

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

**CYBERSECURITY
INDUSTRY LEADER**
MAGAZINE

Since 2012

Over 1.2M Readers

IN THIS EDITION:

...170 Packed Pages...

Combatting Insider Threats

DDoS Attacks & Mitigation

Email Security Best Practices

Understanding the GDPR

Cybersecurity Predictions

Handling a Data Breach Properly

Securing the Energy Grid

Industrial Internet of Things (IIoT)

Prepping for Election Hacking

Third-party Patching

...and much more...

MARCH 2018

MORE INSIDE!

CONTENTS

<i>4 Areas with a Growing Cyber Risk of Digital Extortion.....</i>	<i>6</i>
<i>Are your emails safe?</i>	<i>9</i>
<i>Cyber-attacks thrive the market for Managed Security Services</i>	<i>14</i>
<i>Safer Internet Day 2018: Where You're Falling Short on Your Online Ad Campaigns.</i>	<i>18</i>
<i>Security Remains Top Concern for IBM AIX Community</i>	<i>23</i>
<i>Pentester Syndrome</i>	<i>33</i>
<i>IMPORTANCE OF "The General Data Protection Regulation" in Cyber Security World</i>	<i>38</i>
<i>How We Can Secure The Energy Grid and the Smart Home Of The Future</i>	<i>42</i>
<i>Cloud Clout & the Chinese agnostic.....</i>	<i>46</i>
<i>GDPR Privacy Laws: Ramifications and Possible Interdictions for Open Source Security Vulnerabilities</i>	<i>52</i>
<i>Tech and IT Companies are Driving Cloud Security Investments</i>	<i>57</i>
<i>Don't Get Caught by Ransomware</i>	<i>60</i>
<i>SSH: The Two-Edged Sword in Your Security Strategy.....</i>	<i>63</i>
<i>Third-Party Patching.....</i>	<i>66</i>
<i>Ahead of the 2018 US midterms, how can we respond to foreign voting interference?</i>	<i>76</i>
<i>Attackers on Rampage</i>	<i>82</i>
<i>Computer Bug History – Notable pests from the last 30 years.....</i>	<i>86</i>
<i>Keep hackers from boarding your network with a Cyber No-Fly list</i>	<i>89</i>
<i>Top 5 Ways to Combat Insider Threat</i>	<i>93</i>
<i>Top Threats of 2017 – Get Ready 2018, Here We Come</i>	<i>96</i>

CONTENTS (cont')

<i>Security Awareness Training (Version 4.9)</i>	100
<i>IloT Security and the Threats invited by Public Networks</i>	102
<i>Is C-Level Security Talk Resulting in Action?</i>	106
<i>The Security Behind E-Signatures</i>	109
<i>Data Breach Risks and Responses for Business Leaders</i>	114
<i>Misaddressed emails were the #1 data security incident reported in 2017</i>	118
<i>Could our web dependency cost us a lot?</i>	123
<i>Cybersecurity facts to focus on in 2018</i>	126
<i>Shining a Light on the Dark Web</i>	130
<i>Infection Monkey’s Controlled Chaos in Network Engineering</i>	135
<i>Password Security - MFA and SSO Explained</i>	139
<i>Don’t let vulnerabilities win: Patch it so it holds</i>	143
<i>Special Report: How Will The 2018 GDPR Changes Work?</i>	147
<i>Case Study: Neil Daniell, Information Security Specialist at People’s Bancorp</i>	153
<i>SiteLock Research: Businesses See More Effective Website Attacks in Q4 2017</i>	156
<i>Smart Home Cyber Security</i>	158
<i>Demystifying the Source Code vs. Binary Debate</i>	162
<i>Types of DDoS and How to Prevent from DDoS Attacks</i>	167
<i>Free Monthly Cyber Defense eMagazine Via Email</i>	169
MARKETING AND PARTNERSHIP OPPORTUNITIES	170
<i>Job Opportunities</i>	171

FROM THE EDITOR'S DESK



Dear Readers,

We're only weeks away from attending our sixth RSAC conference as an industry leading publication. I remember when our Publisher reached out to me

in 2011 and asked if I could join the team and help out and by 2012, we were in business. Now we have more than 1.2M annual readership and growing daily.

We cannot thank you enough. As a result, we've decided to continue to expand the Cyber Defense Media Group (technically our parent company) by adding CyberDefense.TV to our portfolio. This will follow our expansion into the UK and EU with an office in London and with help from friends in China, our upcoming Hong Kong office. We are here for you – our readers and are so thankful to the sponsors, public relations and media outlets we work with in partnership to bring you some of the best possible content and information about cyber security.

In this edition, overpacked with great articles and content, you'll learn some of the best infosec practices, tips, tricks and ideas from industry leading thought leaders. Let's continue to make 2018 our best, most proactive year together! See you at RSAC!

To our faithful readers,

Pierluigi Paganini

Editor-in-Chief, CDM

CYBER DEFENSE eMAGAZINE

Published monthly by Cyber Defense Magazine and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

PRESIDENT

Stevin Miliefsky

stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH

Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Sarah Brandow

sarahb@cyberdefensemagazine.com

Interested in writing for us:

marketing@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

Toll Free: 1-833-844-9468

International: +1-603-280-4451

SKYPE: cyber.defense

<http://www.cyberdefensemagazine.com>

Copyright © 2018, Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC
PO BOX 8224, NASHUA, NH 03060-8224
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.

FOUNDER & PUBLISHER

Gary S. Miliefsky, CISSP®



Learn more about our founder at:

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

Providing free information, best practices, tips and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security.



RSA[®] Conference 2018

San Francisco | April 16 – 20 | Moscone Center

The logo features the word "NOW" in large, bold, multi-colored letters (green, purple, orange) with the word "MATTERS" in smaller white letters inside the "O". The background is a white circle with a network of blue and purple lines and dots.

WE SPEAK CYBERSECURITY. YOU TOO?

At RSA Conference, cybersecurity is our favorite language. And, not to brag, but we're pretty well-spoken. Every year, RSAC brings out the best in cybersecurity. And this year is no exception:

- More than a dozen keynotes from industry experts like Paul Kocher of Cryptography Research, Christopher D. Young of McAfee and more
- Over 650 of cybersecurity's top companies, including Dashlane, GoSecure Inc. and GreeNet
- Relevant seminars, tutorials and trainings, and more immersive learning opportunities
- 550+ sessions to keep you on the cutting edge of your field

And if you register for RSAC 2018 before April 13, you'll get \$300 off a Full Conference Pass. So you can hang with the experts. And save like one, too.

READY TO TALK THE TALK?

