CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

IN THIS EDITION

Top 25 Women In Cybersecurity

Know Who to Call When Phishing Strikes

Ensuring the Security & Productivity of an Increasingly Remote Workforce

2019: Why Invest in Secure File Transfer This Year

What Does Breach Prevention Mean

Building a Career in Incident Response

Ransomware Terrorism: Should We Be Worried?

...and much more...

AUGUST 2019

MORE INSIDE!

CONTENTS

Top 25 Women in Cybersecurity 12

5 Simple Ways to Keep Your Personal Information Safe Online 24

Your Enterprise Network: On-Premise, Cloud-Based, And the Transition In Between 28

Is Your Organization Ready For The Windows 10 Migration? 32

Bitglass 2019 Cloud Security Report 35

Security by Design for Mobile Apps 48

Comprehensive Cyber Security for Digital Era! 52

GDPR 56

One of the Greatest Threats Facing the Iot: Router Security 59

How to Reduce Your Company's Susceptibility to Hacking 62

10 Steps to Kicking Off Your Insider Threat Program 65

How Is Machine Learning Helping Cyber Defense? 68

What Is DNS Hijacking And How Can You Mitigate? 71

The Top 4 Application Security Defenses You Didn't Know You Needed 75

July Patch Tuesday 79

How To Prevent Your Data Loss Using Enclosed Data? 81

The Iot Headache and How to Bolster Defenses 85

Cybersecurity & Your Company 87

The Smart Encryption Procedures and Policies 90

Five Ways a Software Defined Perimeter Is Better Than VPN 93

The Email Tracking and Fraud Prevention 96

The Foundation Common to Most Security Frameworks: Addressing Configuration Controls 99

CONTENTS (cont')

Virtual Private Server Market to Hit US$ 2 Billion by 2025 104

Stay One Step Ahead Of Hipaa Compliance 108

The Dangers of HTTPS: When Secure Is Not Safe 111

Going for Gold – Why Hackers Are Looking For Active Directory Golden Tickets 113

Overcoming Zero Trust Challenges in the Federal Government 116

Is Your Organization Driving the Getaway Car for Cybercriminals? 119

Let's Come At The Cybersecurity Skills Gap From A New Angle 124

Facing the Reality of VPN Security Flaws, And How to Overcome Them 127

Data Manipulation Attacks Difficult To Detect But Preventable 130

Privacy Regulations Are Popping Up Everywhere 133

Reducing the Occurrence and Impact of Data Breaches through Strong Practices and Procedures 137

Will Your Wordpress Site Be Breached In 2019? 142

The Role of Certifications for a Cyber Security Professional 145

To Pay or Not To Pay, That Is the Question 149

Today's Cyber Threats Demand Enhanced Strategies and Solutions 152

Reducing the Insecure Deserialization Risk 158

@MILIEFSKY

From the

Publisher...

New CyberDefenseMagazine.com website, plus updates at CyberDefenseTV.com & CyberDefenseRadio.com

Dear Friends,

Striving to reach our goal as the #1 source of all things InfoSec knowledge – best practices, tips, tools, techniques and the best ideas from leading industry experts, we've hit some exciting inflection points including reaching two million unique website visitors this year and almost 80,000 double opt-in email membership, which is nearly 3x last year's numbers. We've had o*ver 1.5 million DNS queries per month at CyberDefenseMagazine.com – that's phenomenal growth!* We're tracking our results on various independent websites that track keywords across the global internet and here's where we stand today: https://essentials.news/en/future-of-hacking.

We also offer our own statistics that you are free to reuse anytime, from this page: http://www.cyberdefensemagazine.com/quotables/.

I am so thankful and honored to each of you – readers, partners, customers, employees, consultants, supporters and so very importantly – Robert Herjavec and Dr. David DeWalt for joining in with me to judge the Black Unicorn Awards for this year.

We've announced who the finalists are, here: http://cyberdefenseawards.com/black-unicorn-awards-finalists/ and will be announcing the winners, here: http://cyberdefenseawards.com/black-unicorn-awards-winners/ on August 6, 2019 during Black Hat USA 2019. We'll be releasing a 52 page Black Unicorn Report for 2019 at that time. Make sure you bookmark those pages so you can get your copy of this important industry report.

Finally, last, but most definitely NOT least, we've found our Top 25 Women in Cybersecurity for 2019 and hope you will join us in congratulating them – you can LinkedIn with each of them, here: http://cyberdefenseawards.com/top-25-women-in-cybersecurity/. Let's all keep on innovating and finding ways to get one step ahead of the next threat!

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

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

From the Editor's Desk…

Our theme for this summer remains "turning on the Human Firewall" and that means …***Training Training…Training***

From KnowBe4 to Hacker.House to InsiderThreatDefense.US we see a common thread – you can dramatically bolster your "Human Firewall" if you first, turn it on.

How to turn on the Human Firewall?

With training by experts. Kevin Mitnick will teach you social engineering 101 and KnowBe4 will provide you with the most advanced antiphishing and compliance tools.

Hacker.House will teach you how to be the best penetration tester, yourself. Why hire consultants who don't care about your business every day of their lives?

Finally, with most breaches happening from the inside-out, it's time to get vigilant and train yourself for insider threat mitigation at InsiderThreatDefense.US.

To our faithful readers,

Pierluigi Paganini

Editor-in-Chief

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

PRESIDENT & CO-FOUNDER
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

EDITOR-IN-CHIEF & CO-FOUNDER
Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

EDITOR-AT-LARGE & CYBERSECURITY JOURNALIST
Yan Ross, JD
Yan.Ross@cyberdefensemediagroup.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

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

http://www.cyberdefensemagazine.com

PUBLISHER

Gary S. Miliefsky, CISSP®

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

WE'RE CELEBRATING

7 YEARS OF EXCELLENCE!

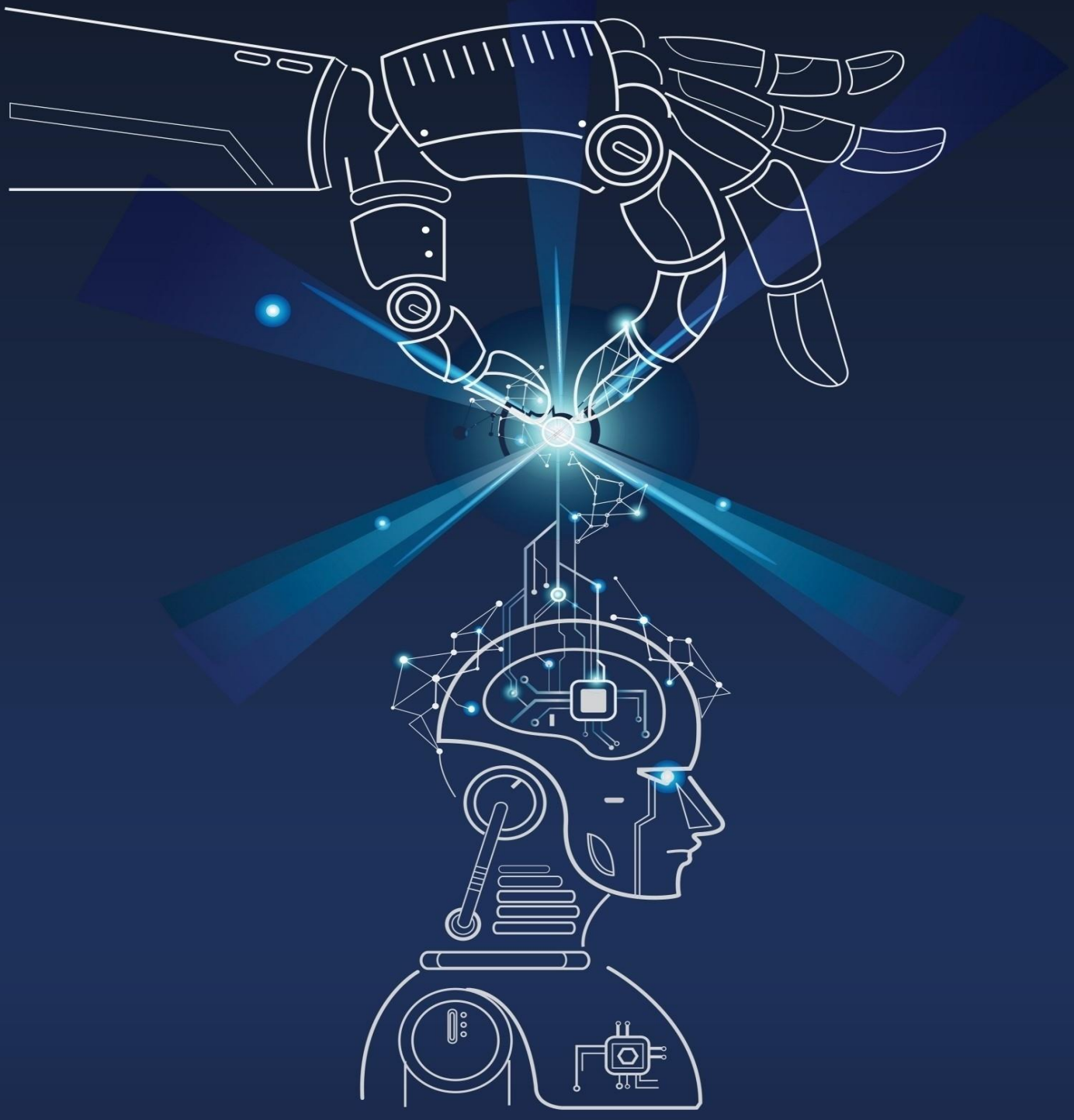
Providing free information, best practices, tips and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS


SPONSORS

InfoSec Knowledge is Power
Free Cybersecurity Resources



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

Setting the Standard

in Cyber Defense Training & Education

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

CORPORATE | GOVERNMENT | MILITARY | EDUCATION

- Powerful Hyper-Realistic Range Simulation
- Industry Certifications
- Executive & Senior Leadership Cyber Workshops
- Associate, Bachelor's & Master's Programs

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

Learn More

regent.edu/cyber | 757.352.4590

REGENT UNIVERSITY | Institute for Cybersecurity

Database Cyber Security Guard

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

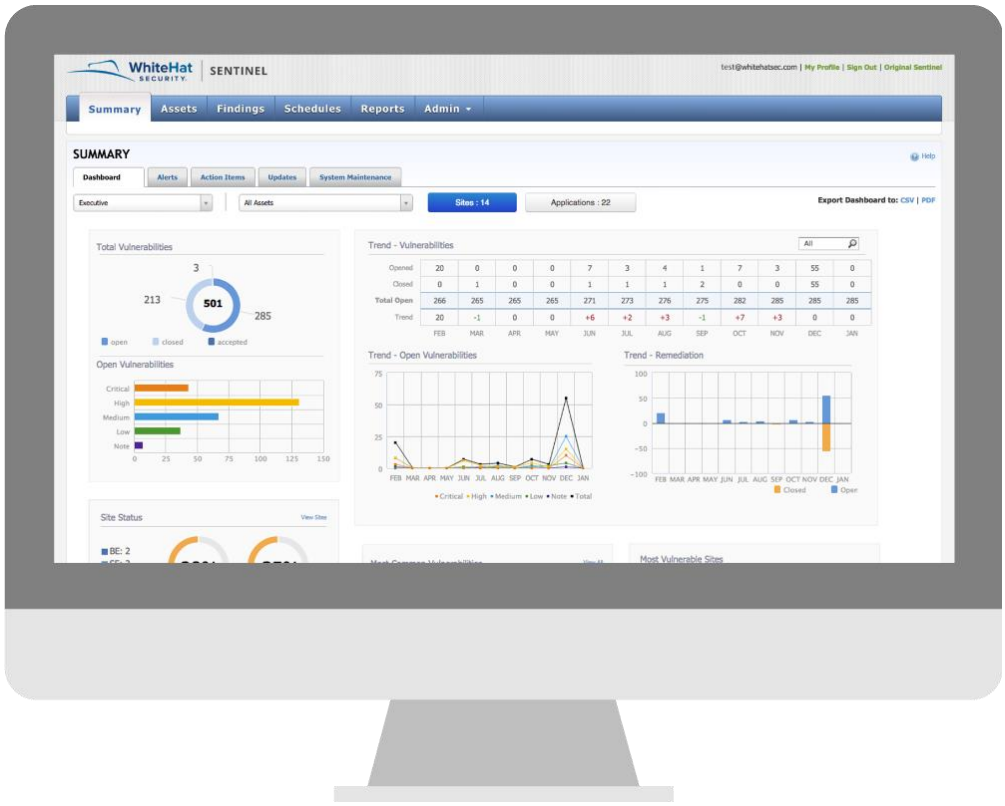
Average data breach costs $7.3 million dollars. Would have immediately shutdown the Equifax and Marriott hackers.

Product Features

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

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

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



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

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

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

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

A customized review and complimentary final executive and technical report

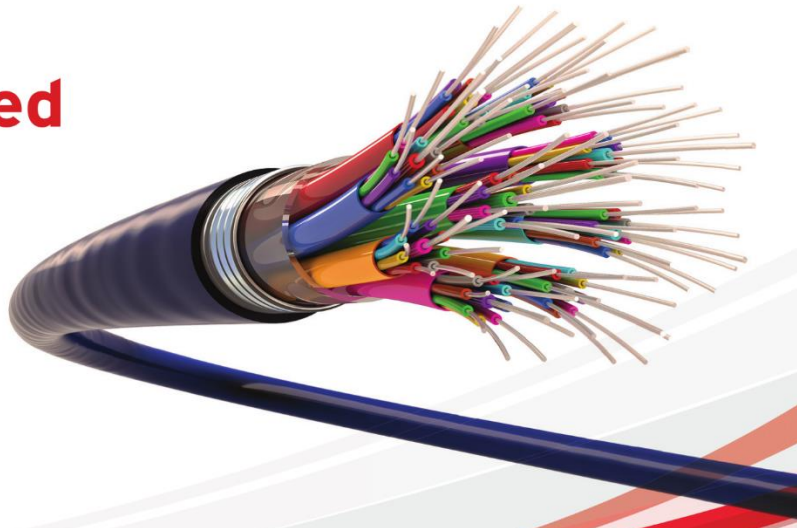
Click here to sign up at this URL: https://www.whitehatsec.com/info/security-check/

PLEASE NOTE: Trial participation is subject to qualification.

TREND MICRO

POWERED BY XGen SECURITY

Detect and prevent breaches at wire speed



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

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

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

NSS LABS RECOMMENDED

Proven capability

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

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

Industry leading threat intelligence

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

Please get in touch:
Bharat Mistry, Principal Security Strategist
Bharat_mistry@trendmicro.co.uk

www.trendmicro.co.uk/xgen-cyber

Award Winners

Top 25 Women in Cybersecurity

Cyber Defense Awards in conjunction with Cyber Defense Magazine is pleased to announce the Top 25 Women in Cybersecurity for 2019. We narrowed our list down from three hundred candidates and evaluations based on open source intelligence (OSINT) on these women including their LinkedIn profiles as well as numerous interviews to only 25 winners this year.

Our Publisher has interviewed some of these winners in his www.cyberdefensetv.com hot seat program – where they had to answer difficult and challenging questions – completely unprepared and unscripted. You can search at the TV site or follow those linked, below.

In addition, our search focused us on some of the top innovators, with boots on the ground, women in cybersecurity making a difference every day. It, therefore, gives us great pleasure to recognize and celebrate the accomplishments of these deserving women in one of the most challenging and demanding fields of information technology and computing – that of cybersecurity.

Here are the winners

Catherine A. Allen, Chairman and CEO at the Santa Fe Group

For more than 30 years, Catherine A. Allen has been an outstanding leader in technology strategy and financial services and a key thought leader in business innovation. Today, Catherine is Chairman and CEO of The Santa Fe Group, a strategic consulting company based in Santa Fe, NM. The Santa Fe Group specializes in briefings to C-level executives and boards of directors at financial institutions and other critical infrastructure companies, and provides management for strategic industry and institutional projects, including the Shared Assessments Program, focused on third party risk. Catherine is active politically in national and local spheres, including being a former member of President Obama's Economic Development and Small Business Committees and the New Mexico State Investment Council. Catherine was honored in 2007 by *US Banker Magazine* with the Lifetime Achievement Award for her outstanding contributions to financial services and technology. In 2013, she was honored with the Lifetime Achievement Award for her contributions to technology by the Executive Women's Forum. She was honored with the 2015 Leadership Award by the Griffith's Society. She is the recipient of an Honorary Doctorate of Humane Letters from the University of Missouri, recognizing her professional achievements in financial services and technology. Learn more about her at: https://www.linkedin.com/in/callen8/ and watch our CyberDefenseTV interview with her at: http://cyberdefensetv.com/santa-fe-group-fostering-connections-more-secure-economy/

Jennifer Arcuri, CEO Hacker.House

Founder of Hacker House, Inno-Tech Network, video producer, serial entrepreneur, and Cyber Security Ethical Hacker. Experienced in information security, fund raising, social media, ecommerce, social commerce, website development, idea/brand development and implementation, mobile development/marketing, effective presentation and negotiating skills, creative problem solving, improvising, efficiency, highly enthusiastic networks of professionals, particularly entrepreneurs and investors in cyber security, entertainment, media, and tech based clusters in London, Newcastle, Oxford, Cambridge, Los Angeles, New York, SF, Silicon Valley, Across the ASEAN region, Middle East, South Africa, Scandinavia, and most of Europe.

Learn more about her at: https://www.linkedin.com/in/jenniferarcuri/

Illena Armstrong, VP, Editorial, SC Media/Haymarket Media

Illena Armstrong is VP, Editorial, at SC Media, the leading business media brand for the information security industry. She spearheads and manages all editorial strategy and content development for SC Media, as well as plays a key leadership role in driving the brand's overall business and commercial development. She does this by working with indefatigable colleagues and managing a dedicated team who are in offices across NY, Oregon and Michigan.

Her multifaceted media leadership role harnesses her creativity, drive, journalistic prowess, brand-building experience and business acumen. It encompasses editorial, design, website/digital, marketing, social media, event, and overall business/commercial oversight responsibilities for SC.

Learn more about her at: https://www.linkedin.com/in/illenaarmstrong/

Dr. Bhavani, Cyber Security Researcher & Educator, University of Texas @ Dallas

Dr. Bhavani Thuraisingham is the Louis A. Beecherl, Jr. Distinguished Professor of Computer Science and the Executive Director of the Cyber Security Research and Education Institute at The University of Texas at Dallas (UTD). She is an elected Fellow of several prestigious organizations including ACM, IEEE, the AAAS, National Academy of Inventors and the the British Computer Society. She has received prestigious awards in cyber security including the IEEE Computer Society's 1997 Technical Achievement Award for "outstanding and innovative contributions to secure data management", the 2010 ACM SIGSAC Outstanding Contributions Award for "seminal research contributions and leadership in data and applications security", and a 2013 IBM Faculty Award in Cyber Security. She has unique experience working in the commercial industry (Honeywell), federal research laboratory (MITRE), US government (NSF) and academia and her 36 year career includes research and product development, technology transfer, program management, and consulting. Her work has resulted in 100+ journal and 300+ conference papers, 100+ keynote addresses, and 6 US patents. She has authored 15 books and edited 12 more. She was educated in the United Kingdom and received the prestigious earned higher doctorate (Doctor of Engineering) from the University of Bristol, England for her published research in data security since her PhD. She is a STEM mentor to women and minorities and has given talks at SWE, WITI, and CRA-W. She serves on multiple advisory boards and has been a software consultant to the US Dept. of Treasury since 1999. Learn more about her at: https://www.linkedin.com/in/dr-bhavani-thuraisingham-aka-dr-bhavani-75305127/

Anne Bonaparte, CEO at Appthority

Innovative entrepreneur and company builder known for scaling emerging companies through high growth stages to become market leaders that endure. Anne's foundational experience leading $500M divisions of large technology companies complements her serial success partnering with technology founders to unlock potential and capture market value. Deep functional leadership in global sales, strategy, business development and product delivery. Specialties: Growth, SaaS, Cybersecurity, mobile, enterprise. Learn more about her at: https://www.linkedin.com/in/annebonaparte/ and watch our CyberDefenseTV interview with her at: http://cyberdefensetv.com/appthority-preventing-mobile-breaches/

Carolyn Crandall, Chief Deception Officer, Attivo Networks

Ever wonder if life could be more fun? As a person who thrives on being a high-impact player, I have had the continuously good fortune of being on the leadership teams of some of high tech's fastest growing companies. Over my career, I have built new markets and gained the reputation of a global marketing authority with repeated demonstrations of unprecedented revenue growth, market leadership, and company valuations.My curiosity and passion for learning has enabled me to build a unique breadth of experience in market building disciplines that I have applied across hardware, software, cloud and service technology offerings. I have a unique depth of experience in building brands and markets, new market category creation, awareness building, product marketing, digital marketing, demand generation, social media, blogging, and partner marketing. I can move seamlessly from strategy to high-velocity hands-on execution. My track record includes successfully taking companies from startup to IPO and through to multi-billion dollar sales growth. Learn more about her at: https://www.linkedin.com/in/cacrandall/ and watch our CyberDefenseTV interview with her at: http://cyberdefensetv.com/attivonetworks-deception-technology-that-really-works/

Mischel Kwon, Founder and CEO, MKACyber

I'm experienced in application development, network architecture and implementation and building and managing Security Operations Centers (SOC). I design and guide MKACyber's approach and methodology to security operations and have built an organization of elite SOC experts who partner with our customers to help them change the way they approach security operations. I also work closely with CISOs and executive teams to help them elevate security operations to a Board-level business discussion. Learn more about her at: https://www.linkedin.com/in/mischelkwon/

Galina Datskovsky, CEO, VaporStream

I am an internationally known expert in the fields of compliance, information governance and associated technologies with over 20 years' experience. I am technology expert and hold a PH.D. in computer science. I am also a CRM. I have excellent management skills. I currently serve on multiple boards.

Specialties: Information governance, compliance, information security, records management, information technologies, SAAS platforms, Big Data/ Dark Data processing. I am a excellent team builder and leader. Learn more about her at: https://www.linkedin.com/in/galina-datskovsky-72953a12/ and watch our CyberDefenseTV interview with her at: http://cyberdefensetv.com/vaporstream-secure-messaging-for-the-enterprise/

Deidre Diamond, Founder and CEO, CyberSN

Combining my 21 years of experience working in technology and staffing, my love for the cyber security community, and a genuine enthusiasm for people; I created Cyber Security Network (http://www.cybersn.com), a company transforming the way Cyber Security Professionals approach job searches. CyberSN.com will remove the frustration from job-hunting, and aid in interpersonal connections and education.

Throughout my career I have built large-scale sales and operations teams that achieved high performances. Creating cultures based on an anything is possible attitude allows people to achieve above and beyond the usual. By establishing an open communication framework throughout an organization; I have created cultures of positive energy, career advancement and kindness that enables teams to reach beyond peak performance and have fun at work.

Learn more about her at: https://www.linkedin.com/in/deidrediamond/

Michelle Drolet, CEO, Towerwall

As the CEO of a small, woman run business and one of Towerwall's resident information security experts, I assist organizations through the process to help them protect critical data by the evaluation, establishment, education andenforcement of sound information security, network security and data security programs and practices.

Learn more about her at: https://www.linkedin.com/in/michelle-drolet-a926b79/

Hong Jia, Co-founder, Chief Security Researcher, AppEsteem Corporation

Hong Jia is chief research officer in AppEsteem, leads unwanted program analysis and deceptor application hunting. She was Co-founder and head of response and research in ThreatBook Labs, a startup company based in China providing threat intelligence services. Hong led ThreatBook's effort in threat incident response, threat intelligence research, data mining and correlation data study applied to research in threat intelligence.Prior to joining and setting up ThreatBook Labs, Hong worked as the principal lab manager of response and research at Microsoft Malware Protection Center (MMPC), with labs in Redmond (WA), Vancouver (BC) and Beijing. She has been leading MMPC labs' effort to protect billions of computer from malware through fast incident response, deep malware family threat research and machine learning driven automation for malware clustering and classification. She also served as liaison between MMPC and China security companies, and has helped in a number of MMPC security program's deployment in China through her strong industry relationships with security organizations and vendors. Hong gained valuable experience working at Microsoft and collaborating with security industry during her 15 service in Microsoft.

Learn more about her at: https://www.linkedin.com/in/hong-jia-02234654/

Jane Frankland, CISO Advisor, Author, Keynote Speaker

By the time I was 29 I'd built a 7-figure global business. I did it within 2yrs. Whilst building a business is a huge achievement it's not the hardest thing in business to do. The hardest thing is turning around a company that's failing. I've done both and without investment. I've a diverse background, from being nominated as a Young British Designer after graduating to building my own global hacking firm and becoming a board advisor, awards judge, awards winner, LinkedInTop Voices and a top 20 cybersecurity global influencer.

Having been in cybersecurity for over 21-years I've held senior executive roles at several large PLCs and been actively involved in OWASP, CREST and Cyber Essentials. With a proven track record in working with some of the world's biggest brands and delivering fast revenue growth, I've learnt how to communicate business strategy with senior executives and cybersecurity needs with technical staff. Being able to translate between both requirements has enabled me to orchestrate faster, smoother and more effective engagements.

Learn more about her at: https://www.linkedin.com/in/janefrankland/

Dr. Lydia Kostopoulos, Founder, Sapien21, Senior Researcher, ESMT Berlin

My work and interests center primary around the following:

Technology: To include emerging technology ethics, strategy and policy; as well as national security related technology strategy and policy.

Women Issues: To include the promotion, advocacy and awareness for practical women's work wear; and the promotion of my functional suits as a means to encourage change.

Health & Wellness: Contribute to greater awareness on health and wellness among my friends and family and others; as well as myself.

Art: I am passionate about using art as a medium to raise awareness about disruptive technologies that affect humanity, and leverage art to create a more inclusive civic debate. Learn more about her at: https://www.linkedin.com/in/lydiak/

Keenan Skelly, VP Global Partnerships & Security Evangelist at Circadence

Experienced Vice President with a demonstrated history of working in the computer and network security industry. Skilled in Crisis Management, Intelligence Analysis, Government, Law Enforcement, and Emergency Management. Strong operations professional with a M.P.S. (Master of Professional Studies) focused in Cybersecurity Strategy and Information Management from The George Washington University.

Learn more about her at: https://www.linkedin.com/in/keenan-skelly-

Lisa Jiggetts MBA, CISSP, Founder & President, Women's Society of Cyberjutsu

She founded, in 2012, the Women's Society of Cyberjutsu (WSC) as a National 501(c)3 non-profit community, focused on empowering women to succeed in the cybersecurity industry. WSC's mission is to advance women in cybersecurity careers by providing programs and partnerships that promote hands-on training, networking, education, mentoring, resource-sharing and other professional opportunities.

For more information, please visit http://www.womenscyberjutsu.org and learn more about Lisa at: https://www.linkedin.com/in/wsccyberjin/

Dervla Mannion, Vice President Sales Operations at Trend Micro

Dervla is a infosec leader with a long-term pan-European track record of achieving sales and business success. She is a member of Trend Micro EMEA's Management Council. Board Member of IT@ Cork, European Technology Cluster.

Experience within a wide variety of management & leadership roles; and have a broad perspective on the integration of markets, trends, competitors and customers to deliver big results. Enjoy making sophisticated and complex things happen - translating this to meaningful plans for broader teams. Flourish driving operational transformation – within sales and non-sales environments. Persuasive, motivated, versatile, detailed and curious.

Learn more about her at: https://www.linkedin.com/in/dervlamannion/

Masha Sedova, Co-founder Elevate Security

Masha Sedova is an industry-recognized people-security expert, speaker and trainer focused on engaging people to be key elements of secure organizations. She is the co-founder of Elevate Security, an innovative new approach to security awareness. Elevate's Security Behavior Platform delivers highly scalable personalized engagement, meaningful measurement, and practical feedback to motivate, reward and reinforce smart security behaviors of employees. Before Elevate, Masha Sedova was a security executive at Salesforce where she built and led the security engagement team focused on improving the security mindset of employees, partners, and customers.vThe scope of her work ran the gamut from general awareness such as phishing and reporting activity to secure engineering practices by developers and engineers. In addition, Masha is a member of the Board of Directors for the National Cyber Security Alliance and a regular presenter at conferences such as Blackhat, RSA, ISSA, Enigma, and SANS. Learn more about her at: https://www.linkedin.com/in/msedova/

Michelle Nguyen, Director of Enterprise Sales, Remediant

Accomplished cybersecurity sales executive offering rare combination of experience in selling software and services to CISOs at Fortune 50 companies, with firsthand experience in raising capital, creating, building, and exiting a startup business.

Women in Tech and Girls in Stem advocate.

Learn more about her at: https://www.linkedin.com/in/nguyenwin/

Meerah Rajavel, CIO, Forcepoint

As an experienced executive, I excel at promoting transformation, innovation, profitability and agility for business through technology. I am a passionate leader who inspires and motivates team to achieve extraordinary business outcome through entrepreneurial thinking and collaborative cross-functional partnerships. Specialties: Change Agent, Innovation/ Intrapreneurship, Cloud computing, SaaS, business intelligence, Communication & Collaboration, User Experience, ERP, CRM, Product Engineering/R&D, New Business Model/GTM, supply chain, sales & channel experience, co-innovation / strategic partnership with COTS providers, unique ability to understand the business and apply elegant technology solutions which deliver substantial value.Currently, as CIO of Forcepoint, I lead the digital and operational transformation with focus on customer centricity, scale for rapid growth and operational efficiency while minimizing risk. Learn more about her at: https://www.linkedin.com/in/meerah-rajavel/

Sigalit Shavit, CIO, CyberArk

Sigalit Shavit is Chief Information Technology Officer at CyberArk. She is responsible for providing and managing the information technology and security infrastructure that enables CyberArk's business objectives. Shavit brings more than 26 years of executive and IT inter-disciplinary experience to CyberArk – demonstrating an innate ability to tightly align the technology roadmaps of IT organizations with business objectives. Prior to joining CyberArk, Shavit served as Global CIO and Head of DevOps at ECI Telecom Ltd. Previously, she served as VP and CIO of FedEx, Israel. Shavit has also held several senior IT positions at various technology companies where IT constituted an integral part of the business value chain and production systems. Shavit holds a B.Sc. in Industrial Engineering and Information Systems from the Technion – Israel Institute of Technology.

Learn more about her at: https://www.linkedin.com/in/sigalit-shavit-499ab61/

"There's something to be said about Women's intuition when it comes to cybersecurity. We're proud to share the Top 25 Women in Cybersecurity who use their unique talents, skills and intuition to take cyber defense to new heights," said Gary S. Miliefsky, Globally Recognized Cyber Security Expert and Publisher of Cyber Defense Magazine.

http://cyberdefenseawards.com/top-25-women-in-cybersecurity/

Christine de Souza, Cyberspace Operations Strategist at SOSi

Experienced professional in the information assurance and cyber security industry. Experience includes involvement with cyberspace operations and information assurance, as well as activities relating to defending the national cyber security posture, meeting security requirements, and assisting in government compliance through validation of security controls and vulnerability assessments. CSFI Presentations include the following: Speaker for the Cyber Pavilion run by the Military Cyber Professionals Association (MCPA) at the Association of the United States Army (AUSA) 2017 Conference (October 2017) - Washington, D.C. Topic: Cyberspace Operations and the Cyber Mission Force.

Learn more about her at: https://www.linkedin.com/in/christinecsfi/

Ellen Sundra, CISSP, Vice President of Americas, Systems Engineering at ForeScout Technologies Inc.

With more than 20 years of experience in the cybersecurity industry, Ellen leads the Americas System Engineering team for Forescout Technologies. Together, Ellen and her team are responsible for designing customized security solutions for Commercial and Public Sector customers. Prior to joining Forescout, Ellen was a network architect and security advisor with iPass, UUNet and WorldCom. Ellen earned a Bachelor of Arts in computer science from Rollins College and is a Certified Information Systems Security Professional (CISSP).Learn more about her at: https://www.linkedin.com/in/esundra/ and watch our CyberDefenseTV interview with her at: http://cyberdefensetv.com/forescout-unified-device-visibility-and-control-it-and-ot/

Kara Sprague, Executive Vice President and General Manager, Application Services at F5 Networks

I'm a leader in developing and driving growth strategies for innovative high-tech product and service providers. I publish and speak frequently on technology disruptions and IT infrastructure topics. I am a practicing martial artist - a third degree black belt in Taekwondo.

Learn more about her at: https://www.linkedin.com/in/ksprague08/

Debbie Umbach, Vice President of Marketing at BitSight Technologies

B2B Technology Marketing is my passion. With a background in IT consulting, product management and product marketing at companies ranging from 20 employees to 70,000, including category creators Akamai, SAP, RSA, VCE, and now BitSight, I provide unique perspectives along with executive experience. As VP of Marketing at BitSight, I lead a team that has established BitSight as the Leader in Security Ratings, a market our founders created in 2011. I am responsible for the company's global marketing strategy, including corporate communications, demand generation, channel marketing, live events, and product marketing.
Since joining BitSight in 2014 as employee #39, I have worked with the team to grow our customer base more than tenfold to 1,000 customers, including 30% from outside of the US. In 2016, BitSight was selected by Forbes as one of 25 companies on its Next Billion Dollar Startups list.

Learn more about her at: https://www.linkedin.com/in/debbieumbach/

Nicola Whiting, CSO, Titania

Experienced Chief Strategy and Operations Officer. Specialising in enterprise security automation software (self-healing systems), business development, trust based selling and neuromarketing.An Amazon bestselling author, I've written for magazines such as the Huffington Post, Defence Contracts Bulletin, Defence News Online and Signal.I am Neurodiverse (Autistic) and advocate forDiversity in all forms. Awards/Recognition:UK Cyber Awards: UK Cyber Citizen 2018/2019 AFCEA International / SIGNAL Magazine: Sparky Baird Award 2018. Security Serious Unsung Hero Awards:Security Leader & Mentor 2018. SC Magazine: Top 20 most influential women working in cyber security. 2017 & 2018. Learn more about her at: https://www.linkedin.com/in/nicola-whiting-40069b14/ and watch our CyberDefenseTV interview with her at: http://cyberdefensetv.com/titania-find-the-security-gaps-before-the-hackers/

Congratulations


ARTICLES

5 Simple Ways to Keep Your Personal Information Safe Online

Protecting your personal information can help reduce your risk of identity and data theft. Take these necessary safety precautions to avoid being a victim of hackers

By Susan Alexandra, Contributing Writer, None

Connecting to each other is now a need of everyone. From checking emails to communicate with our loved ones, we daily spend hours on the internet; where a major chunk goes to social channels. According to Statista, “the daily social media usage of global internet users amounted to 136 minutes per day, up from 135 daily minutes in the previous year”.

What Hackers can do with my Personal Information?

With the continuous increase in data breaches and data thefts, it’s very important for us to think about our privacy and security. If you are a victim of data theft, your information can be use for different purposes. According to VPNPro, “with just a few details, like your date of birth, social security number, etc., scammers can use your information to take out loans, get credit cards, or use it for more sophisticated phishing attempts”. Not only this! Hackers can collect your private messages, videos and images and send it to others.

5 Tips to Protect Your Personal Information Safe Online

Spending time on the internet and social channels is good for us, as it helps us to get connected with our loved ones. But do we really care about our data privacy? How much time do we spend to keep our personal information safe? The good news is that you can continue using the internet, but in a safer manner, without interfering with your normal online habits. Here are 5 basic ways to help you protect your personal information safe.

1. Regularly update your security

Many people don't update their systems because they think that it is time consuming or they simply don't care about it. If your system is outdated, you can be an easy target of hackers. They can send viruses, trojans and different types of malwares to your device.

With the latest development and method used by hackers, it's very tough for software companies to ensure the privacy of their users. This is the reason we regularly got releases, patches, security updates and fixes.

Keep your system up to date and make sure to use the latest version of every software that is installed in your system. You can also turn on automatic updates so you don't have to think about it. Make it your habit to run regular scan for your system.

2. Set Strong password

People usually set weak passwords that are easy to remember. Many of them, don't even change their passwords for months; even years. As a result, many accounts get compromised due to these easy to guess passwords.

Always use strong password for your system, social and other online accounts including your credit, bank, and others. A complex password must have a combination of letters (mixed case), numbers and special characters. Set unique password for each account and change it once a month.

You can also use a password manager that can store all your passwords in a secure database. The best thing about password manager is, all your saved passwords are encrypted by default to others and that are only visible to those who have login details.

3. Keep Your Browsing Secret

Nothing is free in this world. And if something is free, you are definitely paying for something in return. Free public Wi-Fi network is a good example for this. Pubic networks are convenient, but it doesn't guarantee your security. With few tricks and the right tools, anyone on the same Wi-Fi network could be spy you're browsing activities. That person could be a hacker, data snooper or a data theft.

People use public networks to use their social account, check their emails, or to do online transaction. If you must log in or transact online on public Wi-Fi, it's recommended to use a virtual private network, which encrypts your activity so that others on the same network can't track your activity. Make sure to use a legitimate service that you pay for. Once you get home, keep where you surf a secret by browsing in private or incognito mode.

4. Never click on emails from unknown sources

Email attacks (including Phishing, Spam, Spyware, Adware etc) are on the rise these days. We daily receive suspicious emails that requires personal information or have malicious links. These emails often used to steal user details, including account credentials, credit card numbers or passwords.

An attacker can easily trick users into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. Malicious links include spelling mistakes or changes in the domain names.

To stay safe from such attacks, you need to be extra careful while reading emails and clicking on the external links. Also, do not share your personal details with anyone.

5. Backup your data

In the past few years, we have seen a huge increase in ransomware attacks. Hackers usually encrypt user data and ask to pay ransom to decrypt the files of their system.

One of the best ways to protect your data is to keep your computer backed up. Remember to back up twice a month and set your computer to auto update. You can also use an external hard drive as a way to back up your data. This will provide you an extra layer of security, especially when protected with software that enables you to access your data.

Help avoid compromising your information by taking these simple measures to ensure your personal data is safe from any potential threats. If every individual adopts these steps, the possibility of a cyberattacks can be decreased.

About the Author

Susan Alexandra is an independent contributing author at Security today and Tripwire. She is a small business owner, traveler and investor in cryptocurrencies.

Your Enterprise Network: On-Premise, Cloud-Based, And the Transition In Between

By Jim Souders, Chief Executive Officer, Adaptiva

Companies routinely struggle to quickly, easily, and effectively push critical content and updates to every system within their enterprise.

Endpoint security has always been a challenge for the enterprise. Companies routinely struggle to quickly, easily, and effectively push critical content and updates to every system within their enterprise. Despite all of the advances in endpoint security, software distribution often remains a painful task, particularly as the majority of businesses still rely on a client-server infrastructure to handle the task.

Their on premise solutions come with significant hard costs. To handle the constant barrage of updates and security fixes, organizations place servers everywhere to stage content, which then requires on-site server maintenance. So, in addition to the cost of the servers, they need to pay staff to tend to them and purchase costly amounts of bandwidth and storage.

