinical support staff, healthcare is a free-range market for thieves. Where did the breach originate? Many times, it's difficult to identify the source and whether it was intentional or not.

### **Outsourcing healthcare job functions overseas invites PHI compromise and data breaches**

Do patients know what their data is used for when it is collected? Do they know where that data is stored? Are they advised how their PHI is handled when seeing a doctor or healthcare provider? When your healthcare provider changes, does that information stay behind for good or is it destroyed once it is handed off to the next healthcare professional? What happens when the physician uses a dictation service or a billing service based in another country? Does HIPAA cover these entities? The short answer is no. Even with the most robust business associate agreements, HIPAA's strength and reach does not protect this information from falling into the wrong hands. To add a scarier aspect to all this, many providers do not realize some or all of their services are offshored away from the protection of HIPAA. To date, there is no law requiring a vendor to disclose this. If the provider doesn't know, you can all but guarantee the patients do not know either.

### **Solutions & Challenges**

The Health Insurance Portability and Accountability Act (HIPAA) was created in 1996; one of the law's principal purposes is to protect sensitive patient information. Other objectives of the Act were to combat waste, fraud and abuse in health insurance and healthcare delivery. It brought about much stiffer penalties for those who breached the newly imposed regulations and gave lengthier sentences for those who wished to criminalize healthcare. Even with the stiff financial penalties for breaches, the problem has not abated and continues to grow.

The Centers for Medicare & Medicaid Services (CMS) threw their hat into the ring to help offset the out-of-control fraud, waste and abuse that was happening for decades within CMS regulated programs. As part of the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) initiative, it was required by Department of Health and Human Services (HHS) to issue new cards that would no longer display the cardholder's Social Security number no later than April 2019. In the past, all a would-be criminal would need to commit fraud was a copy of a patient's Medicare insurance card and a date of birth. Of course, the fraud was rampant.

One suggested solution to this challenge would be to require medical providers and facilities to guarantee the security of the patient's private information and impose additional penalties to those exposing a patient's secured data. It's worthy of consideration.

---

## Transparency

The key component that has been missing for decades is transparency for patients. There are few other services in life we receive that we don't know exactly what we are being charged and what that charge is for. Can you imagine having your car serviced and you are given a cryptic statement that doesn't clearly list what is to be done and how much each item costs. You have no way to compare to see if what you were going to receive is even comparable, reasonable, or necessary. And to boot, you are told there was no way to estimate your cost but please sign here that whatever the cost, you agree to it. Imagine grocery shopping this way or having your yard landscaped in this manner.

Audit reports of employees printing documents as simple as determining who ran, accessed, and downloaded reports with patient data can go a long way to shoring up internal management's handle on what is happening with this very sensitive data on a daily and ongoing basis.

A strong cyber defense can identify trends and anomalies in people's behavior, which is the first step in stopping cyber criminals before they ever get started. Recently, an employee with the State of California in the I/T department at copied more than 1,400 Covid test results with no apparent reason. Understanding the motivation behind why cyber healthcare criminals are doing what they are doing, lends us clues and answers as to how to get ahead of them and implement the right technology solution to stop them before they get started.

## Real Time Access

When patients can see changes happening to their health record in the same way we can access our credit report is when this theft and fraud can be come to a grinding halt. If you were able to see any new charges paid on your behalf today rather than weeks, months, or years later, it would offer a real time solution to combatting this ever-growing problem.

## Conclusion

In the age of one click ordering and speedy delivery, we take for granted the security or lack thereof, behind some of our most important and guarded personal information, our private health information. Making informed decisions and authorizing the right type of consent to those who handle this information is vitally important and ultimately falls to the responsibility of the patient. As in many other facets of life, personal responsibility is king. When in doubt as to where your personal health information is going to end up, demanding to know who else will have access to it, when it will be accessed, and how long it will be accessible, are all questions we have a right to have answered to our satisfaction.

---

### About the Author

Christian Gitersonke is the CEO of Health Insurance Answers. He has run multiple revenue cycle management companies on behalf of physicians, works closely with electronic health record organizations and advocates for patients' rights, protection of protected health information, and transparency in healthcare. Christian is endorsed by providers as well as community organizations that seek to make healthcare work for patients through protection and proper disclosure. He also serves on multiple boards for post-secondary education as an advisor.