Register today: www.rsaconference.com/cyberdefense-us18

Follow us on: #RSAC     

4 AREAS WITH A GROWING CYBER RISK OF DIGITAL EXTORTION

by Derrick Rice, Principal Consultant, Asylas

In a world where it's becoming the norm to use digital assets as a medium of exchange and to see systems updating information as soon as it's received, it's no secret that our digital footprints are growing exponentially. This growth in our online presence and our reliance on online tools increases the cyber risk that your business can be taken out entirely by a digital extortion attack.

Many attackers use ransomware as their weapon of choice, denying a business access to its data and demanding a sum of money for its return. And, as the internet expands, [attackers are finding more ways](#) to interrupt critical processes in hopes that it will force a business into paying them off.

So, what new technologies are attackers targeting, and what can you do to keep your business up and running? Here are some things to keep an eye on:

1. **Phones:** Now that you can share money and files away from your desktop, computers aren't the only devices you need to worry about protecting. Once a hacker taps into your mobile phone, he can listen to your calls, read your text messages and access your address book and apps. He can also guide you to download malware that leads to a ransomware attack.

What can you do? Always be wary of what company information your employees can access from their personal devices. If they store sensitive data or files on their phones and later connect them to an [unsecure network](#) (i.e. a public WiFi network), bad actors can access that information rather easily, steal the data and demand ransom. Any personally identifiable information should only be made available through your company's secure network. Make sure employees understand and are trained on these policies.

2. **Social media:** If an attacker gains access to your company's social media account or creates a fake account under a name similar to yours, he can do instant and irreversible damage to your organization's reputation. Attackers can share fake information on behalf of your business, gain the trust of your clients and followers and post sensitive information for the world to see, demanding a hefty fee to give you access to the account(s). Once this information has been shared, it's difficult to remove from the public eye.

What can you do? Businesses should treat their social media accounts as if they're bank accounts. Set up two-factor authentication, create strong passwords and limit account access to only a few employees. Monitor social platforms for any fake accounts that may have been created in your company's name, as

these can be just as damaging to your reputation as having your official account overtaken.

- 3. Real-time services:** Any business that offers real-time services (such as banking institutions, healthcare providers, etc.) should be especially alert for extortion attacks. Attackers know that interrupting key components of what makes your business function will put more pressure on you to resolve the issue quickly. And sometimes, resolving the issue quickly might mean paying the attacker what he's asking for in order to avoid a longer downtime.

What can you do? Make sure you have adequate backups of your data and a recovery plan in place. Establish guidelines for how long your business can afford to be down and how long it will take you to restore data afterwards. Set up processes for determining where attacks may be coming from (especially if your organization employs hundreds to thousands of people), and make sure your employees know how to report any suspicious activity.

- 4. Cryptocurrency:** With any digital asset that can equate to cold hard cash comes the threat of extortion or theft, and cryptocurrency is not immune. If you choose to buy bitcoins, be aware that attacks have already begun, and [they will only become stronger and more frequent](#).

What can you do? Stay on top of the latest industry news and laws, and use [backup and encryption methods](#) to your advantage. Don't save the passwords to your digital wallet on any personal devices or online password banks. And, when you're not using it, make sure you store your digital currency offline.

While new technologies and digital services can pose a significant threat to your brand and critical processes, ensuring you have the proper planning and detection methods set up can save you a lot of headaches – and money – as extortion methods expand.

About the Author

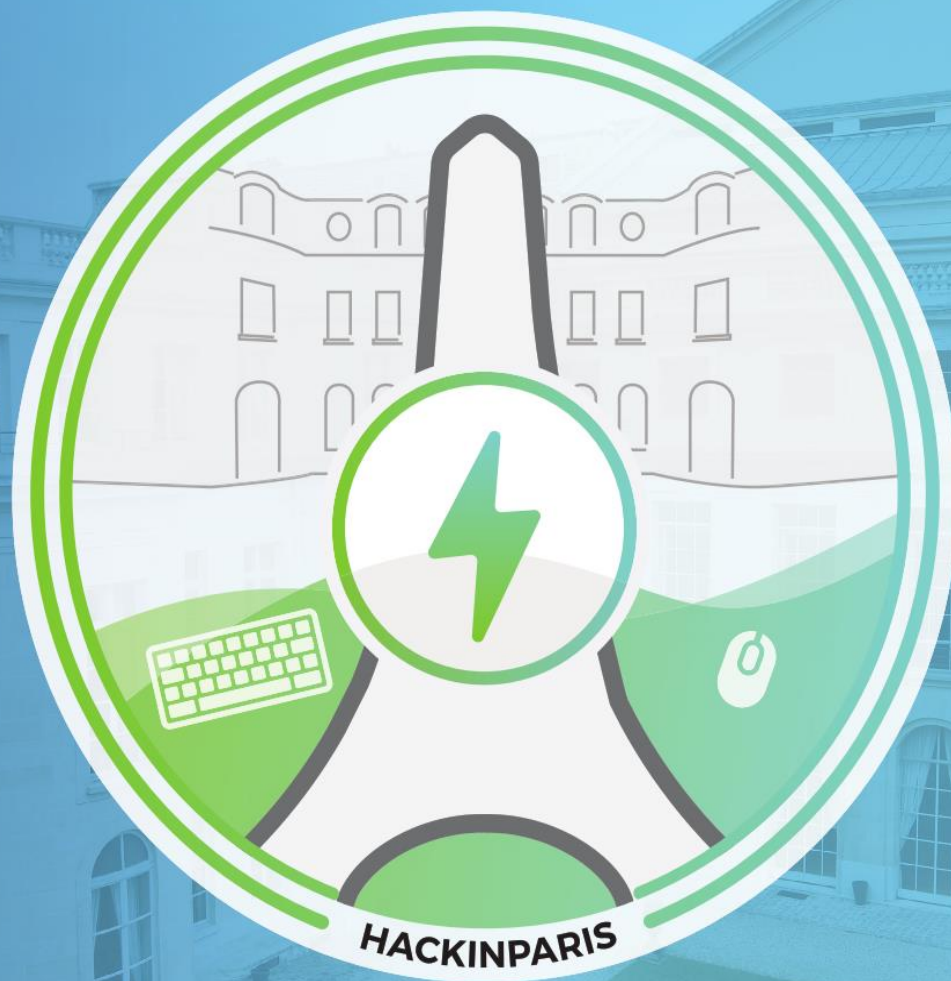


Derrick Rice is principal consultant at Asylas, a security, privacy and risk-consulting firm located in Nashville, TN.

With over 15 years in IT, Derrick's experience ranges from systems administration to technical leadership roles.

He is committed to helping people understand and eliminate the inherent threats to their businesses.

He focuses primarily on private-sector privacy (CIPP/ US) and HIPAA regulation. Learn more at <https://www.asylas.com/>.



8TH EDITION

2018

Trainings: 25 - 27 June

Talks: 28 - 29 June

organized by



www.sysdream.com

MAISON
DE LA
CHIMIE

www.hackinparis.com

ARE YOUR EMAILS SAFE?