The proliferation of mobile devices certainly hasn't made things any easier for IT teams. Mobile requires a different way of operating and handling even the most basic security fixes. But, it's a regular part of

business that cannot be ignored. The last thing IT needs is for an employee's mobile device to wreak havoc on the company's network.

This is why the idea of modern endpoint management is so appealing. Enterprises deluged with content and application updates are desperate for a single, unified tool that efficiently controls every endpoint—be it someone's desktop machine, laptop, or mobile device. Companies are beginning to experiment with the idea of moving all of their applications to the cloud to reduce costs and increase the ease of managing and updating endpoints. Unfortunately, the industry is not quite there yet. The general consensus is that the transition of workloads from traditional premise-based client management tools like Microsoft System Center Configuration Manager to full modern cloud-based management solutions will, at best, take years to complete, as this transition is no small undertaking.

Microsoft's co-management solution for Configuration Manager has begun to emerge as a popular transitionary solution to enable companies to begin moving toward the future. Co-management is essentially all about the workload. It enables the different workloads on both machines and devices, handled either by traditional premise-based life cycle management or by a cloud-based modern device management solution, like Microsoft's Intune or VMware's AirWatch, to work simultaneously based upon set policies.

With Microsoft throwing its support behind co-management, enterprises gain some confidence that eventually migrating to full cloud-based environments will become a real possibility. Co-management offers a bridge for the interim, and how a company develops and executes its transition strategy is absolutely critical.

Distribution model is key

When thinking about securing endpoints and properly managing workloads, both now and in future environments, it's important to first consider howcontent and updates are delivered across all endpoints. The reason the delivery mechanism should be a factor is because it underlies every decision a company makes in deploying content and making the necessary subsequent security updates—on premise, in the cloud, or somewhere in between.

Because traditional software distribution models often have the potential to impact network performance and day-to-day business functions, updates and content tend to be pushed at night or over the weekend when they won't have such a negative impact on systems or employees. This leads to short windows of time to get necessary content distributed and prolongs the time frames to get essential software deployed across the whole enterprise. But, just as endpoint management is changing, so is the method of distribution. In an era of very real cyber threats, enterprises can't wait days or weeks for patches and updates to reach every endpoint anymore. They need speed, scale, and the assurance of reliable delivery with every piece of content. This is why peer-to-peer content distribution models have gained such popularity.

Peer-to-peer has evolved profoundly in recent years and has proven to be the best model to assist enterprises in securing every endpoint. Content and updates can be fully automated and immediately, intelligently delivered to every endpoint that requires them as workloads are shifted accordingly. This is

done at scale with no detrimental effect on the network or end-user device. Even when a company begins to move its applications to the cloud, and as co-management becomes more commonly utilised, IT still needs an efficient and cost-effective way to get enterprise-size content to every relevant device and machine.

Enterprises that have already adopted an intelligent peer-to-peer content distribution solution are in prime position to move forward with the transition to modern, less infrastructure-intensive endpoint management.

3 keys for modern management

Regardless of where companies are in the process of migrating to modern management, they should consider embracing and utilizing automated software and content delivery solutions that fulfil three main requirements. Solutions should be:

Platform agnostic: Companies need to seek solutions that leverage technologies that work across the continuum, from traditional PC lifecycle management to cloud-based modern management. The solutions should be capable of delivering content regardless of whether a company uses platforms from Microsoft, VMware, etc. or any combination thereof and without requiring a replacement of existing technologies or adding additional agents to the endpoints.

Cloud-enabled: Content won't come solely from multiple premises-based servers in the future. Enterprises should have the option to completely eliminate costly infrastructure by moving to the cloud or embracing a hybrid approach between cloud and on-premises solutions. A modern management approach should be able to reduce infrastructure requirements to the fewest servers required—if not eliminate them altogether—and work with any cloud provider and content delivery network.

Co-management capable: Any enterprise software delivery mechanism should make it possible to work with a single agent that is intelligent enough to deliver updates and applications from either on-premises or the cloud at the same time. Additionally, any solution should support various device types so that they can function effectively both now and in the future.

With this approach, companies have the flexibility to make the transition from what works for them today to add more cloud and modern management features over time.

While endpoint management in the enterprise is evolving, it's never as fast or easy as teams envision it. Changes that involve security are particularly complex and require painstaking attention to ensure that no vulnerabilities are exposed. Co-management offers a way for companies to transition on their own timetables without compromising security. Enterprises just need to make sure that as they develop modern environments, the delivery mechanism is flexible enough to meet their needs.

About the Author

Jim Souders is CEO of Adaptiva. A global business executive with more than 20 years' experience, Jim excels at leading teams in creating differentiated software solutions, penetrating markets, achieving revenue goals, and P/L management. Prior to Adaptiva, Jim led high-growth organizations from start up to public offering and acquisition in a variety of advanced technologies, including IT infrastructure management, cross-platform mobile application development, WAN/LAN optimization, and wireless supply chain automation systems. For more information, please visit www.adaptiva.com and follow the company on LinkedIn, Facebook, and Twitter.

Is Your Organization Ready For The Windows 10 Migration?

Synopsis: *Organizations should look at the migration to Windows 10 as an opportunity to upgrade their Windows management. But they must also take measures to maintain security against evolving threats.*

By Kevin Alexandra, principal consultant at BeyondTrust

Organizations worldwide are still coming to grips with the migration from Windows 7 to Windows 10. As we draw closer to the January 2020 deadline, Microsoft is committing to a renewed focus on the enterprise and to unify the Windows experience across devices, from the phone in your pocket to the display in the boardroom. The update also addresses pre-breach threat resistance by removing or defending against the attack vectors used by the malware and hacking industry.

Although many are already capitalizing on the transition as a chance to strengthen their overall IT, and better protect endpoints for individual users, others are stalling.

In fact, earlier this year, Microsoft announced that 184 million commercial PCs are still running Windows 7 across the world — and that's excluding the People's Republic of China. But as the deadline for Windows 7 extended support draws to a close in 2020, it's important for IT professionals to prepare and become better informed on the implications of the migration for their business today.

Addressing Modern Security Challenges

Windows 10 is considered the most robust Windows operating system so far; therefore, it's little surprise that countless organizations trust in Microsoft's cloud-based modern management approach to facilitate heightened security and agile IT capabilities.

But mobile device management solutions mean that employees must have administrator rights to do their jobs on a daily basis — a potential security risk. So, while Microsoft is enabling organizations to deploy Windows 10 support and adopt modern management more easily, it's important that businesses understand that the operating system alone is unable to protect businesses from evolving threats.

To protect their organizations, CSOs, CISOs, and other IT security professionals need to think more strategically when migrating to Windows 10.

For example, in a survey of 500 global IT and cybersecurity professionals last year, vulnerable endpoints were the top security concern of migrating from Windows 7 to Windows 10 for 40% of respondents. Meanwhile, for all regions except the United Arab Emirates (UAE), the biggest challenge for securing remote workers and employees that leverage bring your own device (BYOD) on Windows 10 was ensuring that endpoints were secure. UAE respondents were most concerned with malware attacks.

These concerns are not misplaced, with many breaches arising due to employees working remotely and enjoying access to data from their own devices. To help mitigate this threat, CISOs should remove admin rights wherever possible and implement a thorough training program to ensure that employees understand why this is happening, along with the correct steps that must be taken to continually mitigate the threat of exposed endpoints.

Privilege or No Privilege?

There have been two main types of account — administrator and standard user — in every version of Windows to date, and Windows 10 is no exception. But with the knowledge that removing admin rights could mitigate 80% of all critical Microsoft vulnerabilities reported in 2017, the specific security threat that overprivileged admin users pose to their businesses is clear.

Fortunately, the removal of admin privileges from employees is relatively simple on Windows 10. However, although this process does result in improved security, it can present some usability challenges. Because many day-to-day tasks and applications require admin rights, their loss can hamper a workforce's efficiency in carrying out their responsibilities.

This is a conundrum for businesses, which must aim for maximum security but also avoid locking too many users out of the systems they need. IT and security leaders must weigh this balancing act on a

case-by-case basis and, if they do remove admin rights, ask which of their existing practices should be tweaked to avoid the challenges associated with them.

Optimizing the User Experience

Although Microsoft rolls out updates to its operating system twice yearly, its modern management still doesn't allow for a distributed set of employees to install key applications in a secure, user-friendly way. For example, when admin rights are taken away, IT staff can have difficulties in accessing the network and helping users to install software — ultimately detracting from the overall user experience.

But IT leaders should note that the transition to Windows 10 doesn't need to be a sprint. For example, by evaluating which devices require an upgrade, they can use previous operating systems for some areas of the business while simultaneously implementing Windows 10 for others. This will enable organizations to benefit from the security in Windows 7, for example, while also benefiting from the flexibility of newer systems.

Summary

The migration to Windows 10 is an opportunity for organizations worldwide to upgrade their Windows management. But it's vital that the flexibility that the new operating system offers is balanced with measures to maintain an organization's security against evolving threats.

According to the same research I cited earlier, more than half of the respondents believe their organization is ready for the Windows 10 migration, however, the other 44% are unsure about preparation plans or do not feel prepared. With just about six months to go for Windows 7 end of life, organizations must take proactive steps now. By thinking carefully about the points outlined in this article, IT leaders can plan a smooth transition to Windows 10.

About the author

Kevin Alexandra is an experienced Technical Consultant who has been working in the IT industry since he was 13. Kevin combines his passions of technology, learning and sharing to help BeyondTrust customers globally navigate the ever-changing space so they can make informed, logical business decisions in what is a very crowded and complex market.

Bitglass 2019 Cloud Security Report: Only 20 Percent of Organizations Use Cloud Data Loss Prevention Despite Storing Sensitive Information in The Cloud

67 Percent of Organizations Believe Cloud Apps Are as Secure as or More Secure Than On-Premises Apps

CAMPBELL, CA – July 17, 2019 – Bitglass, the Next-Gen CASB company, has just released Guardians of the Cloud, its 2019 Cloud Security Report. As organizations migrate more of their data and operations to the cloud, they must maintain a robust cybersecurity posture. To uncover how well they are accomplishing this, Bitglass partnered with a leading cybersecurity community and surveyed IT professionals about cloud security in their organizations.

Each year, Bitglass conducts research on the state of enterprise cloud security in order to identify key trends and common vulnerabilities. This year's report found that 75 percent of organizations leverage multiple cloud solutions, but only 20 percent have visibility over cross-app anomalous behavior. With more and more organizations storing sensitive information in the cloud – information like customer data (45 percent), employee data (42 percent) and intellectual property (24 percent) – adopting proper cloud security measures is critical.

Key findings:

- Despite a change in their order, the top priorities from 2018 remained top priorities in 2019; this year, the top three were defending against malware, reaching regulatory compliance and securing major apps in use.
- The use of CASBs for malware protection has increased from 20 percent in 2018 to 31 percent in 2019.
- Access control (52 percent) and anti-malware (46 percent) are the most-used cloud security capabilities. However, these and others – like single sign-on (26 percent) and data loss prevention (20 percent) – are still not deployed often enough.
- Malware has emerged as the most concerning data leakage vector, with 27 percent of respondents citing it as the number one concern for their organization. Conversely, concern about leakage through unsanctioned cloud apps fell from 12 percent in 2018 to 5 percent in 2019, showing that organizations are becoming aware that there are threats greater than shadow IT.
- Cost is the leading concern for organizations evaluating cloud security providers. Other critical concerns include ease of deployment (46 percent), whether the solution is cloud native (45 percent), the ease with which cross-cloud security policies can be enforced (36 percent) and the solution's ability to integrate with various cloud platforms (36 percent).

"Data is now being stored in more cloud apps and accessed by more devices than ever before," said Rich Campagna, chief marketing officer of Bitglass. "This report found that 93 percent of respondents are at least moderately concerned about their ability to use the cloud securely, and that the adoption rates of

basic cloud security tools and practices are still far too low. Many organizations need to rethink their approach to protecting data, as traditional tools for safeguarding data on premises are not capable of protecting data in the cloud."

To learn more about how cloud security has shifted over the past year, download the full report here: https://pages.bitglass.com/CD-FY19Q2-Guardians-of-the-cloud-report_LP.html?&utm_source=pr

About Bitglass

Bitglass, the Next-Gen CASB Company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.

U.S. Press Contact

Emily Ashley

10Fold for Bitglass

(916) 710-0950

bitglass@10fold.com

EMEA Press Contact

Lesley Booth

Touchdown for Bitglass

lbooth@touchdownpr.com


bitglass
GUARDIANS OF THE CLOUD
2019 CLOUD SECURITY REPORT

As organizations migrate more and more of their data and operations to the cloud, they must ensure that they maintain a robust cybersecurity posture. However, frequent breaches in the news seem to suggest that many companies are not prioritizing security to the degree that they should. To uncover the state of enterprise security in the cloud, Bitglass partnered with a leading cybersecurity community and surveyed IT professionals.

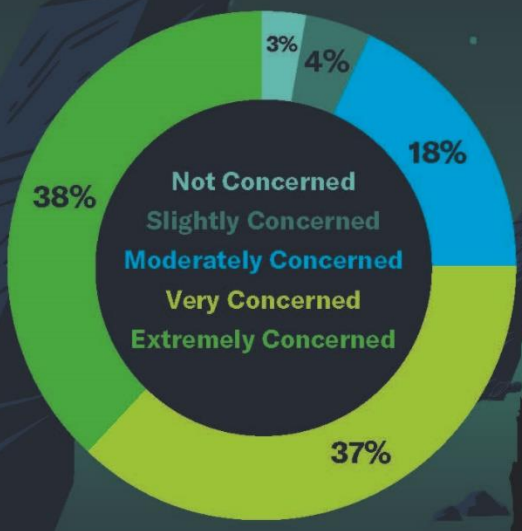
AWESOME MIX 2019

Organizations' leading cloud priorities have shifted over the past year. While defending against malware has ascended to the top spot, discovering unmanaged apps in use has fallen to number six. Despite a change in their order, the top three priorities from 2018 are each still in the top three in 2019. Finally, it is concerning that securing mobile devices isn't a higher priority in light of recent Bitglass research which found that **85%** of companies now enable bring your own device (BYOD).

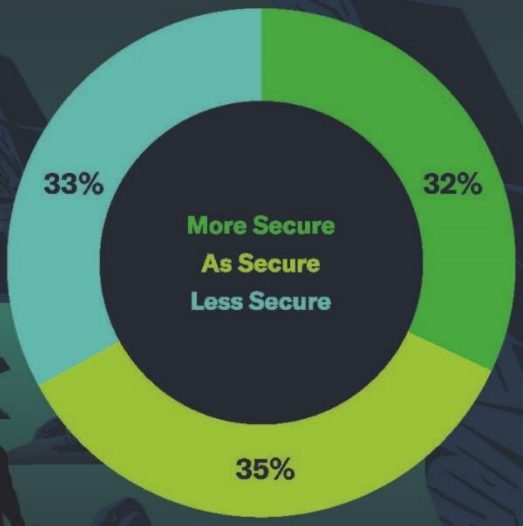
SECURITY IN THE SKIES

67% of respondents believe cloud apps are as secure or more secure than on-premises apps—this is significantly higher than the **40%** recorded in 2015. Despite this, **93%** of respondents are at least moderately concerned about the security of the cloud. In other words, organizations know the cloud itself is highly safe, but are wrestling with their responsibility to use it securely.

How concerned are you about the security of the cloud:



When compared to on-prem apps, public cloud apps are:



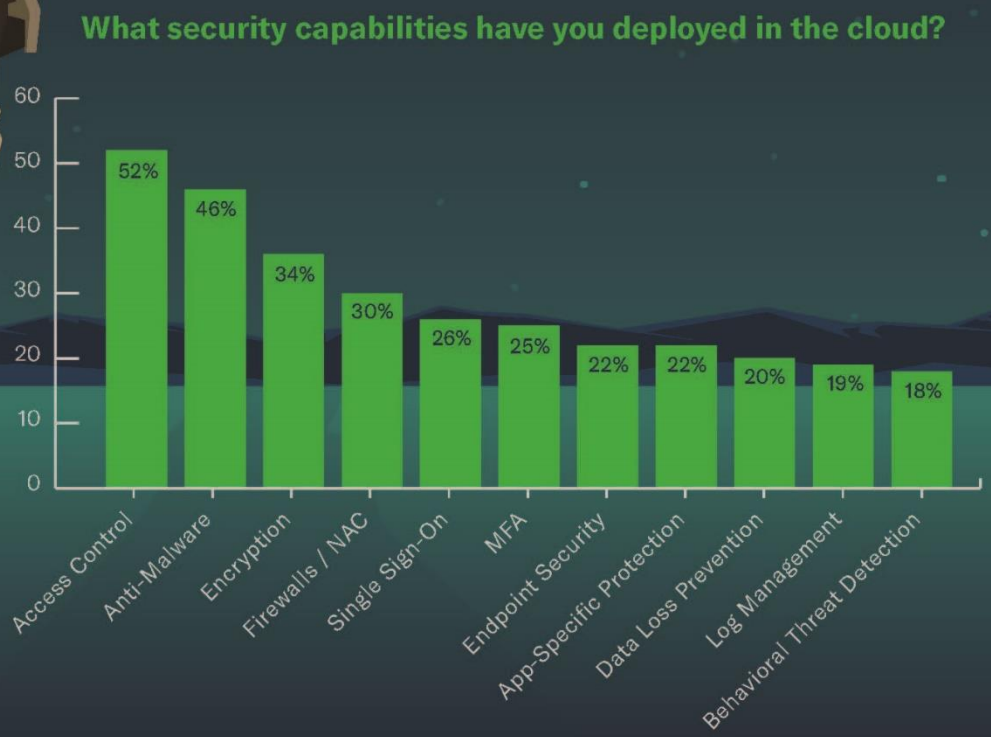
A GALAXY IN NEED OF SAVING

Organizations are moving workloads and data into the cloud, granting them greater productivity and flexibility, but increasing the likelihood of data leakage where proper security is not employed. As **45%** of respondents store customer data in the cloud, **42%** store employee data in the cloud, and **24%** store intellectual property in the cloud, adopting the appropriate security measures is clearly critical.

What type of corporate data do you store in the cloud?

WEAPONS SYSTEMS

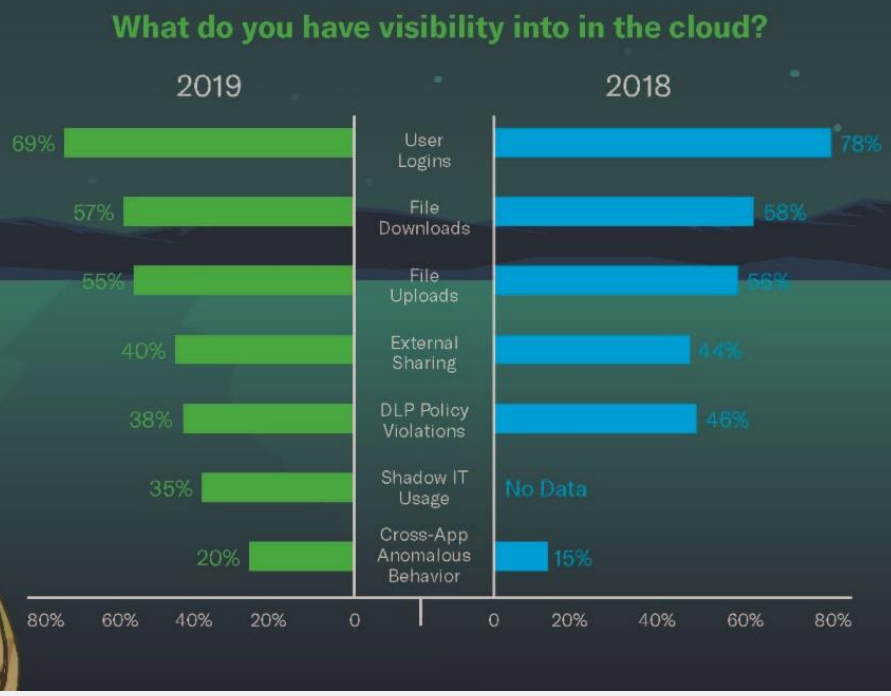
Access control (**52%**) and anti-malware (**46%**) are the most-used cloud security capabilities. However, these and others—like single sign-on (**26%**) and data loss prevention (**20%**)—are still not deployed often enough. Additionally, as **66%** of respondents said that traditional security tools don't work or have limited functionality in the cloud, adopting appropriate cloud security solutions becomes even more critical. Fortunately, cloud access security brokers (CASBs) can provide many of these essential capabilities.



KNOWHERE YOUR DATA IS GOING

Despite a slight increase since last year, a mere **20%** of organizations have visibility over cross-app anomalous behavior. This is a critical requirement as only **25%** of survey respondents are "single cloud" today. Unfortunately, corporate visibility over every other category decreased since 2018. This may be due to the growing number of cloud apps and personal devices over which IT struggles to gain visibility.

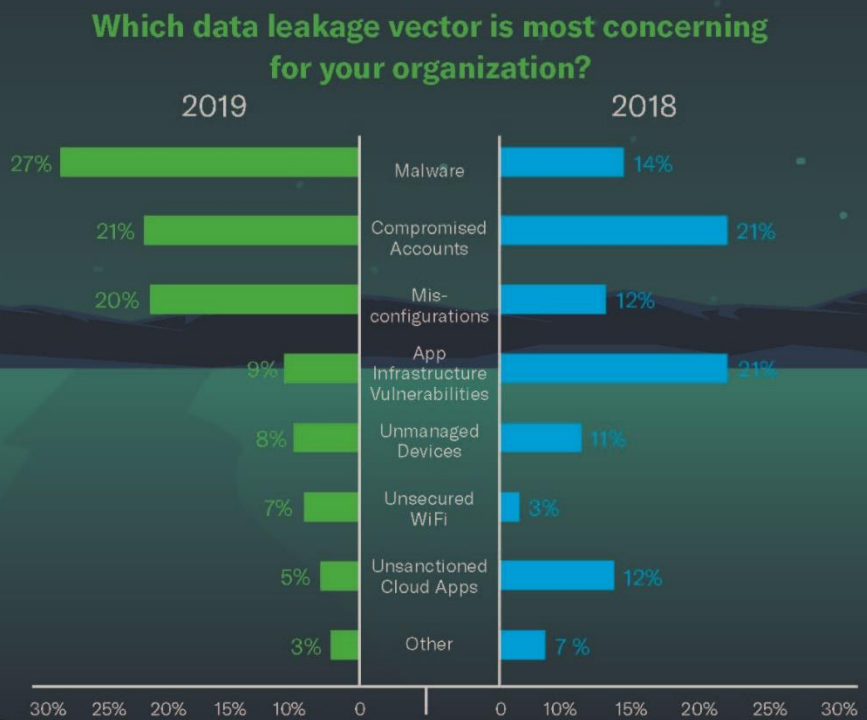
While the high percentage of organizations that have visibility into user logins (**69%**) suggests that the first step of cloud security (identity management) has been taken, many organizations still lack visibility and control over what happens after authentication.



HOLES IN THE HULL

Since 2018, malware has emerged as the most concerning data leakage vector; it was selected by **27%** of respondents. Conversely, unsanctioned cloud apps falling from **12%** to **5%** shows that organizations are becoming aware that there are data leakage threats greater than shadow IT.

Concerns about app infrastructure fell from **21%** in 2018 to **9%** in 2019. At the same time, misconfigurations ascended from the middle of the pack (**12%**) to third place (**20%**). These stats highlight the growing awareness that the cloud itself is highly secure, but that organizations must use it in a safe fashion.

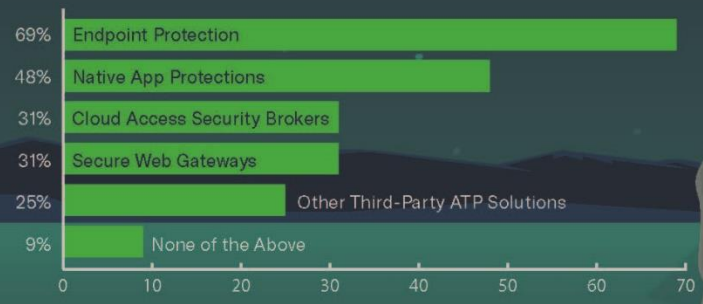


DEFENSES AT THE READY

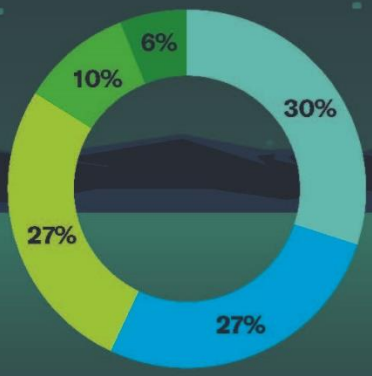
Successfully defending against malware requires organizations to utilize a three-pronged strategy that encompasses devices (endpoint protection), the corporate network (secure web gateways), and the cloud. While a few cloud apps provide some built-in malware protections, most do not. As such, a combination of tools is necessary. Fortunately the use of CASBs for malware protection has increased from **20%** in 2018 to **31%** today.

The use of agents to secure personal devices (which violates employee privacy and creates deployment challenges), decreased from **38%** in 2018 to **30%** in 2019. Blocking personal device access to corporate data (which hinders employee efficiency and flexibility), increased from **21%** to **27%**.

What anti-malware tools does your firm use to secure cloud data?



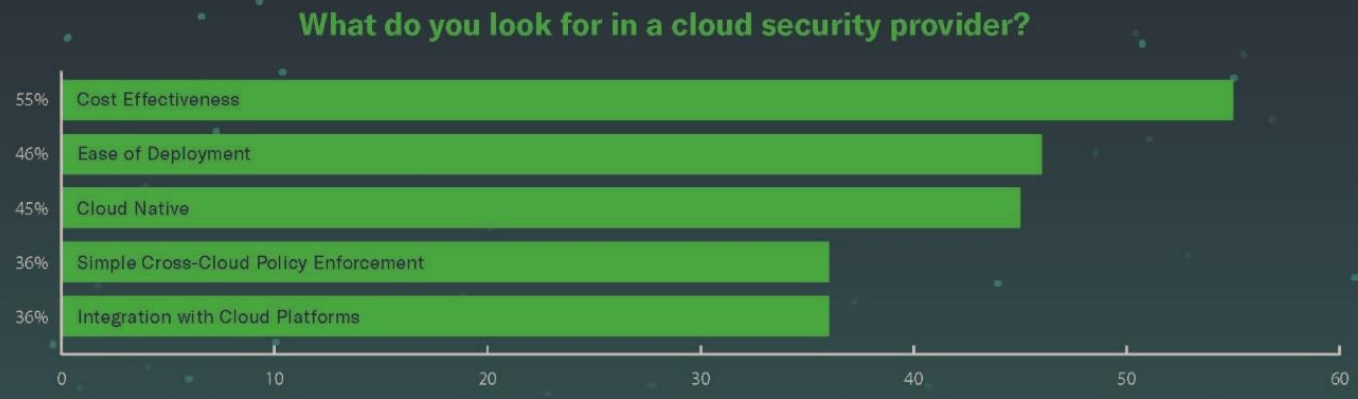
How does your firm secure corporate cloud data on personal devices?

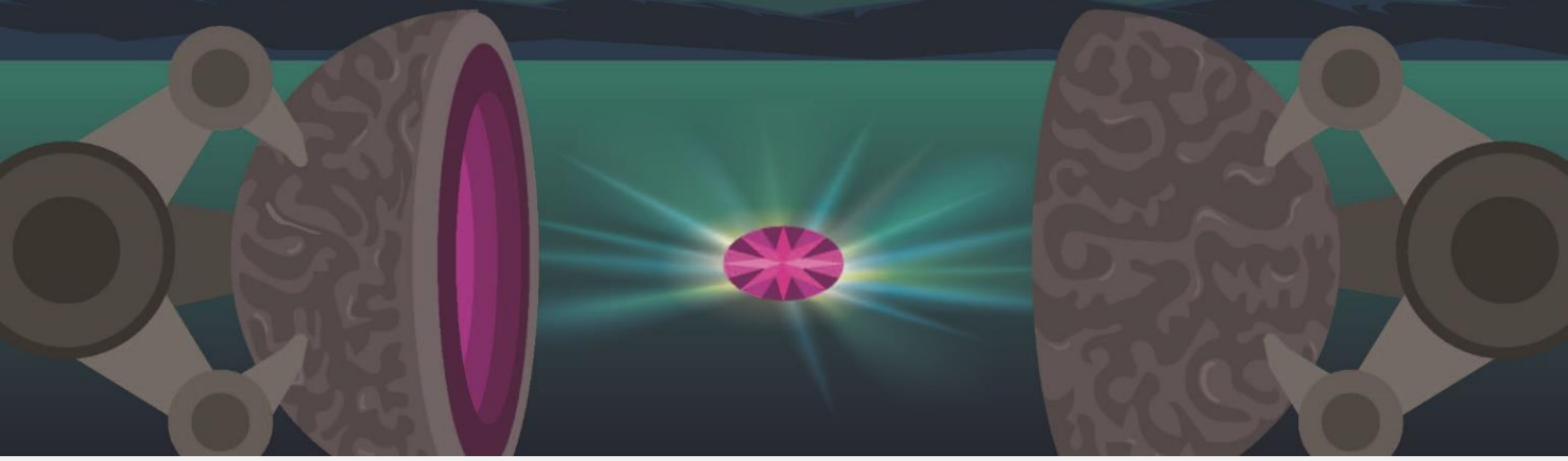


Agent-Based Tools Like MDM
Block Personal Device Access to Data
Use a Trusted Devices Model
Grant Access to Any Device
Apply DLP at Upload or Download

TOOLS FOR SAVING THE GALAXY

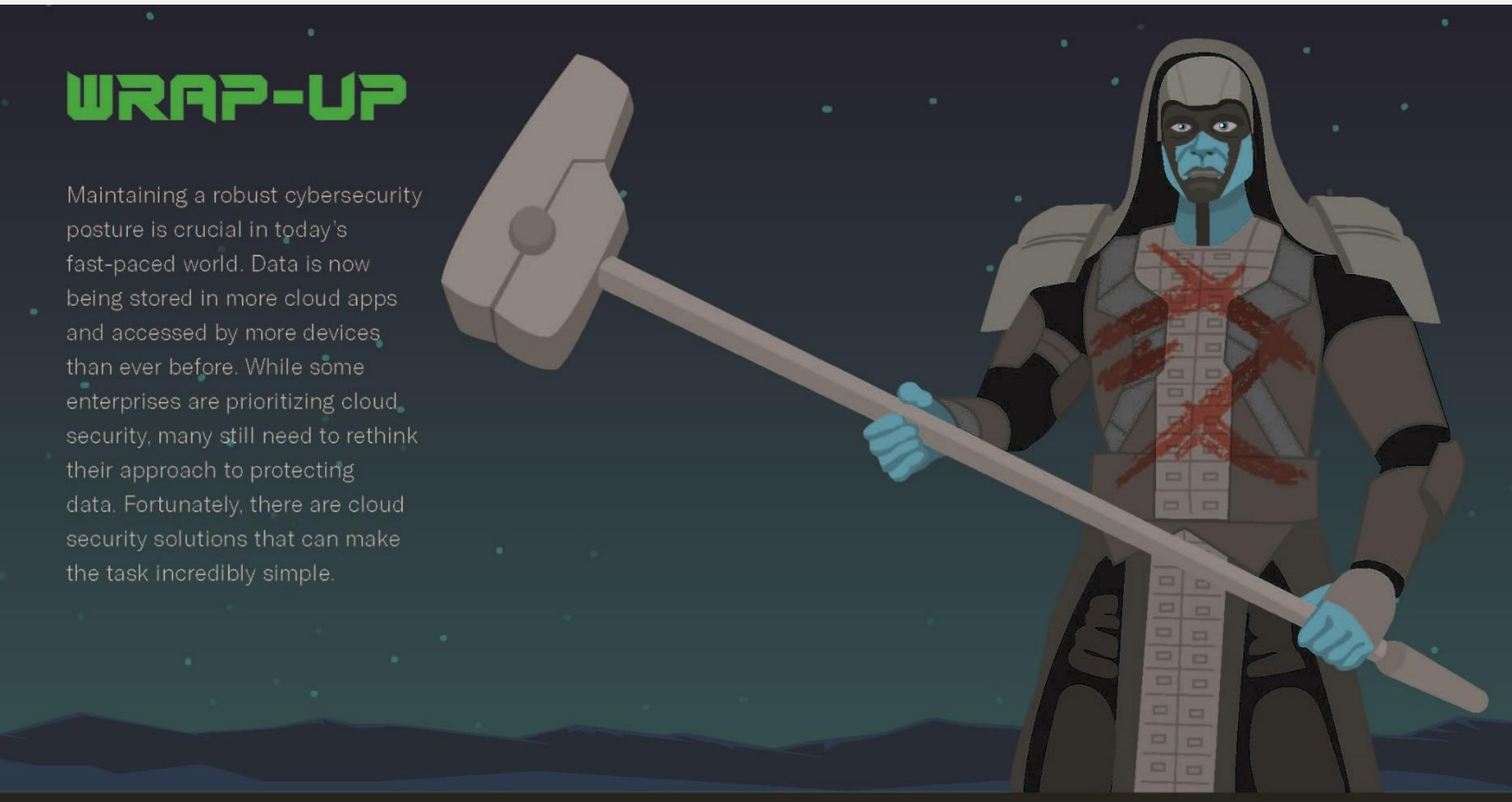
Interestingly, cost is the leading concern for organizations evaluating cloud security providers. Other critical concerns include ease of deployment (**46%**), whether the solution is cloud native (**45%**), the ease with which cross-cloud security policies can be enforced (**36%**), and the solution's ability to integrate with various cloud platforms (**36%**).





WRAP-UP

Maintaining a robust cybersecurity posture is crucial in today's fast-paced world. Data is now being stored in more cloud apps and accessed by more devices than ever before. While some enterprises are prioritizing cloud security, many still need to rethink their approach to protecting data. Fortunately, there are cloud security solutions that can make the task incredibly simple.



bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

ABOUT BITGLASS

Bitglass, the Next-Gen CASB company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.

Security by Design for Mobile Apps

With enterprise becoming increasingly reliant on mobile apps for many of its everyday business communications, processing sensitive data through these apps could pose a significant risk to data security. There is a requirement to provide app developers with standards that will achieve security by design.

By Elisabetta Zaccaria, Chairman Secure Chorus

With the amount of digital information being transmitted via mobile apps rising at a dramatic rate, protecting this information from falling into the hands of cybercriminals has become a significant challenge.

With mobile apps, the data exposure risk stems mainly from the variety of data and sensors held in mobile devices, the use of different types of identifiers and extended possibility of users' tracking the complex mobile app ecosystem and limitations of app developers, as well as the extended use of third-party software and services.

These risks mean that when it comes to the implementation of core data protection principles in mobile apps – as stipulated by the EU General Data Protection Regulation (GDPR) – there are serious challenges. The application ecosystem complexity, including app developers, app providers as well as other actors in the ecosystem (operating system providers, device manufacturers, market operators, ad libraries, and so on) is the main factor that hinders mobile app developers and providers compliance with the GDPR, e.g. the requirement to implement data protection by design and by default, during data processing.

The intricacy of the jurisdictional applicability of the GDPR doesn't make it any easier. This Regulation applies to the processing of personal data by a controller or processor established in the EU, regardless of whether the processing takes place in the EU or not. It also applies to the processing of personal data of 'data subjects' based in the EU by a controller or processor not established in the EU, where the processing activities are related to: the offering of goods or services, irrespective of whether a payment from the data subject is required, to such data subjects in the EU; or the monitoring of their behaviour as far as their behaviour takes place within the EU. The GDPR finally applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

The compliance of mobile apps with the GDPR may therefore not be a concern limited to EU enterprises, but to a much wider pool of organisations falling in the above jurisdictional applicability. To resolve these challenges, there is now a need for greater industry-wide cooperation on the development of standards to make mobile apps secure by design.

Technology standards are published documents that establish specifications and procedures in the areas of product reliability, safety, security and interoperability (in order to achieve compatibility with other technology products). Because of their widespread availability and applicability, they have the further benefit of fostering innovation, often simplifying the product development process.

The reason mobile apps need to be secure by design is because the requirement to prevent (and in some cases provide) access to sensitive communication is deeply inscribed in modern legislation, which aims to protect a variety of interests, ranging from the basic civil liberties of an individual at one end of the spectrum, to the protection of the security of a nation against criminal activities at the other.

This is due to the fact that, while they have many legitimate purposes, secure communications may also be used in the commission of criminal activities. It follows that law enforcement services need tools to investigate cybercrimes as well as other cyber-facilitated forms of crime.

Rights of the individual need to be evaluated in relation to the rights of others to find a balance between the individual interests and the greater interest of all citizens of a nation. In the case of serious crimes, law enforcement may need to lawfully gain access to relevant communications.

The EU General Data Protection Regulation (GDPR) has made efforts to reconcile the individual's right with other relevant rights. On the one hand, the regulation requires businesses to protect personal data during any of its data processing activities (introducing end-to-end encryption as a viable method to achieve such protection), while on the other, it requires businesses to be able access personal data that may be encrypted, in order to comply with lawful interception as well as 'Data Subject Access Requests'. Specifically, Article 15 of the EU GDPR provides that EU citizens (the 'data subject') have the right to receive confirmation that an organisation is processing their personal data, as well as the right to receive a copy of that data. Individuals also have the right to obtain a variety of supplementary information.

Encryption is a cryptographic method in which data is turned into an encoded and unintelligible version, using encryption algorithms and an encryption key. A decryption key or code enables others to decode it again.

The technical challenge introduced by the GDPR is made clear when we examine the mobile applications (apps) we use in our day-to-day business communication. Many of these come with end-to-end encryption. But, most of these applications are built in such a way that businesses cannot decrypt the data being processed by such technologies. This data may include personal data and therefore in case of a 'Data Subject Access Request' places a requirement on the business to decrypt such data and provide it to the EU citizen in question.

Security gaps created by non-compatible technologies connecting to mobile apps create major information security challenges. These gaps present an increasing requirement for mobile apps to be interoperable and secure by design in order to ensure secure data processing between apps and other technologies they may exchange data with (or otherwise process data).

Secure Chorus is a not-for-profit membership organization in the field of information security, working with mobile app developers, as well as other secure communications technology providers, to address secure data processing. We have addressed this cybersecurity requirement through a strategy of government-industry collaboration, with industry members developing a number of mobile apps based on common technology standards to ensure that the app architecture facilitates the exercise of data subject rights under the GDPR.

Secure Chorus supports MIKEY-SAKKE an open identity-based public key cryptography, which provides for end-to-end encryption and can be used in a variety of environments, both at rest (e.g. storage) and in transmission (e.g. network systems). Designed to be centrally managed, it gives enterprises full control of system security as well as the ability to comply with any auditing requirements, through a managed and logged process.

MIKEY-SAKKE has been standardised by the Internet Engineering Task Force (IETF). Access to this type of globally accepted, strong and reliable cryptography has become vital to app developers that are becoming increasingly aware of the widespread risks associated with internet use.