Christian can be reached online at [christian@healthinsanswers.org](mailto:christian@healthinsanswers.org),  
<https://www.facebook.com/healthinsanswers>,  
<https://www.youtube.com/channel/UCbia0MOqTYGEFZ2ZRAosLDQ>  
and at our company website <http://www.healthinsanswers.org>





## Overcoming Security as a Barrier to Cloud Adoption

By Ron Newman, SVP at NTT Ltd. Security Division

The last year has forced organizations into change, both planned and unplanned. Companies have had to pivot, rethink their business strategies and accelerate their digital transformations. A recent [study](#) found that nearly 90 percent of decision makers believe the COVID-19 pandemic has forced them to rely on technology more than ever before. For many organizations, this includes moving workloads to the cloud, a migration that has become somewhat of a necessity for businesses across the globe. Hybrid cloud services, for example, offer benefits, such as assurance of business continuity, resilience, and agility, all issues pushed to the forefront during the COVID-19 pandemic.

A recent [report](#) found that nearly 94 percent of organizations responding to the survey agreed that the hybrid cloud is critical for meeting their immediate business needs. More than six in 10 of respondents said they are already using or piloting hybrid cloud services, with another third planning to roll out a hybrid cloud solution in the next one to two years.

---

Still, there are a hiccups holding some organizations back from embracing the cloud. Many survey participants see cloud security and compliance issues as problematic and a barrier to cloud adoption.

### Security concerns in the cloud

Cloud security is complex, and most organizations want a complete picture of the risk. Over a third of the survey respondents migrated applications or data away from the public cloud to private or non-cloud environments, with more than four in 10 moving to non-cloud environments. And just under 30 percent of those organizations that migrated data from the public cloud named a security breach as the primary driver of their migration to private or non-cloud environments. Meanwhile, close to half of those responding said that data security management is the number one barrier to adopting the hybrid cloud.

With its heightened prominence, security has moved from a cost center to an enabler of organizational transformation. But cloud customers are concerned about their cloud providers becoming targets, with a larger attack surface area to secure. Ultimately, security becomes a shared responsibility in the cloud, with both providers and customers playing a major role. But cloud customers can take steps to ensure their applications and data are as secure as possible.

### Securing your cloud-based data

First, cloud users should view and establish security as an enabler of digital transformation. With better security, experiences with cloud-based applications can be improved for both a company's customers and its employees. On the other hand, insecure applications hurt customer experience, brand reputation, and company revenue. I would recommend that cloud users build security into their applications from the very start. Businesses and their products and services should be secure by design to minimize risk.

In addition, organizations moving to the cloud can seek partners that can help them with their cloud journeys. The right partner can secure mission critical applications using cloud and data center infrastructure. Using a partner to take a platform-wide approach enables discovery, configuration, integration, and the management of services across multiple enterprise applications and technology partners. This provides cloud customers with optimized outcomes and the realization of their business goals.

For more on securing your cloud environment, [click here](#).