UNDERSTANDING THE DIFFERENT TYPES OF EMAIL SECURITY SOLUTIONS

by Scott Raspa, VP, Sales & Marketing, Graphus

When we're talking about cybersecurity, the first thing that comes to mind isn't always emails. However, up to 91 percent of cyber attacks actually arrive in your inbox. These email-based attacks come in multiple forms:

- **Phishing:** this is an attempt to steal login credentials pretending to be a trusted site - like your bank or G Suite login.
- **Spear Phishing:** this is similar to a phishing attack however these are much more targeted and personalized. The attackers have done their research and send personalized messages to the target.
- **Malware** (attachments, links, drive-by downloads): these are attacks that contain malware. It could be a malicious attachment, link, or even a drive-by download.
- **Email Scams:** this can be similar to a phishing attack however it doesn't necessarily spoof a trusted identity. For example, cyber criminals could pretend to be your vendor and send you an invoice for payment. This is also known as business email compromise (BEC).

So, when you're focused on making your company safe from threats, you should begin by carefully considering how to protect your email communications from these types of attacks.

Below we'll break down the different types of solutions and if they protect against these types of attacks. Now keep in mind that not all solutions are created equal so a company in one category (ie Endpoint systems) may have more functionality than another company in that same category. The information below is meant to be more of a guide in helping you better understand how these solutions protect your organization from the above attack types. Also note, where it says "partial" it means that these solutions don't necessarily offer full/complete protection for that particular attack type.

THERE ARE MULTIPLE WAYS TO CAN TACKLE EMAIL SECURITY:

1. ENDPOINT SECURITY SYSTEMS

Endpoints (PCs, laptops, mobile devices, etc.) can be critical risk factors for your organization. To keep endpoints secure, you'll need an endpoint security management system in place. This can be either a software application or a dedicated appliance that enables you to discover and manage any devices trying to access the corporate network. An endpoint security system enables you to limit access from non-compliant devices or quarantine them in a virtual LAN (VLAN). Within this field, [Tanium](#) and [FireEye](#) are suitable options for businesses. Tanium is essentially a search engine for IT data; you can search for devices (even those you don't know about), find vulnerable endpoints and take appropriate action. FireEye conducts automatic searches for malicious endpoint activity, allowing you to isolate compromised devices quickly.

Protection:

- Phishing - No
- Spear Phishing - No
- Malware - Yes, if the malware gets downloaded on the endpoint
- Email Scams - No

2. ANTI-SPAM PROTECTION

No anti-spam method is perfect, and usually any spam filtering system requires a multi-pronged approach: end-user action, automated tools, email sender action and legal regulation. End users must be encouraged to be careful providing the corporate email address, avoid using it on forms, online publications and so on. Automated systems can provide further protection by screening for known spam addresses (blacklisted senders), scanning inbound messages for viruses and using machine learning to remain constantly up to date. Relevant options would be [SpamTitan](#), which can be installed locally or in the cloud, and [Symantec Email Security](#), which strengthens the security level of Office and Google products by conducting careful email screening before delivery.

Protection:

- Phishing - Yes (for generic phishing attacks)
- Spear Phishing - No
- Malware - Partial (No for 'zero day malware')
- Email Scams - No

3. MESSAGING SYSTEMS (SECURE EMAIL GATEWAYS IS THE RIGHT TERM)

For more extensive protection, some companies turn to messaging security systems, like [ProofPoint](#) and Mimecast. More than just filtering out spam, these products offer enterprise-grade security, applying analytics to block phishing by identifying the original sender, blocking ransomware attack, spotting spam via social media, and much more.

Protection:

- Phishing - Yes
- Spear Phishing - Partial
- Malware - Partial
- Email Scams - Partial

4. PHISHING TRAINING

Your biggest risk to email security is, of course, human error. Uninformed employees put any security system at risk. Training your employees in staying safe when emailing is critical to protecting your company from cybercrime. Researchers found that [email security fails 10.5 percent of the time](#). Because of this, you must make sure you have a "human firewall" in place when all else fails. The fastest growing vendor in anti-phishing training is [KnowBe4](#), which offers training programs and a platform that simulates phishing attacks to keep employees on their toes. [PhishMe](#) offers similar training and simulations, as well as incidence response optimization through automation and reporting.

Protection:

- Phishing - Partial
- Spear Phishing - Partial
- Malware - No
- Email Scams - Partial

5. NEXT GEN EMAIL PROTECTION

At the most sophisticated end of email security, cloud-native email platforms use big data, machine learning and custom algorithms to protect cloud-based email solutions like G Suite and Office 365. Top performers in this space include [Graphus](#) and [GreatHorn](#), both cloud-native automated security platforms which protect Outlook 365 and G Suite users from ransomware, malware, spam and other targeted attacks. (next

gen integrates at an API level - traditional gateways sit inline and don't have complete access to all the datasets necessary for detecting a threat)

Protection:

- Phishing - Yes
- Spear Phishing - Yes
- Malware - Yes
- Email Scams – Yes

SO, WHAT DOES ALL THIS MEAN FOR YOUR ORGANIZATION?

No single email security approach is going to work for every organization. Each company has its own risks, challenges, budget restrictions, legacy security solutions and cultural factors to consider. That said, one thing is for certain: a thorough, well-implemented system should include multiple solutions to cover all your bases. For instance, if you already have anti-spam software, consider adding phishing training and endpoint security.

No email security system is 100-percent secure but you can minimize risk and maximize efficacy by leveraging multiple solutions.

About the Author



Scott Raspa is the VP, Sales & Marketing for Graphus. He has been in sales & marketing for 15+ years with the last 8+ years focused on solving complex cybersecurity problems. At Graphus he leads all sales and marketing efforts. Graphus is a social engineering defense company based in Reston, VA. Their simple, powerful, and automated solution employs artificial intelligence to establish a TrustGraph™ between people, devices, and networks to reveal untrusted communications and detect threats. Scott can be reached online at

(sraspa@graphus.ai, @sraspa) and at our company website <https://www.graphus.ai>

Defence **iQ** presents the first

BIG DATA ANALYTICS FOR DEFENCE



In partnership with the



Defence and Security
Accelerator

Conference Workshop Day: 26th June 2018 | Main Conference Days: 27th-28th June 2018 | Millennium Cophorne Tara Kensington, London

SECURE. ANALYSE. ACTION.