MIKEY-SAKKE is configured so that each user is attached to a Key Management Server (KMS), where the keys are issued to users by an infrastructure managed by the business' IT department. This ensures that the ability to decrypt content remains private to the individuals communicating. However, in exceptional cases such as a 'Subject Access Request', it also allows the business to derive a valid decryption key from the Key Management Server. To audit an encrypted communication, the organisation should export a user-specific and time-bound key from the KMS. This key enables an audit function to decrypt a specific user's communications for a specific time period (e.g. week or month). The KMS is able to log this action to ensure that it is accountable.

All Secure Chorus member technologies use MIKEY-SAKKE. This has enabled Secure Chorus to define with its members a range of interoperability standards that ensure members' products can work with one another and the systems implementing these technologies. The adoption of MIKEY-SAKKE and of Secure Chorus' interoperability standards by app developers, help them to develop products which meet the GDPR compliance requirements of enterprise customers.

Mobile apps built with such standards would allow enterprise customers to maintain data encrypted during any data processing undertaken by the app, as well as by other technologies the app may be connected to. In addition, the enterprise costumer would be able to decrypt data in case of a lawful interception request or a 'Data Subject Access Request' under the GDPR, by exporting a user-specific and time-bound key from the KMS.

Following two years of collaborative work Secure Chorus, has recently announced the completion of its first set of interoperability standards for encrypted voice calls. The completion of this first set of interoperability standards for encrypted voice calls, specifically aimed at enterprise users has created a much-needed breakthrough, setting a strong step ahead to develop interoperability standards for developers of mobile communication apps.

About the Author

Elisabetta is co-founder and Chairman of Secure Chorus, prior to which she was Group Chief Strategy Officer & Chief Operating Officer of Global Strategies Group, where she set the strategy and co-led the cybersecurity company's explosive growth, turning the start-up into a $600million revenue international information security business in six years.

About Secure Chorus

Secure Chorus is a not-for-profit membership organisation serving as a platform for multi-stakeholder cooperation, for the development of forward-looking strategies, common technology standards and tangible capabilities in the field of information security.
For more information visit www.securechorus.org and follow the company on LinkedIn and Twitter.

For further information please contact:

Secure Chorus Ltd via PRPR
Elisabetta Zaccaria, Chairman
Stephen Brown, Director

PRPR
Peter Rennison
Email: pr@prpr.co.uk
Phone number: +44 (0) 7831 208109

Comprehensive Cyber Security for Digital Era!

Demystifying the requirements and identifying the right solution with necessary ingredients

By Lalit Shinde, Head of Partnerships and Business Dev., Seceon Inc.

In today's digital era, almost all organizations whether large, medium or small are looking for comprehensive cyber security solution that would stop any cyber security attack and protect them from any damage. Most small and medium organizations are relying on trusted managed service providers (MSPs) to recommend and provide these solutions, while most large organization may have in house security experts or trusted managed security service providers (MSSPs) to implement these. These MSPs and MSSPs are looking for the cyber security frameworks including the most popular NIST framework created by US govt. to improve their security posture and deploy the solution(s) that help fulfill this framework.

On a cyber security vendor side, there is also a sudden rush within the last few years to create a one-stop solution that caters to comprehensive cyber security so that they can be preferred vendor of choice with managed security service providers and with large enterprises. Most next-gen firewall and anti-virus companies are buying other innovative products to fill the gaps and create this one stop solution, also

called ‘Defense in Depth’ product lines. However, ‘Defense in Depth’ approach is flawed and usually leads to much higher cost without solving the fundamental requirements of comprehensive cyber security.

So, what is the primary goal of “Comprehensive Cyber Security for Digital Era”? It’s a) to protect the organization from all known and unknown cyber-attacks and b) if an attack happens, to proactively detect it at an early stage and contain or eliminate the attack to minimize the damage. In short “Stop the Data Breach from causing any damage to the organization” – whether that damage is legal, financial, competitive, and/or nation-state based.

Let us look at what are the basic requirements of “Comprehensive Cyber Security”. The key requirements start with comprehensive visibility – if you can’t see the assets, the users, the traffic, and the vulnerabilities; you can’t protect the organization from attacks originating from them. Basic Security hygiene is important from protection from most common and known attacks perspective, but it’s not sufficient. Proactive detection based on behavioral science to detect anomalies has become the need of the hour. However, most machine learning and behavioral science-based solutions produce lot of false positives and create an alert fatigue. It’s very important to also have advance correlation engine, which correlates historical situational context along with machine learning anomalies to reduce the false positives and accurately find the real attacks rather than getting bogged down by least important issues. Once the attack is detected, the solution should also provide automated real-time response built in. The organization cannot rely on human intervention by Security Operations Center (SOC) analyst to analyze it before responding. The solution should respond automatically and stop the threat. The SOC analyst can analyze it and adjust later, but the attack needs to be stopped immediately in an automated manner. Furthermore, this solution and framework has to be continuously adjusted and adapted to changing posture of the organization in digital era where more content and applications are moving to the cloud and employees are preferring to work from anywhere, using any smart device to access the organization’s data which has to be omnipresent.

However, the ‘Defense in Depth’ model that most cyber security vendors are building through acquisitions of various silo products is not addressing the requirements of the ‘Comprehensive Cyber Security’. It’s making the overall solution very costly because of the multitudes of silo products required to achieve it and the increased complexity to manage them. Moreover, it seldom actually achieves the stated primary goal, ‘To stop the data breaches’ at any cost.

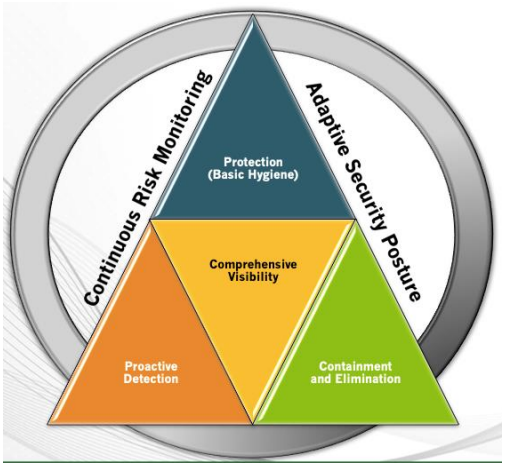


Figure 1: Requirements of Comprehensive Cyber Security

So, let us look at what a ‘Comprehensive Cyber Security’ solution should have. First and foremost you need a fast-big-data streaming platform. But don’t confuse this with handling of large data-lakes. There is a lot of confusion, most vendors when they talk about fast big data, they think that it’s storing, ingesting and analyzing the petabytes of data using data-lake. This is a flawed strategy. You don’t want results after few hours or days. You want them in real-time, so you need fast big data streaming platform that produces results in real-time within seconds.

Figure 2: Comprehensive Cyber Security Solution Ingredients

Ingesting data from variety of data sources is a key to both from comprehensive visibility perspective and also from changing organization landscape as well. More and more organizations are adopting cloud and mobile world with smart devices. With changing landscape, the solution mandates Dynamic Threat Models (DTM), which automatically adapt to the change. Having inbuilt DTM engine is far better than relying on security analysts to write the correct set of rules and then keep on fine-tuning it to capture sophisticated attacks. Such a method is clearly error prone and handles the attacks after the fact. Some customization is important, but most of the attacks related threat models have to be in built into the solution.

Machine learning (ML) and Artificial Intelligence (AI) based behavioral science has a critical role to play in finding all sorts of anomalies in application, devices and users behavior, but it could lead to massive alert fatigue. Most Security Information and Event Management (SIEM) solutions have tried to retrofit ML algorithms into existing platforms and this strategy definitely leads to alert fatigue for the end user. That's why an advanced correlation engine that correlates the anomalies with situational context and historical context is important to reduce the false positives and eliminate alert fatigue. Also any built-in threat models and ML/AI based engines need to adapt itself dynamically to changing organization posture with dynamic thresholds and changing global threat intelligence with dynamic periodic feed. Finally, the solution should not only proactively detect but also contain or eliminate the attacks by providing actionable intelligence and automated infrastructure to orchestrate and apply right set of policies.

Overall the comprehensive cyber security for digital era requires a platform that is built grounds up with the key ingredients required to protect any size organizations. Organizations and service providers must evaluate the vendors against these principle ingredients and requirements before they put their money on it.

About the Author

Lalit Shinde, Head of Partnerships and Business Development, Seceon Inc. Lalit currently leads the strategic sales partnerships and business development for Seceon. He is an Industry Leader with over 24 years of expertise in Strategy, Product Management. Product Development and Business Development. He has a great track record of identifying market opportunities, developing breakthrough products and driving market share from product introduction to significant revenue. Before joining Seceon, Lalit was in leadership position with Juniper Networks in Strategy Planning, Product Management and Product Development roles. His technology expertise includes Network Security, Automation, Control and Data plane APIs, Network Orchestration and Controllers, SDN/NFV, Broadband and Business Edge Services, Routing, Switching and Security Products and Technologies. At Juniper, Lalit got the BNG router introduced into major Tier1 SPs in Europe, Americas and APAC region, developed product strategy with customer focus and won several multi-million $ deals. As an Engineering Manager, he also managed and developed the BNG team globally from scratch. Prior to Juniper, Lalit has worked with Cadence Design Systems and Texas Instruments as Lead architect in developing industry recognized award winning products. He received his MBA from NYU Stern School of Business. He also has MS in Computer Science from IISc, Bangalore and BS in Electronics and Telecommunications from VJTI, Mumbai. Lalit can be reached online at lalit.shinde@seceon.com and at our company website www.seceon.com.

GDPR

One Year On

By Robin Bingeman, Managing Director, Cryoserver

On May 25th 2018, the EU rolled out a new set of data privacy laws under the General Data Protection Regulation - more commonly known by the acronym of GDPR. The aim of GDPR was to set a standardised level of data protection for individuals across the EU. The negotiations for this new legislation took more than four years, with regulations concerned with how businesses should handle, store and protect consumer data.

Regardless of Brexit, the ICO (Information Commissioner's Office) and UK Government have stated that the UK will still have to comply with GDPR. In fact, any overseas businesses dealing with consumers and other businesses in the EU27 must be GDPR compliant.

In the lead up to the GDPR deadline, the ICO called for GDPR compliance rather than enforcement, but news headlines focused on the eye-watering fines - enough to scare any business into getting themselves in line with the regulations.

For companies in breach or found to be non-compliant, there are two tiers of administrative discretionary penalties that can be levied:

€10 million or 2% annual global turnover – whichever is higher; or

€20 million, or 4% annual global turnover – whichever is higher.

It is important to note that fines are imposed on a case-by-case basis. Now that we're a year on from GDPR being rolled out, it's time to look back and reflect on its impact.

What Have We Learnt One Year on From GDPR?

GDPR has reshaped the rules of data management and marketing, making the data and email compliance landscape much more complex. From collecting personal data via cookies so that information can be used for marketing purposes, to storing personal data, explicit consent must be given by the individual, and sometimes more than once.

Alongside this, individuals will have the right to submit a SAR (Subject Access Report) request to businesses. Under GDPR, employers must respond, "without undue delay and in any event within one month of receipt of the request." This shortened the previous 40 day limit required under the DPA (Data Protection Act).

What's interesting is that a recent survey had shown that three-quarters of UK organisations failed to address personal data requests within the 40 day period, with some businesses not even responding to consumer and employee requests at all. Alongside this, according to Corporate Counsel, there have been 59,000 data breaches reported in the EU since the introduction GDPR, including 10,600 breaches from the UK.

Despite the warnings presented in the lead up to the introduction of GDPR, there have been a number of data scandals over the past year. The European Data Protection Board, stated that since May 25th 2018, 206,326 data breaches were reported by supervisory authorities in the first nine months of the GDPR being rolled out. Alongside this, authorities in 11 EEA countries issued administrative fines totalling €55,955,871. In 2018 alone, the supervisory authorities in Germany handed out a total of 41 fines.

Uber - November 2018

In November 2018, Uber were fined £385,000 for paying off hackers who had stolen the personal details of 2.7 million UK customers. Uber hadn't informed their customers about the breach.

Using "credential stuffing" (injecting usernames and password pairs into sites until they found a match), the hackers had accessed Uber's cloud-based storage system and downloaded names, phone numbers and emails of customers, as well as 82,000 driver records. Following this, Uber paid the attackers a $100,000 ransom so that they would destroy the data, but it took them more than a year to tell the affected customers and drivers.

Due to the size of the breach, the sensitivity of the data stolen and the length of time it took Uber to notify those who were affected, they were fined £385,000. Alongside this, 174,000 people in the Netherlands were also affected, leading the DPA (Dutch Data Protection Authority) to impose a separate £532,000.

Google - January 2019

In January 2019, French data protection watchdog, CNIL fined Google the largest GDPR fine to date - £44 million. This was because Google were found to violate GDPR in two ways. Their data processing practices were found to be "massive and intrusive", and it was also found that their data processing wasn't transparent enough when it comes to creating a Google account through an Android device. CNIL had found that when consumers submit a SARs request from Google, information gets "spread across multiple pages", making it "not easily accessible for users".

According to CNIL, when it comes to Google processing data, the purposes of the processing were too vague and generic, meaning users weren't able to fully understand them. Alongside this, it was found that the consent obtained for ad personalisation was not valid.

The Operational Impact of GDPR

It's expected that "Copycat legislation" will come into force in the next few years in terms of GDPR regulations - Canada, Singapore, the US, Australia and Brazil are, for example, introducing similar legislation.

In 2017, cyber attacks on organisations cost the UK economy £10 billion, with seven out of ten companies falling victim to a cyber-attack or breach. According to the Data Security Confidence Index, 58% of organisations collect sensitive data via email. Should the sensitive information sent via an unencrypted email from your business be infiltrated, your business will be found to be in breach of GDPR. With spam attacks, email spoofing and phishing being prominent forms of cyber crime, it's never been more important for you to use email software that's secure and will protect your business. After all, at every single part of its journey, an insecure email is at risk

CEOs, managers and business directors need to educate themselves and their employees about the importance of cyber security, and start putting extra precautions in place, so that they can create a more GDPR compliant future.

About the Author

Robin Bingeman is the Managing Director and one of the original development team who brought Cryoserver to the market as the expertly simple email archiving solution to solve issues which law firms, forensic teams, data protection officers and government agencies were experiencing on a daily basis. Under his steady leadership, Robin has boosted the development of Cryoserver into a technology used by all types of businesses spanning across 25+ countries. With over 18 years in the email industry, Robin is a thought leader on email management, compliance and privacy laws such as GDPR. Robin can be reached online at our company website, https://www.cryoserver.com/.

One of the Greatest Threats Facing the Iot: Router Security

Why routers are among the most vulnerable devices in the IoT - and what we can do to protect them

By Nitzan Daube, CTO, NanoLock Security

The IoT is a growing piece of the puzzle for daily life in today's modern technological age, and networks are at the center of this growth. Nowadays, you'd be hard-pressed to find a commercial, residential or even public outdoor area that does *not* have at least one router on a network. Homes, businesses, cities, and public infrastructure are all using WiFi, and it is not uncommon to see even basic home routers with multiple devices sitting on them at a time. But with millions of new routers being set up daily comes an increased security risk – and hackers and cyber terrorists are taking note.

Routers are notoriously known for their vulnerability and susceptibility to attack. According to a 2018 quarterly report from security firm eSentire, the group found a 539% increase in attacks targeting routers since 2017, and research from the American Consumer Institute (ACI) found that five out of every six, or 83%, of WiFi routers in US homes and offices leave their users at risk of cyberattacks, due to inadequately updated firmware for security vulnerabilities.

Many attackers will enter unsecure routers by remotely gaining access to the device, often via the CPU, and then installing malware that can then be used to collect data, gain access to additional routers, and cause irreparable damage to the device. In 2018, hackers conducted such an attack on a large-scale with the VPNFilter malware attack that infected over 500,000 consumer routers globally, calling special

attention to the damage that can be inflicted when malware is permitted to manipulate the software of a router, rendering devices inoperable and allowing personal data and credentials to be stolen.

The recent TP-Link Router Zero-Day Bug is another example of the hardware and software-based methodology in which hackers are accessing and manipulating routers. In March 2019, a zero-day bug was uncovered in the TP-Link SR20 smart hub and home router. The bug would allow an attacker to execute arbitrary commands on the device, foregoing arbitrary commands on the device. This flaw would allow attackers to remotely gain access to the device's firmware and manipulate it, while also gaining network access.

Another similar bug that happened within the last few months, called the Thangrycat bug, was found in the Cisco 1001-X series router, and allows hackers to gain root access to the router, and once inside, can disable the router's vulnerable Trust Anchor. A Trust Anchor is meant to be a final layer of security for devices, so any disruption to the Trust Anchor could cause an entire unit to be exposed and become manipulated. The Thangrycat bug is believed to be a physical flaw, and thus cannot be remedied with a simple software fix.

With new bugs and vulnerabilities being exposed on what seems like a weekly basis, it has become clear that router security is among the biggest threats impacting the IoT today. The danger and impact of such attacks is particularly impactful on consumers or small businesses, and infrastructures that may not have the technical knowledge or expertise resourced to identify or understand the threat before it is too late. This impact also extends beyond the use of personal-use routers to routers used in hospitals, government buildings, and other sensitive environments where the data to be manipulated could have potentially severe impact. And as smart home devices are increasingly installed in both homes and businesses, that threat can move beyond accessing a password to a website or personal photos; it can also impact the security of cameras or locks that allow hackers to gain physical access as well.

The entire IoT utilizes routers and is increasingly at risk due to newly developed malware and attacks directed at penetrating the CPU of these devices.

In order to ensure that routers are protected at both the software and hardware level, as well as on the network, it is imperative for new cybersecurity solutions to be implemented. It is not enough to protect the memory and the firmware. Unfortunately, firmware comes with bugs and it must be regularly updated to stay secure and working properly. Over-the-air (OTA) updates are equally problematic because the OTA solutions are based on software agents in the ECU and cloud services that deploy the updated images.

One consideration is a cloud-to-flash protection approach, that blocks access to firmware, boot images and critical code through a hardware-root-of-trust in the flash memory, effectively securing connected edge devices from persistent attacks like VPNFilter or bugs like TP-Link and Thrangrycat. By securing the flash memory and installing cloud-to-flash protection into devices on the factory floor, routers and other connected edge devices are protected throughout their entire lifecycle. This approach is also both processor and operating system agnostic and requires virtually zero processing power or additional energy.

This approach could be installed as the router is developed on the factory floor, building in a security management platform that doesn't rely on future hardware fixes or software patches to keep devices safe, easing the cost burden for manufacturers further down the line. Even vulnerable end-of-life firmware updates are shielded from attack.

Routers sit at the center of IoT and are critical for its growth. It is imperative for IoT infrastructure manufacturers to address these vulnerabilities before they are exposed, with solutions that allow them to monitor and protect from the moment a device is developed, to when it is operational in the real-world, throughout its entire lifecycle. Hackers and cyber attackers are becoming more sophisticated in their attacks using routers, so it is important that new methods like cloud-to-flash that don't utilize the CPU and managed security that offers insightful data are implemented into devices before its too late.

The fate of the IoT will rely on it.

About the Author

Nitzan Daube is CTO of NanoLock, where he brings extensive experience in software, high-tech business and bridging the gap between marketing, project management and engineering. He has worked with companies like Microsoft, National Geographic and Cellepathy in various executive-level software and hardware management capacities. Connect with Nitzan on LinkedIn at https://www.linkedin.com/in/nitzan-daube-729b1/ and at our company website www.nanolocksecurity.com.

How to Reduce Your Company's Susceptibility to Hacking

Thinking before the attack not abou the aftermath

By Zack Schuler, founder and CEO of NINJIO

When most people think about cybercrime, they think about headlines: data breaches that affect hundreds of millions of customers, crippling financial losses for companies, and outraged lawmakers interrogating CEOs in front of the cameras. In other words, they think about the *aftermath* of cyberattacks instead of the attacks to come.

While this is understandable for the average consumer, it's far less defensible for the companies that are at ever-greater risk of being hacked. Too many companies are reactive instead of proactive about cybersecurity – according to PwC's 2018 Global State of Information Security Survey, less than half of respondents have adopted preventive security measures such as vulnerability and threat assessments. Similarly, the second-most-cited vulnerability in the 2018-2019 EY Global Information Security Survey is "outdated security controls."

Meanwhile, the number of attacks continues to rise: Since 2014, the FBI's Internet Crime Complaint Center (IC3) has received more than 1.5 million complaints, and the number has increased every year (from under 270,000 in 2014 to more than 350,000 in 2018). Losses over this four-year period totaled almost $7.5 billion. Other data reflect these findings – according to the 2019 Cost of Cybercrime Study by Accenture and the Ponemon Institute, the average number of security breaches increased from 130 in 2017 to 145 in 2018, while the average cost of each incident jumped from $11.7 million to $13 million.

This glimpse at the state of cybersecurity in the United States isn't promising – even though attacks are becoming more frequent and more costly, companies' cybersecurity platforms aren't keeping pace.

Despite the statistics, it often takes a crisis to shift companies into a security-oriented mindset. EY Global reports that 76 percent of organizations "increased their cybersecurity budget after a serious breach" – yet another sign that they didn't take cybersecurity seriously until it was too late.

While preemptive cybersecurity measures like threat assessments and up-to-date security technology can help companies fend off attacks, what if companies could prevent hackers from selecting them as targets in the first place? What if, instead of merely decreasing the likelihood that an attack will be successful or mitigating its consequences, they could decrease their *susceptibility* to hacking altogether?

Consider the following scenario: The CEO of a company is an active social media user who shares a whole lot of personal material online – family updates, travel plans, political opinions, daily habits, and many other forms of identifying information. While this may seem innocuous (it's not as if he's posting bank account information or confidential data), he's giving hackers a huge stockpile of information that they can exploit to infiltrate his company.

For example, let's say the CEO posts about an upcoming conference where he'll be interacting with many potential clients and keeping up with his daily responsibilities remotely. This is the perfect time for hackers to launch a business email compromise (BEC) attack – a form of social engineering in which cybercriminals impersonate someone in a position of authority at a company to steal sensitive information.

Little does the CEO know, his email account has been compromised and hackers have been monitoring his social media profiles for months, giving them abundant information to craft a believable fake email. They send the CTO a message that goes something like this:

"Hey Jan – IBM is interested in working with us on that infosec project we discussed a few months ago! I just chatted with the CISO and we have a call set for the Tuesday after I get back. I'd like to show him the prospectus before I leave, but I forgot my login info. and locked myself out of our system. Could you send updated credentials ASAP? We're meeting in an hour."

All the information hackers needed to create such a realistic scam email could be found on social media, from a Facebook picture of the CEO with IBM's CISO at the conference to a LinkedIn post about how long the conference would last to updates on Twitter about the company's latest information security initiatives. This isn't to say the CEO's posts were a serious case of security malpractice – social media can be a great way to generate interest in your company, engage with customers, and share important information. But even heavy social media users can limit their risk by making their personal accounts private, only sharing intimate details about their lives with people they know, rejecting strange friend requests and connections, never posting sensitive content, and considering the security implications of everything they post.

Cybersecurity professionals have to recognize that even the most seemingly inconsequential disclosures can lead to multi-million-dollar data breaches, and social engineering hacks like BEC are often what precede these breaches. The 2018 FBI IC3 Internet Crime Report found that BEC was by far the costliest type of cybercrime last year, causing almost $1.3 billion in losses. This means the best way to prevent the most harmful form of hacking is to have educated employees who can spot attempts to manipulate them and who always verify the identity of anyone requesting sensitive information.

Your first and last line of defense against social engineering hacks like BEC is the development of a culture of security. Just think of how many billions of dollars and how much consumer trust could have been saved if even a fraction of the companies hit with BEC schemes last year had better-trained employees. In fact, if those employees had adopted safer social media habits, hackers may not have even tried to attack their companies in the first place.

About the Author

Zack Schuler is the founder and CEO of NINJIO, an IT security awareness company that empowers individuals and organizations to become defenders against cyber threats. He is driven by the idea of a "security awareness mindset," in which online safety becomes part of who someone is – almost an element of their DNA. This mentality is what gives people the ability and the confidence to protect themselves, their families, and their organizations. Prior to launching NINJIO, Zack was the founder and CEO of the IT services company Cal Net Technology Group. Over the course of fifteen years, what started as a solo-preneur venture based from the trunk of his car, turned into a multi-million dollar business. Cal Net was acquired by Olympic Valley Capital in 2013.

In addition to his entrepreneurial pursuits, Zack is a member of the Forbes Technology Council and is on the board of governors for Opportunity International, an organization that provides microfinance loans, savings, insurance, and training to over 14.3 million people who are working their way out of poverty in the developing world.

10 Steps to Kicking Off Your Insider Threat Program

By Mark Wojtasiak, vice president, Code42

Malware, ransomware and other external cyber threats are usually the security threats that grab the most headlines. You might be surprised to know that insider threats are one of the largest unsolved issues in cybersecurity, according to McKinsey. A staggering half of all data breaches between 2012 and 2017 were derivative of some insider threat element. And in the last month alone, we've seen three high profile cases of employees stealing sensitive information from McAfee, Desjardins Bank and SunPower Corp.

However, while businesses know they have to address this looming risk, they're often stuck trying to figure out, "*Where do we start?*"

Sure, it's easy to just say, "*build a comprehensive insider threat program,*" but that's daunting, time-consuming, expensive and complex. Building an insider threat program goes far and beyond "best practices." It usually involves an entire team dedicated exclusively to insider threat detection and response, which sounds nice, but not realistic for those security teams working with a tight budget and limited team resources.

The complexity doesn't stop there. The root of this approach is – dare I say it – legacy data loss prevention. Its 'prevention-first' approach and rigid policies frustrate users with barriers to productivity which, most of the time, lead to workarounds and loopholes.

This is doing your organization and employees more harm than good. We all need something simpler because insider threats show no signs of diminishing.

Here are 10 critical steps that make it faster, easier and more cost-effective to build your insider threat program:

1. **Get leadership buy-in:** This might seem like a no-brainer, but it's critical to the development of your security and IT team (and your future efforts) as value-adding business partners.

2. **Engage your stakeholders**: The buy-in campaign doesn't stop with the executive team. Think about the individuals that would lose the most if an insider threat event were to take place, and bring them into the fold from the start.

3. **Know what data is most valuable**: You should have a pretty sound idea of what data is most valuable after speaking with leadership and line-of-business stakeholders. You might be thinking, "*all data has value*," which is true, but these conversations will be essential to learning about the types of unstructured data to keep a watchful eye on, and which types of high-value unstructured data will require more creative means of tracking.

4. **Put yourself in the shoes of an insider:** Think critically about the value in taking or moving information. What would they do with it? What tactics or workarounds might they employ to help them get the job done?

Seem straightforward? Up until this point, you should be determining the types of data you're protecting and understanding the key indicators that might point to insider incidents. Keep reading – here's where things get simpler.

5. **Determine common, everyday insider triggers**: Don't get wrapped up in building a robust program with different types of classification schemes and policies that try to monitor every possible scenario. Instead, focus on your "foundational triggers," or most common use cases that make up the vast majority of insider threat incidents, such as departing employees à la McAfee, high-risk employees, accidental leakage and organizational changes.

6. **Create consistent workflows:** Investigating suspected data exfiltration can be complex and time consuming, so it's important to define the key workflows for each foundational trigger. For example, when an employee departure is triggered, make sure you clearly define the workflow/plan of attack for this trigger and consistently execute on the steps you've established.

7. **Establish a game plan:** Once a workflow is triggered and potential data exfiltration identified, establish which key stakeholder is responsible for directly engaging with the employee/actor. Using the employee departure example again, this would likely trigger engagement from HR and the line-of-business manager. This clear line of communication not only separates security and IT teams from the "data police" reputation, but also allows them to focus on data monitoring, detection and remediation.

8. **Spread the knowledge:** Small- and medium-sized businesses are typically working with a strained budget and limited resources, so a fully dedicated insider threat team – while ideal – isn't always realistic. While your security and IT team should be able to handle the monitoring, detection and remediation responsibilities, they shouldn't have to shoulder the full burden. Educating and training your stakeholders on the full scope of the insider threat program will prove critical so that they have a clearer understanding of what's being monitored, specific case triggers, key workflows, rules of engagement and the tools needed to accomplish all of this. This training should also clearly define roles and responsibilities in the event of a triggered workflow.

9. **Open the lines of communication:** In order to maintain a healthy working relationship between your employees and your security/IT teams, it's critical to communicate that your organization tracks file activity. Reiterate that the program is applicable to everyone – without privileges or exceptions – and is designed to maintain employee productivity, while protecting the organization's most valuable assets – its data.

10. **Start now before it's too late:** The most successful insider threat program starts long before a trigger. A trigger event shouldn't be the reason why you're implementing your monitoring, detection and remediation technologies. A strong insider threat program continuously runs and provides context and complete visibility into all data activity at all times.

The industry needs to stop seeing insider threats as "employees stealing stuff" when in reality, it's about the actions (good, bad, indifferent) that people take with any kind of data that puts the customers, employees, partner or company's well-being at risk. Initiating an insider threat program with a simpler, workflow-based starting point around three to four high-risk triggers can effectively address 80 percent or more of your risks to insider threat.

About the Author

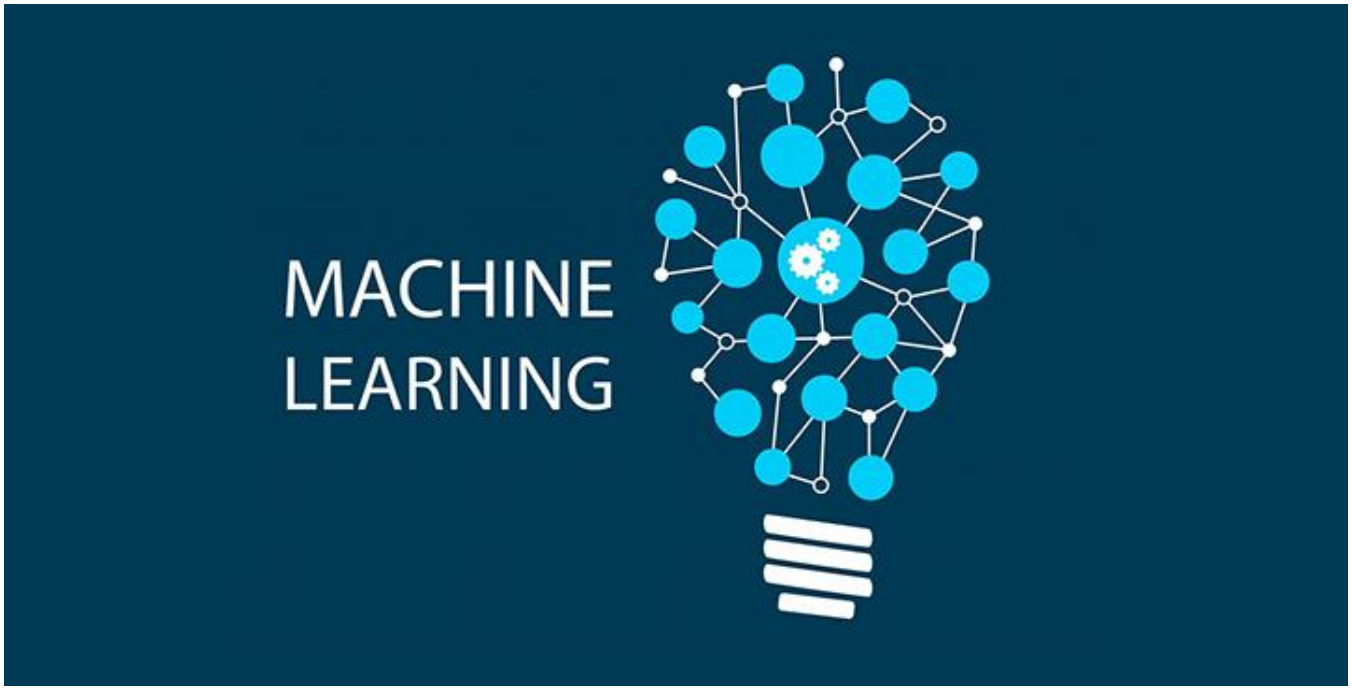
As vice president of portfolio marketing at Code42, Mark leads the market research, competitive intelligence and product marketing teams. Mark joined Code42 in 2016 bringing more than 20 years of B2B data storage, cloud and data security experience with him, including several roles in marketing and product management at Seagate.

How Is Machine Learning Helping Cyber Defense?

By Richard Meadow

Cyber defense needs to be constantly adapted in order to keep up with the developing threats thanks to more sophisticated technology. Thankfully, that's where machine learning steps in. Though many people may not be entirely familiar with machine learning and what it has to offer, it is already making an impact on their daily lives. Shaping the future to create a safer, more efficient world to come.

Although the idea of machine learning is not exactly new, it's experienced its biggest level of growth in the past decade due to increased interest. So, what exactly is machine learning and how can it help cyber defense? We break it down below.



What Is Machine Learning?

Machine learning falls under the umbrella of artificial intelligence. It essentially refers to the technology whereby a computer has the ability to comprehend and organise data, using algorithms to learn and adapt. It analyses large volumes of data and then interprets it into performable tasks. It can then use this information to refine its knowledge and make predictions for the future. Sound familiar? It should. Businesses such as Google, Apple and Amazon Alexa developer teams already use this technology to analyse user's search activity and make suggestions for future purchases or articles.

Already, it's being used across many industries. From helping take the pressure off teachers in the education industry, to greatly reducing data analysing time in law. In fact, there are few industries that

are not using machine learning in one way or another. The only limit once the technology is developed is how far each industry is willing to take it. Currently, artificial intelligence is not being used to its full capabilities.

How Is It Currently Helping Cyber Defense?

It makes sense that machine learning should be used to help in some way for preventing cyber-attacks and malicious behaviour given its advanced capabilities. It can learn what it deems to be "normal" online behaviour and then distinguish suspicious behaviour using a custom algorithm. This could be a game changer for hackers, who will find it harder than ever to get into a system once it's protected by machine learning security.

Here are some of the most important problems facing websites and ways in which machine learning is impacting cyber defense to prevent them:

Watering Hole

This term refers to when hackers try to attack a site that has a high number of traffic. The hackers then try to gain users' data, drawing it from whoever has visited. Machine learning can prevent this by creating algorithms for the site. It ensures the security standard by analysing the path of visitors coming to the website. Machine learning works by predicting outcomes and learning from them, whether they were correct or not. By applying this logic, it can detect whether users are directed to malicious websites by following previous visitor paths. It can then alert the user that the site may be harmful, giving them the option to go back.

Ransomware

Ransomware defines the combination of ransom and software. This is when a hacker gets hold of private information or data and demands a sum in exchange for the encryption key to the stolen files. AI can use deep learning algorithms to detect unknown ransomware and analyse the behaviours of ransomware attacks. This can then be used to check the files so security actions can be taken before it infiltrates the whole file system and locks access to the computer.

Webshell

Webshell is a piece of code inputted onto a website by a hacker which allows them to make changes on the web root directory of the server. Hackers can even access customers personal credit card information if it's an e-commerce site. They can also modify the transactions, so the payments go through a different path, exploiting the system so they receive the payment. Machine learning can help by indemnifying normal behaviour from potentially harmful behaviour. Files capable of harmful activity can be isolated before they have the chance to exploit the system.

The Future of AI

The future of AI and machine learning is looking bright, particularly when it comes to cyber defense. Machine learning has come a long way in a short space of time, improving the work environment for many industries as well as impacting customer experiences. The technology is yet to reach its peak, but businesses will do well to fully embrace it when it does.

Even in its infancy, it's already changing industries and how they operate, it's only a matter of time before it infiltrates other industries in the future. If machine learning keeps improving the way it is now, there is every reason to believe it will save many hacking instances from taking place. The possibilities are endless if machine learning is welcomed with open arms.

About the Author

Richard Meadow is a Freelance writer interested in technology and enjoys researching new subjects to write about. Currently, with the help of Apadmi, Richard research has lead into cyber defense and looking into the latest updates and technology is his current passion.Richard can be reached online at richardtmeadow@gmail.com and his Twitter handle is @meadow_richard.

What Is DNS Hijacking And How Can You Mitigate?

By Yair Green, CTO, GlobalDots

DNS (Domain Name System) is crucial to all organisations that rely on the Internet for conducting business – it's critical for the performance and reliability of your internet applications and cloud services. DNS failure or poor performance leads to applications, data and content becoming unavailable, causing user frustration, lost sales and business reputation damage.

DNS hijacking attacks have become widespread so what can be done to mitigate them.

DNS overview

Domain Name System (DNS) servers are often called "the phone books of the Internet" and are used to resolve human-readable hostnames into machine-readable IP addresses. They also provide other useful info about domain names, such as mail services. For example, if you know someone's name but don't

know their phone number, you can use a phone book to find their number. DNS services use the same logic. When you request data for a web location you type in its name and then the DNS servers find their IP address. Such internet phone books greatly influence the accessibility of Web locations which is exactly why DNS is crucial for any organisation that relies on the Internet to connect to customers, partners, suppliers and employees.

The Internet maintains two principal namespaces - the domain name hierarchy and the Internet Protocol (IP) address spaces. The Domain Name System maintains the domain name hierarchy and provides translation services between it and the address spaces. Internet name servers and a communication protocol implement the Domain Name System. A DNS name server is a server that stores the DNS records for a domain name; a DNS name server responds with answers to queries against its database.

What is DNS Hijacking?

DNS Hijacking, also called Domain Hijacking, is when bad actors redirect or "hijack" DNS addresses and reroute traffic to bogus DNS servers. Once a DNS address is successfully hijacked to a bogus DNS server, it translates the legitimate IP address or DNS name into the IP address of the hacker's malicious website of choice.DNS hijacking can be used for pharming (in this context, attackers typically display unwanted ads to generate revenue) or for phishing (displaying fake versions of sites that users access whereby data or credentials are stolen from them).

Many Internet Service Providers (ISPs) also use a type of DNS hijacking to take over a user's DNS requests, collect statistics and return ads when users access an unknown domain. Some governments use DNS hijacking for censorship, redirecting users to government-authorized sites. DNS hijacking can occur with any size website, directing folk to malicious websites without their knowledge. Since the website owners depend upon legitimate DNS servers that are issued by their Internet Service Providers (ISP), DNS hijackers use malware in the form of a Trojan to exchange the legitimate DNS server assignment by the ISP with a manual DNS server assignment from a bogus DNS server.

When users visit legitimate websites, they're automatically hijacked to a malicious website disguised as the legitimate one. The switch from the legitimate DNS server to the bogus DNS server goes unnoticed by both the user and the legitimate website owner. At this point the malicious website gets to do pretty much anything it wants, for as long as the person using it believes it's where they're meant to be.

As a cyber-attack, DNS Hijacking has a host of uses, including injecting malware into your machine, promoting phishing scams and advertising on high-volume websites. Ultimately, it's possible to suffer a data breach following a DNS Hijack, as credentials can easily be mined while the victim is active on the attacker's bogus site.