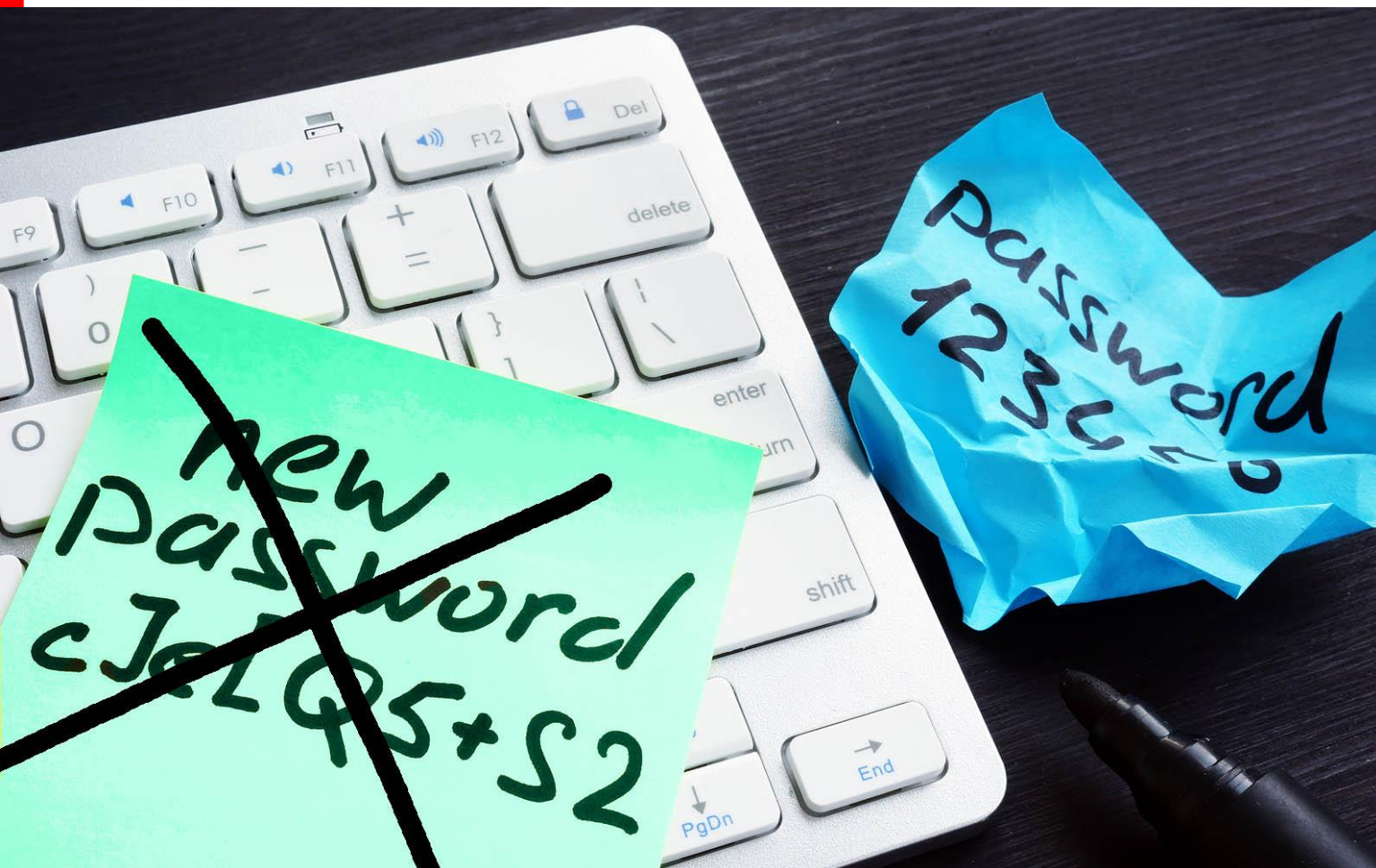
### About the Author

By Ron Newman, SVP at NTT Ltd. Security Division

Ron oversees strategy, services and execution for NTT's Security Division in the Americas. He brings his more than 25 years of experience in the information security industry to drive growth, implement solutions to improve efficiency, lower costs, and reduce risk, and lead business transformations.

Ron can be reached via his LinkedIn profile or at <https://hello.global.ntt>





## Three things' organizations must do to secure “passwordless”

By Jerome Becquart, COO, Axiad

The pandemic forced organizations to accelerate their journey to passwordless with secure authentication methods such as multi factor authentication (MFA), as individuals were expected to access the corporate network from a diverse number of locations, without compromising security or operational capacity. According to [Gartner](#), 60% of large enterprises and 90% of midsize businesses will be using passwordless authentication by 2024. But passwordless in isolation is not enough. In order to maximize the strength of your offering, you need to ensure your authentication methods are standardized and automated across your organization.

### The Problem

Instituting new security programs—particularly when it comes to identity security—ultimately relies on the end user consistently adhering to the new policies. It only takes one instance of circumventing controls

---

to expose your company to a hacker. This problem is further compounded by the fundamental failure of passwords as a method of authentication. Many organizations spend in excess of \$1 million in password-related IT support according to Forrester, and by some estimates, over [80%](#) of data breaches can be related back to poor password hygiene in one form or another.

Practically of course, it is a lot more difficult to enforce a passwordless system across every employee logging into each device or system they use. If an authentication credential is expired for example, or temporarily misplaced, how do employees regain access to the system without using insecure one-time passwords, costing the organization valuable resources? How long does the end user sit idly waiting for a solution before simply thinking (from an operational standpoint) that the lesser of two evils would be to find a workaround in the system, which would leave the organization open for threat actors to gain a foothold into the corporate network.

### The 3-step solution - fostering a company-wide policy of security culture

Attempting to solve the problems described above can be difficult, often placing undue burdens and costs on an over-stretched and underfunded IT department, who are already dealing with the huge task of transferring huge swathes of the workforce to a remote model. Here are 3 key steps to help you increase security policy compliance, decrease IT burdens, adopt a passwordless security approach, and bolster end user self-sufficiency -- all critical issues to address as you ensure secure remote work.

First, it is important that you **make the case for security as a primary concern to all individuals**. As it only takes one individual error in order to let a hacker into the network, then take responsibility for explaining the consequences of this action to your employees through security training, both in terms of personal consequences for them, and the wider consequences for the business should a breach occur.