A senior speaker panel, including:



Dr. Peter Lenk ,
Branch Chief Service
Strategy and
Innovation, **NATO
Communications
and Information
Agency**



Brigadier General
Juergen Broetz,
Chief, Military
Intelligence,
Bundeswehr



Brigadier Rob
Sergeant, Head
of Future Force
Development,
British Army



Engineer General
of Armament
Caroline Laurent,
Director of Strategy,
Directorate General
of Armaments
**French Ministry of
Armed Forces**



Colonel Steven
Desjardins,
Director, Canadian
Intelligence Corps,
**Canadian Armed
Forces**

Benefits of attending:

- ➔ **Achieve technical superiority** by incorporating cutting edge technologies in data analytics and Artificial Intelligence, with proven success in the commercial sector
- ➔ **Maximise the window of opportunity to exploit intelligence** by enhancing the speed and accuracy of data analysis using new AI and machine learning capabilities
- ➔ **Eliminate the threat of data hacking** by understanding how to develop secure and bespoke solutions for your needs alongside big data storage experts
- ➔ **Optimise your data analysis processes** by using the data analytics tools recommended by experts deploying high-end technical capability in the civilian sector
- ➔ Align your systems to the military requirement by **engaging directly with the senior decision makers** and capability directors from the Armed Forces, responsible for building big data capabilities into their own defence organisations

2018 Partners:



+44 (0) 207 036 1300 | ENQUIRE@DEFENCEIQ.COM | BIGDATADEFENCE.IQPC.COM

CYBER-ATTACKS THRIVE THE MARKET FOR MANAGED SECURITY SERVICES

GROWING VOLUMES OF DATA ON ACCOUNT OF INCREASED IOT ADOPTION AND INCREASED MOBILE DEVICE USAGE AMONG CORPORATE EMPLOYEES HAVE MAINLY FUELED THE DEMAND OF MANAGED SECURITY SERVICES ACROSS THE WORLD.

by Kevin Stewart, Research Manager, Research Cosmos

Managed security services market has witnessed an up thrust with the advent of new innovations and increased cyberattacks inside the Information Technology (IT) industry. As the name itself indicates, managed security services are the protection provided to any company's network or the information system within in the organization or by some trusted third-party providers. Some of their work includes incident responses, intrusion detection and alerts, firewall monitoring, security audits, system upgrades, vulnerability assessments, and so on.

The [global managed security services market](#) is predicted to have a net worth of USD 17 Billion in 2016 and is estimated to cross USD 35 Billion by 2022, with market size growing at an annual rate greater than 14% in between the years. The recent market study also discloses that around 82% of IT professionals are interested in using or already using the facilities of managed security services.

The increase in cybercriminal activities, complex cloud infrastructures, and continuous log monitoring and auditing have become a great challenge for IT industries to depend solely on their internal security processes. This, in turn, led to the proliferation of managed security services from external providers directly impacting the growth of its market share. The market analysis also confirms that the shortage of in-house skilled professionals, advanced cyber threats, and affordable third-party services had risen the significant demand for managed security services.

Contemporary trends in the market:

Mobile devices market rise had tremendously influenced the need for security services. The migration of workforce to cloud and the use of big data analytics has also impacted the market size lately. The introduction of technology in almost all the fields have also been a great concern and propels the need for managed security services.

Of all the verticals that use the managed security services, the Banking, Financial Services, and Insurance (BFSI) segment bags the major portion of market revenue. The strict regulations to protect the customers' confidential data and transactional information had kept the emphasis on banking and financial institutions to use trustworthy security services. The continuous cyber-attacks for theft and increased concerns of customers are also driving the managed security services market growth.

Compared to large-scale businesses, Small and Medium Enterprises (SMEs) are observed to gain more interest in using the managed security services. The requirement for advanced security at an affordable cost is the prime factor influencing the market growth in SMEs. Also, SMEs are the easy targets in many cyber-attacks due to their insufficient infrastructure and it helps the SMEs to lead the market revenue for managed security services in future as per the market forecast.

Intrusion preventions systems (IPS) and intrusion detection systems (IDS) of the managed security services applications have gained a wide fame dominating the global market share. The continuous monitoring for any unwanted intrusions and their management has garnered the demand for IPS/IDS services.

Geographical presence:

The prevalence of cyber-crimes across distinct parts of the globe has raised the demand for managed security services. With respect to the regions, North America holds the major chunk of managed security services market. The increased focus on information security, more investments in technology, growing security service providers, and strong financial status are some of the major factors owing to the market growth in North America. The United States of America is the strongest contributor to market in North America. The frequent occurrence of cyber-attacks has led to the demand for managed security services in the Asia Pacific and the Middle East in recent times.

Major market vendors:

Cybersecurity has raised the bar for growing managed security services providers and potential to unlock great fortunes. However, there are some key market contributors that hold the international markets for a long time now. The top players among those are IBM Corporation, Symantec Corporation, SecureWorks Inc, Cisco Systems, AT&T, HP, CSC, BT Group, Fortinet Inc., Verizon Communications, Solutionary, Inc., Rapid 7 Inc., and Trustwave Holdings, Inc.

A sample of the report is at <https://www.researchcosmos.com/request/1804057967>

About the Author

Kevin Stewart, currently working as a Research Manager is having a considerable amount of experience in IT industry. Kevin is having a strong analytical and strategic mind and good at providing compelling insights for the business development. He is well-versed in the research process which includes reviewing the collected data, authoring reports and making business-oriented recommendations to clients. He also holds firm knowledge at predictions and identifying the trends that can impact the market and business growth. Kevin can be reached online at kevin@researchcosmos.com and at <https://www.researchcosmos.com>



CYBER SECURITY



International Conference on **Mechatronics & Robotics** Helsinki, Finland

Major Session on
Artificial Intelligence future of Cyber Security



Register and Save 20%-MR18CDM20

Contact: Kevin Mathew | Program Manager
Mechatronics & Robotics 2018
Mail: roboticsmeet@enggconferences.com

robotics-mechatronics.enggconferences.com

**October 0
15-16**

**2
1
8**

SAFER INTERNET DAY 2018: WHERE YOU'RE FALLING SHORT ON YOUR ONLINE AD CAMPAIGNS.

by Roy Dovaston, Operations Lead, Click Guardian

On 6th February 2018 'Safer Internet Day' was celebrated across the globe with the slogan "Create, Connect and Share respect; A better internet starts with you". The active involvement of more than a thousand organizations throughout the UK has helped to inspire a national conversation with regards to the use of technology in a responsible, respectful, critical and creative manor, leading many business owners to reevaluate their digital stature.

With this assumed industry awareness of cyber-threats, you would think things have improved. However, progress has proven to be essential by recent reports, indicating that advertising fraud – and more specifically, click fraud (the repetitive clicking of competitors' ads to deplete their daily advertising budget and rapidly diminish profits) - is at its highest ever frequency.

Highlighting the lack of efficient web security, Safer Internet Day emphasizes the regularity of cyber threats and the benefits in discussing preventative methods. However, with many businesses continuing to fall victim to click fraud, that additional assistance might be required in preventing loss of profits as a result of this digital crime.