DNS hijacking attack types (6 main types)

- Local DNS hijack — attackers install Trojan malware on a user's computer, and change the local DNS settings to redirect the user to malicious sites.
- Router DNS hijack — many routers have default passwords or firmware vulnerabilities. Attackers can take over a router and overwrite DNS settings, affecting all users connected to that router.
- Man in the middle DNS attacks — attackers intercept communication between a user and a DNS server, and provide different destination IP addresses pointing to malicious sites.
- Rogue DNS Server — attackers can hack a DNS server, and change DNS records to redirect DNS requests to malicious sites.
- Recursive DNS hijacking — because DNS resolving is hierarchical with caching at the ISP level, hackers take over ISP recursive DNS resolvers and provide fake answers to end users.
- Registrar record modification — the domain registrar provides the names of the authoritative name servers to the top level DNS. An attacker hacks into the domain registration records and modifies them to point to a rogue server.

Mitigation Methods

Upgrade DNS in the Application Infrastructure

The lack of attention of DNS lags behind the innovation of the infrastructure in the cloud, creating cracks for possible exploitation. As organisations increasingly embrace a new generation of "cloud first" computing environments with multiple, connected clouds, data centres and CDNs, they also need to adapt and upgrade the underpinning infrastructure, including DNS and security technologies and policies.

Use DNSSEC

Application layers use security protocols (like HTTPS, DMARC, etc.), and DNS is no exception. The Domain Name System Security Extensions (DNSSEC) is one of them. DNSSEC reinforces the authenticity of DNS query responses by using digital signatures to authenticate communications, protecting applications (and the caching resolvers used by those applications) from using fake DNS data in cache poisoning and spoofing attacks. Historically, organizations have held back from using DNSSEC, because implementing it would mean sacrificing the DNS traffic management capabilities they rely on to deliver high quality online services. However, with recent technological developments, this is no longer a problem.

Secure access

Use two-factor authentication when accessing the authoritative DNS provider and the registrar, to avoid compromise. If possible, define a whitelist of IP addresses that are allowed to access DNS settings.

Client lock

Check if your authoritative DNS provider and your registrar support client lock (also known as change lock), which prevents changes to your DNS records without approval from a specific named individual.

Mitigation for end users

End users can protect themselves against DNS hijacking by changing router passwords, installing antivirus, and using an encrypted VPN channel. If the user's ISP is hijacking their DNS, they can use a free, alternative DNS service such as Google Public DNS, Google DNS over HTTPS, and Cisco OpenDNS.

External Monitoring of DNS resolution

Even if end users are protected and your authoritative DNS is secure, a local ISP can be compromised, affecting millions of end users. Run continuous DNS resolution tests from as many locations as feasible, and alert your security team on suspicious changes.

Whilst DNS hijacking has become a serious problem for many enterprises and end users, implementing the correct mitigation method goes a long way towards solving the problem.

About the Author

Yair Green is the CTO of GlobalDots, and a Cloud, Security and Web Performance Evangelist.

www.globaldots.com

The Top 4 Application Security Defenses You Didn't Know You Needed

By Jonathan DiVincenzo, Head of Product, Signal Sciences

Application security isn't a young buck anymore. The Open Web Application Security Project (OWASP) is 15 years old. But while application security is well into its teenage years, vulnerabilities like SQL injection and XSS still dominate the rankings of the OWASP Top Ten. This is concerning. But what's more concerning is that while attack vectors and techniques are still largely the same, software development models have completely shifted, as with the proliferation of microservices architectures, for example.

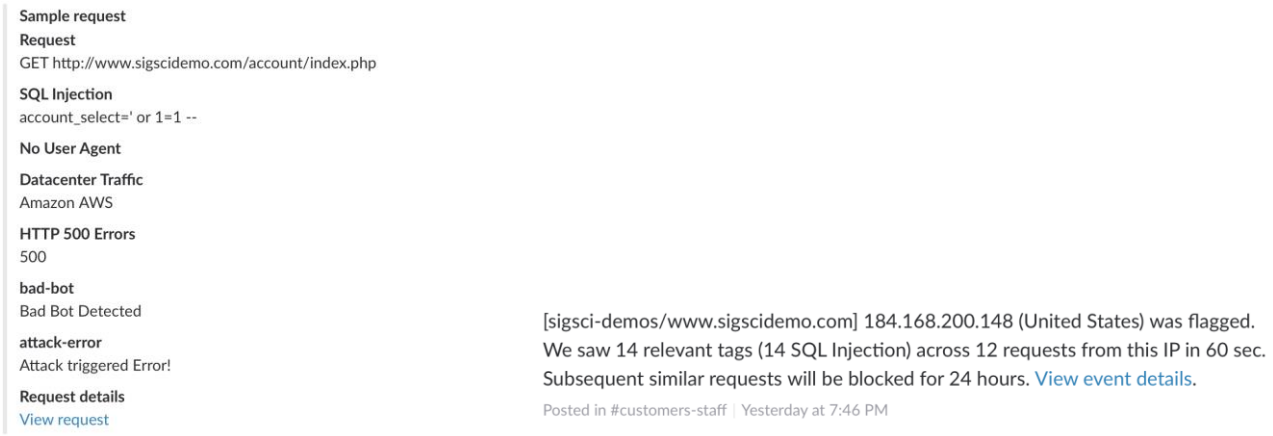
One major change in software development is the delivery cadence of an application. Instead of a mainly static application that changes only a handful of times per year, deploys now happen continuous. Further, most software development teams have adopted DevOps and have operational insight (via dashboards and metrics) and operational control (via chatops) without root access.

APIs are everywhere and new architecture patterns like microservices are here to stay. But application security problems still persist because all these services run on *http, making them susceptible to existing http vulnerabilities*. In DevOps and computing, there are four application security defense needs that organizations cannot do without:

1. ChatOps

With the rise of Internet Relay Chat (IRC) replacement systems like Slack or Teams, there has been an outcropping in the DevOps movement known as ChatOps. This encourages alerting, system actions and events to live where the development team already is: in chat, rather than in logs.

Application security programs should distribute events back to the developer teams. When under attack, messages should appear in Slack showing that defensive measures were taken, like this:



The goal is to bring the team together and keep security data in front of the people who create and deliver the application or service without getting in the way.

ChatOps even offers simple command driven feedback, a developer or security practitioner can quickly use a ChatOps bot to query a specific metric and it will retrieve the appropriate data.

2. Data Visualization and Dashboards

Web Application Firewalls (WAFs) have largely gone un-visualized for their entire existence -- developers who actually wrote the applications don't have access to their security data. Some of the legacy WAF vendors provide high level metrics; however, most of their offerings resemble log management software and pre-paid analyst services.

Visualization is an absolute must-have. In the modern era of DevOps, sharing is key. Two basic questions that Zane Lackey, CSO at Signal Sciences often asks are:

1. Am I being attacked right now?
2. Where are the attacks being successful?

Answering these two questions require visual representations in order to detect outliers and statistically relevant data.

3. Business Logic

There are inherently parts of an application that are more important to your business than others.

Do you care if someone attempts XSS on your site? **Maybe**.
Do you care if the number of failed logins has spiked in the last hour? **Probably**.
Do you care if those are two events are correlated? **Definitely**.
Do you care if you are seeing SQL injections and HTTP 500's spike at the same time? **You bet!**

When dealing with business logic and attacks specific to the application being defended, its critical to be able to correlate disparate data sets. This includes:

- XSS, SQLi, CMDEXE, and other application security attacks
- HTTP errors, Tor exit node traffic, and other anomaly flows
- Account Creations, Successful Logins, and other business flows

4. Defense against Bots and Scrapers

Some products specialize in keeping out bots and scrapers. Other products like honeypots specialize in enticing them. Not all bots are *http*-based, however most application security defense has some method to deal with bots coming in over *http* whether that be through:

- CAPTCHAs
- Analyzing traffic sources
- Fingerprinting traffic and headers
- Anomalous traffic patterns

Since not all bots are *http*, a pure application security defense approach won't cut it. However, most AppSec programs implement a safety valve at the *http* layer.

While application security is no longer in its infancy, the playing field is constantly changing and attackers are pushing the boundaries of their methods. Pin this list to the fridge as your development team experiments with new architectures -- it will save you some serious headaches down the road.

About the Author

Jonathan DiVincenzo, Head of Product at Signal Sciences, the fastest growing web application security company in the world, brings his engineering background together with a passion for taking mere ideas and turning them into products. He has experience working in both large companies and startup environments, where his impact in leadership, engineering and product development leaves its mark.Learn more about Signal Sciences online at www.signalsciences.com or follow us on Twitter at @SignalSciences

July Patch Tuesday

Microsoft Resolved a Total of 77 Unique CVEs, Including Two Zero-Days that Have Been Reported in Attacks in the Wild

By Chris Goettl, Director of Product Management, Security, Ivanti

Microsoft has released an update for everything including the kitchen smart sink! Ok, maybe not for sinks, but there are updates for the Windows OS, Office, .Net, SQL, VSTS and an Advisory for Microsoft Exchange Server! There are also updates for the following development binaries: Azure IoT Edge, Azure Kubernetes Service, Azure Automation, Azure DevOps Server, ASP .Net Core, .Net Core and Chakra Core. It is quite the lineup.

Microsoft resolved a total of 77 unique CVEs this month including two zero-days that have been reported in attacks in the wild and six public disclosures.

The first exploited vulnerability (CVE-2019-0880) is an Elevation of Privilege exploit in splwow64 affecting windows 8.1, Server 2012 and later operating systems. If exploited, an attacker can elevate their privilege level from a low to a medium-integrity. Once they have elevated their privilege level, an attacker could exploit another vulnerability to allow them to execute code.

The second exploited vulnerability (CVE-2019-1132) is also an Elevation of Privilege exploit. In this case the vulnerability is in Win32k and affects Windows 7, Server 2008 and Server 2008 R2. While an attacker would have to gain log-on access to the system to execute the exploit, the vulnerability, if exploited, would allow the attacker to take full control of the system.

Mozilla released updates for Firefox and Firefox, ESR resolving 21 vulnerabilities and 10 vulnerabilities respectively. Both are rated as critical and include vulnerabilities that could lead to information disclosure, sandbox escapes and remote code execution.

Adobe released multiple updates today for Dreamweaver, Experience Manager, Bridge CC and Flash Player. Dreamweaver and Bridge resolve a single CVE each which are rated as Important. Experience Manager resolved three vulnerabilities including one Moderate and two Important. Flash Player did not appear to include any CVEs.

Oracle is releasing their Critical Patch Update next week Tuesday, so expect updates from all your favorite middleware and Java.

This is a good time to bring up development tools. As the industry continues the shift toward DevOps and integrating with development binaries like Java, there are new considerations that you need to account for in managing the vulnerabilities in your environment. Java 11 changed the paradigm. There is no longer a JRE and a JDK. With Java 8 applications, a developer would build the application using the JDK and when the application was deployed to a system it required Java JRE to run. Each quarter when Oracle would release an update, the application did not require a change, but you needed to update the JRE instance to remove vulnerabilities. With Java 11, the JRE components are built right into the application. So as Oracle releases Java 11 updates resolving security vulnerabilities, a developer will need to update their version of the JDK and build the application again to include the new JRE components if any were vulnerable.

Microsoft released updates for several development tools including .Net Core and ASP .Net Core this month that similarly need to update the SDK component, then build the application and redistribute to resolve the vulnerabilities. Other examples of development binaries include Apache Struts, ChakraCore, ASP.NET CORE, Open Enclave SDK and many others.

About the Author

Chris Goettl, is director of product management, security, Ivanti. Chris is a strong industry voice with more than 10 years of experience in supporting, implementing, and training IT Admins on how to implement strong patching processes. He hosts a monthly Patch Tuesday webinar, blogs on vulnerability and related software security topics, and his commentary is often quoted as a security expert in the media.

Chris can be reached on Twitter @ChrisGoettl and at Ivanti's website: www.ivanti.com.

How To Prevent Your Data Loss Using Enclosed Data?

By Milica D. Djekic

Before we try to make some suggestions how to prevent your data loss in the practice, we should attempt to explain what we mean by such an occurrence. Your confidential data could get be the target of the both – cyber espionage and cyber sabotage, so far. In the both cases, your critical information could stay with you – especially if you deal with their backup, but the cybercrime underground could get in their possession. In any matter, your data would be in the hands of malicious actors and they literally can do anything with such lost findings. The data loss is an emerging concern to the modern cyber defense and security – in general, so we should think smart how to prevent such stuffs even happen. The unauthorized accesses to some IT infrastructure could cause the data leakage and their misusing which could be so alarming to any organization guaranteeing it is capable to protect its IT asset. Today the hackers would so easily obtain the sensitive information about some device or the entire network and try to do an espionage stealing everything being so valuable. The main challenge is how to prevent your data from being lost through the cybercrime operations and to be clear – there is no the silver bullet to such a scenario for a reason any single cyber security activity would need a lot of effort to get maintained. The purpose of this review is to make some suggestions and possibly offer some constructive ideas to the cyber defense community how to approach such a problem, so far. The price of the confidential details on the marketplace is extremely high and the socio-economical impacts to any private or business asset

could be so dramatic. There is the strong need to protect your critical data from being stolen or destroyed for a reason the consequences could be so serious and once lost data could serve to far more dangerous purposes. In addition, you should think hard how to prevent the hackers from making the breaches to your IT system and taking from there anything they can get in so illegal manner.

What are the enclosed data?

The good trick with the data being the part of some cyber asset is to make them being enclosed to that device on. What would we mean by the enclosed data? Those kinds of details would not get allowed to get moved or better say – manipulated by anyone attempting to do so from the outside mainly using the unauthorized tools for such a business. There is the certain set of rules that should get followed in order to make your confidential information being manageable from your machine only and getting accessible from the remote locations that got the permission to deal with them, so far. In other words, you need the well-developed systems that would allow you to, for instance, attach your files to your email messages, upload them to some websites or social media accounts or save them on some removable device from your computer only. If anyone would want to make a copy of your sensitive data and re-direct it to some remote device – you should cope with the solution that would ban any unauthorized access to your files and folders. This research effort would just give some ideas and suggestions how such a secure system should work, but – in our opinion – there is still a plenty of hard work for the R&D teams that should make the serious preparation and planning for that project. So, anyone getting the permission to manage data from your machine would get in position to do so including the security professionals who would use the pro tools for connecting to your infrastructure and getting the chance to transfer your data to their computing devices. In other words, anyone who would want to apply any operation to your sensitive data on your machine should get the permission to do so. In case of malicious hacking tools, such an access should get prohibited, so far.

Why does smart programming matter?

If you make the good preparation to your programming algorithm and if you predict any single step with the user's experience being correlated with your final product, you can expect that your software would do exactly what you want it to do. In other words, it's so important to get your developer's instructions, functions and procedures into the logical order and carefully put under the consideration every single requirement of your project, so far. The developer's environment would seek from you the skill in some programming language and does not matter which programming language you speak – you should understand that the end user's experience is the ultimate goal to any developer's project. Apparently, there is the huge need for the security researchers as well as computer science engineers who would get capable to forecast everything being from the strategic importance to the project and get the skill and expertise to deal with the everyday concerns as well as the new and improved versions of their creation. For instance, in so many programming languages – you can define the path to your final destination that should get followed in order to manipulate with the content being at that location within your working surroundings. If you figure out that you can intelligently take advantage over some programming commands and your developer's skills – you would realize there are the heaps of undiscovered opportunities waiting for the developer's community to get used to the extremes.

How to protect your IT asset from the external incidents?

If your sensitive data are enclosed to your IT system and there are some restrictions about who can handle them – it's quite obvious that there would be the lower risk to the cyber attacks coming from the outside. Maybe you would not prevent your machine from being breached, but you would definitely protect your data from being stolen and misused which is the main point of this suggestion. Yet, the open question is that you would not prevent your assets from being breached and you would only be able to prevent your data from being stolen which could be the sword with the two edges for a reason the hackers of the tomorrow could choose to damage or even destroy your critical data certainly causing their loss. The black market actors would rather select to steal anything they can steal and so many cyber espionage groups would give up once they get they cannot take anything from your machine. On the other hand, anyone being malicious within the cyberspace would be satisfied with the data and operating system demolition for a reason they would believe that's the way to defeat their opponent or at least get paid.

The role of remote assistance permissions

If anyone would like to access your machine remotely – he should need the permission for such an intervention. In other words, the IT systems of the future should cope with some bans about who can make a breach to your infrastructure decreasing the chance to the attackers to do the complete data loss. Also, it's quite clear that so many cybercrime groups could get in possession of the professional tools or there could be some state-sponsored hackers who could apply such software to overplay our suggestion. Anyhow, the good data loss prevention strategy could be from the crucial significance for the cyber security of the tomorrow.

Some future perspectives

The good point of this discussion is that there are some ideas how to prevent the data loss at some level and in order to fully protect our cyber assets – we should think a bit about the combination of the cyber defense tactics and countermeasures that would help us to manage the risk intelligently. Any cyber breach could get discovered using the intrusion detection and prevention techniques and if there are some well-developed incident response strategies – the chances to your enemies to cause you the harm could be far more decreased. The final imperative to this suggestion would be to progress with the higher and higher levels of protection that could offer us an opportunity to prevent some variations of the data losses and possibly the cyber breaches opening an option to make much smarter and more secure surroundings to our end users. Finally, we are fully aware that the human beings would rather choose to get the machines serving to them and relying on the expert's knowledge in resolving any inconvenient situation on, but at this stage that is still so far away. The technological solutions got no brain and they can do only what we want them to do, so as we are looking for the theory of everything in the physics and the fact is we are still satisfied with the small pieces of the science – we should know that the comprehensive solution in the cyber defense is still the distant future project and there are a countless number of small steps we need to take in order to get there.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, 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 and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. 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). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

The Iot Headache and How to Bolster Defenses

By Dr. Mike Lloyd, CTO, RedSeal

There's a saying in the security world: 'if it's on the network, it belongs to the CISO'. And CISOs have risen to the occasion, developing and honing a bag of tricks that work reasonably even in the face of morphing attacks and unwitting employees. But now, with increasing numbers of very different devices connecting to the internet, CISOs are realizing that their standard bag of tricks doesn't work on the Internet of Things (IoT).

First, what do we even mean by Internet of Things? I've discussed this with several experts in the area and I find those thinking about security have the best definition – 'it's IoT when we can't get standard telemetry'. That is, the best definition I've encountered for the Internet of Things is about blindness and lack of knowledge.

We now have the technical means to cheaply put just about any device online. But that very cheapness is part of the problem – IoT devices compete on price and are hemmed in by strong cost constraints. If we connect a lightbulb to the internet (and yes, people do), you can bet the network functionality will be the cheapest version the manufacturer can get. Within that cheap functionality, security is one of the first things to go.

One of the key tricks in a CISO's bag is updating applications early and often with the latest fixes. But they can't update a lightbulb, or an industrial turbine, or every medical device in a hospital. Security and patching infrastructures don't exist for these special-purpose IoT devices. It requires specific expertise and adds expense to keep up with the endless findings of security researchers. As a result, nobody is responsible for managing security updates for all the Things we're bringing to the Internet.

Other CISO tricks involve installing security agents on every device and scanning networks for known vulnerabilities. But you can't install a security agent onto an insulin pump, or an industrial controller, or a lightbulb. And, you can't use vulnerability scanning – the main method for finding known security weaknesses in traditional IT infrastructure. If you do, at best a traditional scanner will struggle to identify the special-purpose device, but at worst, it might even crash the fragile Thing you're trying to identify.

So, what can our CISO do in this world where traditional techniques don't work well? It's not as if a typical organization can just refuse to go along with IoT – these devices are proliferating rapidly. I've found that the best strategies are segmentation and resilience.

Segmentation makes sure that IoT devices have no access – even indirectly – to the outside world. These endpoints cannot be trusted and can't be forced to run whatever control software you want. Instead, you must contain them, keeping these fragile and risky devices away from each other and anything else they could harm.

That is, as the endpoints get dumber (due to their focus on doing one job well), the network must get

smarter. Network perimeters aren't dead. Rather, they've gone everywhere. We now need internal perimeters around all the uncontrollable endpoints in our networks.

Resilience is also key, because perfect protection and containment are not possible. Experienced organizations balance their efforts between protection and recovery, recognizing that incidents are inevitable, but serious damage is not. Resilience means understanding your infrastructure ahead of an attack, thinking through how an incident could spread, and building response and containment plans, just the way first responders anticipate and practice for the inevitable bad days.

IoT presents novel challenges for today's CISO. The three-step strategy recommended here starts by understanding the categories of IoT devices that you use (whether you planned to or not).

Next, realize that standard techniques we use to control general-purpose computers don't work, and so we have to rely on segmentation. Third, we cannot expect to stop all incidents, so having a well thought out containment plan, based on real knowledge of your environment, is essential to damage control. This is how CISOs can deal with the IoT headache and deliver resilience in this complex new world.

About the Author

Dr. Mike Lloyd has more than 25 years of experience modeling and controlling fast-moving, complex security and network systems and holds 21 patents. He joined RedSeal as the Chief Technology Officer (CTO) in 2004 and has been growing the company's brand and reputation through its technological innovations ever since.

Dr. Mike can be reached online at RedSeal's website https://www.redseal.net/

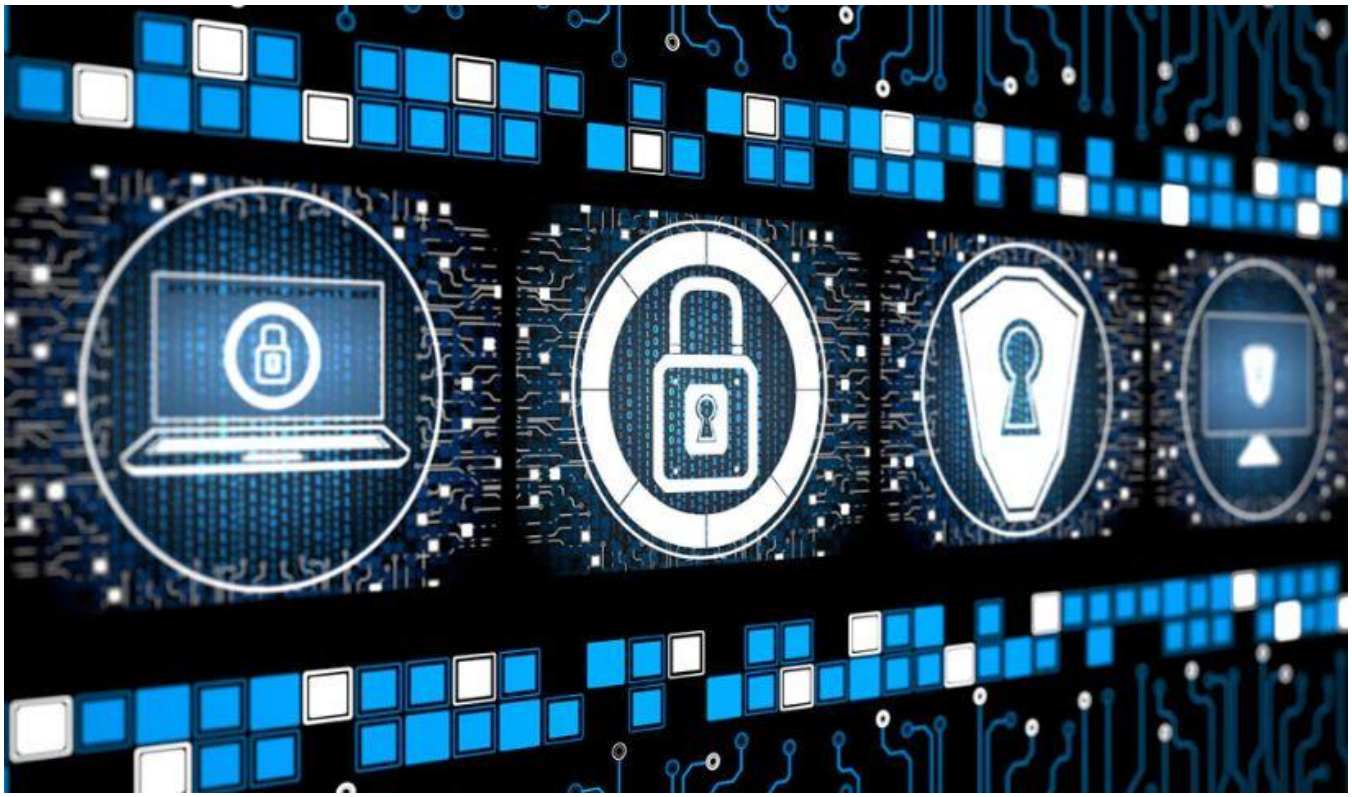
Cybersecurity & Your Company

Identifiable Threats and How to Block them

By Frances Dewing, CEO, Rubica

As more smaller companies rely on technology to do their day-to-day business, their risk of being hacked increases. For some people, this may seem counterintuitive. Hacking larger corporations offers bigger payoffs and we tend to only hear of cyber attacks on big companies such as Adobe, Sony and Equifax. On the other hand, smaller businesses do not have the resources nor the money to invest in robust cyber infrastructures, leading them to be vulnerable. The result is loss of money, production and client information – and negative impact on reputation. These smaller businesses can also be the gateway to access the information of big corporations. For example: The Target hack, which resulted in tens of millions of consumer's credit card details stolen, stemmed from hackers infiltrating a small HVAC company which allowed them to access credentials to Target's network.

According to Small Business Trends, 43% of cyber attacks are targeted at companies with 250 employees or less. A small business is particularly at risk if they have frequent wire transfers or payment transactions, deal in customer personally identifiable information (PII), financial info, health data, intellectual property, or contract with larger entities or high-profile individuals (where they could be targeted as a weak link into them). Fortunately, there are a few things companies can look out for to prevent risks.



Mobile Devices

We do a multitude of things on our mobile devices: texting, gaming, GPS, calendaring, emailing, web browsing, social media, photo sharing, banking, streaming, even buying a home. The list goes on. With the rise of portable devices that house all our information and online habits, so comes the rise of targeting those devices. Mobile devices are more apt to be used as a hacker entry point due users clicking-without-thinking and falling for phishing and social engineering schemes. If a person uses their phone for personal and business use, which a majority of the population is known for, it becomes a juicier target for criminals due to the increased opportunities to gain access to the device through personal and business activities.

Recently, there has been a rise in virtual worlds, live action gaming, and a pivot from console-based to mobile-based gaming. While this innovation opens more doors for developers, it also opens up more doors for hackers. STEM games have been a known vector for nation state actors for years, and now with more games showing up in the app store, these games will become a gateway for cybercrime.

Greyware

Malware often hides in plain sight, disguised as legitimate apps, games or software – even available in the official app stores waiting for unsuspecting users to download. When these programs are downloaded and their terms and conditions are accepted, consumers are voluntarily - albeit, unwittingly - giving these malicious programs access to read, write, modify and steal data from their phones. This is the problem with "greyware" – it's not black or white, or a per se violation of the rules. It finds a loophole in the system and exploits it to evade policing. This is what cybercriminals do best. Use our own habits, systems and blind trust against us.

Data itself is valuable. If an organization can gather info about consumers and their behavior – where they go, what they do, and when they do it – that's powerful information that can be used to influence and manipulate them.

Persistent & Patient Cyber Actors

The thing about cybercrime is that it doesn't hit right away. Sometimes it's a waiting game. Command-and-control (C2), Advanced Persistent Threat groups (APT) and backdoor malware provide cybercriminals access to devices and networks and the ability to exfiltrate data or initiate other later attacks. They pursue their objective over months and sometimes years. They also adapt to defenses and will most likely retarget victims.

Knowing that these factors can happen at any time, here are a few tips to help prevent cyber-attacks:

Think before clicking. Beware of phishing and social engineering in traditional channels (emails and social media) and emerging channels (gaming). Behavioral-based detection & IDS/IPS solutions (like Rubica) can help detect and block malicious sites and software, but educating your team is worth investing in. If employees understand the part they play in security and how their actions can impact the business, they are more likely to think before they click.

Scrutinize app permissions. Although there are harmless uses for device permissions, these same permissions can also be used to surreptitiously download malware or steal account login information. Be particularly wary of permissions like "read/write/modify files or storage," access to camera, microphone or GPS, "retrieve list of running apps," download files without notification, and "display over other apps."

It's not just about which permissions – it's about who has access to the permissions. Only give access to trusted apps.

Use a continuous monitoring, detection, & response system. Diligently analyzing the traffic flowing in and out of the network and device(s) is one of the only ways to prevent certain threat vectors. Intrusion detection and prevention systems (IDS/IPS) can be installed on the company network or on each device to monitor and defend regardless of what network is connected. Threat-hunting in the "calls over the wire" is one of the best positions to detect hidden malware reaching out for instructions or pulling down the next phase of the attack.

Ensure the whole team has multifactor authentication enabled on all email accounts. Email is still the most common delivery method for malware. Only allow employees to access their work email from secure work devices (not their personal device or a device shared with a family member). Passwords for email should be completely unique and never reused on another site.

About the Author

Frances Dewing is the CEO of Rubica. Since the company's inception, Frances built and directed Rubica's core operations teams, including cyber operations, customer support, finance, legal and human resources. Formerly COO of Concentric Advisors, a consultancy specializing in cyber and physical security for some of the world's most high-profile figures, Frances was instrumental in developing Concentric's business in Seattle and Silicon Valley. Frances is a Washington State attorney with a JD from the University of Washington. She can be reached online via LinkedIn and at our company website www.rubica.com

The Smart Encryption Procedures and Policies

By Milica D. Djekic

The need to hide the message from your opponent would exist since the beginning of the ancient time. With the first countries and the rise of human activities and progress through the history – the people would feel the need to camouflage what they really know in order to take advantage over such findings. Many folks would believe that the cryptography would come with the first electronics and digital systems, but that's not the fact for a reason so many cryptographers would work in the past trying to protect someone's interests and infrastructure, so far. Through the previous times, there would be a lot of army or rulers' couriers who would take the messages from one place to another and once they come to the certain destination – they would put those pieces of information into the hands of so skillful encryption staffs. Also, you could try to imagine how knowledgeable the people in the past were for a reason they would perfectly know how to develop some cryptosystem on the piece of paper or the part of skin and explain to the origin and destination forces how to prepare and decrypt their secret contents. The point is so many armies, law enforcement and military officers through the past times would so carefully go through so useful training and learn the secrets of the good crypto-protection. Also, there would always be the people who would so elegantly play with the mathematics and the beginnings of the engineering and who would get capable to invent the new and new cryptosystems that would be the good enough to offer some kind of advantage to their countries, militant groups or the overall communities. So, the history of cryptography is so huge and maybe even today we can talk about some smart encryption and the fact is that sort of benefit would be present, so far – but we should get that the smart cryptography is not only the product of this time and so many competitors even in the ancient time would believe for themselves

they would deal with something being such smart – especially if they took advantage or got the war relying on such a solution.

The challenge of endpoint security

With the nowadays digital age, we would use the computing units and some kinds of communications channels in order to transfer the secret message from one point to another. It's quite well-known that the hackers as well as cyber criminals would so easily threaten the endpoints of some digital system for a reason if we cope with the device getting the internet connection – that device could get exposed using so simple hacking tool. In other words, there is some concern that if you are encrypting and decrypting the message or the entire file on your computer someone getting in possession of your IP address could make a breach to your asset and get which sort of password or key you are using for the purposes of your cryptographic needs. So, the crucial question here is how to manage your secret key and which communications line to use in order to make the safe transfer from one place to another. The point is anyone could do the espionage of your endpoint spot being connected to the web and so easily see what you are typing on your screen. For the purposes to avoid such a scenario – we would kindly suggest to do encryption and decryption of your sensitive content on the computer that is not connected to the internet for a reason that would decrease the chances to the bad guys to discover what you do on your machine. Apparently, that's not any kind of the absolute security because there are so many professional defense tools that could expose your electronic device even if it is not linked to the web and in so many cases, such a system could belong to some competitors' governments. Differently saying, there is only the good practice that can support you to manage your risk at the lower possible level and if such a procedure helps you to get the battle you can say you got so smart in front of your ongoing enemies.

How to manage your cryptographic key

In the modern days, there are a plenty ways to manage your cryptographic key or the entire cryptosystem. For instance, you can always use some well-protected communications channels in order to pass your key through so and also, some experts would suggest applying the web-based encryption key management. Remember – we would always talk about the risk coming from being online for a reason in such a case – even kid can expose your machine and see what you do with there. Maybe the old good advice could work even today and that is we could try to transfer the cryptographic key and the entire encryption procedure instructions using the special courier, so far. By this we would not mean that you should send your secret content by post, but let's say there should be some trusted ways of delivering the confidential information on. In such a manner, we can talk about the in person approach that could be the quite suitable one for the intelligent encryption key management. As you know, today everyone would be so dependable on cyber technologies and maybe the old good courier getting the packed message could be the right choice to so many military needs and applications especially if we know that the air forces could seek only 24 hour to deliver anything anywhere over the globe.

There is no an absolute security

As it's well-known, there is no the silver bullet to any concern in this world, so the similar case is with the cryptography. Many people across the globe would want to rule the world and the mission of the competitive security should be to get at least one step ahead of the threats. In other words, the one who has the advantage would control his society and the role of the defense is to offer the protection and the same human rights to all people worldwide. In the essence, it's not easy at all to accomplish such a

mission and there would always be some obstacles and drawbacks on your way on to secure your country and the entire nation. On the other hand, on that road you should figure out that even if you establish some solution – it can always collapse if you are not willing to put a lot of effort on in order to maintain the healthy condition, so far.

It's only the matter of time and effort

In addition, even the strong encryption systems appearing as the smart approaches of nowadays could get defeated and it's only the matter of time and effort how your opponents would do so. They would be that smart if they offer you some sort of advantage over some historical moment and so rarely during some time epoch. So, if you are clever enough to win only one battle using your crypto algorithm – you can say such a solution got quite purposeful for your current needs. If not, you should look for the better choice – otherwise your enemies would defeat you, so far.

The final discussions

So, the aim of this effort is to discuss the smart cryptographic procedures and policies and indeed, there is some good practice within any defense force that should get followed in order to maintain the risk at the acceptable level. No one would ever get absolutely secure and it's only about how hard you should work in order to break someone's defense. Through the history, the security forces would use so many sorts of intelligence and in order to remain competitive they would adjust their actions depending on the situation on the battlefield. Finally, the one who would win the war would get considered as smart at that moment only. What got so unavoidable at anytime is the change and even if you are doing your best to manage some state – so many of them could try to challenge your attempts, so far!

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, 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 and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. 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). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

Five Ways a Software Defined Perimeter Is Better Than VPN

By Etay Bogner, Founder & CEO, Meta Networks

Can virtual private networks, created over 20 years ago, still provide an adequate solution for secure remote access these days?

The well-defined network perimeter that VPNs were designed to protect, has essentially been dissolved with the wide-spread adoption of cloud-based, virtualized infrastructures. How can an enterprise enforce security for remote users when its network resources are no longer just inside a data center? When employees, partners and customers are accessing cloud services and Internet apps?

With apps moving to the cloud and users moving off the network, a cloud-based software defined perimeter (SDP) provides a much more suitable solution that addresses enterprise needs and resolves VPN's inherent shortcomings. Gartner defines software defined perimeters as "a logical set of disparate, network-connected participants within a secure computing enclave. The resources are typically hidden from public discovery, and access is restricted via a trust broker to the specified participants of the enclave, removing the assets from public visibility and reducing the surface area for attack."

As organizations begin to weigh the benefits of software defined perimeters over VPNs, here are five ways SDPs are winning the debate against corporate VPNs.

1 – Tighter Security

The most concerning security flaw with VPNs is the fact that once a remote user is authenticated he or she is considered trusted and is granted excessive access to network resources. Generally, VPN access is overly permissive, granting remote workers access to more of the network than is required to complete their tasks. As a result, network resources are unnecessarily visible, overly vulnerable, and open to attack.

A software-defined perimeter replaces this flawed VPN site-centric security approach with an identity-based approach that enforces a customized policy for each user device. There are no trusted zones and an IT administrator must grant users permission to access specific applications. All other network resources that are unauthorized to a specific user are simply invisible.

Some SDP solutions also provide continuous authentication and verification of the user and/or device at the packet level using identity-based networking technology. Finally, all network traffic is logged for audit and investigation.

2 – Better End User Experience

Anyone that has used VPNs is familiar with the notoriously slow and unreliable performance. And if one is on the job and involved with multiple applications in different locations, the frustration of repeatedly connecting and disconnecting to remote applications is not an uncommon experience.

With SDPs, the user experience is dramatically different. A global network of points-of-presence (PoPs) provides a network backbone that reduces latency and optimizes the routing of data. Therefore, instead of connecting to a specific site, a remote user connects to the nearest local PoP, which provides better performance and quality of service from anywhere in the world.

The single connection to the overlay network provides access to all the applications needed, regardless of their location.

3 – Reduced Management and Administration

Any enterprise that has expanded a single data center into multiple cloud deployments, has experienced how VPN management balloons in complexity, with IT administrators required to configure and synchronize VPN and firewall policies across multiple locations.

SDPs, on the other hand, offer a much simpler management and administration than any number of data centers and cloud deployments. Administrators can onboard each network resource to an SDP platform once and manage all policies centrally in the cloud, avoiding the need to configure and sync across different locations. There is little to setup or maintain and upgrade in the data center or VPC, since all logic and security definitions are done in the SDP cloud platform.

4 – Better Scalability

VPN infrastructure is installed to support tens of thousands of user sessions. However, this equipment is primarily in place at very large organizations and is costly to purchase and manage at scale. For many companies, VPNs are installed and expanded as demand requires. As the business grows and adds additional VPN connectivity to provide support for business partners and customers, both the management complexity and costs rise significantly.

With a fixed price per user regardless of how many network resources the user needs to access, an SDP solution with a cloud-native infrastructure can quickly, easily, and affordably scale up to millions of concurrent users leveraging a backbone of global PoPs. There's no need to sink additional funds into larger appliances each time new connections are added.

5 – Greater Flexibility at a Lower Cost

While VPNs do offer the flexibility of connect multiple sites, datacenters, and virtual private clouds (VPCs), adding entities drives up costs due to the need for more powerful appliances and additional licenses. Additionally, the expense and management complexity that increases along with each additional piece of infrastructure rapidly pushes the VPN outside of budgetary limits. Unless your enterprise is a large one with deep pockets and a sizable IT department and budget to match, users are likely to find these connection options more time and financial resource intensive.

An SDP cloud platform will typically not charge by the number of data centers or sites added, but rather by number of users connected, which results in lower total costs.

Taking the Next Step

Transitioning from VPNs to a software defined perimeter solution does not require a complete overhaul of your IT infrastructure. In fact, it does not require any overhaul at all.

Next generation SDPs let you adopt Google's BeyondCorp approach of a software defined perimeter without changing any of your network infrastructure or applications. You can provide remote/mobile employees, partners, contractors and customers with convenient, granular access to specific web or legacy applications - with tighter security, and without the need for a conventional VPN.