Second, ensure that **your passwordless authentication system does not exist in a vacuum**. Users are often resistant to change, and will procrastinate and delay any proposed changes (renewing and replacing credentials) while their existing credentials continue to work: Don't let them. Consider implementing technology that will flag users attempting to bypass the authentication protocols you have in place and automatically reroute these users to a system that requires specific actions to be taken before the user can access their corporate network. The empowerment this gives a company from a security perspective cannot be understated: It provides enterprises with a security standard, which can be consistently applied across the entire company, without impacting employee productivity.

Third - and arguably, most crucial - ensure that shaping user behavior happens **without the involvement of IT support**. If this process can be automated, it can avoid undue burdens being placed on already overstretched IT teams and their involvement in every individual incident of authentication being bypassed. In turn, this will help to free up IT teams for their own projects. When the teams are not constantly putting out fires, they can also work to proactively improve the IT posture of their enterprise.

---

## A cultural shift in authentication

Strong authentication methods need to be recognized as a hugely successful and effective method of dealing with cybersecurity threats that impact the ability of a business to function, grow and thrive. Whether we like it or not, passwordless is coming: Gartner's predictions tell us that we need to be imminently ready for this seismic shift in authentication. By making it simple for employees to uphold secure best practices your organization can successfully become passwordless and better protect themselves from breaches, no matter where your employees work and without adding any additional layers of complexity for the end user.

### About the Author

Jerome Becquart is COO of [Axiad](#). Jerome has over 20 years of experience in identity and access management solutions, including 15 years at ActivIdentity. Jerome's management experience includes roles in operational management, sales management, professional services, product and solution marketing, engineering, and technical support. After the acquisition of ActivIdentity by HID Global in 2010, Jerome served as general manager of the HID Identity Assurance business unit. He chaired the Global Platform Government Task Force for three years, and served on the board of directors of this Industry organization.





## Time Is Money: How to Minimize Data Breach Damages with Early Detection

In the current landscape of cybersecurity, most CISOs have come to understand that breaches are inevitable – however, with early detection and remediation, organisations can significantly reduce the harmful impacts of a breach, writes Karl Swannie, Founder of Echosec Systems.

By Karl Swannie, Founder, Echosec Systems

Data breach recovery is only as successful as the time it takes to find and remediate the compromise. Thanks to reports like [IBM's 2020 Cost of a Data Breach](#), we know that damage scales with the length of a breach lifecycle. In the cybersecurity world, days can mean millions.

---

So why does it still take businesses 280 days, on average, to find and contain a breach? And what can CISOs and IT Managers do to minimize this timeframe and—as a result—financial and reputational losses?

There are a number of reasons why compromise often takes so long to detect and address. For one, enterprise cybersecurity is notoriously underfunded. According to [ISACA's 2020 State of Cybersecurity Report](#), 60% of respondents claim that their cybersecurity budget is either somewhat or significantly underfinanced. Underfunded cybersecurity programs usually lack the security infrastructure, personnel, and training required to avoid attacks or respond effectively when a breach inevitably occurs.

Organizations also sacrifice speed-to-information without security automation. According to IBM, fully deployed automation can reduce breach lifecycles by almost 25% compared to security systems with no automation. Attacks can fly under the radar if companies aren't diligent about [third-party compromise](#). And there's the fact that, between nation-state actors, criminal groups, and the COVID-19 pandemic, [attackers are becoming more sophisticated](#) by the day.

We also know that early breach detection isn't always about visibility into your internal systems and data feeds. Breach indicators are often first detectable on public online sources like deep and dark web forums, paste sites, and marketplaces where data is monetized or freely available. If you're not including obscure online sources within your threat intelligence toolkit, you're missing a potential opportunity to reduce detection and remediation time.

### What's At Stake: A Quick Recap

As a security professional, you're probably well aware of the cost of late detection. According to [IBM](#), enterprises with over 25,000 employees are looking at a breach price tag of \$5.52M—but organizations can save an average of \$1.12M if they shorten its life-cycle to under 200 days. This cost captures expenses related to crisis management, lost business, regulator communications, and victim response.

These numbers don't include regulator expenses for non-compliance. For example, under GDPR regulations, breached organizations must report incidents within 72 hours or risk hefty fines in the millions. Businesses also risk potential lawsuits and the immeasurable cost of losing customer and stakeholder trust.