Recently, it has been reported that "cyber-attacks are becoming more 'technically sophisticated,'" and so the task of understanding the diverse array of potential cyber-threats cluttering the web could be an infinite one, with little reward for both small and large businesses reliant upon online marketing and advertising.

It has been argued that the most damaging form of online fraud is 'click fraud' – a method capable of 'swallowing the internet' and the critical data of which it comprises. This form of online fraudulence has rapidly increased in popularity over recent years; with statistics indicating a rise of almost 10% in the space of just one year alone. Similarly, it has been found that an appalling 50% of billed for ads were generated by non-human traffic. This hidden hacker evidently goes undetected by a significant number of businesses, emphasizing the need for Safer Internet Day and its key focus.

Click fraud is the illegal and repetitive clicking of online ads to waste a business's daily advertising budget and as a result, ruin their success and financial gain. Like many other forms of online fraud, click fraud is becoming all the more diverse and can harm

online campaigns in a multitude of formats. For example, this fraud may be carried out manually at the hands of 'click farms' i.e. establishments based in poverty-stricken countries where low-paid employees are solely hired to click your ads.

Alternatively, new software allows 'click-bots' to automatically infect a computer without the owner's knowledge or permission, repetitively clicking ads on sites to their detriment. This form of click fraud is particularly concerning, as the software is not subject to human limitations such as working hours or technology know-how.

In either instance, click fraud not only appears to be increasingly common but ever-more versatile, ruining the success of online campaigns with ease. It may also be argued that no matter which methods are implemented, the source of such fraud often lies within the hands of your competitors, with the fundamental goal of diminishing your resources.

In 'the age of technology' and following events such as Safer Internet Day, it would be widely assumed that cases of security failings are both minimal and easily preventable, particularly as click fraud is fundamentally a criminal offence prohibited across all major marketing platforms. Whilst infamous channels such as Google have implemented methods of preventing click fraud, these are not entirely successful. It appears that the most efficient method of protecting an online campaign, personal information and customer data is for business owners to further educate themselves – maintaining safer internet throughout 2018 and beyond.

To assist with the daunting task of protecting your online campaigns, Roy Dovaston of Click Guardian, the UK's number one click fraud prevention service, below outlines several tips to avoid click fraud, as well as stating why establishing and maintaining a safer internet is crucial.

Firstly, the most basic form of click fraud prevention is observing the behavior of your competitors who are more often than not the source of such criminality. To identify these competitors, you should begin by monitoring who is rivalling your keywords in search engines - it is highly likely that these will be the businesses most inclined to commit click fraud on your campaigns.

While it is important to remain vigilant towards your competitors, business owners must remain equally as observant of their own campaigns. It would prove useful to check ratings daily on your ad campaigns for irregular spikes in clicks – if a dramatic improvement occurs for no apparent reason, it may be necessary to delve more deeply into the source. More specifically, the IP addresses these from which these clicks originate.

The significance of such IP addresses is key; it is useful to remember that these must all be different. Although it may be an arguably obvious concept, this is essential in detecting and preventing fraudulence. Typically, your ad will show up on search engines and websites for a unique user every time and so genuine traffic is attained through different IP addresses.

If there are multiples of the same IP address, this highlights a possible case of click fraud, and further measures must be taken.

As a first small step, you can limit the damage caused by click fraud by pausing your account, give you the opportunity to consider the incident and think about your next steps. This alleviates the risk of such fraud persisting and wasting your PPC budget – stopping this threat in its tracks.

It may also be beneficial to limit the exposure of your ads by setting specific spending caps on your overall campaign or alternatively, your hourly or daily budget. This allows for regular re-evaluation of your campaigns success and highlights any areas of possible weakness or vulnerability, better protecting your marketing budget. Similarly, the use of diverse or long-tail keywords within your ads may be useful. Often, primary key words are highly sought after and may therefore attract questionable behavior from competitors seeking the same words.

Once essential alterations to your ads have been established and preventative budgets set, it may be necessary to consider the audience targeted by your ad. The main appeal of utilizing online marketing is to significantly widen your audience pool, who could be reached at just a click. However, entirely unrestricted exposure of your ad may not be as beneficial as initially presumed.

As mentioned previously, notorious ‘click farms’ are often based in developing countries where there are staggeringly low labor rates. Hiring low-paid workers, your competitors can conduct click fraud without notable financial costs. To avoid this, we recommend stopping running ads in countries in which you are more inclined to experience such sabotage. Consider strategic location filtering to prevent you from spending unnecessarily, even where not exposed to such fraud.

Finally, the most efficient method of click fraud prevention is the use of click fraud prevention services. For example, Click Guardian offers a detection and protection service which monitors all clicks on your ads, tracks the behavior of your visitors and automatically blocks AdWords if excessive clicking is detected. Once a block is issued, adverts are no longer delivered to the perpetrator, meaning vulnerable advertising budgets will remain intact. The use of such proactive software eliminates the pressure

for business owners to prevent click fraud who often solely react to an issue and are limited in their efficiency by human factors alone. Alongside this, the affordability of these external programmes allows for their use in any size business.

Safer Internet Day 2018 inevitably drew attention to the ongoing concern surrounding click fraud, among the many cyber threats brought up by this event. Evidently, Safer Internet Day continues to be an ideal method of promoting the safe and positive use of digital technology, encouraging business owners to explore the role they are playing in helping to create a better and safer online community for both them and their customers.

The internet is an invaluable source for any company, no matter its size or notoriety and helps to promote a business through social media whilst eliminating any restrictions implemented by location. Nowadays, it is almost impossible to survive within the industry without use of the internet and at least some form of online exposure. The discussion inspired by Safer Internet Day must not fade and continued efforts to remain educated and informed are crucial for prosperous business owners, with due diligence to the concerning rise of click fraud.

Should you need help preventing click fraud, visit: <https://www.clickguardian.co.uk/>

About the Author:

Roy Dovaston, Operations Lead, Click Guardian



Having been managing Google Ads since the inception of Google AdWords, Roy is the owner of pay per click agency and anti-click fraud specialist Click Guardian – in 2014 Roy realised a major issue was going undetected in the form of excessive clicks on his client’s ads. Click Guardian was born from this insight and now actively protects thousands of AdWords advertisers in

the fight against click fraud. Roy can be reached online via our company website: <https://www.clickguardian.co.uk>



Still need to register for this year's RSA Conference?

If you haven't registered yet for the RSA Conference in San Francisco next month, here's a little help!