About the Author

Etay Bogner is the CEO and co-founder of Meta Networks, a technology leader focused on helping organizations rapidly provide secure remote access for employees, contractors and partners to corporate applications and the internet.

The Email Tracking and Fraud Prevention

By Milica D. Djekic

Since the early beginnings of digital systems and the first discoveries of the email data exchange – there have been the heaps of methods how to misuse such communications and commit some kind of fraud over the content being sent through the email channel. In other words, just try to imagine if any of your confidential information such as technical documentation, intellectual property or corporation's stamps and signatures would get transmitted through the internet and the bad guys would come to the possession of those sensitive details. Indeed, there would be feasible to obtain so many frauds over those contents claiming that you are someone else that would so freely manage those data and try to take some kind of financial advantage over those findings. The fraud by itself is so impactful crime that would take a lot of money per a year from anyone being targeted by that sort of criminality. For instance, there is not the rare case that so many cybercrime groups would hack the colleges and Universities worldwide and steal the templates of the degrees, diplomas and certifications and once they get such a frame – they would complete it using the fake information and sell it on the black market and someone getting no correlation with – let's say – the medicine would show the doctor's degree on the job's interview and maybe get the chance to start his medical professional career somewhere. Also, it's possible to steal the entire interview selection procedures from someone's computer or another device and prepare your skillful fraudster to take advantage over such knowledge. The similar scheme could get applied in any other fields of human activities and if the background check is not straightforward – the people could easily get the victims of so simple email tracking espionage. For such a reason, it's so crucially important to protect your email account and ban the access to the cyber criminals to so easily monitor your email communications. In the practice, there are some methods how to prevent your email from being traced, but in so many cases

– if the hackers deal with the professional tools, they can track any email account either it is assured or not.

The concept of untraceable email

The first indications that we could cope with the untraceable email correspondence would appear approximately 30 years ago with the development of the Tor's project. Indeed, there are no known hacking tools that would offer the opportunity to the ordinary cybercrime groups to stalk the onion email accounts. The fact is those accounts are not with the well-designed access control and so many bad guys could try to approach the accounts simply obtaining the login details or guessing them. The Tor is the system that would offer us the chance to lead so confidential communications providing us the option to deal with the great amount of security, privacy and anonymity. The similar case is with the email data transfer and those solutions would also cope with the good level of intractability. As it's well-known, the Tor is the environment being suitable for the both – good and bad guys – and it would use so called the role-based access control. That would mean that anyone getting the login information can approach any account and not only that. Namely, anyone with the admin or super user permissions could investigate any account being from the lower priority, so far. It's quite clear that so many defense forces would deal with those products and they would be in position to see what anyone being the part of the Tor's network including its email account does within such a surrounding.

The Darknet and security, privacy and anonymity

In the reality, there are a plenty of the Darknet solutions being accessible through the deep web. Those systems would go far more below the surface of the regular internet and offer so many secret details. Such an environment would be so handy place for the hackers, cyber criminals, activists and even defense professionals. The Darknet by itself could be the real oasis to many dealing in so illegal manner, but in our belief – it would still be controlled by the good guys. So many defense and intelligence agencies would use the findings being available through the Darknet in order to understand the malicious actors' behavior, motives and actions, so far. The point is the Darknet would provide some scale of security, privacy and anonymity, but that sort of protection could get managed by the defense services that would use such an infrastructure in order to attract the bad guys and lately investigate and remove them from the web. As it's quite well-known, the cyberspace is so overcrowded spot and the places with the huge concentration of the people could get suitable for committing any kind of the criminality. The similar situation is with the Darknet and the fact is the one who has the control over such an environment would take advantage over the rest.

The frauds being possible applying the email communications

In the practice, so many email accounts would be the cloud-based ones and there would be present some possibilities to track those spots. The point is so many confidential information would be exchanged through the email communications and someone only tracking some private or business correspondence could get in possession of so valuable details. It's the quite common case that the open documents would get sent through the email correspondence and that's the pretty big advantage to the hackers who could put under the surveillance the entire small businesses dealing with so poor cyber defense and making the good incomes per an annum. In other words, someone doing the cyber espionage could obtain so significant details and use them to trick someone who got absolutely no idea that those data are stolen and can serve for the financial benefits only. We believe that it's quite obvious that so many fraudsters

would get correlated with the cybercrime rings and those folks would simply monitor someone's email accounts and get whatever they want to have. On the other hand, it's quite logical that the hackers could make the breach into someone's IT system, but it's also quite convenient to track someone's email communications.

Some countermeasures to these scenarios

As we would suggest, the small businesses coping with the poor cyber security and contributing a lot to the entire economies could be so easy target to the bad guys. In so many parts of the world, the small businesses would get recognized as the critical infrastructure being from the strategic importance to the entire nations. In our opinion, the best feasible way to prevent these scenarios even happen could be to run some awareness campaigns and programs that would warn and teach the people how to deal with such situations. The situational awareness could be from the crucial significance to many and even if we make the untraceable email with the great access control – there is no place for a relaxation for a reason the attack could appear whenever, so far.

The conclusions

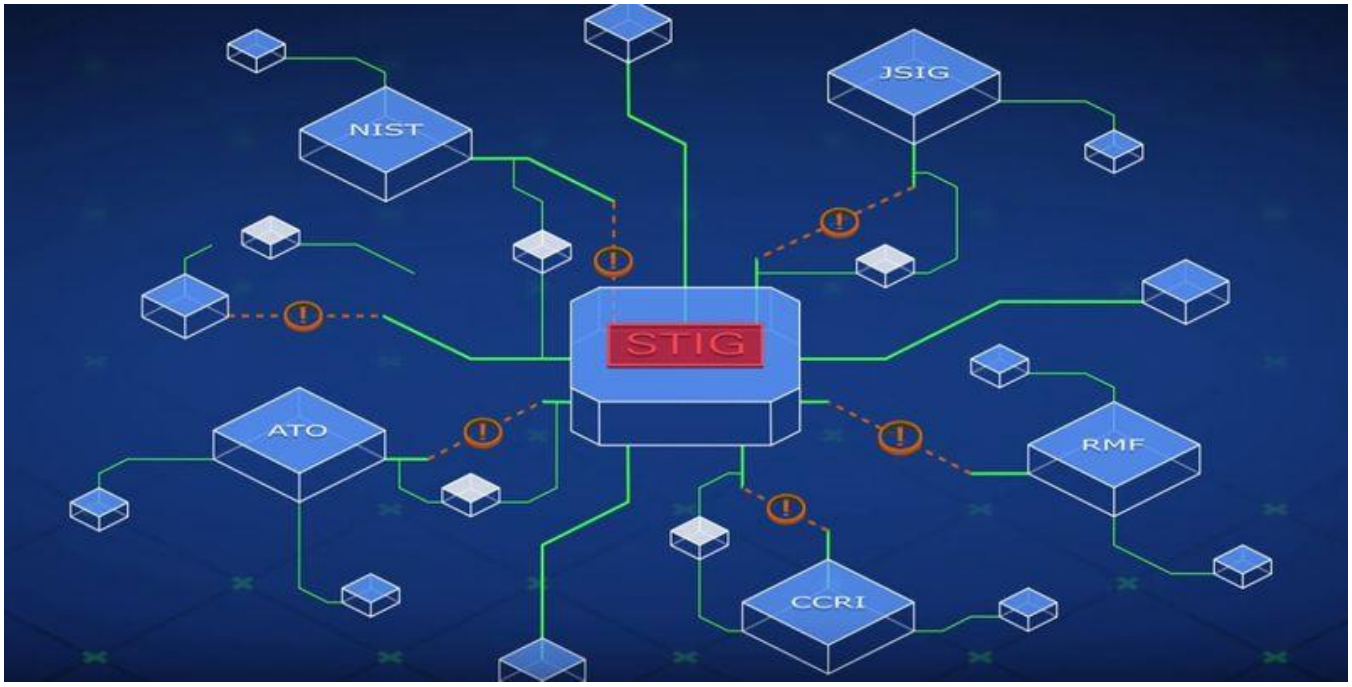
Finally, what we need at this stage is so branding new and innovating technology that would give us the chance to combat the cybercrime as well as the frauds anytime and anywhere. It's quite obvious everything got correlated with everything and the entire defense and intelligence landscape could seem as so complex and dynamic. The point is it's so necessary to think in advance and figure out how your threats think and what they really want, so far. Only then you would be in position to overcome all possible obstacles and talk about some sort of the best practice on.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, 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 and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. 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). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

The Foundation Common to Most Security Frameworks: Addressing Configuration Controls

By Jeff Elliott



We have entered the era of multiple security frameworks. Sometimes mandatory, often voluntary, security frameworks are created to provide federal and commercial organizations with an effective roadmap for securing IT systems. The goal is to reduce risk levels and prevent or mitigate cyber-attacks.

To accomplish this task, security frameworks typically provide a series of documented, agreed and understood policies, procedures, and processes necessary to secure the confidentiality, integrity and availability of information systems and data.

In the United States, the overarching framework is the National Institute of Standards and Technology (NIST) Cyber Security Framework. As part of the Department of Commerce, NIST is responsible for developing technical standards and guidelines for information security, among other things. Although the NIST standards apply to U.S. federal agencies and critical infrastructure, it is also widely used throughout the private sector.

In addition, specialized frameworks are less comprehensive and address specific aspects of information compliance. HIPAA, for example, provides security requirements to protect patient privacy; PCI in the retail sector address credit card processing, FedRAMP covers Federal cloud standards and the energy sector relies on the NERC Critical Infrastructure Plan. The list is long, and today even individual States are adopting their own cyber security frameworks (i.e., NYDFS).

If there is a drawback to security frameworks, however, it is that most provide a "30,000-foot view" of information security. Most identify potential risks as well as how to protect, detect, respond and even recover from cyber-attacks. Specific implementation steps, on the other hand, are rarely addressed.

However, there is one critical exception. At the core of most, if not all, the frameworks are a set of security-related controls that affect the security posture and/or functionality of the system.

Now, with established, recognized standards to accomplish this network security "hardening," along with new automation solutions, IT personnel have an effective starting point and foundation for implementing security frameworks.

Critical Security Controls and Configuration Settings

Critical Security controls provide specific safeguards for any and all systems connected to the network, including mainframe computers, servers, endpoints, attached devices, network appliances, operating systems, middleware, and applications.

The controls impact areas such as access control, audit and accountability, identification and authentication, contingency planning, incident response, configuration and change management, physical and environmental security. By changing configuration settings in hardware, software, or firmware, companies can improve their security posture.

Of all the available frameworks, NIST SP 800-53 provides the most comprehensive baseline for security controls in its latest published revision, which are prioritized and categorized by level of risk.

However, it is still up to the individual organization to establish company-specific configuration settings and changes to registry settings, account, file directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

This task often falls to information security and IT staff, many of whom lack the background and training in the area. This introduces the potential that systems will be under-protected and/or left with exploitable security gaps.

As a result, many organizations – even those that apply security frameworks voluntarily – are moving away from proprietary security hardening efforts in favor of recognized and established best practices. This simplifies deployment and configuration, enhances change control and automates auditing – significantly reducing risk.

Fortunately, NIST and other security frameworks point to either of two publicly available configuration standards, the Security Technical Implementation Guides (STIGs) or the CIS Benchmarks.

STIGs and CIS

The STIGs, published by the Defense Information Systems Agency, a support agency for the Department of Defense (DoD), outline hundreds of pages of detailed rules that must be followed to properly secure or "harden" the DoD computing infrastructure.

Although STIGs are mandatory for DoD agencies, any civilian agency and even commercial companies are welcome to use the STIGs.

For most commercial organizations, however, CIS is the security standard of choice. Originally formed in 2000, CIS Center for Internet Security, Inc. is a nonprofit organization with a mission is to "identify, develop, validate, promote, and sustain best practice solutions for cyber defense."

CIS employs a closed crowdsourcing model to identify and refine effective security measures, with individuals developing recommendations that are shared with the community for evaluation through a consensus decision-making process.

"Most organizations need a starting point that works today and that they can explain in simple language to their board on what needs to be done, and that is really where the CIS Benchmarks and CIS Critical Security Controls provide is that starting point," says Curtis W. Dukes, Executive Vice President & General Manager of the Best Practices and Automation Group at CIS.

Although there are minor differences between the STIGs and CIS Benchmarks, the two overlap and are pretty much interchangeable, says Brian Hajost of SteelCloud, an expert in automated security control compliance.

However, implementation of either STIG or CIS Benchmarks can be a challenge if the process isn't automated in some manner, due to the disparate requirements and configurations of networks.

Changes to security settings can also have unintended consequences. When the configuration settings of an application are re-configured, it can cause the installed application to "break," meaning it won't install and/or run properly.

"If the same security policies and configurations could be implemented on all systems, compliance would be a rather easy exercise," explains Hajost. "All applications respond to security policies differently. Because configuration settings have the potential to 'break' applications, the settings for each system, therefore, have to be uniquely adapted or tuned to each application in the operational environment."

For example, if some of the configuration settings of a Windows or Linux operating system on which an application operates are re-configured, the application will break. If an application requires specific settings to operate and those settings are prohibited or blocked, the application will fail to load or operate. And so on.

Often, server policies must be manually adjusted on an application by application, server by server basis – a painstaking task that can take many weeks and often falls to system administrators, application administrators or information assurance staff.

"There are thousands of IT staff that are tasked with addressing compliance manually, but many are not experienced or trained in it," says Hajost. "So, they muddle through, but the initial effort can take weeks or even months."

This is where automation can come into play. Software tools can automate implementation of a security benchmark, even across complex and disparate environments with varying security policies.

ConfigOS from SteelCloud, currently supports more than 6,000 standard CIS and STIG configuration settings. The software produces a domain-independent comprehensive policy "signature" including user-defined documentation and policy waivers. In this step alone, weeks, or months of manual work can be completed in an hour.

The signature and documentation are included in a secure, encrypted signature container that is used to scan endpoints (laptops, desktops, physical/cloud servers) without being installed on any of them. The time it takes to implement hundreds of configuration security settings on each endpoint is typically under 90 seconds and ConfigOS can handle multiple implementations at a time.

Hajost estimates automating the process reduces initial hardening time by 90 percent, while reducing system security policy maintenance expenses by about 70 percent.

Automated software also simplifies ongoing compliance, which in IT is a constantly evolving process.

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

Limiting Risk/Liability

Although automating configuration security settings can be of immense value, it is not intended to provide a complete cyber security framework. Still, the automation and associated documentation provided can play a critical role in reducing legal liability and attaining cyber insurance.

Dukes of CIS points to recently enacted legislation in Ohio and 2017 in California that establishes legal protections for organizations that have implemented an established security framework, such as the CIS Critical Security Controls, should the organization suffer a data breach.

“If a data breach gets litigated or adjudicated in a court of law, you want to be able to demonstrate to a judge or jury that you had reasonably implemented and followed a security best practice framework,” says Dukes.

Although many of the security frameworks are still voluntary in the commercial sector, Dukes has seen increased adoption from forward-thinking organizations in the retail, IT consulting and academia sectors.

“In the near future, more security frameworks are going to move from being voluntary to mandated,” explains Dukes. “Organizations should spend time getting educated and starting the process toward more effective cyber defense now, and not wait until it is mandated. There is too much at stake.”

For more information about ConfigOS from SteelCloud call (703) 674-5500; or visit www.steelcloud.com.

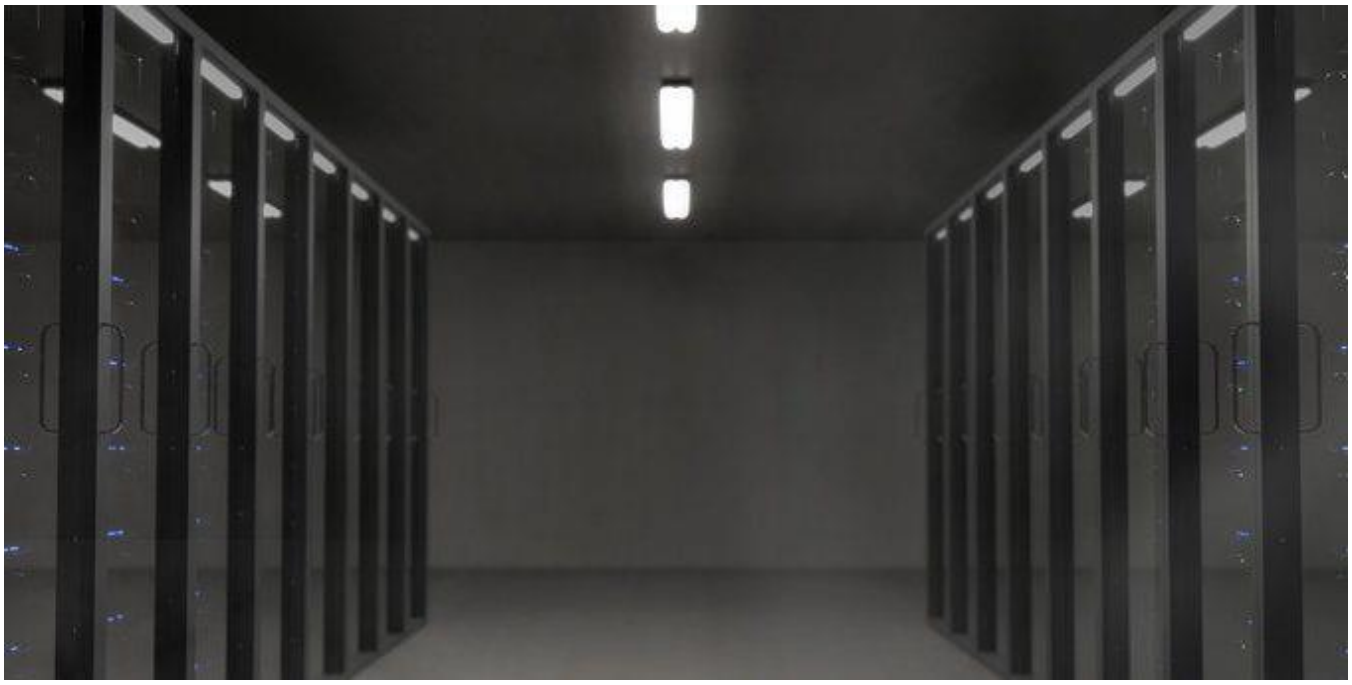
About the Author

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

Virtual Private Server Market to Hit US$ 2 Billion by 2025

The IT & telecom sector is expected to hold a virtual private server market share of over 25% in 2025 due to the growing demand for secured virtualized infrastructure

By Preeti Wadhwani, Assistant Manager (ICT) at Global Market Insights



The Virtual Private Server Market is set to grow from its current market value of more than $1 Billion to over $2 billion by 2025; as reported in the latest study by Global Market Insights, Inc.

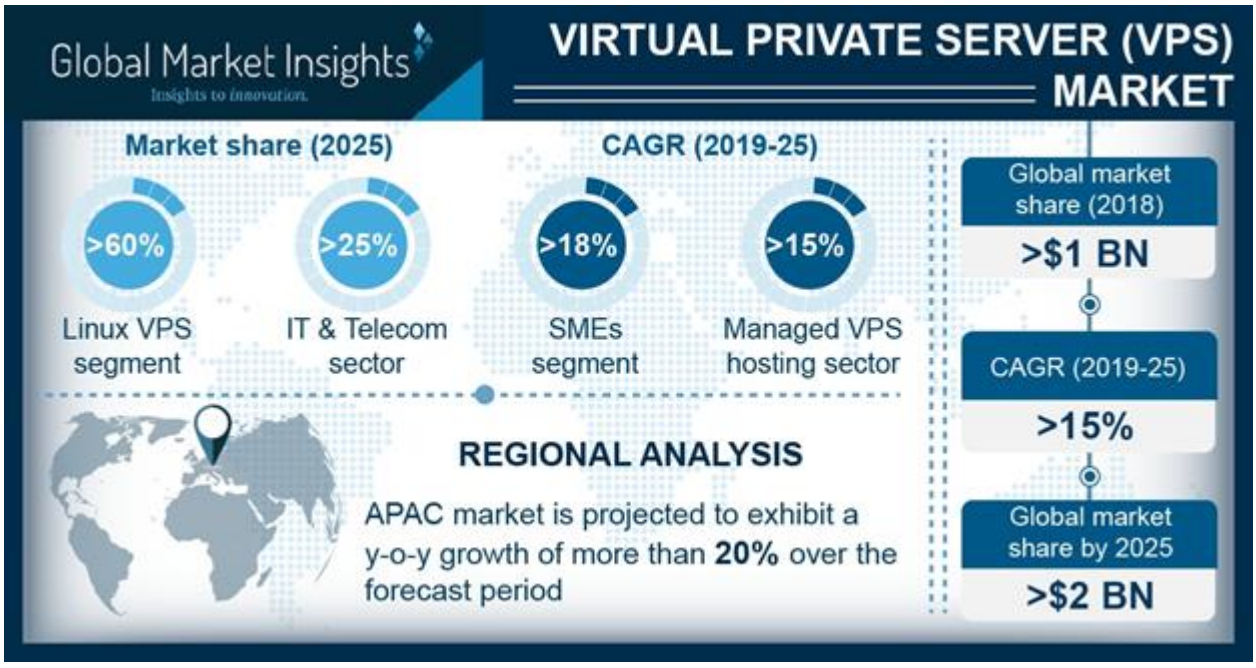
The virtual private server market growth is attributed to an increase in demand for secured hosting by enterprises, rising adoption of virtualization technology, and supporting digitalization initiatives in developing countries. The increasing adoption of cloud technology across the enterprises for hosting and supporting critical business functions is another factor contributing to VPS market share. The enterprises' approach for enhanced control over the servers without interference from the other shared servers is enabling them to migrate to VPS over the traditional physical servers.

The demand for cost-effective server hosting solutions is supporting the virtual private server market demand. Owning a private physical server involves huge capital and operating expenditure. The SMEs do not usually wish to invest in owning a dedicated server for hosting their websites. VPS helps enterprises in providing full control over their network resources without any involvement of the VPS provider. VPS users do not need to build their own physical server, which helps in reducing capital and operating expenses of enterprises. The use of virtual server significantly reduces the power requirement of physical servers. The virtual server also reduces the large space required for deploying and managing

physical servers. The VPS service providers, such as GoDaddy, Digitalocean, and DreamHost, provide different affordable VPS plans for the enterprises.

The managed VPS hosting segment is expected to grow at a CAGR of over 15% during the forecast period due to the increase in complexities in server maintenance & monitoring tasks. The server involves complex functions, which require special skills and training to handle these functions. These complex functions of server maintenance are handled by highly trained and competent experts in managed VPS hosting solutions. Also, managed VPS services offer a high degree of resource scalability. The customers can dynamically scale their usage of key server resources, such as RAM, CPU, and bandwidth, as per their computing requirements. Since major server maintenance & monitoring tasks handled efficiently by service providers, the customers can invest their in-house resources on their core competencies to generate new revenue streams for the organization

The Linux operating system segment is expected to hold a virtual private server market share of over 60% by 2025 due to its open source nature. The Linux VPS hosting provides flexibility, greater control, and functionality over the traditional Windows OS. It also provides a wide range of features with minimal hosting charges due to the elimination of licensing fees. It offers users the ability to regulate servers' space and bandwidth as per their changing requirements. Users get root access, just as on a dedicated server, providing greater control, more features, and ways to directly access files that are often faster than using the cPanel GUI.



Ubuntu Linux distribution is projected to hold around 30% virtual private server market share by 2025 due to frequent updates released for Ubuntu OS to match the changing enterprise network demands. Ubuntu VPS allows enterprises to scale up their resources, such as RAM, CPU, and bandwidth, to match their websites' growing needs. Ubuntu VPS system is partitioned, which helps in offering complete security to the enterprise server from other servers. This segregation ensures that enterprises' servers

will have their own guaranteed resources (RAM, CPU), which will remain unaffected by other users on the system.

The SMEs segment is expected to grow at CAGR of over 18% over the forecast period due to the increase in the adoption of virtualization technology. The availability of limited resources for maintaining the dedicated physical servers is enabling SMEs to shift toward VPS. The VPS helps SMEs to have a dedicated virtual server with a per pay-as-you-use model, which allows them to pay for the resources as per their requirements only. The VPS also helps in eliminating the space required for the physical server, which will reduce the cost of the excessive space required for bulky servers.

The IT & telecom sector is expected to hold a virtual private server market share of over 25% in 2025 due to the growing demand for secured virtualized infrastructure. The increase in the number of online cyberattacks is prompting IT & telecom companies to deploy secured servers. The VPS ensures better privacy and security for enterprises' files. The servers running in an isolated environment are protected from stability and security issues related to the other systems in shared server models.

The Asia Pacific virtual private server market is projected to exhibit a growth rate of over 20% during the forecast period due to an increase in government support for virtualized data centers in developing countries such as India and China. For instance, in May 2018, National Informatics Centre (NIC), a premier science and technology organization of Government of India, launched a National Data Centre in Bhubaneshwar to offer uninterrupted secure hosting for various e-governance applications. This new data center helped in extending government support for 35,000 virtual servers.

The VPS service providers are partnering with cloud service providers to enhance their virtualization capabilities and sustain in the virtual private server market competition. For instance, in June 2019, GoDaddy, a leading VPS hosting service provider, partnered with Amazon Lightsail, Amazon's cloud platform, to simplify WordPress virtual server management. This partnership helped WordPress customers in easily managing their server instances for free. The key players operating in the VPS market are Amazon Web Services, Rackspace, Digitalocean, DreamHost, United Internet AG, A2 Hosting, Linode, Inmotion Hosting, Plesk International, Tektonic, Vultr Holdings Corporation, GoDaddy, Liquid Web, OVH Group, Endurance International Group, Kamatera, Inc., Bluehost, Savari Technologies Pvt. Ltd., and cPanel, LLC.

Source: www.gminsights.com/pressrelease/virtual-private-server-vps-market

About the Author

Preeti has more than 5 years of experience in market research and consulting. She has hands on expertise in ICT, Semiconductor and Electronics industry with focus on niche and emerging technologies including cloud, software-define, IoT, virtualization, containers and analytics-based markets. She has worked with global clients in the ICT, Semiconductor and Electronics industry with consultative approach to identify market growth opportunities through competitive analysis, bench-marking, forecast, and new market penetration. Preeti can be reached online at (EMAIL, TWITTER, etc..) and at our company website https://www.gminsights.com/

Stay One Step Ahead Of Hipaa Compliance

By Adnan Olia, Chief Operating Officer, Intradyn

HIPAA compliance is a challenge — ask anyone in the health care industry and they'll likely tell you the same. Health-related organizations at every level, from small private practices to hospitals, struggle to stay within the scope of HIPAA compliance, in large part due to the fact that HIPAA is so broad.

For a bit of context, let's take a look at how HIPAA is defined. Passed in 1996, the Health Insurance Portability and Accountability Act (more commonly known as HIPAA) "establishes, for the first time, a set of national standards for the protection of certain health information […] The Privacy Rule standards address the use and disclosure of individuals' health information — called 'protected health information' by organizations subject to the Privacy Rule — called 'covered entities,' as well as standards for individuals' privacy rights to understand and control how their health information is used." The U.S. Department of Health & Human Services (HHS) defines Protected Health Information (PHI) as "any individually identifiable health information held or transmitted by a covered entity or its business associates."

In summary, HIPAA exists to protect patients' private data against fraud and theft and dictates how that data can be distributed. If it seems relatively straightforward, that's because it is — until you factor in how HIPAA is enforced. HIPAA applies to PHI that's transmitted electronically and "covers a large range of data transfer protocols, from handling face-to-face interactions to transferring and backing up data." Because the channels through which we communicate have expanded to include digital platforms, such as social media, text messaging and email, it's easy to see why it's so challenging for organizations to maintain HIPAA compliance. In fact, many health care organizations that think they're HIPAA compliant (or at least claim to be) actually are not.

That's troubling for a few reasons: First and foremost, it leaves health care records (and patients' private information) vulnerable to data breaches. Between 2009 and 2019 there have been 2,546 significant health care data breaches (those involving more than 500 records), resulting in the theft or exposure of 189,945,874 health care records. Also, health care orgs deemed non-compliant face harsh penalties. Fines for HIPAA violations can range anywhere from $100 to $50,000 per violation, with a maximum penalty of $1.5 million per year — and that's on top of potential civil and criminal penalties.

Given the severe consequences of failure to comply with HIPAA standards, it's imperative that health care orgs do everything within their power to get their affairs in order, starting with the following:

- **Be better prepared for eDiscovery requests and HIPAA audits.** When it comes to HIPAA audits, it isn't a matter of *whether* you'll be audited, but *when*. There are measures you can take, such as thoroughly documenting HIPAA policies and procedures within your organization, conducting routine risk assessments and creating in-depth training materials, to prepare for when that day inevitably comes. It's also in your best interest to implement a software solution that makes it easier for your legal team to respond to eDiscovery and litigation requests to streamline the audit process.

- **Properly maintain — and dispose of — patient data.** The key to properly maintaining patient data is to enforce strict data security standards. The HHS defines these standards under its Security Rule; requirements include detailed administrative and technical requirements, as well as implementation specifications and organizational and documentation requirements.

  As far as the disposal of patient data is concerned, PHI cannot be disposed of unless the individual identifying information is removed or destroyed. This is easier said than done in the world of electronic communications, and the HITECH government mandate complicates things further, so be sure to do your due diligence prior to disposing of anything.

- **Maintain an email archive.** Email archiving isn't required under HIPAA's Security Rule but storing all electronic communications in a single location can go a long way toward ensuring HIPAA compliance. That's because maintaining an email archive makes it easier to screen incoming and outgoing emails, create custom retention policies, index and search emails, monitor who has access to your organization's emails and quickly recover any emails that were accidentally deleted.

- **Develop a comprehensive HIPAA disaster recovery plan.** One of the administrative safeguards outlined in the HIPAA Security Rule is that health care orgs must have a contingency plan in place, one that includes a detailed disaster recovery plan.

That plan should consider the following:

  - Does the plan address issues specific to my operating environment?
  - Is a copy of the plan ready and accessible at more than one location?
  - How will operations be conducted in the event of an emergency?
  - Which members of my organization will be responsible for carrying out operations in the event of an emergency?
  - How will confidential data and safeguards for that data be restored after a disaster?

Even health-related organizations that are diligent about HIPAA compliance make mistakes from time to time. Don't let that discourage you — so long as you make a good faith effort to cover all of your bases, you can provide your patients with peace of mind and rest assured that your business is well-protected.

About the Author

Adnan A. Olia is a senior member of the Intradyn team and is responsible for keeping an eye on the regulatory and technological marketplaces. Adnan provides thought leadership in the archiving and compliance sector to help Intradyn understand the latest trends in business innovation.

can be reached online at LinkedIn: linkedin.com/in/adnanolia and at our company website /www.intradyn.com

The Dangers of HTTPS: When Secure Is Not Safe

By Eric H. Perkins, Sr. Security Risk Analyst, Edelman Financial Engines

The web, as we know it, is going through a major shift to encrypt all traffic to better secure user data by fixing many serious vulnerabilities, like eavesdropping and content hijacking. In fact, you've probably noticed that major web browsers even warn you before connecting to a non-secure website. So, when you see that green lock icon in the URL bar that means it's safe, right? **Wrong.**

Being secure, simply stated, is not the same as being safe. The term "safe" implies the site in question is free of malware and/or nefarious activity. In the context of your web browser, the term "secure" simply means that your information is being properly encrypted while connected to the site. It's this term that is being visually represented with the green lock icon found on webpages that start with HTTPS, a secure data networking protocol. Ideally you want to only interact with sites that are both safe and secure.

The HTTPS protocol was designed to help protect data in motion by encrypting each internet session. This encryption is what protects your data from being accessed if intercepted. However, it doesn't ensure the site is trustworthy and it wasn't designed to protect you from malware and/or phishing attempts.

The once coveted “green lock” that was mainly used for financial transactions is now available for free to anyone; including malicious actors. In fact, it has been reported that 58% of all phishing related websites are now hosted using HTTPS. It is for this reason that no one should assume a website is “safe” just because it’s being hosted using HTTPS. It’s still very important to visually identify the lock icon when transacting with any website but understand that it doesn’t necessarily indicate that a site is legitimate. Attackers mimic a target website by simply copying the code from a legitimate site and pasting it to their malicious site; making it nearly impossible to differentiate the good from the bad.

Therefore, you should never click on links in suspicious emails. Instead, get into the habit of using a password manager to store known good bookmarks or reputable search engines to visit sites of interest versus clicking on links provided within emails. Additionally, always verify the domain address within the URL bar as well as identifying the secure lock icon before providing any form of personally identifiable information or login credentials. For those who want extra validation, websites like VirusTotal can be leveraged to scan and verify if the URL is considered “safe”.

About the Author

Eric H. Perkins is currently the Sr. Security Risk Analyst for the largest independent investment advisory firm in the Nation. Before joining Edelman Financial Engines, Eric began his career in network security while serving as an active duty Information Security Officer in the US Army both in country and while deployed to Afghanistan. Eric holds numerous IT certifications to include CISSP and is a relentless advocate for security awareness. Eric can be reached at eperkins21@protonmail.com or online at https://www.linkedin.com/in/erichperkins/.

Going for Gold – Why Hackers Are Looking For Active Directory Golden Tickets

Matt Lock, Director of Sales Engineers, Varonis

Any business that has more than a handful of employees is likely to have a reasonable amount of physical property that needs locking up – safes, individual offices, equipment, garages and, not least, of all the outside doors and windows to the premises. In order to make sure that everyone in the organisation can access what they need to, particularly in the event of a keyholder being on holiday or off ill, a copy of all the keys is likely to be held in a central place. This will ideally be a lockbox, to which only a couple of trusted employees have a key.

To burglars, these lockbox keys offer unfettered access to an organisation's entire estate. If they can get hold of one key, no matter how hard this might be, they are able to get hold of every key.

In the digital world, the equivalent of the lockbox key is the credentials of the data administrator on an organisation's Active Directory, known as a 'Golden Ticket'. This provides threat actors with permission to access anything and everything on an organisation's network – files, logins, system settings and so

on. As in the real world, gaining such a level of access is rare, but potentially catastrophic for an organisation.

However, even if they gain lower-level access to Active Directory, threat actors can start working their way through a system and escalating their privileges until they hit the motherlode. In fact, Active Directory is critical to every step of the cyber kill chain from reconnaissance, to denial of service, to exfiltration.

Knowing your weaknesses

Active Directory employs Kerberos as its primary authentication security mechanism. Kerberos uses tickets, also known as Ticket Granting Tickets (TGTs), to authenticate users. While Kerberos offers incredibly powerful protection through strong cryptography and third-party ticket authorisation, there are still a number of vulnerabilities threat actors can exploit to access Active Directory.

Aside from the Golden Ticket attack mentioned above, popular Active Directory attack methods are Pass the Hash; Pass the Ticket; and the Silver Ticket. Many of Active Directory's vulnerabilities are down to the almost archaic NTLM encryption, which is very weak by today's standards. For instance, in Pass the Hash, threat actors can use brute force to uncover the password of an NTLM hash to authenticate to Active Directory. In fact, to perpetrate a Golden Ticket attack, cybercriminals need the NTLM hash of the hidden KRBTGT account that encrypts the authentication tokens to the domain controllers.

Aside from the technical weak points, threat actors will try to exploit the human element to break into an organisation's systems. When looking to extract login credentials from staff, cybercriminals will use deceptive emails that either contain malicious links and attachments or purport to be from someone official demanding a username and password.

Proactive security

There are a number of steps an organisation can take to prevent cybercriminals accessing their Active Directory and stealing the keys to the kingdom. The first is to know everything there is to know about your own Active Directory. What are the naming conventions? Security policies? Who are the users? And so on. Knowledge is power and by having this information to hand means that you have the power to better protect Active Directory.

This knowledge must be kept up to date with the use of regular monitoring so that any unusual logins or changes can be spotted and acted upon. To monitor everything on Active Directory in a thorough and timely way would be almost impossible to manage manually. Fortunately, automation can serve as a watchdog and alert the security team to any suspicious behaviour or activity.

Also worth considering is placing those valuable domain controllers on a server that is not directly connected to the internet. This will make life harder for attackers as their lateral movement and potential to escalate privileges will be curtailed.

On the subject of privilege, organisations should implement a policy of 'least privilege'. This states that staff only have access to those files and folders necessary to do their jobs. 'Least privilege' restricts the ability of cybercriminals to move through a network as each account is limited in what it can access.

A multi-layered approach

Even with the best cybersecurity tech in the world, threat actors will still try to break into a system by preying on human weakness. To mitigate this, staff need to be trained to become cybersecurity aware, including how to create strong passwords and to recognise the traits of a phishing attack.

As a further layer of defence, system administrators should have an account for day-to-day use and one specifically for performing system changes. Such admin accounts should be restricted to assigned systems to limit the potential of cybercriminals accessing an entire network by breaking into just one account.

By proactively implementing this multi-layered approach to cybersecurity, businesses can ensure cybercriminals don't strike gold in their efforts to access Active Directory.

About the Author

Matt Lock, Director of Sales Engineers, Varonis.Matt has more than 17 years' experience in the field of Network Security, which includes extensive contracts with many global businesses, including BP and JPMorgan. Specialising in risk assessment, risk management, policy compliance, security reviews and managing network behaviour anomaly systems, Matthew now leads Varonis' sales engineering team in the UK, Ireland and Middle East, ensuring the team is helping customers and partners from a range of sectors in data governance projects, and organizing, securing and managing their unstructured data.Matt can be reached at @Varonis and at our company website https://www.varonis.com/

Overcoming Zero Trust Challenges in the Federal Government

By Lisa Lorenzin, Director of Emerging Technology Solutions, Zscaler

As federal agencies deploy mobile-friendly, cloud-based infrastructures, cyber threats are also evolving to prey on vulnerabilities in these new environments. Agencies need to take a proactive approach to stay a step ahead and keep data safe, regardless of location and device.

To combat these threats, and take advantage of the TIC 3.0 guidance, federal IT leaders are turning to zero trust security models. The concept evolved in the private sector, as federal agencies have been slower to explore zero trust models due to a combination of factors, such as perceived liability, resistance to change, regulatory and certification requirements, data classification, and the need to work across multiple functional areas.

When choosing a zero trust solution, agencies need to balance access/productivity/performance and security concerns—at the same time, they need to future-proof their environments. The question is, "Can zero trust solve today's and tomorrow's challenges while meeting federal security guidelines?"

Defining Zero Trust

Zero trust is a bit of a misnomer—the true goal is actually to *establish* and *maintain* trust, so we can enable users to access the resources they need to support their missions. We start off by not implicitly trusting anyone, then figure out who we can trust, how we know we can trust them, and what we trust them to access.

The initial intent of zero trust was to help control on-premises user access to internal applications. Today, the same concept applies to users accessing private applications in externally hosted environments. Federal IT leaders should think of zero trust as "context-based trust." It is not a matter of whether the user is on or off the network, or the application is internal or external, but whether the user is authorized to access the application.