### Early Detection & Remediation Strategies

How can you support earlier breach detection within your organization? The good news is that several solutions are within reach. [Varonis](#) suggests the following high-level strategies to minimize breach lifecycles:

- Invest more in comprehensive cybersecurity solutions, particularly those harnessing automation.
- Improve communications with executives and board members to factor cybersecurity concerns into org-wide budgeting and decision-making.
- Establish a dedicated cybersecurity and incident response team.
- Develop and routinely test a breach response plan so that you're better prepared for remediation.
- Prioritize other cybersecurity best practices, such as limiting file permissions within the organization and educating employees about cybersecurity.

---

But that's not all. We mentioned earlier that early breach indicators are often present on public online sources, such as the deep and dark web – sometimes even before a compromise is apparent on your systems.

Cybersecurity teams can avoid these blind spots by leveraging tools and data feeds that monitor a variety of hidden online spaces for mentions of your company or sensitive assets – like email addresses and other internal data. Improving data coverage isn't the answer to early detection, but it can go a long way to support a more proactive solution.

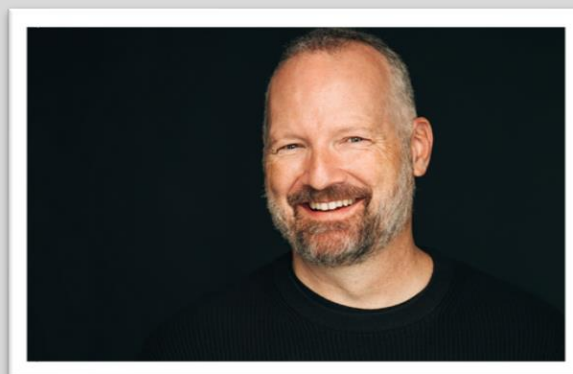
Many of these obscure data sources, which include unindexed chan boards, forums, and paste sites, are not crawled by commercial threat intelligence solutions—which is why it's important to examine data coverage when evaluating new vendors. Relevant sources emerge quickly on the deep and dark web. Your cybersecurity analysts [don't have time](#) to navigate these sources manually for potential risks, so let your software do the work for them.

[Most CISOs understand](#) that breaches are inevitable. But with early detection and remediation, organizations can significantly reduce fiscal damages, protect their data subjects and IP, and preserve their reputation.

As attack surfaces increase through digital transformation and workforces turn domestic, early detection strategies are essential for business growth in 2021 and beyond.

### About the Author

Karl Swannie is the Founder of Echosec Systems. Founded in 2013, Echosec Systems is an advanced digital threat intelligence technology provider that monitors data across mainstream social media, decentralized social networks, messaging apps and the dark web. Headquartered in Victoria, British Columbia, Echosec Systems has created a range of unique software solutions to provide organizations with an all-in-one toolkit to create an easy-to-understand, comprehensive picture of potential threats online, without the risk of drowning in data. Karl can be reached through [LinkedIn](#) and at [Echosec.net](#).





## Why We Care About Cybersecurity Hygiene

By James Opiyo, Senior Consultant Security Strategy, Kinetic By Windstream

Maintaining good cybersecurity hygiene habits is just as important as maintaining good personal hygiene habits. We must maintain high cybersecurity standards to protect our digital health from some common cyber threats.

### Common threats to our digital health

- Malicious software (malwares) designed to steal information and or cause damage to our connected devices.
- Viruses that infect connected devices and then spread to others while giving cybercriminals access to those devices.
- Ransomware malware that *kidnaps* a connected device and prevents an authorized user from accessing the affected device until a ransom (usually cash) is paid.

- Phishing scam where cybercriminals attempt to steal sensitive data (SSN, Credit Card numbers etc.) using deceptive electronic messages e.g. email, text messages, pop-up windows etc. They use fake websites, emails, etc. and lure users to disclose sensitive information. They may, for example, send a link masked to look like your bank's legitimate web address and ask you to click on it and login to your bank. This will give them access to your real login credentials which they can use to log into your real bank account and steal money, personal information etc.

### Cybersecurity hygiene habits to help mitigate common threats

- Install reputable antimalware & antivirus software to prevent malware attacks.
- Create complex passwords that cannot be easily guessed. For example, using combinations of at least 12 letters, numbers, and special characters.
- Secure your Wi-Fi network with a strong password and router name. Turn off remote management of the router and ensure that the router offers WPA2 or WPA3 encryption to maintain the highest level of privacy of information sent via your network.
- Change the manufacturer default passwords for all your smart devices e.g. smart thermostat, smart doorbells, smart locks, etc. A hacker can easily download a smart device's user manual and get its default password.
- Update software and apps regularly to maintain latest version of software patches that fix security flaws.
- Permanently delete sensitive data from your computer and keep your hard drive clean.
- Never click on a link, open pop-up, etc. from unknown source.