Use the promo code X8ELINOM to receive a complimentary Exhibit Hall Pass. Then any time between April 16-19, stop by the GoAnywhere booth (#4411 in the North Hall) to learn how to:

- Streamline and secure your file transfers
- Protect sensitive data with encryption and auditing
- Meet critical compliance regulations (e.g. PCI DSS, HIPAA, the GDPR)



GO ANYWHERE[®]
A HelpSystems Solution

We can also help you achieve a multi-layered approach to cybersecurity. Ask us about the following cybersecurity offerings:

- Security Policy Management
- Identity and Access Management
- Virus and Malware Protection
- Threat Identification and Response
- Managed Security Services

Want to brush up on our cybersecurity solutions before the conference?

Visit www.helpsystems.com/cybersecurity



SECURITY REMAINS TOP CONCERN FOR IBM AIX COMMUNITY

SURVEY OF AIX IT PROFESSIONALS ADDRESSES CHALLENGES AND SECURITY SOLUTIONS THEY PLAN TO IMPLEMENT

by Tom Huntington, Executive Vice President, Technical Solutions, HelpSystems

Did you know that 2018 marks the 30-year anniversary of the IBM i platform? Did you further know that IBM will announce the new POWER9 hardware this year? OK, those were easy. Here's a real stumper: Did you know that nearly 75 percent of IBM i shops are using open source development tools on IBM i?

In 1986, IBM launched AIX®, its open standards-based UNIX operating system. Now, more than 30 years later, this popular platform runs on IBM POWER® servers and supports critical applications for organizations around the world. With such a strong presence in IT environments, AIX and its specific usage is of great interest to IT experts as they evaluate their own technology ecosystems in light of changing security, regulatory, and efficiency requirements. HelpSystems conducted a survey among 935 IT professionals from various industries around the world to gauge how AIX is being used and the role it will play for IT leaders in the coming years. Following are key findings as it relates to security.

Highlights

IT pros report high satisfaction with AIX and rely on it to run critical business solutions. Although some plan to move to Linux and Windows, many will broaden their AIX footprint indicating the platform delivers the performance, reliability, and security core business processes demand.

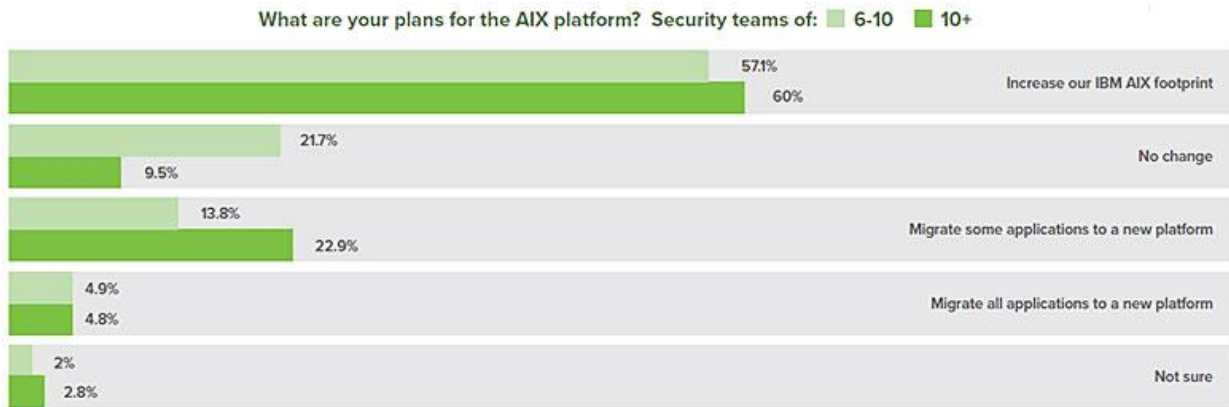
- 89.5 percent report AIX provides a higher ROI than other servers.
- 81.6 percent use AIX to run at least 25 percent of their core business processes.
- 54.1 percent expect to increase their AIX footprint, while 18.2 percent will migrate *some* of their applications from AIX to a new platform.
- 5.7 percent plan to move *all* of their applications from AIX to a new platform, and 4.8 percent will do so in the next five years with Linux and Windows being the preferred options.

Maintaining cybersecurity and high availability/disaster recovery capabilities are top of mind. While many organizations are proactively putting security solutions in place for their AIX servers, others state having no plans for such measures despite the prevalence of cybersecurity threats and regulatory requirements.

- Almost all respondents (94.8 percent) reported their organizations must adhere to regulatory compliance requirements including Sarbanes-Oxley (SOX), PCI DSS, HIPAA, and GDPR. Interestingly, many noted a lack of technology proven to protect against common threats. In fact, more than half of respondents said their companies lacked virus protection, network firewalls, two-factor authentication, or database encryption. This is despite the fact that industry regulations require or strongly suggest these types of capabilities.
- 28.6 percent have two or fewer IT staff members focused solely on cybersecurity, while 71.4 percent have three or more.
 - 64.8 percent of those with 10 or more security staff members ranked high availability/disaster recovery as a top challenge, with 35.2 percent noting cybersecurity as a concern. By contrast, those with a security staff of two or fewer ranked cybersecurity as a lower priority.
- Almost half of respondents (46.5 percent) named high availability/disaster recovery as a top IT concern for their AIX environment over the next 12 months, likely stemming from the dependence on AIX for core business processes. Companies cannot afford downtime in this environment.

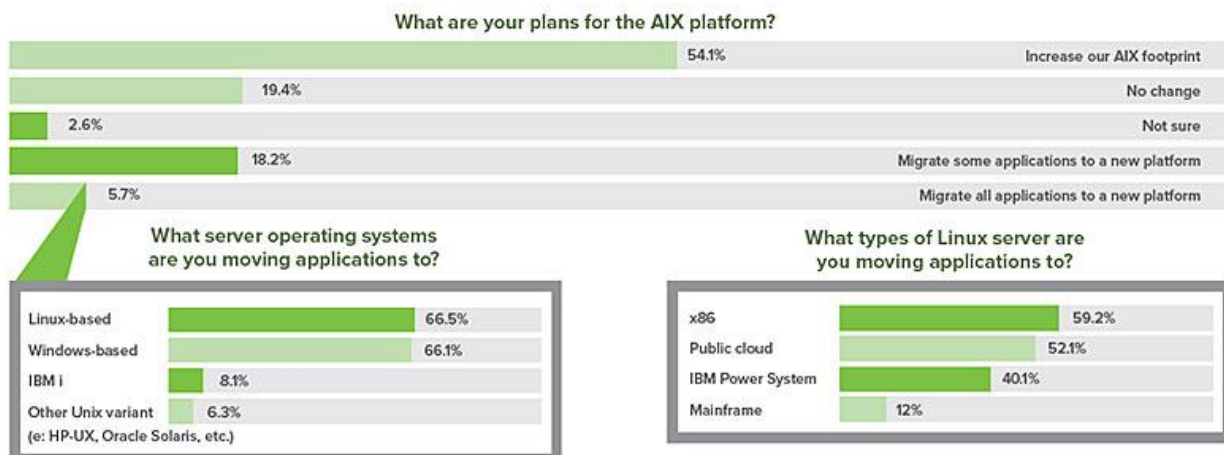
Organizations with larger security teams are more likely to increase their AIX presence despite a lack of related skills

- 31 percent of respondents working in teams with six to 10 security professionals said AIX skills were a challenge, yet 57.6 percent plan to increase their AIX usage. 40 percent of those with security teams of more than 10 people also noted AIX skills were a challenge, but 60 percent will increase their AIX footprint. This indicates IT professionals believe AIX to be the preferred platform for running critical apps. They will likely lean on vendors and contractors with the necessary security expertise to fill these skill gaps.