Federal IT leaders will need to ask themselves several questions when considering zero trust adoption: "What will this solution look like? How do we scale it? How do we get access to resources through it? How do we get the visibility we need? How do I meet the Trusted Internet Connection (TIC) mandate if the solution is cloud based? Is my provider FedRAMP authorized?"

A Phased Approach

As agencies develop zero trust solutions, they need to consider how to integrate them with their current architecture and security controls. Agencies need solutions that provide seamless access for the user and full visibility and control for the backend administrators, regardless of the device or the user's location.

Many federal agencies already have elements of zero trust in their infrastructure and should not require significant new technology acquisitions. Endpoint management, Continuous Diagnostics and Mitigation (CDM), software-defined networking, microsegmentation, and cloud monitoring are components of zero trust that may be in place.

Federal IT leaders should take a phased approach to simplify solutions into relevant use cases that advance mission goals. To support this approach, they should make two initial determinations. First, identify the most significant pain points or areas of vulnerability. Second, choose one of those challenges and identify an affected user community as well as the resources they need to access.

"You have to understand the importance of your data and how you access it," said Jeffrey Flick, Acting Director, Enterprise Network Program Office, National Oceanic and Atmospheric Administration, at an ACT-IAC zero trust panel in May 2019. "This goes back to your mission, and everybody has different kinds of missions, so zero trust implementations will need to be very scalable."

Once both are specifically identified and tightly scoped, agencies can run a pilot. Agencies don't have to buy a set of appliances, rack and stack them, load-balance and protect them, and so on—instead they can sign up for an initial subscription in a cloud-based, scalable solution. If successful, agencies will have a better understanding of the potential benefits of expanding deployment across the organization. Zero trust adoption should be a journey focusing on short-term accomplishments toward long-term goals.

Mission-Driven Effort

One fundamental truth across public and private sectors is that people fear change—and implementing zero trust requires a "whole-of-agency" effort. Since zero trust solutions are new to government, implementations shouldn't be strictly driven by IT; they should be a mission-driven effort.

Zero trust by nature impacts program security, risks, and performance. To assess the risk of adopting zero trust technologies, agencies should consult an internal expert with enough technical background and policy awareness to assess possible solutions and understand potential benefits of zero trust technologies. Through collaboration, program and IT leaders can design and implement zero trust together to ensure success and compliance with policies such as FedRAMP, TIC, and FISMA.

Private/Public Partnership

One key question to consider before adopting zero trust is who to choose as your partners. Industry partners need to understand an agency's unique needs and risk profile—there is no one-size-fits-all solution.

The federal government is better positioned now than ever to adopt zero trust. And implementing zero trust has many benefits beyond improved cybersecurity, including seamless user experience, better performance, lower cost, and consistent control and visibility regardless of user and application location.

To learn more, read the ACT-IAC Zero Trust White Paper. It provides key concepts, recommended steps, information on required federal certifications, and lessons learned working within federal environments, as well as details on pilot programs—putting you on the path to successful implementation.

About the Author

Lisa Lorenzin is Director of Emerging Technology Solutions for the Americas at Zscaler, specializing in secure access to private applications and a contributor to open standards for endpoint integrity and security automation from the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF). She's worked in a variety of Internet-related roles since 1994, with over 20 years of focus on network and information security, and is currently concentrating on zero trust networks, software-defined perimeter solutions, and seamless user experience across cloud and mobile environments. Lisa can be reached via email at llorenzin@zscaler.com or on LinkedIn at https://www.linkedin.com/in/lisalorenzin. You can read other articles by Lisa on the Zscaler website: https://www.zscaler.com/.

Is Your Organization Driving the Getaway Car for Cybercriminals?

A Reality Check on Ethics and Technology to Thwart Data Breaches and Fraud

By Simon Marchand, Chief Fraud Prevention Officer for Nuance Communications

3.6 trillion – that's the dollar amount that fraud costs the global economy each year. Let that sink in for a minute: $3.6 trillion.

Odds are you can name any industry, and it's been affected by a data breach. In fact, some of the largest data breaches in 2019 have included everything from a fast food chain and large-scale retailer to a global car manufacturer and an IT outsourcing and consulting giant. Bottom line: Every organization is a target, with the potential for major negative, headline-grabbing fallout.

And although the case for why companies should protect their data is clear—companies lose less money and customer information is kept safe from predators—what's not often addressed are some of the more disconcerting aspects of data breaches. Namely the ethics of allowing that 'target' status morph into a 'win' for cybercriminals.

Which begs the question: What's the responsibility of corporations toward fraud and identity theft?

Of course, organizations have the obligation to protect their customers' information. If not by law, it is a moral responsibility when people trust you with so much sensitive information. But I think it goes beyond that. Many would argue (myself included) that organizations have a corporate social responsibility to protect not only their customers from fraud, but to act more widely to prevent fraudsters from using information obtained elsewhere. Not only should we prevent data breaches leading to information from being stolen, but corporate responsibility should guide us in preventing the information from being used in our own organization. And, ethical standards and rules supported by technology need to be part of every single organization's cybersecurity strategy.

Understanding Data Breach Fallout: From the Dark Web to Funding Other Crimes

Perhaps one of the best ways to articulate why organizations need to step up their cybersecurity strategy is to better understand what happens to stolen data.

The market for personally identifiable information (PII) on the dark web is massive, and over the years, fraudsters have become more sophisticated in terms of their ability to acquire more than just one PII item. For instance, the 2017 Equifax data breach revealed not just the names but also the social security numbers, birth dates and addresses of almost half of the total U.S. population (143 million individuals)—critical, personal information that is like gold to fraudsters. And, although according to The Identity Theft Resource Center the overall number of U.S. data breaches tracked decreased the following year by 23% from 1,632 data breaches in 2017 to 1,244 in 2018, the reported number of exposed records containing sensitive PII jumped an alarming 126% between 2017 and 2018 to more than 446 million.

The shelf life for this type of stolen data is oftentimes long, being made available to the highest bidder on the dark web and then sold at a couple dollars a piece to bulk pricing for credit card numbers. When illegally acquired user-generated passwords and PINs are added to the mix, this underground marketplace can be quite lucrative for cybercriminals who use the profits to purchase goods as well as fund terrorist groups and other criminal activities.

This all being said, in the case of the Equifax data breach, is Equifax the only responsible organization, or should we also look at organizations with too little controls in place that will allow new accounts being setup using the Equifax breach information? What's the extent of a corporation's responsibility toward the usage of stolen data? Is it just global risk assessment and accounting for potential losses in the overall budget or does it extend beyond that?

Furthermore, what role did the corporation accepting the risk or the bad debt play in facilitating such criminal activities?

Bottom line: the focus on protecting our customers' data is oftentimes insufficient. We must also put controls in place to prevent fraudsters from exploiting our organizations for a profit, with previously stolen data.

Are You Taking Corporate Social Responsibility or Driving the Getaway Car?

While it is true that consumers need to take it upon themselves to use the available tools designed to protect them, such as using multi-factor authentication or opting for biometrics over user-generated PINs and passwords, corporations also need to step up to the plate big time to thwart these attacks. They need to understand that, as a target, they must ensure they are putting the proper controls in place to stop fraudsters with stolen information from getting into their own accounts not only because it's the right to do morally, but also because the reputational risk of doing too little can be tremendous.

Although the global voluntary International Standard ISO 26000 identifies consumer data protection and privacy as a key consumer issue that corporations should be addressing, this is just a guidance for organizations in the public and private sectors that want to operate in a socially responsible manner. It is not the law of the land.

To help pivot companies toward taking the right cybersecurity steps, a handful of U.S. lawmakers are working to enact legislation to prosecute companies and their executives who fail to protect consumer privacy. In Canada, measures have already been taken to remedy this issue. The Personal Information Protection and Electronic Documents Act (PIPEDA) requires Canadian businesses to report any breach of privacy (any loss or mishandling of PII that might lead to a real risk of significant harm such as financial loss or identity theft) to the Office of the Privacy Commissioner of Canada. According to PIPEDA, "Failure to report the potential for significant harm could expose private-sector organizations to fines of up to $100,000 for each time an individual is affected by a security breach, if the federal government decides to prosecute a case."

In the U.S., the Corporate Executive Accountability Act proposed in early April by Sen. Elizabeth Warren (D-Mass.) would impose jail time on corporate executives who "negligently permit or fail to prevent a violation of the law that affects the health, safety, finances or personal data" of one percent of the population of any state. While in spirit this proposal is a nice attempt to address this massive growing issue, it only applies to companies that generate more than $1 billion in annual revenue and to companies that are either convicted of violating the law or settle claims with state or federal regulators, which ultimately does not address most data breaches given their size and scope. A slightly more aggressive data privacy law proposed by Sen. Ron Wyden (D-Ore.) would give executives up to 20 years in prison for violations of their customers' privacy.

But should companies wait for laws to be put in place, or should they be ahead of the issue?

How Can Businesses Grab Hold of this Issue?

For starters, it is a shared responsibility among CISOs and IT teams as well as fraud and operation teams to understand the fraudulent entry points into their businesses. As the channels for businesses grow, so too do the points of entry for fraudsters. Fraudsters do not approach account access in a siloed manner. Instead, they take advantage of the growing channels and devices—mobile apps, contact centers, smart speakers, etc.—using them all as entries points into an organization. In addition, new and repeat career criminals attempt to steal from institutions every day. If they find a weakness in a channel, they will continue to go back to that channel and then turn to another one when that initial channel no longer works. And, even if some industries find the number of frauds committed on the voice channels might seem to go down, call center agents are still heavily targeted by fraudsters and socially engineered to

obtain valuable information that is then reused on other channels against the same organization. Relying on passive biometrics authentication is the best way to make the call center more secure against experienced fraudsters.

Second, to truly combat fraud, businesses need to have a cross-channel security approach that stops fraudsters wherever and however they attack. In other words, businesses need to invest in the right tools to protect them, and make sure that these technologies are capable of fraud detection and fraud prevention, as well as authentication. Taking a multi-authentication approach is critical, with proven technologies like voice biometrics, behavioral biometrics, device prints, face prints working in tandem to cover all channels. The goal is to stop focusing our efforts on the attack vectors but rather on the attacker themselves, who can be identified by multiple biometrics. Once we change our perspective on how to combat fraud, we can be one step ahead.

Third, companies need to bring ethics to the forefront. This means acting in a socially responsible manner. They need to stop categorizing fraud as a normal cost of doing business. It is not. They also need to understand that turning a blind eye to this crime is fostering other crimes. As such, organizations must try to stop fraud and should implement technologies facilitating the reporting of criminal activity to law enforcement agencies. It's not just better for business, it's the right thing to do.

Biometrics technologies including voice have already prevented hundreds of millions of dollars from getting into the wrong hands. For instance, HSBC recently reported that voice biometrics has helped it weed out fraudsters and prevent over £300 million ($336 million+) from falling into the hands of criminals since the software was deployed in the UK. Royal Bank of Scotland's Head of Fraud Strategy and Relationship Management also credited voice biometrics for helping the financial institution discover that among the 17 million inbound calls it received in less than a year, one in every 3,500 calls was a fraud attempt.

The use of biometrics enables anti-fraud teams to now link seemingly unrelated cases to a small number of individuals, and it allows them to build solid cases with strong evidence that can then lead to prosecution.

Ethical decisions coupled with the latest in biometrics technologies are the only way that corporations can start having a real, concrete impact in the fight against fraud and targeting the fraud problem to its root.

About the Author

Simon Marchand, CFE, C.Adm., is Chief Fraud Prevention Officer for Nuance Communications' Security and Biometrics division. Based in Montreal, Marchand plays a strategic role in evangelizing fraud prevention solutions, delivering product roadmap guidance and fostering ties with the fraud prevention community. Marchand brings over a decade of experience in telecom and banking to his role as Chief Fraud Prevention Officer. Prior to Nuance, he held key fraud prevention positions at Montreal-based Laurentian Bank, Bell, and most recently Québec's Order of Chartered Administrators, where he managed its professional inspection program.

Simon Marchand can be reached online at his LinkedIn account and at our company website https://www.nuance.com/en-gb/index.html

Let's Come At The Cybersecurity Skills Gap From A New Angle

By Aidan McCauley, Vice President of Technology Investments, IDA Ireland

Chess players know the satisfaction of solving a skills gap. Succeed in advancing a pawn completely across the board and it can become a queen, bishop, rook, or knight. The player now has a piece with more ways, more angles, to come at opposing pieces.

One skills shortage problem in the larger world is the lack of individuals trained to thwart cybercriminals' malicious actions. The size of the shortage is daunting. Worldwide over the next five to seven years, businesses could find themselves unable to staff north of three million positions for cybersecurity professionals.

In the United States the cybersecurity professional's shortage is an equal opportunity problem, with firms in every part of the country experiencing some degree of talent shortfall. Comparisons to chess notwithstanding, this is no game, although it can seem that cybercriminals are continuing to make the world their playground with impunity. For example, security firm Cybersecurity Ventures says that 2021 will see costs from cybercrime jump by $3 trillion from 2015. And just a few of the concerns that the December 2018 McAfee Labs Threats Report notes are underground forums role in pumping up cybercriminals' effectiveness, the emergence of new malware families, and the rise of IoT malware 200% over the previous year.

What's at Stake

The cybercrime problem can rob us of, or slow progress toward, solutions that include preventing, diagnosing and treating diseases by using the data medical wearables gather. Or hinder real-time data collection that can let factories change when and how machines are used in order to cut power consumption, aiding sustainability.

Industry and government alike have a vital interest in defending against actions that hurt our ability to lengthen patients' lives, create environmental sustainability, and keep us reliably connected with one another—to name just a fraction of what a secure cyberworld enables.
Despite this common interest, one could argue that fighting cybercrime has been well-intentioned, with noteworthy gains from both business- and government-led efforts, but nevertheless not as powerful as needed.

So why not use every move available to us, including that of bringing industry, cybersecurity agencies, the government, researchers, and academia together? Cyber Ireland has been inaugurated to make that move. It is a cluster organization set firmly upon, among other pillars, the recognition of coordinated efforts' multiplied worth when it comes to massive problems. Top U.S. tech firms — like Google, Microsoft, Facebook, IBM, Dell, SAP, Cisco and others with a strong vested interest in digital security — located in Ireland helped lay the groundwork for this expansive cybersecurity initiative. The foreign direct investment agency IDA Ireland and Cork Institute of Technology created Cyber Ireland, Representatives from cybersecurity agencies, government, industry and academia make up its board. Dr. Eoin Byrne, cluster manager of Cyber Ireland, rejects the idea that the organization's objectives extend only to filling the cybersecurity skills shortfall. It's not only that we can address issues that the industry currently faces and will face beyond just security, it's also that we have the advantage of building upon U.S. businesses, Irish government, and academia already having put their heads together as far back as April 2017 to understand the key challenges for the cyber security and technology sector," Byrne says.

Virtuous Cycle

Another plus for Cyber Ireland? It launches at the same time that those who are part of the region's supportive cybersecurity ecosystem are finding that the ecosystem's growth is bringing benefits that in turn lead to more growth and more benefits—a virtuous cycle. For example, the "pure-play" security companies, e.g., McAfee, Symantec, Trend Micro, have added core engineering to locations in Ireland, representing expansion beyond support and shared services. More evidence that companies are confident that cutting-edge cybersecurity solutions can be fostered here: Galway is the site of the HP Enterprise Global Cyber Defense Center; In 2016, Docusign opened its Cybersecurity Centre of Excellence in Dublin to protect its customers' data and privacy.

Also fueling this thriving ecosystem are the cybersecurity professionals being trained by the well-funded Cybersecurity Skills Initiative (CSI). Like Cyber Ireland, CSI has at its core goals which were set and/or

clarified during the above-mentioned collaboration among academia, U.S. firms, and the Irish government. CSI-graduated cybersecurity professionals will within three years be employed by multinationals in Ireland, and by other businesses as well, although it is expected that multinational firms will have the majority of the hires. Trained graduates are already part of the cybersecurity workforce, and the number of graduates in three years will be around the 5,000 mark, while the number of participating firms is planned at 4,000 firms.

Engaging closely with their counterparts at Skillnet, Ireland's corporate-government training partnership, CSI educators have designed a cybersecurity skills curriculum. In doing so these educators relied for core content on input from U.S. companies as to what's needed to assure successfully trained professionals. IT professionals being trained by CSI can participate in cross- and up-training. Programs come in several varieties including 12-week courses, graduate programs, and two-day foundational courses for non-technical employees.

At the same time that CSI is training the individuals who will devise the strategies vital to ongoing cybersecurity, Cyber Ireland will be aggressively pursuing an important goal: seeing to it that resources and knowledge flow freely among R&D in academia, business enterprises, and cybersecurity agencies.

Taking a new angle on cybersecurity with innovative and collaborative action is making the right move.

About the Author

Aidan McCauley is Vice President of Technology Investments at IDA Ireland to contact him email: aidan.mccauley@ida.ie or for information, visit https://www.idaireland.com/. Optional- infographic - https://www.idaireland.com/newsroom/publications/why-ireland-for-cyber-security

Facing the Reality of VPN Security Flaws, And How to Overcome Them

NEXT UP, SOFTWARE DEFINED PERIMETERS

By Don Boxley, CEO and Co-Founder, DH2i

Virtual private networks (VPNs) have served as a valued tool on most data and cyber security professionals' tool belts. However, today's data reality -- where cloud, IoT, big data, and other progressive applications reign supreme -- many are learning the hard way that traditional VPNs simply cannot support today's data security demands. Others are unknowingly in for an inevitable rude awakening. However, more proactive organizations are already exploring or have deployed more advanced solutions that are able to meet today's security requirements, as well as provide additional IT, business and budget benefits.

A Brief Look Back

For many years now, the VPNs have served as the most common way to "securely" access networks. Unfortunately, however, while the main business advantage of using a VPN is generally regarded as improved security via the technology's end-to-end encryption capabilities, the fact is that VPNs not only expose sensitive data to increased security risks, but in today's cloud-based environment, they actually *magnify* those risks exponentially.

One of the main ways VPNs endanger data security is that enterprises often end up having to manage multiple types of VPN connections to accommodate the networking gear of each third party. (The alternative—requiring vendors to use just one VPN—can be very costly.) Not only is this juggling act an administrative nightmare, but it also creates much more room for lateral movement attacks, since it massively expands the network surface area that's exposed and vulnerable since users gain access to a "slice of the network," so to speak. Not only do inbound connections create attack surfaces, but without application-level segmentation, it's impossible to reduce attack surfaces, leaving networks vulnerable.

Why Now?

Why now, when VPNs have been the venerable "go-to" for secure endpoint connections that safeguard data from hackers? The answer lies in the fact that VPN technology was not designed for a world of mobile devices, virtual teams, and third-party vendors tapping into the network; it was made with traditional on-premises security in mind. The VPN model came into being in a different era—when an on-premises, non-cloud environment was king, with physical servers and virtual machines. In such a world, VPNs were appropriate. But today, IT is much more likely to incorporate hybrid cloud settings, blending on-premises with public/private cloud environments. Each time you layer on another IT scenario, the chances for data exposure and security breaches increase.

This indicates a significant issue with continuing to buy into the myth of VPN security. Digital transformation has made it much more difficult for organizations across multiple industries to provide business partners and other third parties with the ability to securely access internal data and infrastructure. Organizations simply cannot take this challenge too lightly and just go with what has worked in the past, since granting access to any third party represents a major security risk that can lead to a number of business and technical threats and vulnerabilities that were not in play back when the only concern was on-premises security.

By simply providing a partner or vendor access to your system in a cloud environment means that your security level will instantly plunge. Not only is there a chance of inadvertently inviting malware into your system, but now the safety of your organization's applications and information is at the mercy of that vendor's security controls. If their controls are weak, then so are yours. All that needs to happen for your data to be compromised is for one unapproved source to compromise the vendor's system, and that attacker can gain access to your network. Consider the biggest recent data breaches – many can be traced back to a third-party vendor. Add to this the fact that remote access VPNs are complex to configure, and you have created the perfect storm for a suboptimal system.

Traditional Perimeter Security Is Now Officially Obsolete

For those who continue to depend on VPNs for secure web connections, it is time to face the fact that traditional perimeter security is now officially obsolete. Today, the cloud is ubiquitous. Technology has moved on when it comes to network perimeter security. Proactive organizations have updated their

security strategies to accommodate what work looks like today, and have moved beyond yesterday's VPNs and direct link approaches, as well as their associated security risks.

Next Up – Software Defined Perimeters

A new approach and associated technology is now available, designed specifically from the ground-up to address the aforementioned issues, and to enable enterprises to optimize today's data opportunities. It is commonly known as software defined perimeter (SDP), and it can enable companies to overcome security challenges such as hybrid and multi-cloud deployments, reducing attack surface. How does SDP circumvent VPN's security issues? In a nutshell, it does so by:

- Decreasing lateral attacks – by creating an environment that can be described as "secure by default," which is achieved by providing remote users access only to specific services.
- Providing users access at the application level, moving beyond network-level access.
- Creating greater security by granting connectivity across multiple clouds, sites, and domains to distributed apps and clients.

An SDP allows its users to move workloads as needed from cloud to cloud, leading to the ability to avoid the threat of cloud vendor lock-in. An SDP also eliminates chaos by allowing for installation on any host, without network reconfiguration or appliance hassles.

So, what's holding you back? As a traditional perimeter security, VPNs likely worked for you in the old world of physical servers and virtual machines. But, its likely that even if you have not already experienced a breach, you know they don't have what it takes to protect your data in today's heterogeneous, multi-cloud, advanced application environment. It's time to embrace today's new realities with a progressive security solution that's specifically designed to answer to your requirements, and let go of yesterday's VPN security myth.

About the Author

Don Boxley Jr is a DH2i co-founder and CEO. Prior to DH2i, Don held senior marketing roles at Hewlett-Packard where he was instrumental in sales and marketing strategies that resulted in significant revenue growth in the scale-out NAS business. Boxley spent more than 20 years in management positions for leading technology companies, including Hewlett-Packard, CoCreate Software, Iomega, TapeWorks Data Storage Systems and Colorado Memory Systems. Boxley earned his MBA from the Johnson School of Management, Cornell University. Don can be reached online at don.boxley@dh2i.com. DH2i's website is: www.dh2i.com. Follow DH2i on Twitter: @DH2i.

Data Manipulation Attacks Difficult To Detect But Preventable

By Tim Bandos, VP of Cybersecurity, Digital Guardian

Conventional wisdom says that once an attacker is in the system, moving laterally from network to network, the damage is already done. The adversary has found a way in and more than likely identified the data they're after. They simply need to exfiltrate it—the last step of the kill chain—to land the final blow.

In some scenarios, however, it's what the attacker doesn't do that could have a more devastating outcome on the enterprise.

Data manipulation attacks—attacks in which adversaries don't take data but instead make subtle, stealthy tweaks to data usually to elicit some type of gain—can be just as, if not more crippling for organizations than theft. The ability of attackers to manipulate and shift data around is a real threat, one that could cause widespread financial and even physical harm, if done successfully.

Consider the stock market. Hypothetically speaking, if an attacker were to successfully breach the IT systems and databases responsible for updating a stock ticker symbol and manipulate data to show a billion-dollar tech giant like Apple, Microsoft, Google, or Amazon taking a nose dive, it would cause

immediate chaos, and panic would ensue. It could result in people selling off their stocks in a frenzy—the culmination of a deliberate and effective attack.

Data manipulation attacks don't always have to result in a tangible financial gain. If an attacker managed to carry out a similar attack against health record information for patients in hospitals and altered critical data like drug dosages and prescriptions that need to be administered, it could result in sickness or even death.

These types of attacks are commonly carried out by malicious insiders, individuals who have privileged access to critical data in the first place. If an insider got their hands on blueprints for a manufacturing facility that was being built, they could make minor modifications to drawings that could set the organization up for systemic failure. Understated and difficult to detect, an attack like this could ultimately put a company out of business and give a competitor, perhaps in a nation state, the ability to take over market share. I've seen this play out firsthand. When you have a 'trusted' insider as the culprit, it makes it all that more difficult to detect and track down.

Attackers like data manipulation attacks because they're hard to detect and they undermine trust and confidence; if there's no way to verify that data, like blueprints, documents, or source code are legitimate, it can erode trust from the inside out. Attacks that compromise integrity can jeopardize an entire supply chain. It only takes one flaw, far down a chain, to disrupt or delay the production of goods in an organization's cashflow.

Carmaker Tesla sued a former employee last summer after CEO Elon Musk alleged the insider stole confidential and trade secret information after he failed to get a promotion. While the employee purportedly exported gigabytes of confidential data, he also made changes to the Tesla Manufacturing Operating System, the set of basic commands for Tesla's manufacturing lines—under false usernames—apparently in an act of sabotage. Manipulating sensitive data, like source code, isn't flashy but is something that can cause the market to slowly unravel over time.

For organizations, it's inevitable that attackers will take data; it's more of a challenge to determine when an attacker makes a small change to data, then leaves the scene of the crime. For threat hunters, from a digital forensic perspective, there's typically always a trace left behind. Anomalies in system logs, edits to files at suspicious times, and alarms on threat signatures to detect suspicious techniques and malicious behavior, can be telltale signs of data manipulation.

To combat these types of attacks, organizations need to ensure they have endpoint visibility on their IT systems. If an outsider successfully penetrates a network, they'll need to move laterally through the environment to find the data they're after. It's critical for incident responders or threat hunters to be able to follow in their proverbial forensic footsteps, to proactively hunt and detect this type of activity before something irreversible is done.

The MITRE ATT&CK Framework has generated buzz about across the industry lately for good reason. The knowledge base—a living, breathing breakdown of adversary TTPs and behaviors—outlines in great detail each phase of a cyber attack and the best methods for detecting and mitigating each technique. The framework can greatly help threat hunters looking to speed up their hunting cycle.

While attackers may not necessarily leave the endpoint with data in these types of attacks, organizations would benefit from using endpoint detection and response tools to gain better visibility into behaviors and data movement. Organizations can also use file integrity monitoring solutions to identify and track real-time changes to files, folders, and other settings. Logging activity can also help but it's not a silver bullet. IT teams need to develop internal controls to audit this information and ensure they constantly have eyes on the glass, triaging logs generated by their environment.

Data manipulation attacks can have disastrous consequences and cause significant disruption to a business, country, or even the world in some circumstances. Being prepared is the first step to potentially limiting or preventing the impact of these attacks.

About the author

Tim Bandos is Vice President of Cybersecurity at Digital Guardian. He has over 15 years of experience in the cybersecurity realm with a heavy focus on Internal Controls, Incident Response & Threat Intelligence.

Privacy Regulations Are Popping Up Everywhere

How to Ensure That They Don't Dampen Innovation

By Isaac Kohen, Teramind

The implementation of Europe's expansive General Data Protection Regulation was a clear harbinger that the tech sector was heading in a radically different direction from the lax data standards that governed its first several decades of growth.

Of course, what primarily began as a European mandate quickly left its shores as shifting consumer sentiment and a broad recognition that we needed to place some parameters on the way we handle people's valuable personal data became inevitable.

In the United States, The California Consumer Privacy Act will place data privacy restrictions in Silicon Valley's own backyard, and, similar to the state's impact on the auto industry, it will have repercussions for the rest of the country. Collectively, more than 80 countries have data privacy laws on the books.

In the wake of egregious data breaches at companies like Equifax and Marriott, as well as moral failings from companies like Facebook, it was clear that something needed to be done. However, it was less obvious how that would affect the businesses that these laws regulate.

So far, the results are mixed.

For instance, more than 59,000 data breach notifications were issued in GDPR's first year, and some companies like British Airways and Marriott received hundreds of millions of dollars in fines, reminding companies of all sizes that data protection needs to be a top priority.

Meanwhile, there is evidence that venture capital investment in European tech startups is declining compared to other countries like the United States, where privacy laws are still less defined. What's more, data privacy laws impact the development of artificial intelligence and machine learning by making information less accessible and more risky for companies striving to develop the technology.

To put it simply, restricting innovation is a noteworthy side effect of these data privacy regulations.

In 2019, these regulations are causing companies to redefine their practices while still harnessing the opportunities of the digital age. It's a precarious situation, but it's not one that today's organizations can't meet head on.

Here are three ways that privacy regulations impact every organization and the steps they can take to navigate this new reality.

#1 Companies Have to Protect User Data

In almost every way, data is the lifeblood of the digital economy. Likening personal data to the oil of the internet, Wired described the importance of personal information, writing, "On the internet, the personal data users give away for free is transformed into a precious commodity."

Practically every platform on the internet is powered by this valuable resource, creating a sophisticated market for exchanging personal information. Unfortunately, this data isn't just valuable to the companies that use it to perfect their platforms.

It's extremely valuable to bad actors, and it's susceptible to misuse by both external and internal threats. With the Dark Web providing an expansive market for people's personal information, anyone can capitalize on the vulnerabilities inherent in today's digital ecosystem. That's why Verizon's 2019 Insider Threat Report found that both internal and external threats are primarily motivated by financial gain.

In 2019, companies of all sizes need to be aware that they are storing a highly valuable commodity, and securing this information is critical to their regulatory compliance, customer satisfaction, and financial well-being.

Oddly, this inherently technological problem can be addressed with new and better technology.

Fighting technology with technology might appear anathema on the surface, but by implementing powerful and capable endpoint data loss prevention (DLP) and monitoring software, any company can effectively protect their information from misuse so that they can remain compliant and operational.

For example, this data security solution can

- limit access to sensitive personal information
- prevent unauthorized data movement
- provide real-time alerts for suspicious activity

- create comprehensive record of data access.

Since digital platforms rely on data to fuel their platforms, they have to be especially careful about protecting this information if they want to continue innovating while remaining compliant with data privacy laws.

#2 Modern Work Trends Must Be Managed

The modern office is redefining the nature of work in several ways. Perhaps most obviously, many employees no longer spend all of their time in an office. It's estimated that 70% of people around the world work remotely at least once a week, a reality that produces many compliance and data security vulnerabilities.

When coupled with blurring lines between personal and private technology, it's no wonder that organizations are having a difficult time securing their customers' data. In this environment, accidental sharing, unsecured networks, and other data exfiltration maneuvers create a significant liability for companies offering these perks.

To put it simply, in a stringent regulatory environment, these incentives have many drawbacks for companies trying to remain compliant with the cadre of laws trying to protect consumer data.

However, that doesn't mean that it's time to call the employees back to the office. Instead, train employees on proper data management standards, and enforce data privacy expectations by leveraging your DLP and monitoring software to support these initiatives.

Noting the importance of employee training, the Society for Human Resources Management encourages every organization to prioritize training as a critical component of any data security protocol.

"To ensure that company, consumer and employee information is protected, employers should understand the data-security laws that cover their workplace and train employees to know their role in minimizing the risk of a data breach," the organization writes.

These efforts can be reinforced with the right software, providing both the real-time support to address common cyber attacks like phishing campaigns and malware that are often delivered through email to unsuspecting employees.

Organizations don't have to replace their forward-thinking workforce priorities to achieve regulatory compliance, but they do have to bolster those efforts with training and reinforcement.

#3 Innovation Comes with Accountability

Two of today's most promising new technologies, artificial intelligence and machine learning, require a deluge of data to be successful. In response to recent regulatory requirements, some companies are

pulling back on these initiatives, a shortsighted move that compromises innovation in exchange for compliance.

Instead, there is a delicate balance between innovation and accountability that will mark the next generation of prominent technologies.

Therefore, companies should prioritize the technological infrastructure that can monitor these initiatives while demonstrating compliance. For example, GDPR requires that companies appropriately explain the method and nature of their data processing, so intentionality must be enacted at every level of development.

Regardless of the specific technology, the next generation of innovation will come with accountability, and companies won't have carte blanche to do whatever they want with their customers' data.

We are undoubtedly heading into an era that is increasingly marked by more regulation, not less. Even so, that doesn't mean that innovation has to stall. Instead, today's organizations can embrace this moment as an opportunity to refine their practices and priorities to ensure that their platforms' next iterations are both extremely capable and unambiguously aware of the valuable information that propels their ecosystems.

When the right solutions are implemented, everyone wins. That's the intention of every regulatory effort, and it needs to be the priority of every organization going forward.

About the Author:

Isaac Kohen is the Founder and Chief Technology Officer of Teramind (https://www.teramind.co/), a leading, global provider of employee monitoring, insider threat detection, and data loss prevention solutions.

Reducing the Occurrence and Impact of Data Breaches through Strong Practices and Procedures

By Billie Elliott McAuliffe

From the news on television or stories on the Internet, it may appear that only large companies in certain industries are the targets of hackers and the victims of data breaches. But, that is in no way true. No company, no matter the size or the industry is safe. And, we are all the victims of these data breaches.

Ten years ago, most companies' approach to cybersecurity and data breaches was reactionary. Companies did not have adequate plans in place to handle breaches and executives were often dumbfounded and caught unaware when a breach occurred. After a number of big players (e.g., Anthem, Target, Equifax) fell victim to cyberattacks, more companies began to understand the need for robust cybersecurity, business continuity and incident response practices and procedures. Despite this, many companies are still lagging behind.

The Poneman Institute, in its 2018 Cost of Data Breach Study: Impact of Business Continuity Management, which was sponsored by IBM, surveyed 477 companies in 13 countries that experienced

a data breach in the 2017 calendar year. Each of these data breaches involved the compromise of 2,500 to 100,000 records containing personal information, which cost these companies on average $148 per compromised record. But, according the Poneman Institute, the costs per record are not all equal; costs grow exponentially with the number of records breached. The Poneman Institute estimates that the cost of a 1 million record breach is approximately $40 million while a breach of 50 million records is $350 million. That seems like a large bill to pay for a situation that may have arisen from an employee leaving a laptop open in an unsecure location, a business failing to discover a vulnerability in the company's information technology systems or an employee clicking on a nefarious link in an email.

With costs of a breach this high, one would think that every company would have elaborate cybersecurity, business continuity and incident response practices and procedures in place. Yet, only 55 percent of those surveyed by the Poneman Institute had a business continuity management function or disaster recovery team that was involved in enterprise risk and crisis management. This was to their detriment. Prevention is truly the best medicine when it comes to data breaches.

Hackers often look for information that has value, such as an individual's name plus his/her bank account number, social security number or credit card number. Ensuring that your company's practices and procedures with regard to these types of information provide adequate protection should be the cornerstone of your planning. However, you also need to plan for how you and your team will respond when this valuable information is compromised.

When companies have taken the time to think through and formulate comprehensive incident response policies, the incident response times and costs are significantly reduced. According to the Poneman Institute study, there was a 6.5% reduction in the per capita cost of a data breach and a 44-day reduction in the average time to identify a data breach in companies that had business continuity management/incident response programs in place over those that did not. This works out to be a difference of $690,000 in the average total cost of a data breach ($4.24 million average total costs without business continuity management/incident response programs and $3.55 million for those with such programs) for companies that have robust practices and procedures in place.

Because there is not an overarching federal policy on data breaches, compliance can be complex. There are certain federal rules pertaining to particular types of personal information and certain sectors of the economy, like protected health information, which is protected under the Health Insurance Portability and Accountability Act ("HIPAA"). There is also nonpublic personal information, which is protected under the Gramm-Leach-Bliley Acts of 1999 ("GLBA") and applies to financial institutions such as banks and lending institutions. But, for the most part, general data protection laws come at state level, some even getting down to the county and city level, and, unfortunately, these are laws are far from uniform.

Adding to the compliance difficulty is that many companies are not aware of which laws actually apply to their given data breach. Generally speaking, most of the laws regarding notifying affected persons after a data breach has occurred, the residency of the affected person is the determining factor in which law applies. For example, if a Missouri resident makes a purchase from a business in California, and that individual's information is stolen, the California company would have to comply with Missouri laws with regard to notifying such resident of the data breach. Additionally, since the company was doing business

in California, certain California laws may also apply to such company's use of the individual's information. In other words, one company may have to comply with 50 different laws when making notifications for one single data breach. And, the timeframes for providing notice under some of these laws are very short. You may be subject to providing notification within 72 hours of you becoming aware of the data breach. Hence, being prepared and having a well thought-out plan are crucial.

Why are companies not instituting these robust practices and procedures?

Most likely, it is the time and money required to implement these types of cybersecurity, business continuity and incident response practices and procedures. Significant time and effort must be spent understanding the totality of the companies' systems, how personal information is used and stored and what persons or entities are interacting with such information and why. Further, leadership has to think about all the different places, both likely and unlikely, where a breach could occur.

Additionally, this analysis should not be limited to just your companies' systems, practice and procedures. It also needs to include your vendors. For example, with the Target breach, the bad actor's access to their systems was traced back to an HVAC system provider's network credentials that had been stolen. Therefore, you need to analyze what third parties have access to your network and is that access appropriate for the services being supplied. Does an HVAC provider need to have access to the systems where credit card information is housed and if not, you need to ensure that that HVAC provider's access is appropriately limited. If this vendor does require that type of access, then you need to ensure that it has the appropriate practices and procedures in place to prevent intrusion to your systems occurring through such vendor's systems. This may require a review of your contacts with vendor to include the appropriate contractual obligations on such vendors.

Furthermore, a company needs to understand what types of information are at risk in which systems and how to handle those different risks within its practices and procedures. The personal information at risk if someone breaks into a computer in human resources will different than a computer in sales. These differences need to be evaluated and the practices and procedures need to be modified according.

What are some of the best practices to mitigate risk of a data breach that should be built into these practices and procedures?

Your practices and procedures should:

1. Be flexible enough to allow for changes in risks and attacks. Additionally, the types and levels of security measures need to fit the value of the information and the potential risks to such information.
2. Include appropriate monitoring of your systems and regularly testing for vulnerabilities. As the Ponenam Institute study shows, the faster a breach can be identified and contained, the lower the cost to the company.
3. Provide for education and training of your employees on recognizing a potential attack and taking the appropriate steps if they believe an attack is occurring or has occurred.

4. Have a comprehensive incident response plan that will be implemented by a designated incident response team with clearly defined roles. Determine who will manage the technical side of the breach response (i.e., containment, remedy and mitigation), who will handle notifying the affected persons and governmental entities and who will respond questions from customers, clients, vendors, governmental authorities and/or the media.
5. Provide for periodic review and update of the practices and procedures

You've experienced a breach. Now what?

Stay calm and follow your incident response plan. If you don't have one:

1. Stop or contain the attack, remedy the issue and mitigate the damage.
2. Start an investigation to determine what data has been accessed or compromised.
3. If a crime is suspected, contact the local police or appropriate federal investigative agencies.
4. Contact legal counsel. Members of the Lewis Rice Cybersecurity & Data Privacy Group are continuously monitoring and reviewing the ever-changing data privacy and protection laws and we are here to assist you.
5. Contact your insurance provider. Most companies today have some form of cyber incident coverage within their insurance packages.

The Aftermath of a Breach

Depending on how the breach occurred, you may need to change how your company operates. You should take some time to look at how you and your team identified and handled the breach especially where problems arose, and learn from those experiences to avoid future breaches and/or response issues. You may want consider the following:

1. Do you need to provide additional training to your employees so that this type of intrusion does not reoccur?
2. Do you need to create additional or modify existing policies or procedures to better respond to similar situations in the future?
3. Do you need to change vendors or institute new requirements for vendors to avoid this type of third party intrusion?
4. Do you need to include a defined incident response team into your incident response plan?
5. Do you have the appropriate security measures in place? Do you need to modify any security measures?