### Conclusion

In summary, we should include installing reputable antimalware software, creating strong passwords, keeping our connected devices clean, and always be suspicious of request for information coming from unknown sources as paramount steps to keeping good cybersecurity hygiene habits.

#### About the Author

James Opiyo is a Senior Consultant for Security Strategy at [Kinetic by Windstream](#). Kinetic provides premium broadband, entertainment, and security services through an enhanced fiber network and 5G fixed wireless service to consumers and small and midsize businesses primarily in rural areas in 18 states.

Email: [james.opiyo@windstream.com](mailto:james.opiyo@windstream.com)





# EVENTS

# RSAC<sup>®</sup>Conference2021

May 17 – 20 | Virtual Experience



RESILIENCE

## **BIG NAMES. BIG INSIGHTS. BIG REASONS TO ATTEND RSAC 2021.**

Over two hundred expert-led sessions covering 24 tracks. Thought-provoking keynotes. Cutting-edge innovation. Valuable networking opportunities. In-depth, interactive activities. RSAC 2021 is where the world talks security, and you can be a part of this important conversation.

Join industry leaders and peers at RSAC 2021, a virtual experience, May 17-20. Learn about the latest trends that are most relevant to your needs, advance your career and help shape the future of the industry.

**Register today for the most inspirational four days in cybersecurity at [rsaconference.com/cyberdefense21](https://rsaconference.com/cyberdefense21).**

**#RSAC**



**FOLLOW  
US**



May 6th 2021

24HR VIRTUAL EVENT

Join FREE\* with code: CDM-VIP



APAC > MEA > Europe > LatAm > USA

Join Us Online at Cyber Security for Critical Assets World Summit this May!

On May 6th, 100's of IT & OT security leaders will gather at the CS4CA World Summit to share vital cyber security insights and unite in safeguarding their critical assets and infrastructure. The unique 24-hour agenda will start with expert speakers in the APAC region and transition throughout MEA, Europe, LatAm and USA with presentations, panel discussions, live Q&A's, case studies and plenty of networking too!

**Agenda topics include:**

- Risk-Based Cyber Security in the Critical Infrastructure Space
- Integrated Cyber-Physical Security
- ICS Security Beyond Reactive Measures
- Achieving ICS Intelligence in a Converged IT-OT World
- OT Security in the Age of Digital Transformation & IoT
- And, more!



**Speakers include** CISOs, VPs & Heads of Cyber Security at: **Baker Hughes, ENGIE, Origin Energy, Avangrid, Almirall** & more....



Paul W Brager  
Director, Global OT  
Security Programs  
Baker Hughes



Sarfaraz Ahmed  
CIO & CISO  
ENGIE



Monica Verma  
CISO  
Helsedirektoratet



Brian Harrell  
CISO  
Avangrid



Brad Flanagan  
Head of Cyber Security  
Essential Energy



Bhushan Deo  
CISO  
Thermax Limited



Chinenye Chizea  
CISO  
National Identity  
Management Commission



Ramon Serres  
CISO  
Almirall



Vanessa Gale  
Head of Identity and  
Access Management  
Origin Energy



Dr. Tim Nedyalkov  
Cyber Security Manager,  
Infrastructure ME  
SNC-Lavalin

This is a one-of-a-kind opportunity for critical infrastructure leaders around the world, to come together and safeguard their assets. View the agenda and **secure your place for FREE** using the discount code: **CDM-VIP** at: **[world.cs4ca.com](http://world.cs4ca.com)**



# GISEC

*Live, in-person*

31 MAY -  
2 JUNE 2021

DUBAI WORLD  
TRADE CENTRE

THE MOST INFLUENTIAL AND CONNECTED

## CYBERSECURITY EVENT FOR THE ARAB WORLD

**ENQUIRE ABOUT EXHIBITING, SPEAKING AND SPONSORSHIP**

+971 (04) 308 6267

✉ gisec@dwtc.com

🌐 www.gisec.ae

### OFFICIALLY SUPPORTED BY

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



مركز دبي للأمن الإلكتروني  
DUBAI ELECTRONIC SECURITY CENTER

شرطة دبي  
DUBAI POLICE

دبي الذكية  
SMART DUBAI

### OFFICIAL DISTRIBUTION PARTNER

**SPIRE**  
INFORMATION. SECURED.

### STRATEGIC SPONSORS

vmware  
Carbon Black

Recorded  
Future

### SILVER SPONSORS

BLUVECTOR  
A COMCAST COMPANY

Checkmarx

DARKTRACE

### COUNTRY PAVILIONS

CYBER  
WALES

SecurITy  
made in  
Germany

TURKISH CYBER  
SECURITY CLUSTER

FOR PEOPLE  
SERIOUS ABOUT  
**MICROSOFT**  
**365 & AZURE**

 **ESPC21**  
— **ONLINE**  
01-02 JUNE 2021

REGISTER FREE



[www.sharepointeurope.com](http://www.sharepointeurope.com)