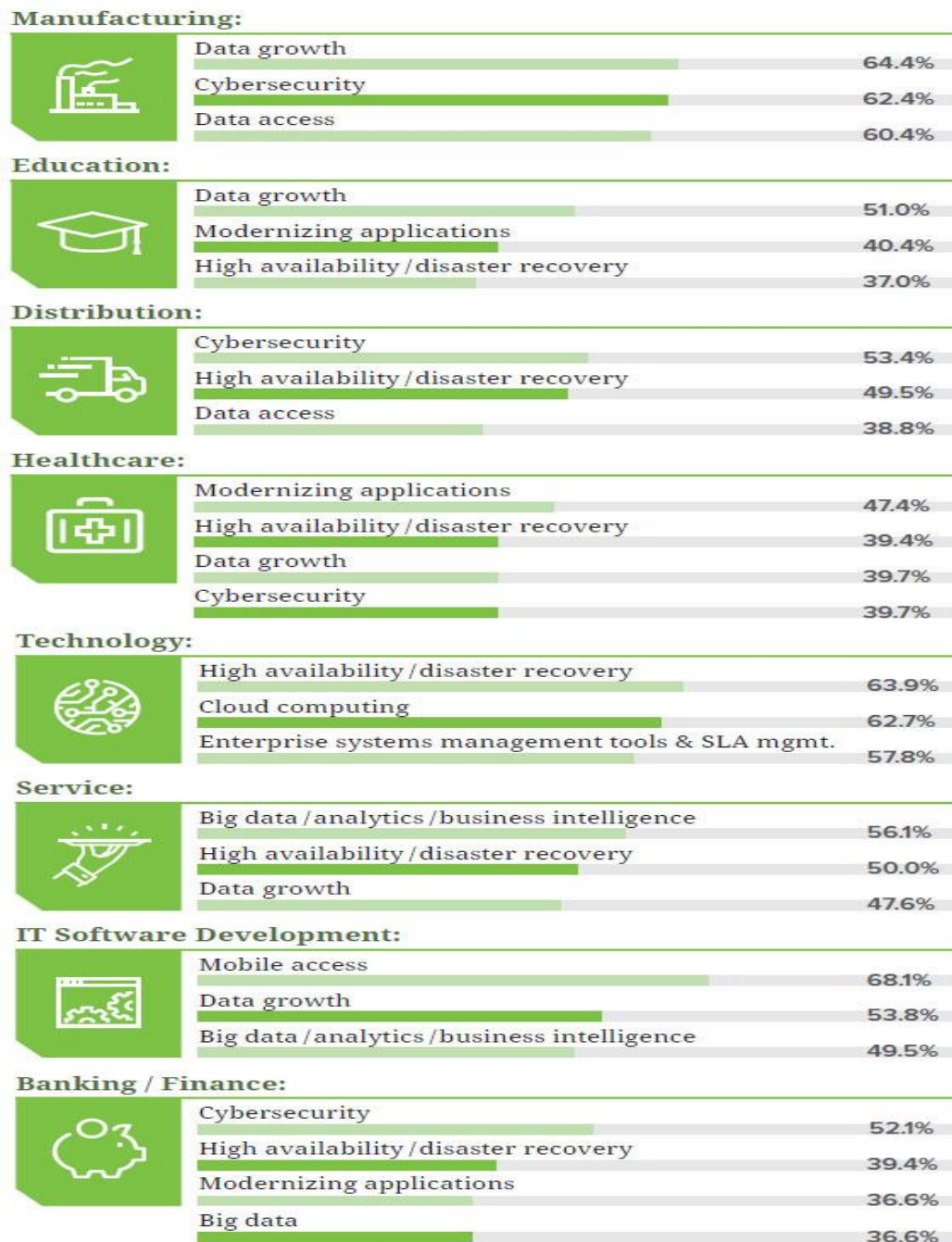


Few organizations plan to move away from AIX completely

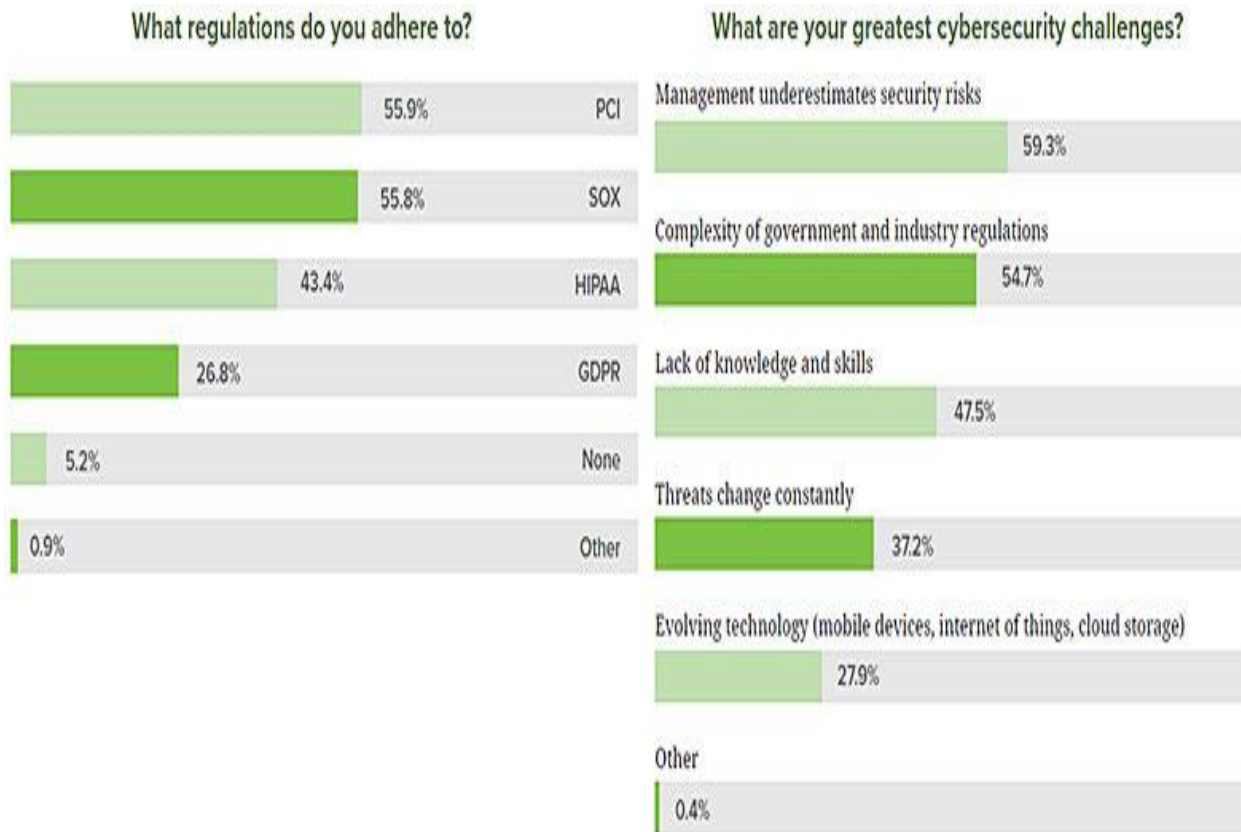
- Only 5.7 percent expect to move all applications to a different platform, with Linux and Windows being the preferred options
- Those moving to Linux plan to use the following servers: x86 (59.2 percent), public cloud (52.1 percent), IBM Power Systems™ (40.1 percent), and mainframe (12 percent). IBM has a notable opportunity with such a large percentage looking at the IBM® Power Systems™ series. The industry buzz around the forthcoming POWER9™ may even be what's behind the favorability of the AIX operating system. Both POWER8® and POWER9™ servers are optimized and priced to meet Linux market needs. The challenge for IBM here will be to prove that the scalability and performance of these servers is a better choice than an Intel® box.