Education and planning are key to successful crisis management. Unfortunately, in the world we live in, data breaches are going to occur. Working with legal counsel to develop good, robust cybersecurity, business continuity and incident responses policies now, will help you respond, both internal and externally, to such breaches in an appropriate and timely manner. It will also reduce the effect of such breaches on your business, decrease the stress and anxiety that come with these types of situations and, hopefully, reduce the ultimate cost of such breaches to your company.

About the Author

Billie Elliott McAuliffe is an attorney with Lewis Rice in St. Louis and is a member of the firm's Cybersecurity & Data Privacy Group. Along with information technology law, Billee has extensive experience software and other technology licensing, cybersecurity and data privacy. Lewis Rice is a corporate member of the International Association of Privacy Professionals (IAPP), a premier global information privacy community.

Will Your Wordpress Site Be Breached In 2019?

By Randy Reiter, CEO, Don't Be Breached and Sql Power Tools

How do Hackers gain access to Wordpress confidential database data?

Wordpress runs 34% of the Internet. The New York Times, USA Today, CNN, Mashable, eBay, Spotify, TechCrunch, CBS Local, NBC and many more use WordPress. One of the things that makes Wordpress so powerful is the abundance of themes and plugins that assist in building a first class web site.

Over 50,000+ WordPress plugins are available from 3rd party organizations. A plugin is software containing functions that can be added to a WordPress website. They can extend functionality or add new features to WordPress websites.

The popularity of WordPress makes it a prime target for Hackers. Annually thousands of WordPress sites get hacked (i.e. data breaches occur). Hackers are after the confidential data stored in the databases that run WordPress web sites. Confidential database data includes names, addresses, payment information and much more.

Zero Day Attacks and not current WordPress or plugins allow Hackers to perform a data breach and steal confidential database data. A Zero Day Attack is the time between when a security vulnerability in a software plugin is published by the author and the updated plugin is applied to a web site to prevent a data breach. Hackers will be aware of the Zero Day vulnerability once it has been publicly announced. Hackers will now attempt to exploit it immediately to gain inside access to the Security Perimeter and steal confidential web site database data.

Other content management system (CMS) such as Joomia and Drupal web sites are also vulnerable to data breaches by Hackers or Rogue Insiders for the same reasons. The 51.3% of Internet websites that don't use a content management system likewise are vulnerable to database data breaches for many of the same reasons.

How to Protect Confidential Web Site Database Data from Hackers or Rogue Insiders?

Confidential web site database data includes: credit card, tax ID, medical, social media, corporate, manufacturing, law enforcement, defense, homeland security and public utility data. This data is almost always stored in Cassandra, DB2, Informix, MongoDB, MariaDB, MySQL, Oracle, PostgreSQL, SAP Hana, SQL Server and Sybase databases. Once inside the security perimeter commonly installed database utilities can be used by Hackers or Rogue Insiders to steal confidential database data.

Non-intrusive network sniffing can capture the normal database query or SQL activity from a network tap or proxy server with no impact upon the database server. This SQL activity is quite predictable. Database servers servicing 10,000 end-users typically process daily 2,000 to 10,000 unique query or SQL operations that run millions of times a day.

Advanced SQL Behavorial Analysis of the Web Site Database Query or SQL Activity

Advanced SQL Behavioral Analysis of the web site SQL activity learns what the normal query activity is. Now from a network tap or proxy server the database query and SQL activity can be non-intrusively monitored in real-time and non-normal SQL activity immediately identified. Non-normal SQL activity from a Hackers or Rogue Insiders can be detected in a few milli seconds. The Hacker database session can be immediately terminated and the Security Team notified so that confidential database data is not stolen.

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 unique SQL queries sent to a database. This type of data protection can detect never before observed query activity, queries sent from a never observed IP address and queries sending more data to an IP address than the query has ever sent before. This allows real-time detection of Hackers and Rogue Insiders attempting to steal confidential web site database data. Once detected the security team can be notified within a few seconds so that a data breach is prevented.

About the Author

Randy Reiter is the CEO of Sql Power Tools. 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 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@sqlpower.com, www.DontBeBreached.com and www.Sqlpower.com/Cyber-Attacks.

The Role of Certifications for a Cyber Security Professional

Creating a win-win strategy

By Pedro Tavares, Founder of CSIRT.UBI & Cyber Security Blog seguranca-informatica.pt

Currently, cybersecurity is a field with a lot of demand, from pure management to researching new threats, responding to massive attacks in real time and keep away enterprises and organizations from data breaches. Formation of new candidates with this encapsulated mindset is seen as a natural course of action due to emergent cybersecurity challenges that expects serious dedication.

Cyber threats are, in fact, growing in size and sophistication. Many multinational companies such as Facebook and Uber made headlines after having their customer information leaked online [1]. To fight this big challenge, there are some resources, such as degrees and certifications that can be taken in order to create more specialized candidates in the field.

According to the Bureau of Labor Standards, "employment of information security analysts is projected to grow 28 percent from 2016 to 2026. Demand for information security analysts is expected to be very high, as these analysts will be needed to create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks" [2].

Creating the right personal sense of achievement

Both employees and organizations get win-win situations through professional certification. There are enterprise and personal certifications that can bring much more expertise and knowledge, both for employees and the company. With this doctrine established, employees will create a more credible image to the clients and build a reputation in the employer's industry.

Increased productivity has a direct impact both in employee's day to day life as well as in the organization's activity in general. Next, we describe some things that need to be kept in mind.

Happier employees

The need for achievement refers to desire of accomplishment, mastering of skills, control, and high standards. This culture needs to be implanted as a new doctrine inside organizations. Motivated people are the key to success.

Increase productivity

The rule of thumb to increase the employee's productivity is the ability to combine new technologies with the right human capital and to change the organization's operations, activities, processes and the way to explore new opportunities. Education and training have a crucial role within this context. And of course, certifications can help you to walk this pathway.

Cultivate employee's skills

New skills contribute to the evolution of the way an organization operates, providing new ideas and perspectives. This point can also be responsible for your career development and to open new opportunities in your life.

The crucial point: salary

And of course, with greater responsibility comes a higher salary!

Cyber Security Certifications

There are certifications within this field that are considered fundamental. These certifications are among the best of and can prepare you for a wide variety of situations.

If we consider the security landscape, for example, we can list CompTIA Security+ and Certified Ethical Hacker (CEH) certifications. These are recognized worldwide and can help you enhance your skills.

In detail, CompTIA Security+ is a certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. This certification focuses on training covers the essential principles for network security and risk management – making it an important stepping stone of an cyber security career.

On the other hand, CISSP course aligned with (ISC)² will train you on the advanced step-by-step methodology that hackers actually use, such as writing virus codes and reverse engineering, so you can better protect corporate infrastructure from data breaches. This CISSP certification course will help you to become Information Assurance Professional who need to understand all aspects of IT Security including architecture, design, management & control. Also helps you to master advanced network packet analysis and advanced system penetration testing techniques to build your network security skill-set and beat hackers at their own game.

The table below depicts more details on security certifications in 2019.

Name	Cost	Requirements
CompTIA Security+	US$269	A minimum of two years experience in IT and network security
GIAC Security Essentials (GSEC)	US$769 / US$1,899	No specific training is required, however practical experience is recommended.
NIST Cybersecurity Framework (NCSF), both Foundation and Practitioner	US$995 for Foundational, US$3,295 for Practitioner	The Foundational course has no prerequisites however you must hold a valid NIST Cybersecurity Foundation Certification or have equivalent knowledge to complete the Practitioner.
Offensive Security Certified Professional (OSCP)	US$800	Penetration Testing with Kali Linux
Certified Ethical Hacker (CEH)	US$500	Attend a five-day EC Council approved training course or have at least two years of information security experience.
Certified Information Security Manager (CISM)	US$760	Five years in cybersecurity and three years in security management
Certified Cloud Security Professional (CCSP)	US$549 per attempt	A minimum of 5 years of full-time, paid, cumulative information technology, including at least three years of information security and one year of cloud computing.

Certified Information Systems Security Professional (CISSP)	One six-hour exam at US$699 plus four additional concentration exams at US$599 each.	At least 5 years of recent full-time professional work experience in 2 or more of the 8 domains of the CISSP common body of knowledge.
Certified Protection Professional (CPP)	US$450	Nine years of security experience, at least three of which responsibility for a security function has been held.

Overall, both companies and employees themselves can gain from this new mindset. Look that a better professional image of the organization can be created, with people specializing in certain points of knowledge. Happier employees motive and influence other people. So, find your certifications and to boost your career via a new kind of culture that you need to absorb.

References

[1] https://www.newhorizons.com/article/the-best-cybersecurity-certifications-to-boost-your-career-in-2018

[2] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

About the Author

Pedro Tavares is a cybersecurity professional and a founding member and Pentester of CSIRT.UBI and the founder of seguranca-informatica.pt.In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, hacking, cybersecurity, IoT and security in computer networks. He is also a Freelance Writer. Segurança Informática blog: www.seguranca-informatica.pt LinkedIn: https://www.linkedin.com/in/sirpedrotavares Contact me: ptavares@seguranca-informatica.pt

To Pay or Not To Pay, That Is the Question

By Chris Bates, VP of Security Strategy, SentinelOne

Every city and government organization should assume they are a ransomware target. Attacks like the ones in Atlanta, Baltimore and Rivera Beach are about more than just criminal payouts - they're paralyzing attacks that can bring a city to its knees, as we're seeing. A lack of cybersecurity resources, maintenance and updates across broad enterprises combined with the human tendency to click through questionable emails makes municipalities an easy target.

Preparing for an attack starts with assuming an employee will introduce malware into the network and taking steps to prevent its spread when that happens. It's incredibly hard to prevent employees from making mistakes, which is why cities need security technologies that prevent ransomware from spreading once the inevitable happens.

From a response standpoint, immediately isolating systems and limiting employees' access to shared systems may help minimize the spread of the ransomware. Legacy AV systems have continually shown that they can't keep up with attacker sophistication and repeatedly miss detecting and proactively blocking malware. 2019 Security Megatrends research by EMA tells us that 90% of respondents that experienced an attack causing significant to severe impact believed an advanced endpoint solution would have

performed better than traditional AV. Moreover, all of the respondents who experienced severe impacts from a malware attack indicated they now intend to replace their traditional AV product with advanced defense technology.

Because attackers are continually perfecting their malware, organizations need to implement AI-powered solutions that can identify and block attacks before they happen, and importantly, rollback ransomware so vital systems do not need to be shut down. What we call 'behavioral AI' is the ability to really detect something and protect from an attack. Not by looking at signatures or at static indicators of compromise, it's by actually looking at the nature of what it does.

But what should you do if disaster strikes? "To pay or not to pay" continues to be a tough decision in each case, and Riviera Beach has set a dangerous precedent by showing cybercriminals that "ask and you shall receive" is a reality. This will surely increase the frequency of municipality ransomware attacks, especially on smaller cities who are even more bootstrapped than the Atlanta's and Baltimore's of the world from a resource standpoint.

Riviera Beach's decision to pay the ransom was surely influenced by Baltimore's decision not to, which has cost the city an estimated $18M in damages – exponentially more than the attacker's ransom request. But paying the ransom is not the answer either as recent research tells us 45% of U.S. companies hit with a ransomware attack paid at least one ransom, but only 26% of these companies had their files unlocked. Furthermore, organizations that paid the ransoms were targeted and attacked again 73% of the time as attackers treat paying companies like ATMs.

The real answer is taking a proactive approach and updating legacy defense systems susceptible to sophisticated attacks, in addition to allocating additional resources to security team staffing, training and support.

The trend of repeated ransomware attacks on cities worldwide is far from over, and Riviera Beach's decision to pay may have made these susceptible targets even more enticing for the bad guys.

About the Author

Chris Bates is the VP of Security Strategy at next-gen autonomous endpoint protection provider SentinelOne. Chris is a trusted professional, adviser, and leader in the information security and technology space with over 23 years of experience. Chris can be reached at SentinelOne website https://www.sentinelone.com.

Today's Cyber Threats Demand Enhanced Strategies and Solutions

By Joseph E. Saracino, Jr., President & CEO, Cino Ltd. Family of Companies, which includes Cyber Security Solutions

The term cyber security has become part of our everyday conversations. Headline grabbing data breaches affecting the sensitive data of millions have become commonplace. In 2018, Lloyd's, the world's specialist insurance and reinsurance market, which underwrites approximately one third of the global cyber market (80% of which is written in the United States), estimated that cyber attacks cost businesses as much as $400 million annually. This figure reflects direct damage and post-attack disruption to their normal course of business. Despite these sobering figures, many organizations aren't taking all the steps necessary to protect their data and that of their customers. Even Information Technology (IT) professionals and Managed Service Providers (MSPs) are not as prepared and trained as they should be in the increasingly more complex arena of cyber security and defense. There are many misconceptions surrounding cyber security held at all levels of many businesses, from the Board and executive team to the IT department and rank and file employees. Gaining a better understanding of

today's cyber security realities, as well as best in class strategies for achieving an optimum cyber security program, is essential to mitigating the heightened risk associates with cyber attacks.

"Dispelling Common Cyber Security Misconceptions"

Among the more common misconceptions regarding cyber security, and one which presents a false confidence, is that having anti-virus software is sufficient. With ransomware a major threat and the ability for hackers to overcome and destroy anti-virus software, this is not a solution. Another myth is that cyber security is an IT matter when, in reality, it should be regarded as a core business discipline to which every member of an organization has a responsibility. This thinking recognizes that an IT system is integral to a company's day-to-day operations (i.e., processing purchase orders, invoicing, data storage, employee benefits and payroll administration, maintaining intellectual property, etc.). Thinking that cyber security is an internal matter is also a mistake considering all of the interactions a company's IT system has with external third parties, from vendors, professional firms, employees' home-based systems, etc. which make it vulnerable to many additional cyber threats. By recognizing that cyber security is a central to a business' operation with many interrelating components from both inside and outside of an organization, a business is better prepared to address today's numerous cyber threats.

"Cyber Security Today"

According to Jupiter Research, the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to an estimated $2.1 trillion globally by 2019. That is four times the estimated cost of data breaches in 2015. This same research firm projects that the average cost of a data breach in 2020 will exceed $150 million by 2020. There are many types of data breaches occurring at a rapid pace today. The Madison Square Garden credit card breach occurred when hackers accessed the credit card information of people used at Madison Square Garden and other related venues. This past November, Madison Square Garden reported that its systems had been compromised during the period from November 2015 to October 2016. Also recently reported was the Marriott International/Starwood multi-year breach which compromised the personal data of up to 500 million customers. Other breaches affecting millions an even billions of records include: Yahoo's 2013 breach affecting 3 billion accounts and its 2014 breach affecting 500 million accounts, the Equifax breach in 2017 affecting 146 million accounts, and the Anthem data breach in 2015 in which 37.5 million records of personal data including health data were breached impacting an estimated 79 million people. As a consequence of this breach, Anthem was ordered to pay a federal government settlement of $16 million. These large breaches are accompanied by other breaches of smaller size, but with significant impact on the companies and individuals affected.

The harsh realities of today's cyber landscape are that there are an increasing number and types of threat looming and waiting to attack IT systems of large, small and middle market enterprises. The size, type or industry doesn't matter. Everyone is vulnerable including nations and their federal, state and local governments. Malicious AI-driven chatbots, crimeware as a service, and the resurgence of ransomware are pervasive. Additionally, cyber attacks on satellites are taking root. There have been reported attacks on telecommunication companies' satellites, as well as the satellite communications systems used by the military, airplanes and ships creating concern that cyber criminals will utilize satellite antennas as weapons to create further havoc.

The leading cyber security threats of 2019 include:

- Ransomworm – The next level of cyber security nastiness that encrypts files and holds them captive until ransom demands are met. When ransomware is attached to a network worm, the level of extortion rises from traditional PC extortion to the Internet of Things (IoT), high net worth users and major corporate disruption.
- Phishing and Whaling Attacks – Where hackers send fraudulent emails from trusted accounts to target businesses through individual staff members. An innocent staff member clicks on the email and then the attachment, at which point the attachment, which is tagged to the email, starts releasing a malware capable of stealing data. Whaling takes this aforementioned cyber attack strategy to the next level by targeting high net worth individuals, often CIOs and CEOs.
- Machine Learning-enabled Attacks – Wherein social engineering attacks are launched and, if the hackers are able to access publicly available data, they proceed to use complex analysis tools for precision selection of target.
- Iot Botnets – Impacting the projected 8.4 billion things that will get connected to the Internet this year, further compromised by Distributed Denial of Service (DDoS).

Keep in mind that, despite these leading threats, the way most systems get hacked today are through attack vectors such as: external hackers, phishing attacks, malware and key loggers, and/or a disgruntled former user such as a former employee. Finally, a common way many companies' systems open themselves to hacking incidences is by simply failing to have or enforce cyber security controls and related policies.

"Increased Regulation and Litigation"

Federal and state governments are responding to the increase in cyber attacks through new legislation. At the federal level, the House Financial Services Committee introduced a bill, "The Consumer Data Security and Notification Act," to amend the Gramm-Leach-Bliley Act to include a national breach notification law for the financial industry which would supersede state laws. The states are also rapidly introducing cyber security legislation. In 2019, 45 states and Puerto Rico introduced over 260 different bills or resolutions to address cyber security and specifically matters relating to the security of connected devices, election security, industry data security and the establishment of cyber security task forces. New York State, for example, issued its New York State Cybersecurity Mandate, which was the nation's first cyber security regulation. It requires regulated financial institutions to establish and maintain cyber security programs to include penetrate testing, vulnerability scanning, and education for all employees, design to protect consumers and the industry. In that regulation was a strong emphasis on establishing a compliance culture at the top levels of these institutions. Europe too has acted to help institutionalize a culture of cyber security with its "General Data Protection Regulation (GDPR) designed to strengthen and unify data protection for individuals in the European Union (EU) and address the export of personal data outside of the EU.

Consumers too are taking their cyber security more seriously than ever, fighting back with increased litigation. Over recent years, we've seen a federal judge in California rule that a consolidated class-action lawsuit filed by those affect by three Yahoo data breaches can proceed; Nationwide Insurance was ordered to pay a $5.5 million settlement, Cottage Health System ordered to pay a $2 million settlement, and Home Depot agreed to settlements totaling $44.5 million stemming from class-action lawsuits related to data breaches affecting 50 million customers. For the 143 million Americans affected by the Equifax data breach, there is a $70 billion class-action lawsuit underway. These lawsuits and the countless others in courts nationwide should give businesses pause to recognize their due diligence, fiduciary and data protection responsibilities which require they implement and uphold best cyber security practices.

"Best Practices for Optimum Cyber Security"

The Information Systems Audit and Control Association's (ISACA) "2019 State of Cybersecurity" research reported that:

- 69% of companies stated that their cyber security teams are understaffed,
- 58% of companies said they have unfilled cyber security positions, and
- Many companies have difficulty retaining cyber security professionals even when they offer training and certification programs.

For all companies, a robust cyber security program stems from the top. Management must be fully-engaged in a cyber security initiative and support it 100%. Without executive buy-in, a cyber security program will not be successful. The C-suite -the CEO, COO, CFO, CISO and CSO – must become informed and proactive, not reactive, regarding cyber security. A culture of cyber security awareness, due diligence and responsibility must prevail. The internal IT team, as well as any external IT professionals used, should be aligned and in direct communication with a cyber security organization; one which specializes in cyber security and has a team of cyber security professionals who are experienced and current on the latest cyber threats and effective strategies for defending against them. Some of these organizations offer mentoring, training and certification programs for their clients' IT teams and MSP staff which should be pursued. Additionally, all employees should be educated regarding their responsibilities to the cyber security initiative. This includes guiding them with policies relating to effective cyber security practices such as changing passwords regularly, being aware of what constitutes suspicious emails, turning off their computers and personal devices at the end of the day, and reminding them that personal devices used for work too must adhere to sound cyber security practices. By building a strong relationship with a cyber security firm based on trust, in the same way a company relies on its accounting and law firms, cyber security will rise to the level of a critical operation.

In addition to cyber security training, key tactical measures that every sound cyber security program requires are:

- Live Penetration Testing – Attempts to penetrate a network from the Internet and external IPs
- Vulnerability Detection – A minimum of two scans per year on an internal network
- Anti-Key Logging Software – Keystroke encryption software to prevent malware from stealing sensitive data
- Identity Theft Protection Services – To mitigate risks and damage
- Ongoing Cyber Security Bulletins and Urgent Alerts – To keep executives, IT staff and MSP staff informed on the latest threats and other timely information
- Cyber Insurance – Liability insurance as well as cyber extortion insurance

"The Inconvenience of Cyber Security"

Cyber security is inconvenient; no question about it. It is, however, necessary and not something that should be left up to others. While organizations should avail themselves of the expertise and experience

of cyber security specialists, they too must be directly involved in their organization's cyber security program, from the top down. Being diligent, informed and armed with the best practices and solutions is an organization's best defense against cyber attacks and their dire consequences.

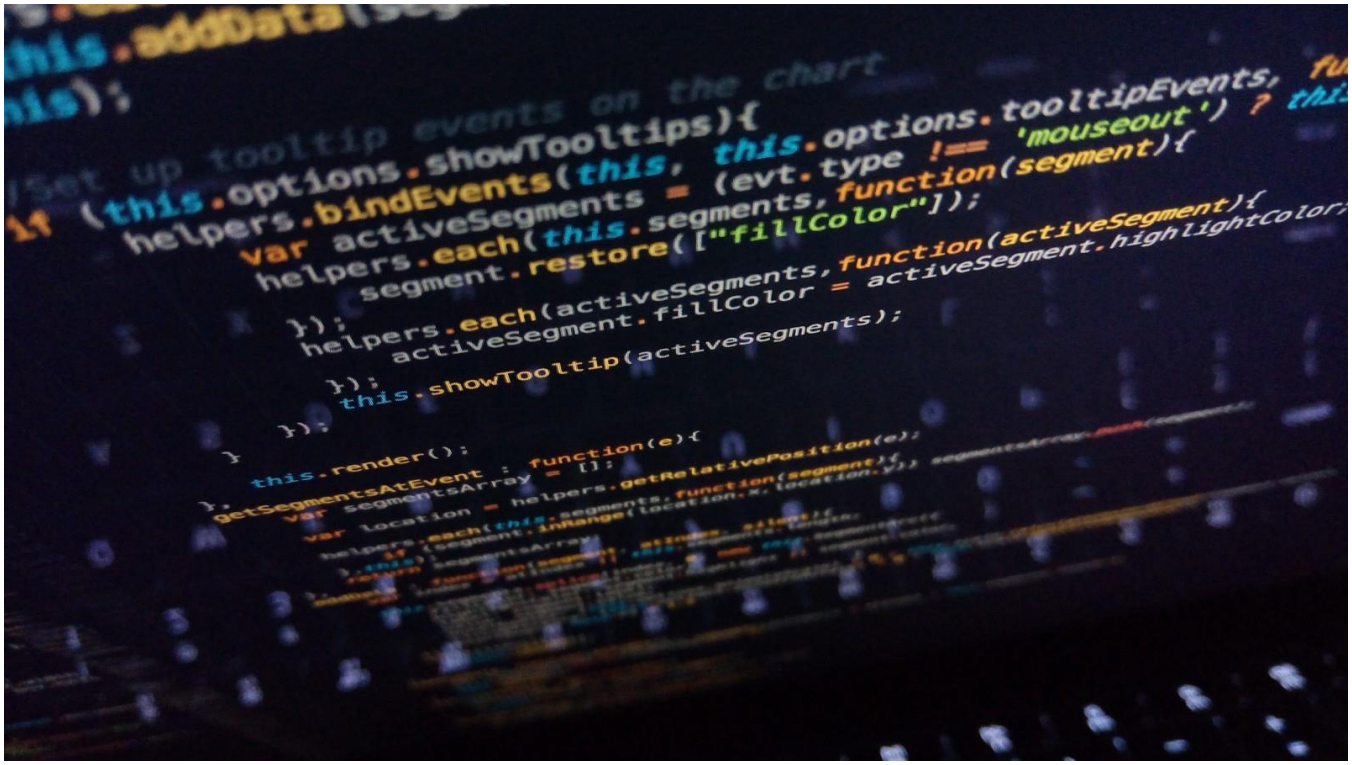
About the Author

Joseph E. Saracino, Jr. is the President & CEO of Cino Ltd. Family of Companies, a leading risk management organization, which includes Cino Security Solutions, a prominent cyber security firm.

Joseph served in the United States Navy as a Naval Intelligence Officer and continues to be active as a Military Education Liaison, VA Certifying Official, as well as a Global Yellow Ribbon presenter to Active Duty troops and Reserve personnel. He also serves as a consultant to Homeland Security and Joint Military Task Force Commands. He is a member of numerous civic and industry associations, works with the New York City Mayor's Office of Veteran Affairs, and is an active participant in the Suffolk County Police Department SHIELD Program which is countering terrorism and crime through information sharing in partnership with the New York Police Department and law enforcement agencies nationwide. LinkedIn: https://www.linkedin.com/in/joseph-saracino-664370b/ You can reach me at: jsaracino@cinoltd.com

Reducing the Insecure Deserialization Risk

By My Apostolos Giannakidis, Security Architect, Waratek



Reducing the Insecure Deserialization Risk

Serializing and deserializing data is a common operation in many web application, mainly due to the speed and ease with which data can be moved between applications. However, what was thought to be an efficient process has turned into a vulnerability nightmare over the last few years, mainly for Java applications, but .NET, PHP, and Ruby have also seen headlines from insecure deserialization attacks. The deserialization problem occurs when applications deserialize data from untrusted sources and is one of the most widespread security vulnerabilities to occur over the last couple years.

A brief background

Serialization, or marshalling, is the process of converting a memory object into a stream of bytes in order to store it into the filesystem or transfer it to another remote system. Deserialization, also known as unmarshalling, is the reverse process that converts the serialized stream of bytes back to an object in the memory of the machine. All main programming languages provide facilities to perform native serialization and deserialization and most of them are inherently unsafe.

The attack mechanism can be summarized in the following steps:

- A vulnerable application accepts user-supplied serialized objects.
- An attacker creates malicious code, serializes it into a stream of bytes and sends it to the application.
- The vulnerable application reads the received stream of bytes and tries to construct the object. This operation is called “deserialization”.
- During deserialization, the malicious code is executed, resulting in a compromised system.

What is the impact of such a system compromise?

Depending on the payload, a deserialization attack could perform Remote Code Injection, Remote Command Execution, Denial of Service, etc. In most cases, the exploit is possible without any authentication. Finally, note that an attack on a server like WebLogic could impact all its running web applications. For these reasons, Java deserialization vulnerabilities are considered to be critical vulnerabilities with a CVSS score from 7.5 up to 10, depending on the environment.

Variations of Java Deserialization attacks

At this point it is important to introduce three variations of the Java deserialization attacks in order to better understand the impact of these attacks.

- Blind deserialization attacks that aim to extract data from the target system in environments where the system is behind a network firewall that blocks outgoing connections or when strict Security Manager policies are in place.
- Asynchronous (or stored) deserialization attacks that store the malicious code in a database or a message queue. The malicious code will be executed when the target system reads data from the database or the message queue and deserializes them.
- Deferred-execution deserialization attacks that do not execute the malicious code during deserialization, but rather after deserialization has completed. This is usually achieved via the finalize() method during garbage-collection.

What is the proper fix?

Is there a solution that solves the problem and stops all of the various types of deserialization attacks? According to CERT “Developers need to re-architect their applications.” Obviously, such a fix requires significant code changes, time, effort and money to achieve this. If changing the source code and the architecture of the application is an option then this is the preferred approach. However, bear in mind that even if an application does not perform any deserialization in its own components, most servers, frameworks and third-party components do. So, it is extremely difficult to be 100% certain that the whole stack does not and will never perform deserialization without breaking existing required functionality.

Especially for enterprise production environments with hundreds of deployed instances, making any source code changes is often not feasible to implement. Typically, for enterprise production environments, any security solution that requires code changes and more than a few minutes of

deployment time is not acceptable, especially for critical vulnerabilities such as the deserialization vulnerability. Enterprise solutions need accurate protection, fast and without requiring source code changes.

CERT alternatively suggests that blocking the network port using a firewall might solve the problem in some cases. However, in most cases this is not applicable. For example, the deserialization exploits in JBoss, WebLogic, WebSphere, etc run on the HTTP port of the web server. Which means that blocking that port will render the server useless. Also, such a solution cannot protect against blind deserialization attacks. Therefore, blocking the network port is not a viable option.

How are vendors addressing the issue?

Without going into much detail of every affected software, the following list shows how some vendors handled the issue:

Spring	Hardened the dangerous classes
Oracle WebLogic	Blacklist
Apache ActiveMQ	Whitelist
Apache BatchEE	Blacklist + Whitelist
Apache JCS	Blacklist + Whitelist
Apache OpenJPA	Blacklist + Whitelist
Apache OWB	Blacklist + Whitelist
Apache TomEE	Blacklist + Whitelist
Atlassian Bamboo	Disabled deserialization

Jenkins	Disabled deserialization + upgraded ACC

Also note that there were even cases where the vendors refused to create a fix for the issue either because they do not acknowledge the problem as their own problem or the affected system is an old version that is no longer supported.

Why blacklisting and whitelisting are bad solutions to the problem

Any security solution that depends on blacklisting of dangerous classes requires profiling of the application in order to verify that these classes are not utilized by the application. Without first profiling the application, it is not possible to blacklist a class because the risk of breaking the functionality of the application is significant. Additionally, adopting a negative security model means that you will never be sure that you have blacklisted everything.

The list of blocked signatures has to be maintained constantly and frequently and by definition it does not protect any unpublished, zero-day exploits. Any security solution that promotes a blacklisting strategy as a solution to deserialization attacks is doomed to fail since it plays the Whack-a-Mole game. Blacklisting is a poor strategy regardless if it occurs at the application layer, the JVM layer or the network layer.
Whitelisting is a better approach than blacklisting. However, to apply whitelisting, profiling of the application is again required. In this case, the whitelist will be a really big list of classes. Such big lists are difficult to manage, especially for enterprise environments. In addition, every time the application needs to upgrade to a newer release, the profiling needs to be performed again and a new white list needs to be created. This considerably complicates the deployment of new releases in production. This usually leads to whitelists that are not updated and, in turn, produces false positives. Finally, even if an enterprise decides to accept the effort to constantly profile their infrastructure and maintain whitelists, they are still vulnerable.

Another suggested mitigation is to blindly block (or whitelist) process forking and file/network IO. Even though this approach will reduce the impact of a deserialization attack, it does not protect against blind attacks for data exfiltration nor Denial of Service deserialization attacks.

Finally, some researchers suggest that using an ad-hoc Security Manager can help mitigate these attacks. However, the truth is that even though it is a good first mitigation step, it is insufficient because of its many limitations.

- Security Managers are known to be easily bypassed.
- It does not protect deferred attacks where the execution of the payload is executed after deserialization, for example via the finalize() method.
- Most DoS deserialization attacks cannot be mitigated by the Security Manager.
- To effectively utilise the Security Manager, another type of white list needs to be created and maintained; thus this approach suffers from the same limitations of the whitelisting.

How can customers with old or legacy versions of affected systems be protected against the Java deserialization attacks?

If the vendors cannot provide patches and the customers cannot make any source code changes, then how can such production systems be protected? The following are the currently available options.

- Web Application Firewalls – WAFs are not helpful here because they have no application context since they can only examine the input and the output of the application. Applying heuristics on the incoming requests is guaranteed to produce false positives and false negatives. Any security solution that has no application context and operates outside of the application cannot adequately mitigate deserialization attacks
- RASP vendors and Java agents that either disable deserialization completely or apply blacklisting / whitelisting on the classes that are getting deserialized.

It's unlikely that we've seen the last of hackers using insecure deserialization to target enterprise systems. With the ubiquity of Java and other languages that rely on serialization for communication, it's a good time to put safeguards in place to protect critical applications.

About the Author

Apostolos Giannakidis, Security Architect, Waratek Apostolos drives the research and the design of the security features of Waratek's RASP container. Before starting his journey in Waratek in 2014, he worked in Oracle for 2 years focusing on Destructive Testing on the whole technology stack of Oracle and on Security Testing of the Solaris operating system. Apostolos is acknowledged by Oracle for submitting two Java Deserialization vulnerabilities that were fixed in the Oracle January 2019 CPU Apostolos can be reached at Twitter @cyberApostle and at our company website http://www.waratek.com

IronNet

Two Years Later

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

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

LESSON 1

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

NOTPETYA CREATED AN UNPRECEDENTED

$10 billion

IN DAMAGE WORLDWIDE[1]

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

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

LESSON 2

NotPetya raised the speed limit for modern cyber attacks.

NOTPETYA SPREAD TO MORE THAN

64 countries

IN JUST THE FIRST

24 hours[2]

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

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

LESSON 3

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

THE FAR-FLUNG INDUSTRIES AFFECTED BY NOTPETYA INCLUDE

shipping, pharmaceuticals, banking, advertising, energy

AND OTHER MAJOR SECTORS [3]

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

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

LESSON 4

NotPetya shows the limits of attribution.

CYBERATTACK ATTRIBUTION IS GETTING MORE COMPLEX, WITH AT LEAST

10 variations

OF NATION-STATE RESPONSIBILITY [6]

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

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

1 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
2 https://www.securityweek.com/petyanotpetya-what-we-know-first-24-hours
3 https://www.securityweek.com/notpetya-attack-costs-big-companies-millions
4 https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/
5 https://ironnet.com/white-paper-survey-download/
6 https://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF


EVENTS

Official Partner

Bundesministerium
Landesverteidigung

CYBER INTELLIGENCE EUROPE

VIENNA AUSTRIA | 25TH – 26TH SEPTEMBER 2019

Esteemed Speaker Line-up:

Major General Helmut Habermayer, Director Capability Development Directorate, Cyber Coordinator, Ministry of Defence, Austria

Heiko Lohr, Head of Cybercrime Sub-Directorate, Federal Criminal Police Office (BKA), Germany

Christian Liflander , Head, Cyber Defence Section, Emerging Security Challenges Division, NATO

Laurent Weber, Managing Director, Governmental CERT of Luxembourg (GOVCERT.LU)

Ondrej Rojcik, Head, Strategic Analysis, National Cyber and Information Security Agency, Czech Republic

Natalia Spinu, Head, Cyber Security Center (CERT-GOV-MD), Moldova

Heidi Kivakas, Chief Specialist, Finland National Cyber Security Centre

Neil Walsh, Chief of Cybercrime, Anti-Money Laundering and Counter Financing of Terrorism Department, United Nations Office on Drugs and Crime (UNODC)

Egidija Versinskiene, Director, Cybercrime Centre of Excellence for Training, Research and Education, Lithuania

Roland Kumnova, Senior Programme Assistant, and OSCE Focal Point on Cyber Security, Serious and Organised Crime Section, Department for Security and Public Safety, OSCE Mission in Kosovo

Klorenta Janushi, Specialist, Standardisation Sector, National Authority on Electronics Certification and Cyber Security, Ministerial Council, Albania

Blerim Krasniqi, Head of IT Forensics, Kosovo Agency of Forensics

Mustafa Afyonluoglu, Cyber Security and Chief e-Government Expert, Turkey

Kadri Kaska, Law and Policy Researcher, NATO Cooperative Cyber Defence Centre of Excellence

SPONSORSHIP OPPORTUNITIES STILL AVAILABLE!

Interested in showcasing your latest solutions/products at our international Cyber Intelligence Europe conference and exhibition please contact us at events@intelligence-sec.com or +44 (0)1582 346 706

Sponsors & Exhibitors

Resecurity

SPECTRAMI Redefining Value

EclecticIQ

For more information visit – www.intelligence-sec.com

Book your place by:
w: www.intelligence-sec.com I e: events@intelligence-sec.com I t: +44(0)1582 346706

INTELLIGENCE-SEC

9-10 DECEMBER 2019
INTERCONTINENTAL FESTIVAL CITY, DUBAI, UAE

المؤتمر الدولي للحد من الجريمة

CRIME PREVENTION INTERNATIONAL CONFERENCE

HOSTED BY

شرطة دبي
DUBAI POLICE

حكومة دبي
GOVERNMENT OF DUBAI

JOIN US IN SHAPING THE FUTURE OF URBAN SAFETY AND SECURITY

Through state-of-the-art national security programs, Dubai serves as a benchmark of urban safety. The city continues to set global standards for crime prevention despite boasting a booming tourism industry and a transient population. Commendably, the organization at the core of these security frameworks is The Dubai Police. With this in mind, we are pleased to organize the Future Crimes Prevention and Reductions World Congress under the patronage of The Dubai Police to highlight the programs underwriting UAE's nation-wide safety strategies while exploring the global initiatives shaping the future of urban safety and security. This unprecedented 2- day summit is dedicated to both strengthening the future of community policing and exchanging best-practices in crime prevention.

The Crime Prevention International Conference is your opportunity to meet all the leading security stakeholders, technology providers and innovative solution providers that could contribute to the emerging security requirements in the Middle East and North Africa. For more information and register, visit dubaipolicecrimeprevention.com or email us at partnerships@gmevents.ae

ORGANISED BY

gmgroupdubai | the-great-minds-group | gmgroupdxb | thegreatmindsgroup.com

GM EVENTS

SPONSORS & PARTNERS

HIKVISION · ring · CRISTANINI CBRN DECONTAMINATION SYSTEMS · AQSACOM · WIREONAIR · Gesab guarantee for the future · النابودة alnabooda

JOS. HANSEN & SOEHNE GULF L.L.C. · CAMINOS Tools, Equipment & Training · AD VANCED SY STEMS · Hytera · PHONEXIA · SAT Scientific Analytical Tools · iPS visionary intelligence

MVP TECH · ESHARAH إشارة · VISLINK Technologies · Covidence miniature surveillance solutions

Indonesia Security Summit 2019

ACCELERATING CYBER SECURITY FOR A SAFER INDONESIA

2ND ANNUAL INDONESIA SECURITY SUMMIT

After a successful launch edition last year, Indonesia Security Summit is back for a second round! Focused on the theme, Accelerating Cyber Security for a Safer Indonesia, the 2nd Annual Indonesia Security Summit is a knowledge-sharing platform for key representatives from the Government, the top CISOs, CIOs, CTOs, senior information security, risk, forensics, compliance, cyber law and law enforcement professionals. The summit will focus on the current state of cybercrime in Indonesia, the latest fraud and breach prevention techniques and will also showcase some of the latest technologies that help combat cybercrime.