Including **CyberSecurity** Keynote by:

**PAULA JANUSZKIEWICZ**  
CEO & FOUNDER OF CQURE, CYBERSECURITY EXPERT

→ HACKER'S PARADISE: Top 10 Biggest Threats When Working From Home



# WSJ PRO

## CYBERSECURITY EXECUTIVE FORUM

JUNE 2, 2021 | ONLINE

# Advancing Security in the New Business Environment

From the landmark SolarWinds cyber breach to the new remote workforce reality that will test privacy laws, it's never been a more critical time for technology professionals to be fully embedded in the business.

The WSJ Pro Cybersecurity Forum will show them how to expand their role past the IT department, as well as how other company leaders can ask the right questions in order to keep systems—and employees—safe.

## Confirmed Speakers



**Raj Badhwar**  
Chief Information  
Security Officer  
**Voya Financial**



**Tami Hudson**  
Chief Information  
Security Officer  
**Randstad North America**



**Kevin Mandia**  
Chief Executive Officer  
**FireEye**



**Cecile Wendling**  
Group Head of Security  
Strategy and Awareness  
**AXA**

**REGISTER NOW FOR YOUR COMPLIMENTARY TICKET**

**CYBER.WSJ.COM**

**USE CODE: CYBERDEFENSE**

In Partnership With



**CYBER DEFENSE**  
— MAGAZINE —  
WHERE INFOSEC KNOWLEDGE IS POWER

**Driving the rapid replacement of cybersecure IEC 61850 systems within the substation, inter-substations, to the control room, and across DER infrastructure**

**5-Day Hybrid Conference, Exhibition & Networking Forum**

**18-22 October 2021 | Sweden + Swapcard**

**150+ IEC 61850 leaders convene in Sweden on 18-22 October 2021, to review the latest implementations of IEC 61850 systems within the substation, inter-substations, to the control room, and across DER infrastructure**

Recent research carried out by Smart Grid Forums among power grid operators worldwide, indicates that Covid-19 has injected urgency into utilities' digitisation plans with profound implications for substation automation teams. This year's 8th annual IEC 61850 Week 2021 hybrid conference will be held 18-22 October 2021 in Sweden and draw together pioneering IEC 61850 implementation leaders for a week-long review of the latest standardisation developments, pilot project results, large-scale implementation experiences, and future application explorations.

The focus will be on driving the deployment of next generation IEC 61850 architectures through more efficient specification, engineering, testing, operation, maintenance, and innovations in cybersecurity within a more rapid 'replacement' environment. Case-studies will focus on implementations of process bus and station bus architectures, with applications within the substation, inter-substations, from substation to control centre, and across distributed energy resources.

**Monday 18th October: Specification Workshop**

The week begins with a hands-on practical workshop providing utilities and suppliers with the opportunity to explore how they can leverage IEC 61850 specification guidelines to improve their collaboration, streamline the end-to-end specification process, reduce duplication of effort, and ensure clarity of utility objectives whilst leveraging supplier expertise.

**Tuesday 19th to Thursday 21st October: Implementation Case-Study Conference & Exhibition**

Over the course of these three days, participants will hear the latest lessons learnt from pilot projects and large-scale deployments of multi-vendor multi-edition IEC 61850 systems worldwide. With case-studies from Europe, Americas, Asia, Middle East and Africa, this is a unique opportunity to gain a global perspective on real-world deployment activity, future system and component requirements, and explore brand new partnership opportunities.

**Friday 22nd October: Cybersecurity Workshop**

The week wraps up with this deep diving seminar into the cybersecurity issues currently impeding the deployment of IEC 61850. With a thorough exploration of IEC 62351 both on a conceptual level and in terms of its application and evolution, participants will come away with a clear understanding of how they can tighten up system security today and what cybersecurity innovations they can plan to leverage tomorrow.

Due to ongoing travel uncertainties, this year's programme will be held in hybrid format, with an onsite experience offered to those who will be permitted to travel, and an online alternative for those who won't.

**For more information please contact:**

Mandana White, CEO, Smart Grid Forums

**Smart Grid Forums Ltd**

PO Box 63594, London, N19 9FT, United Kingdom

T: +44 (0)20 8057 1700 | [registration@smartgrid-forums.com](mailto:registration@smartgrid-forums.com)



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**





# CYBER DEFENSE TV

## INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here...we've launched [CyberDefense.TV](https://www.cyberdefense.tv)

Hundreds of exceptional interviews and growing...

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](https://www.cyberdefense.tv)

## FREE MONTHLY CYBER DEFENSE eMAGAZINE VIA EMAIL

ENJOY OUR MONTHLY ELECTRONIC EDITIONS OF OUR MAGAZINES FOR FREE.

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

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

---

Copyright (C) 2021, 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](mailto:marketing@cyberdefensemagazine.com)  
All rights reserved worldwide. Copyright © 2021, 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](mailto: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.

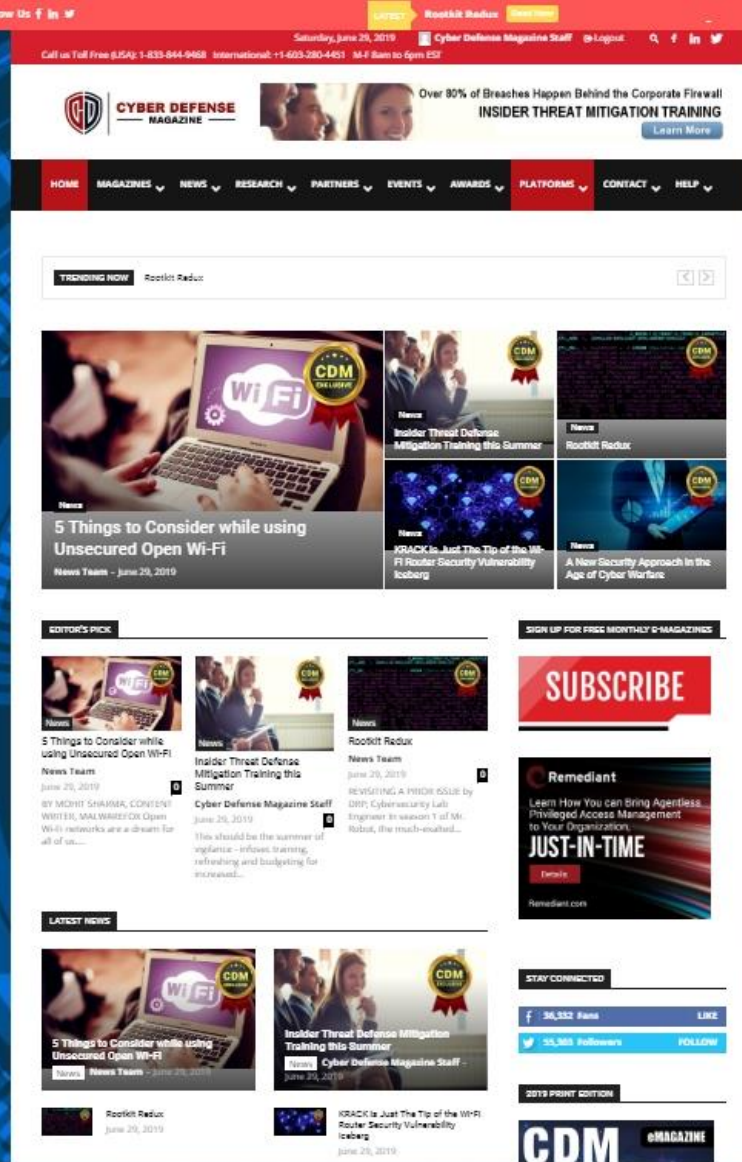
[marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

[www.cyberdefensemagazine.com](http://www.cyberdefensemagazine.com)

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

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 05/03/2021

Books by our Publisher: <https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH> (with others coming soon...)



**9 Years in The Making...**

***Thank You to our Loyal Subscribers!***

We've Completely Rebuilt [CyberDefenseMagazine.com](http://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 [CyberDefenseMagazine.com](http://CyberDefenseMagazine.com) up and running as an array of live mirror sites and our new B2C consumer magazine [CyberSecurityMagazine.com](http://CyberSecurityMagazine.com).

*Millions of monthly readers and new platforms coming...starting with <https://www.cyberdefenseprofessionals.com> this month...*

# CDM

**CYBER DEFENSE MAGAZINE**

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

**eMAGAZINE**

**[www.cyberdefenseemagazine.com](http://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**



**\* with help from writers  
and friends all over the Globe.**