REGISTRATIONS OPEN NOW

JAKARTA, INDONESIA 3 - 4 SEPTEMBER 2019

GOLD SPONSORS

tenable Microsoft CHECKMARX McAfee Together is power. SailPoint

SILVER SPONSORS

CYBERARK DIGIFOR INTERTECH ASIA Digital Security for Everyone Cellebrite Digital intelligence for a safer world Data Expert

LOUNGE EXHIBITORS

ManageEngine a division of Zoho Corp. BIZSECURE Asia Pacific Securing Your Business Gigamon T-Systems arcon

LUNCH SPONSOR

SALT

SATCHEL SPONSOR

QRATORLABS

For more information, visit www.indonesiasecuritysummit.com
To register, contact Praveen venu
praveenv@tradepassglobal.com | +91-88481-81461

TRADEPASS

UNICOM

Agile & DevOps Expo

17 October 2019, London

UNICOM

TestExpo 2019

17 October 2019, London

COUNTER UAS USA

Expert presentations from the US and international military, government and law enforcement agencies

August 20-22, 2019
Washington D.C.

DEFENDING THE SKIES: CUTTING EDGE CUAS SOLUTIONS!

REGISTER TODAY! COUNTERUAS.IQPC.COM

BIS GROUP
Global Conferences & Events Management Company

Renewable Energy Cyber Security Forum

16th - 17th October 2019 - Berlin, Germany

Renewable Energy needs a common understanding of cyber threats and mitigation strategies to enable assets to be protected over internal and external threats

The lack of standards, insufficient board level understanding of cyber threats, legacy assets and new technology pose important challenges for cyber security professionals working in renewable energy, both in Europe and US.

Join industry experts on 2-day event to learn how key players in the renewable energy sector have been able to stay resilient, invest in the right technology and convince their stakeholders it's worth ranking cyber security up in their priority list.

CONFIRMED SPEAKERS:

- Innogy Innovation GmbH
- European Commission
- Siemens Gamesa
- Innogy SE
- Associated British Ports
- GCube Insurance
- LC Risk Ltd.
- Adani Group
- GE Renewable Energy
- WiseEnergy
- PSE
- RES Group
- GE Renewable Energy
- University of Bristol

Some of the Practical Case Studies to be presented:

European Commission - One Size does not Fit All - Cyber Security Recommendations for the Renewables Sector

Innogy SE - IT vs. OT: Differences, Investment Opportunities, Vulnerability Strategies

PSE - Cyber Hygiene - What does it mean in practice?

RES Group - Hands on Case Study: Navigating the Intricacies of a Cyber Attack

Adani Group - How to take the first step to protect your solar assets and map out a successful strategy

Special Offer: Early bird **15%** discount till 26.6.2019
Use code **BIS15DOWN** during online registration

linkedin.com/company/2602008/
twitter.com/BisGrpCom
facebook.com/bisgroupsro/

For further information, please contact us on: linak@bisgrp.com

C-SUITE & SENIOR LEVEL EXECUTIVES ONLY

CYBER SECURITY SUMMIT 2019

PROTECT YOUR BUSINESS FROM CYBER ATTACKS

$150 ADMISSION | Use Promo Code: **CDM19** for $150 Admission.
(Standard Admission: $350)

Register Now at **CyberSummitUSA.com** »

6 CPE CREDITS Full day attendance earns 6 credits following the Summit

2019 CYBER SECURITY SUMMITS

Denver, CO - Apr. 2	**DC Metro, VA** - Jul. 16	**Scottsdale, AZ** - Oct. 17
Philadelphia, PA - Apr. 25	**Chicago, IL** - Aug. 27	**Boston, MA** - Nov. 6
Dallas, TX - May 16	**Charlotte, NC** - Sep. 17	**Houston, TX** - Nov. 21
Seattle, WA - June 25	**New York, NY** - Oct. 3	**Los Angeles, CA** - Dec. 5

THOUGHT LEADERS INCLUDE

Bryan Deyoung
Digital Forensics Lab Philadelphia
U.S. Secret Service

Deb Walter
Manager InfoSec Policy, Standards, Training & Awareness
AmerisourceBergen

Ryan Spelman
Senior Director
Center for Internet Security

Paul De Souza
Founder & President
Cyber Security Forum Initiative

Tory Smith
Special Agent
The FBI

This Pass is for C-Suite & Sr. Level Executives only and includes a Catered Breakfast, Lunch & Cocktail Reception. Sales/Marketing professionals will Not admitted.

INTERACTIVE PANELS

RANSOMWARE
To Pay or Not To Pay - That is the Question!

INSIDER THREAT
Protect Your Enterprise from the Human Element

ORCHESTRATION
CISO & Sr. Leadership's Best Approach to Cyber Defense

CLOUD INSECURITY
Common Pitfalls that Organizations Make when Moving to the Cloud and How to Avoid

INCIDENT RESPONSE
What to do Before, During and After a Breach

To Speak or Exhibit at a future Summit, contact:
MHutton@CyberSummitUSA.com

CYBER SECURITY & CLOUD EXPO WORLD SERIES

EXPLORING THE SECURITY NEEDS OF FUTURE TECHNOLOGY

GLOBAL
25-26 APRIL 2019
OLYMPIA GRAND, LONDON

EUROPE
19-20 JUNE 2019
RAI, AMSTERDAM

N.AMERICA
NOVEMBER 13-14, 2019
SANTA CLARA, CA

TOPICS INCLUDE

- Data Intelligence
- Ecosystem
- Security
- Enterprise
- Privacy
- Governance
- Identity
- Infrastructure

REGISTER NOW FOR FREE

+44 (0) 117 980 9020 | enquiries@cybersecuritycloudexpo.com | www.cybersecuritycloudexpo.com

Co-hosted Events

BLOCKCHAIN EXPO WORLD SERIES

AI & BIG DATA EXPO WORLD SERIES

IoT TECH EXPO WORLD SERIES

GCC FORENSICS
CONFERENCE & EXHIBITION

13 - 14 NOV 2019 | THE GULF HOTEL BAHRAIN

مؤتمر ومعرض الخليج العربي للأدلة الجنائية

THE MUST ATTEND EVENT FOR THE ENTIRE FORENSIC SECTOR IN THE MIDDLE EAST

LAW ENFORCEMENT FORENSICS
FORENSIC LABS | INVESTIGATIONS/RESEARCH
DIGITAL FORENSICS | ACADEMIA
COURT ROOMS AND CRIMINAL LAW | SECURITY

13 - 14 November 2019

www.gccforensics.com

/gccforensic

@gccforensic

@gccforensic

Media Partner

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Supported by

Ministry of Interior

Organised by

CLARION EVENTS

IDENTITY WEEK ASIA

GLOBAL • TRUSTED • VISIONARY

SDW ASIA | PLANET BIOMETRICS ASIA | DIGITAL:ID ASIA

EXPLORING NEXT-GENERATION GOVERNMENT, COMMERCIAL & CITIZEN IDENTITY SOLUTIONS

Identity Week Asia comprises of three world-class events: Digital:ID Asia, Planet Biometrics Asia and SDW Asia- all focused on the concept of identity.

IDENTITY WEEK ASIA

8-9 October 2019

Suntec Convention Centre, Singapore

www.terrapinn.com/identityweekasia

Created by

science media partners

SPARK SOMETHING TERRAPINN

BIS GROUP
Global Conferences & Events Management Company

2nd Annual
Automotive Cyber Security Forum

9 - 10 October 2019 - Berlin, Germany
Venue: Wyndham Garden Berlin Mitte

The discussion during two days will evolve around the approaches and practices on safe operation of systems and meeting the increasing requirements for automotive cyber security, including:

- Challenges in building Cybersecurity Competence. Risks for the Automotive Industry
- Automotive Cybersecurity Engineering – Standards and Regulations to be considered in the Process Landscape
- Major Security Features requested by OEMs
- New Security Risks in Autonomous, Connected Vehicles
- How can we ensure the vehicle itself is safe from cyber threats?
- Overview of EU Commission Initiatives on Securing Connectivity and the Automated Vehicles
- Real incidents and pitfalls. Good practices on securing autonomous vehicles

During the Interactive World Café Sessions cyber security of autonomous and connected vehicles will be discussed in small groups.
In the Chair: Christian Beul, Head of Automotive Strategy & Technical Risk Advisory at INVENSITY GmbH.

SPEAKER COMPANIES:

- Volvo Cars
- European Union Agency for Cybersecurity
- European Commission
- Continental Automotive GmbH
- INVENSITY GmbH
- ITK Engineering GmbH
- Veoneer
- ARRIVAL
- Assured AB
- Vodafone Automotive

Some of the Practical Case Studies to be presented:

Volvo Cars
Elpidoforos Arapantonis
Automotive System and Network Design Engineer

- New Security Risks for Autonomous, Connected Vehicles
- Future connected vehicle and what does "securing" mean?
- The most realistic threats
- What attack surfaces and vectors need to be prioritized

European Commission
Dr. Florent Frederix
Principal Administrator, Trust and Security Unit

- Data privacy and the rights of data subjects
- Cybersecurity schemes to guarantee a secure data exchange
- Certification Schemes
- The extended role of the ENISA
- Recommendation on the security of 5G networks

Vodafone Automotive
Jofre Palau
Principal Product Security Manager

- Automotive Connectivity Cyber Security
- Real incidents and pitfalls
- Mitigating cyber threats to vehicle connectivity
- Connectivity outlook and security implications

Learn more here
www.bisgrp.com
or through
#BISacs

linkedin.com/company/2602008/
twitter.com/BisGrpCom
facebook.com/bisgroupsro/

For further information, detailed agenda and registration please contact us at linak@bisgrp.com, Lina Kozina, Project Lead – Marketing

CYBER SECURITY & DATA PROTECTION

IN PHARMA & HEALTHCARE CONGRESS

25 - 26 September 2019 | ILEC Conference Centre, London, UK

Cyber Security & Data Protection represent a priority for everyone working in Pharma & Healthcare. This congress explores the Cyber Security landscape with a special emphasis on securing the data in these industries, analysing vulnerabilities & threats with the aim of minimising them through current & upcoming technologies & applications. Attendees will benefit from case studies of the successes, strategies & novel technologies for securing data, managing patient risk & streamlining medical device security.

Featuring Keynote Addresses from:

FREDERIC VIRMONT
Merck Group

RAMÓN SERRES
Almirall

450+ Attendees representing global pharma organisations, leading biotech companies & internationally renowned academic institutions.

20+ Presentations & Case Studies focusing on overcoming key vulnerabilities & threats in the Pharma & Healthcare industries, including presentations on Information Security & the use of Blockchain to secure 'omics data.

Including 2 Interactive Streams:

- Analysing and Overcoming Vulnerabilities and Threats in the Cyber Security Landscape

- Strategies & Novel Technologies for Maximizing Data Protection

To view the agenda, click here

What You Can Expect

Companies & institutions at the forefront of this field, including AstraZeneca, Boehringer Ingelheim, Bristol-Myers Squibb & the NHS.

Key focus areas include network security, social engineering, encryption & blockchain & incident response strategy. It also features focuses on the importance of privacy & data protection when it comes to clinical trial & 'omics data.

Our program will bring together senior industry experts & key opinion leaders in Cyber Security & Data Protection. Some of our expert speakers include:

- Victoria Perez Riu, Chief Privacy Officer, AstraZeneca

- Thomas Roth, Global Data Protection Officer, Boehringer Ingelheim

- Matthew Rooney, Chief Clinical Information Officer, NHS

Want more? See our new Content HUB for updates, videos and insights at www.oxfordglobal.co.uk/news

Join our PharmaTec Networking Group on LinkedIn, follow us on Twitter @PharmaTecSeries & join the

Companies to attend or sponsor include: IBM, OnForce, PerkinElmer For the Better, Roche, NOVARTIS, AMGEN, abbvie

To register or for more information

Visit the website: www.oxfordglobal.co.uk/cybersecurity-congress
Contact Bradley Copeman: b.copeman@oxfordglobal.co.uk | +44 (0)1865 248455

Organized by INSURANCENEXUS

CYBER INSURANCE USA 2019

NOVEMBER 4-5, 2019 • HYATT REGENCY McCORMICK PLACE • CHICAGO, USA

Cyber Defense e-Magazine has secured a $100 off registration, quote CYBERDEFENSE100 when you register online at: https://events.insurancenexus.com/cyberusa/register.php

Build the Foundation of Sustainable Cyber Insurance Products Using Innovative Technology

150+ ATTENDEES | **20+** SPEAKERS | **20+** HOURS OF DEBATE

The only conference focused on building sustainable, cost-efficient, bespoke, cyber insurance products

Cyber Insurance USA 2019 (4-5 November) is bringing together senior professionals across all aspects of product creation to deliver on satisfying customer needs by creating a sustainable, customer-centric product.

Walk Away with Practical Knowledge of Transforming Cyber Insurance into a Sustainable Product, Including:

- **Build a sustainable book:** use predictive modelling to be prepared in an event of cyber hurricane.
- **Take charge of silent cyber losses:** establish line of communication between P&C and cyber lines and incorporate clear-cut policy wordings to minimize your exposures.
- **Get ahead in cyber policy underwriting:** collate and utilize data for scenario-based modelling to anticipate potential losses and underwrite prospective coverage grants.
- **Act as partner and preventer:** guide customers in maximizing their security stance and respond to cyber breaches in the most efficient manner.

Speaker Line-Up of Visionaries and Senior Leaders

Joe Turek
VP, Cyber and Professional Liability Midwest Regional Manager
Chubb Financial Lines

Catherine Rudow
VP, Cyber Insurance
Nationwide

Elissa Doroff
VP, Underwriting and Product Manager
XL Catlin

Jonelle Horta
VP, Cyber Underwriting & Risk Management Platform Lead
Allied World

Michael Born
VP, Account Executive
Lockton Companies

Kelly Castriotta
Deputy Regional Head of Product Development Leader
Allianz

Cyber Defense e-Magazine has secured a $100 off registration, quote CYBERDEFENSE100 when you register online at: https://events.insurancenexus.com/cyberusa/register.php

BIS GROUP
Global Conferences & Events Management Company

Renewable Energy Cyber Security

16 - 17 October 2019 - Berlin, Germany
Venue: Eurostars Berlin

How to Develop a Cyber Security Roadmap for your Assets

What steps you should be taking to develop a roadmap to enable your infrastructure to be more secure and ultimately reduce risks for your business? This workshop will be looking at how you can:

- Look at your technical gaps
- Segmentating infrastructure
- Efficiently upgrading firewalls and loggging in events
- Educating stakeholders by creating value for them
- Thinking about risks in terms of severity, likelihood, and the impact downstream
- Finding the necessary expertise by getting an assessment from standard bodies
- Looking at talent and skill set and why unconventional channels should be used

SPEAKER COMPANIES:

- European Commission
- NATO Energy Security Centre of Excellence
- Associated British Ports
- Thames Water
- innogy Innovation GmbH
- PSE
- RES Group
- GE Renewable Energy
- Siemens Gamesa
- Adani Group
- Yaskawa Solectria Solar
- Aperio Systems
- WiseEnergy
- GCube Insurance

World Café Sessions

In the World Café, experts will communicate in small discussion groups dedicated to a specific topic, switching groups periodically. The results and conclusions are reflected then in a common session.

Day 1

- The future landscape of cyber security and resilience for the renewable sector
- Security in renewable energy production: How cyber security is affecting its future

Day 2

- Adapting cybersecurity to OT environments
- Bridging the knowledge gap between IT and OT
- Machine learning and blockchain to protect renewable assets

Some of the Practical Case Studies to be presented:

European Commission - One Size does not Fit All - Cyber Security Recommendations for the RE Sector
NATO Energy Security Centre of Excellence - NATO's approach/strategies to reduce the risk of cyber attacks and build resilience in cyber domain
Yaskawa Solectria Solar - Changes in the US solar market and how it is leading to increased need for cybersecurity
GE Renewable Energy - SCADA Systems to Balance Security Risks with Cost
PSE - Cyber Hygiene - What does it mean in practice?
RES Group - Hands on Case Study: Navigating the Intricacies of a Cyber Attack
innogy Innovation GmbH - Finding cybersec solutions that will tackle (future) energy system security challenges

Learn more here
www.bisgrp.com
or through
#BISrecs

linkedin.com/company/2602008/
twitter.com/BisGrpCom
facebook.com/bisgroupsro/

For further information, detailed agenda and registration please contact us at linak@bisgrp.com, Lina Kozina, Project Lead – Marketing

HELD UNDER THE PATRONAGE OF HIS EXCELLENCY, PRESIDENT ABDEL FATTAH EL-SISI
THE PRESIDENT OF THE ARAB REPUBLIC OF EGYPT, THE SUPREME COMMANDER OF THE EGYPTIAN ARMED FORCES

EGYPT DEFENCE EXPO

7-10 DECEMBER 2020
EGYPT INTERNATIONAL EXHIBITION CENTRE

www.egyptdefenceexpo.com
@egyptdefenceexpo
/egyptdefenceexpo
@visitedex
#edex2020

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

EGYPT INTERNATIONAL EXHIBITION CENTRE
7-10 DECEMBER 2020

400 + EXHIBITORS

30,000 + VISITORS

FULLY-HOSTED VIP DELEGATION PROGRAMME

Media Partner

CDM CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Supported by

Ministry of Defence

Egyptian Armed Forces

Ministry of Military Production

جهاز مشروعات الخدمة الوطنية

Organised by

CLARION EVENTS

CYBER OPERATIONS FOR NATIONAL DEFENSE

2019 KEYNOTE SPEAKERS:

Gen James "Mike" Holmes, USAF
Commander
Air Combat Command

Maj Gen Burke "Ed" Wilson, USAF (Ret.)
Deputy Assistant
Secretary of Defense For Cyber Policy

Ignatius "Buck" Liberto
Chief of Staff
Joint Force Headquarters - DODIN

Robert Kazimer
Deputy Commander
US Army Cyber Center of Excellence

SEPTEMBER 19-20, 2019
ALEXANDRIA, VA

DEFENSE STRATEGIES INSTITUTE
ADVANCING THE MISSION - SUPPORTING THE FORCE

LEARN MORE: CYBERSECURITY.DSIGROUP.ORG

Cyber Security Series

Booking Contact: David Schkade
tel: +420 255 719 045; email: davids@prosperoevents.com

prospero EVENTS GROUP

CYBER DEFENSE MAGAZINE

Get 10% discount with promo code CDMCYBER19

6th Cyber & SCADA Security for O&G Industry 2019

18-20 September 2019, Amsterdam

Speaker companies:

SGN, MAERSK DRILLING, AkerSolutions, NAPCON, NAMUR, International Operational Technology Security Association, Kraft CERT, PETRONAS, EP ENERGY, axite security

Presentations on:

- *Introduction of scenario thinking & Digital Twin*
- *Evolution of cyber security ICS*
- *In the wake of notPetya…*
- *Unrealistic exercises only render you good at exercising*
- *Table Top Exercise - Incident response in OT Environment*
- *Social Engineering Aspects of Cyber Security*

6th Cyber & SCADA Security for Power and Utilities 2019

25-27 September 2019, Berlin

Speaker companies:

VATTENFALL, Sibelga, Vestas, EE-ISAC, DESFA, ENGIE Laborelec, swissgrid, 50hertz, ervia, uponor, DEFENSE

Presentations on:

- *Coordination and cooperation from the Energy CERT*
- *Active Cyber Defense*
- *SOC cooperation: effective response to a rapidly evolving threat landscape*
- *Information Security in the Boardroom & Leadership Team*
- *AI to increase cybersecurity of OT systems*
- *Cyber Resilience in the Electricity Ecosystem*

4th Cyber Security for Transport Sector 2019

26-27 September 2019, Berlin

Speaker companies:

DB, CSA CZECH AIRLINES, MAERSK, ISF Information Security Forum, GENEVE AEROPORT, sporveien, Munich Airport, Swedavia Airports, Stena

Presentations on:

- *Taking on TaaS - Transport as a Service*
- *Securing Supply Chains: Past, Present, Way Ahead*
- *SOC cooperation: Effective response to a rapidly evolving threat landscape*
- *Implementing lessons learned from a major cyber-attack*
- *Experiences from Building Cyber Defense Center*
- *ER-ISAC: Information sharing for cyber security of railway systems*

ITU TELECOM WORLD '19

Budapest 9-12 September

BETTER SOONER

ITU TELECOM WORLD 2019

The global event for governments, corporates and tech SMEs.

Accelerating ICT innovation to improve lives faster.

9-12 September 2019, Budapest, Hungary

ITU Telecom World 2018 is the global platform to accelerate ICT innovations for social and economic development. It's where policy makers and regulators meet industry experts, investors, SMEs, entrepreneurs and innovators to exhibit solutions, share knowledge and speed change. Our aim is to help ideas go further, faster to make the world better, sooner.

Visit telecomworld.itu.int to find out more.

#ituworld
telecomworld.int

Noord InfoSec Dialogue UK

17th & 18th September, 2019

Crowne Plaza, Gerrards Cross

"The Noord Infosec Dialogue is very informative. It's useful to understand what others are experiencing in other industries and helps to validate our own efforts and challenges."

IT Security,
Virgin Atlantic Airways
(Delegate)

noord
be part of the conversation

"Asia's Premier Counter-Terrorism and Internal Security Exhibiton and Conference!"

The 2nd Edition of

CTAX

COUNTER TERROR ASIA EXPO 2019

Co-Located With:

CTAC 2019

An International Conference on Counter-Terrorism and Internal Security

Incorporating 3 Major Segments:

HOMELAND SECURITY ASIA 2019

An International Exhibition On Homeland and Border Security Equipment and Technology

ICIDA

INSTALLATION AND CRITICAL INFRASTRUCTURE DEFENCE ASIA 2019

An International Exhibition On Installation And Critical Infrastructure Protection Equipment and Technology

CDA 2019

CYBER DEFENSE ASIA

An International Exhibition On Countering Cyber Terrorism and Cyber Defence.

OCTOBER

16 - 17

Jakarta International Expo Kemayoran, Indonesia

For more info, contact us:

Phone: (+65) 6100 9101

Email: sg@asiafireworks.com

www.counterterrorasia.com

Organized by:

FIREWORKS TRADE MEDIA GROUP

Fireworks Trade Media Pte Ltd

Strategic Partner:

Supporting Organizations :

Media Partners :

UNDER THE PATRONAGE OF HIS MAJESTY KING HAMAD BIN ISA AL KHALIFA, KING OF THE KINGDOM OF BAHRAIN

WINNER
BEST TRADE SHOW OVER 10,000SQM IN THE MIDDLE EAST
MESE 2018 AWARDS

معرض ومؤتمر البحرين الدولي للدفاع
BIDEC
Bahrain International Defence Exhibition & Conference

BAHRAIN'S PREMIER INTERNATIONAL TRI-SERVICE DEFENCE SHOW

28 - 30 October 2019
Bahrain International Exhibition & Convention Centre

Over 9,000 visitors from **49 countries**

180 + Exhibiting Companies

5 Off-Site Activities + Strategic Military Conference

Fully-Hosted VIP Delegation Programme

www.bahraindefence.com /visitbidec @visitbidec @visitbidec2019

Gold Sponsor

LOCKHEED MARTIN

Officially Supported by

Bahrain Defence Force
Royal Bahrain Air Force
Royal Guard
Royal Bahrain Naval Force
National Guard
Ministry of Foreign Affairs
Ministry of Information Affairs

Media Partner

CDM CYBER DEFENSE MAGAZINE

In Conjunction with

MEMAC
Middle East Military Alliances & Coalitions

Knowledge Partner

DERASAT

Organised by

FAAIYAT MANAGEMENT CO. W.L.L.

CLARION EVENTS

In cooperation with AFCEA

FUTURE FORCES FORUM International Platform for Trends & Technologies in Defence & Security www.future-forces-forum.org

International Security Conference

SCADA SECURITY

Organized as a part of FUTURE FORCES FORUM

4 – 5 November 2019

Hotel DAP, Prague, Czech Republic

Topics

- Current and future cyber threats and their solution
- New trends in technology in the ICS security
- Connected world, Mobility and the Internet of things
- Human factor and related topics
- Public safety in smart cities
- GDPR in environment of the smart cars

Focus

- Security, operational and IT community of the critical infrastructure
- Public sector
- Armed and security forces
- Academia and private sector taking part in the projects of protecting the critical information infrastructure, with more attention given to the current topics of the cyber security

Patronage and professional sponsorship

Register as a speaker, partner or visitor:

www.future-forces-forum.org

SAUDI EMERGING TECHNOLOGIES FORUM

11 - 13 November 2019, RIYADH, SAUDI ARABIA

emergingtechnologiesksa.com

CORRECTION FROM COLLABORATION

FEATURING:

- **Vulnerabilities in Airline Scheduling**
  Bob Kalka
- **Security Built on One Single Premise**
  Drew Vanover
- **Business Cyber Survival: Are You at Risk?**
  Loren Wagner
- **Incident Response: Under the Microscope**
  Tim Opsitnick
- **Malicious Bot Attacks: The New #1 Cyber Threat**
  Carl Gustas
- **The Game of Cybercat & Cybermouse**
  Lawrence Pitt
- **Developing a Security Awareness Program**
  Lauren Zink
- **Implementing Sustainable Compliance Solutions**
  Steven Stransky
- **How to Cyber Secure Your Organization Just Changed**
  Caston Thomas
- **Building a Resilience Cyber Security Strategy**
  Kurt Van Etten
- **Scaling Multicloud and Hybrid Cloud Usage without Sacrificing Data**
  Glen Roebuck

NEW THIS YEAR

Earn CPEs

MONDAY Xcellerate your Career Day

TUESDAY expanded Career Connection

WEDNESDAY-FRIDAY now 3-day ISS SUMMIT

FIVE new focus TRAX within the 3-day ISS

Plus five Keynote Speakers and nearly 100 additional presentations!

For more information and registration to the region's largest IT Security gathering go to:

www.informationsecuritysummit.org

Use Coupon CODE **2019EBRate** for 30% off 3-day ISS

Check Point SOFTWARE TECHNOLOGIES LTD
tenable network security
LOGICALIS Business and technology working as one
CDM CYBER DEFENSE MAGAZINE
Pulse Secure
REDSEAL
okta
Hurricane Labs
IBM

BOOK BY **28TH JUNE 2019** TO SAVE **£300** • BOOK BY **30TH SEPTEMBER 2019** TO SAVE **£100**

SMi Group Proudly Presents the 3rd Annual...

SMi
LINKING BUSINESS *with* INFORMATION

MARITIME INFORMATION WARFARE

18TH - 19TH NOV 2019

Maximising and Managing Information Warfare for the Modern Navy

Copthorne Tara Hotel, London, United Kingdom

BENEFITS OF ATTENDING:

- Keynote Briefing from **Commodore Ian Annett, Assistant Chief of Staff Information Warfare and Chief Information Officer, Royal Navy,** on the **Future of Royal Navy Developments and Capabilities**
- Updates on Maritime **Systems and Platforms across NATO** and how they are improving Data Exploitation
- Emphasis on **Cyber Warfare,** and the importance of more effective Cyber Defence as the maritime sphere becomes more information technology-centric
- Close attention paid to **Artificial Intelligence,** in particular how a mixture of automation, machine learning and unmanned systems are being developed

CONFERENCE CHAIRMAN:

Vice Admiral (Ret'd) Duncan Potts CB, Former Director General Joint Force Development, **Joint Forces Command**

MILITARY AND GOVERNMENT EXPERTS INCLUDE:

Commodore Ian Annett, Assistant Chief of Staff Information Warfare and Chief Information Officer, **Royal Navy**

Captain Matthew McGonigle, Commodore, Littoral Combat Ship Squadron One, **US Navy**

Captain Timothy Unrein, Operations Intelligence, **NATO MARCOM**

Captain Alfred Turner, Joint Military Operations Specialist, Naval War College, **US Navy**

Commander Lee Atkinson, Directorate of Naval Requirements 6, Communications, Information Systems and Cyber, **Royal Canadian Navy**

Commander Juan José Nieto Conde, SCOMBA Technical Director, **Spanish Ministry of Defence**

Commander Miguel Bessa Pacheco, Head of Intelligence Division, **Portuguese Navy**

Commander Amleto Gabellone, Program Manager - Research Development, **NATO STO-CMRE - Centre for Maritime Research and Experimentation**

Mr Bruno Bender, Information and technology Consultant on the RIFAN system, Former French Ministry of Defence, **GICAN**

Professor Richard Crowell, Joint Military Operations Specialist, Naval War College, **US Navy**

Colonel (Ret'd) Ralph Thiele, Managing Director, **Stratbyrd Consulting**

www.maritimeinfowarfare.com/cdmag

Register online or fax your registration to +44 (0) 870 9090 712 or call +44 (0) 870 9090 711

SPECIAL RATES AVAILABLE FOR MILITARY AND GOVERNMENT REPRESENTATIVES

CPD CERTIFIED The CPD Certification Service

@smigroupdefence
#MIW2019


ISAF
IT SECURITY
8TH INTERNATIONAL INFORMATION
& NETWORK SECURITY EXHIBITION
OCTOBER 17TH-20TH, 2019
Istanbul Expo Center (İFM) - Yesilkoy / Istanbul
www.isaffuari.com
MARMARA
TANITIM FUARCILIK
www.marmarafuar.com.tr | Tel: +90 212 503 32 32 | marmara@marmarafuar.com.tr
KOSGEB
BU FUAR 5174 SAYILI KANUN GEREĞİNCE TOBB (TÜRKİYE ODALAR VE BORSALAR BİRLİĞİ) DENETİMİNDE DÜZENLENMEKTEDİR.

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

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

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

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

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

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

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

Visit **https://www.goanywhere.com/think-like-a-hacker**

to get a free copy of our cybersecurity guide.

GO ANYWHERE®
Managed File Transfer

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

"Amazing Keynote"

"Best Speaker on the Hacking Stage"

"Most Entertaining and Engaging"

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

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

CYBER DEFENSE TV

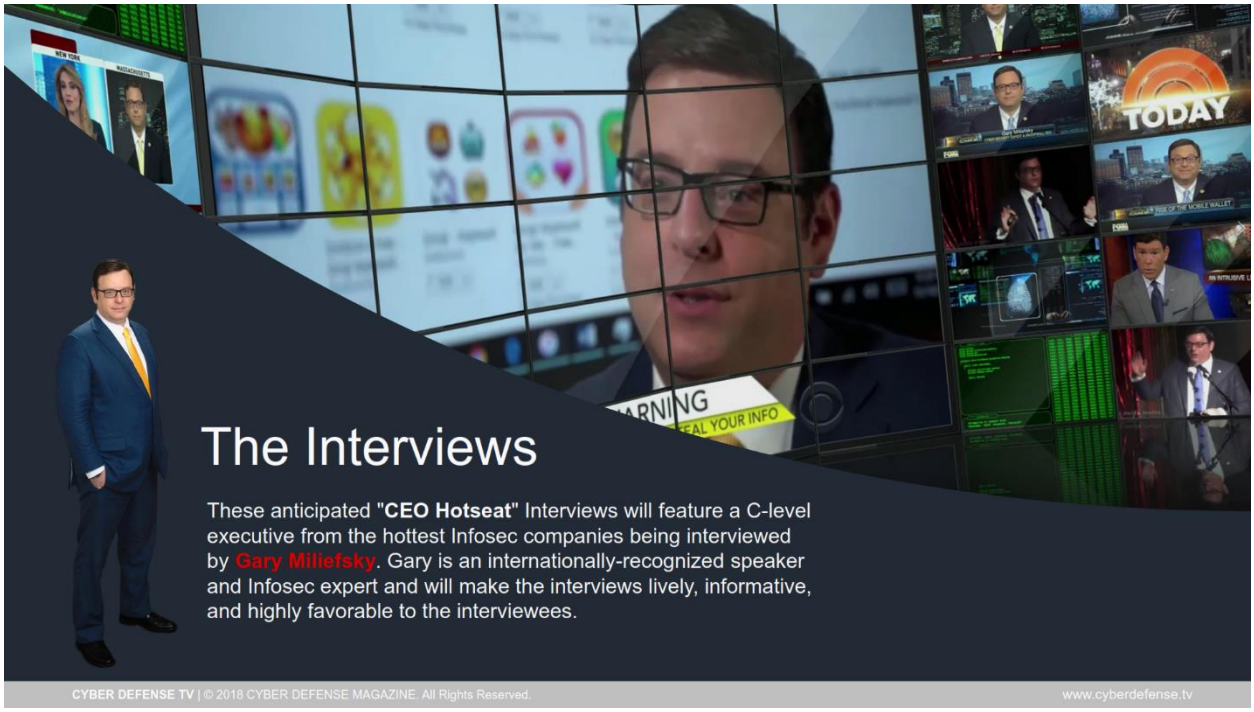
INFOSEC KNOWLEDGE IS POWER

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

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

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

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



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

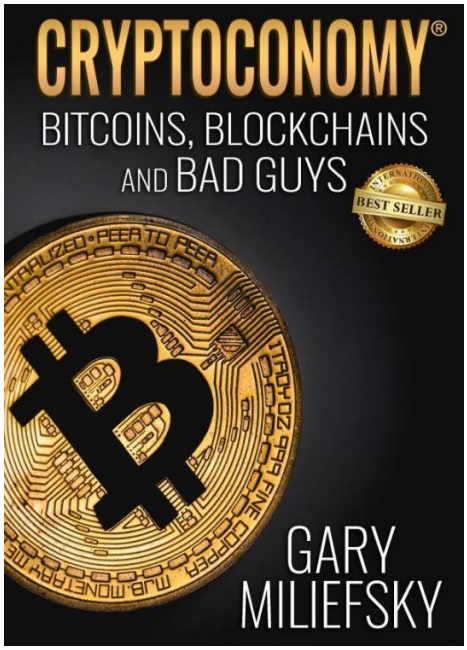
276 Fifth Avenue, Suite 704, New York, NY 1000
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 08/01/2019

TRILLIONS ARE AT STAKE

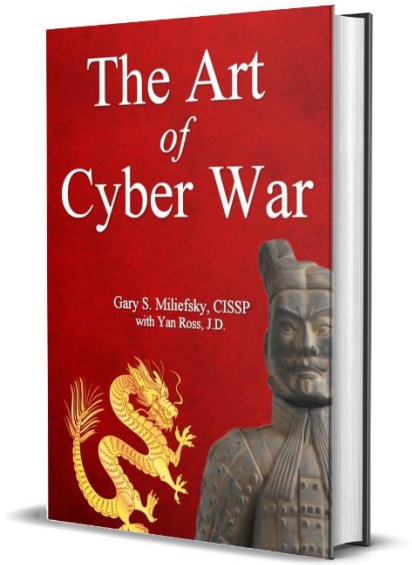
No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES

Released:



https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH

In Development:



Do your file transfers meet the right compliance requirements?

GDPR. DTRP. PCI DSS. HIPAA.

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

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

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

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

GO ANYWHERE®
Managed File Transfer

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

HERJAVEC GROUP

Celebrating Over 15 Years of
Cybersecurity Operations Excellence

At Herjavec Group, information security is what we do.

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

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

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

To your success,

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

Recognized Industry-Wide

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

NIGHTDRAGON

***"NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

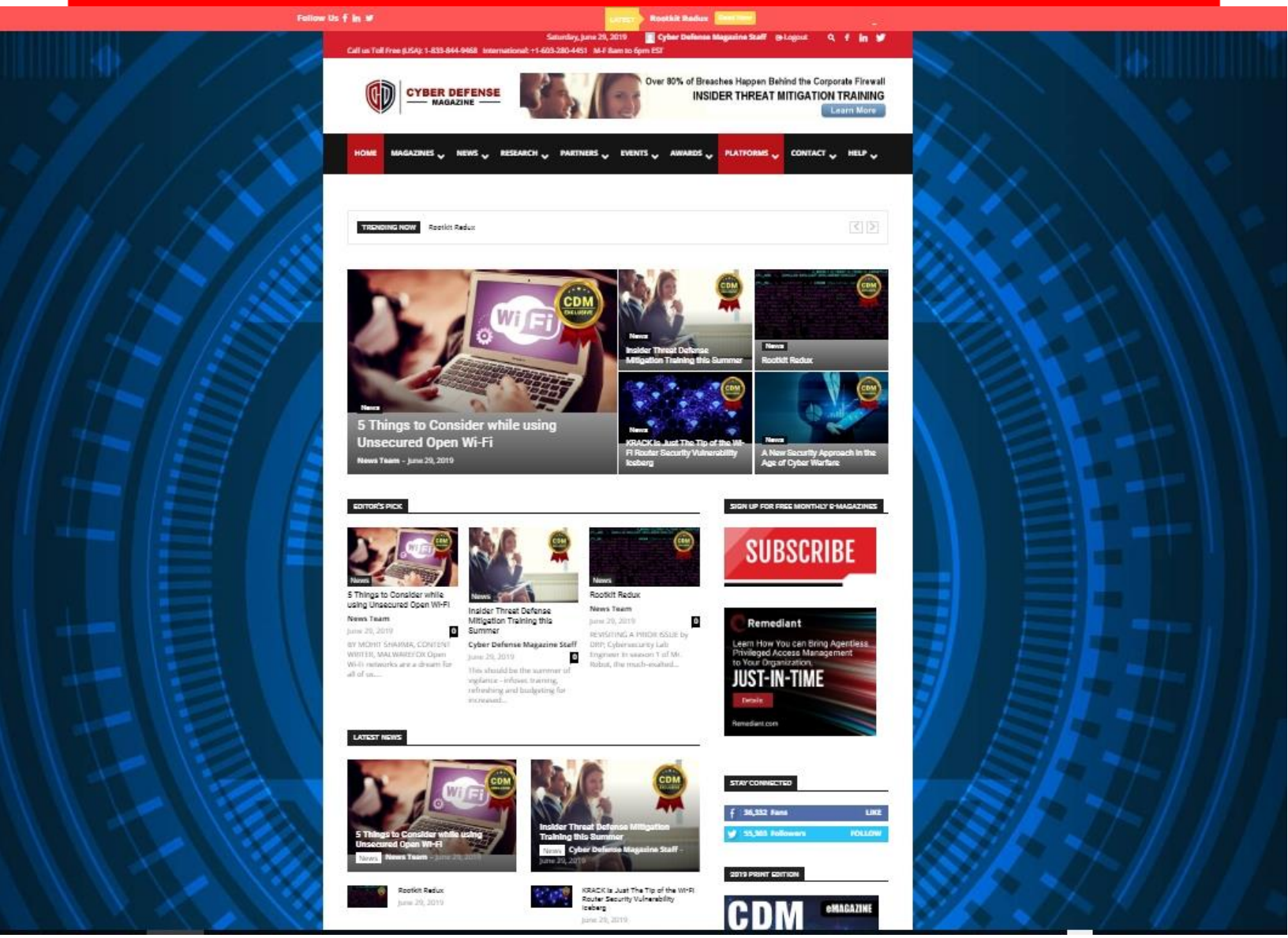
ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

To learn more:
Call +1.512.372.1004, Visit www.brinqa.com

brinqa



7 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're shooting for 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazineBackup.com up and running as an array of live mirror sites.

1.5m DNS queries monthly, 2m annual readers and new platforms coming…

CLOUDSEC2019

PICTURE THIS!

SEE. SECURE. GO FURTHER.

Old Billingsgate, London

Where old industry meets mordern technology

Register Now

CLOUDSEC EUROPE

13th September 2019

www.cloudsec.com