Top IT concerns for AIX environments vary by industry, with high availability/disaster recovery, data growth, and cybersecurity cited most frequently. Among respondents in the top eight industries, which represented 94 percent of total respondents, there was some commonality in top challenges selected. There are also notable plans for implementing security and compliance and reporting solutions across industries, perhaps to address compliance gaps for industry regulations.

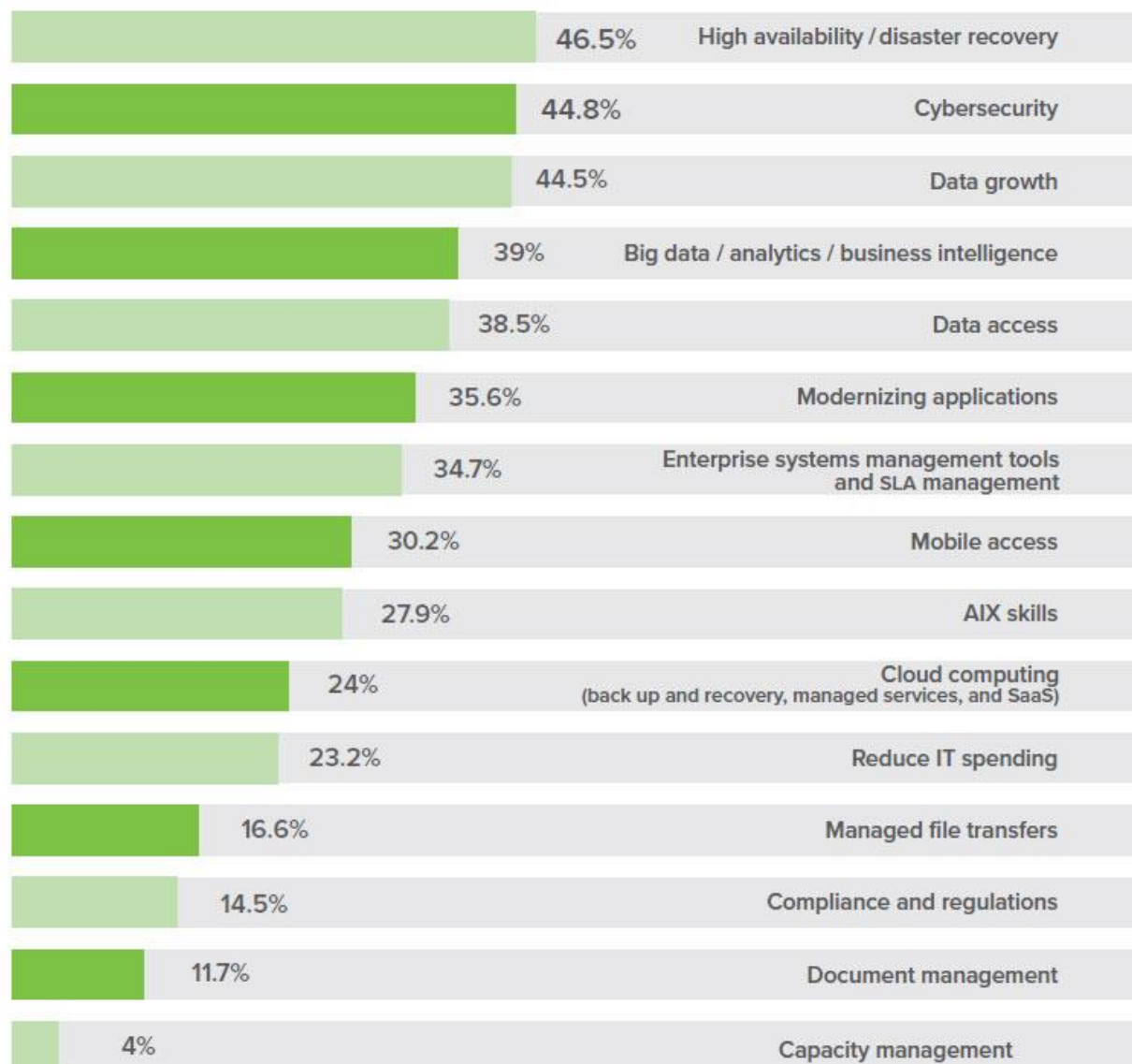


Keeping sensitive information from falling into the wrong hands is top of mind for IT professionals. It seems like every week a new story comes out about a large data breach or an emerging threat. In this survey, 94.8 percent of respondents said their organizations are subject to regulatory compliance including Sarbanes-Oxley (SOX), PCI DSS, HIPAA, and GDPR. This means leaders in almost every industry are responsible for understanding evolving risks and putting the right technology in place as a preventative measure.



Cybersecurity is a top challenge for 44.8 percent of survey participants, and they highlighted numerous concerns that fall into this category. These include the feeling that management underestimates security risks (59.3 percent), the complexity of government and industry regulations (54.7 percent), and an overall lack of knowledge and skills (47.5 percent).

What are the top IT concerns for your AIX environment over the next year?

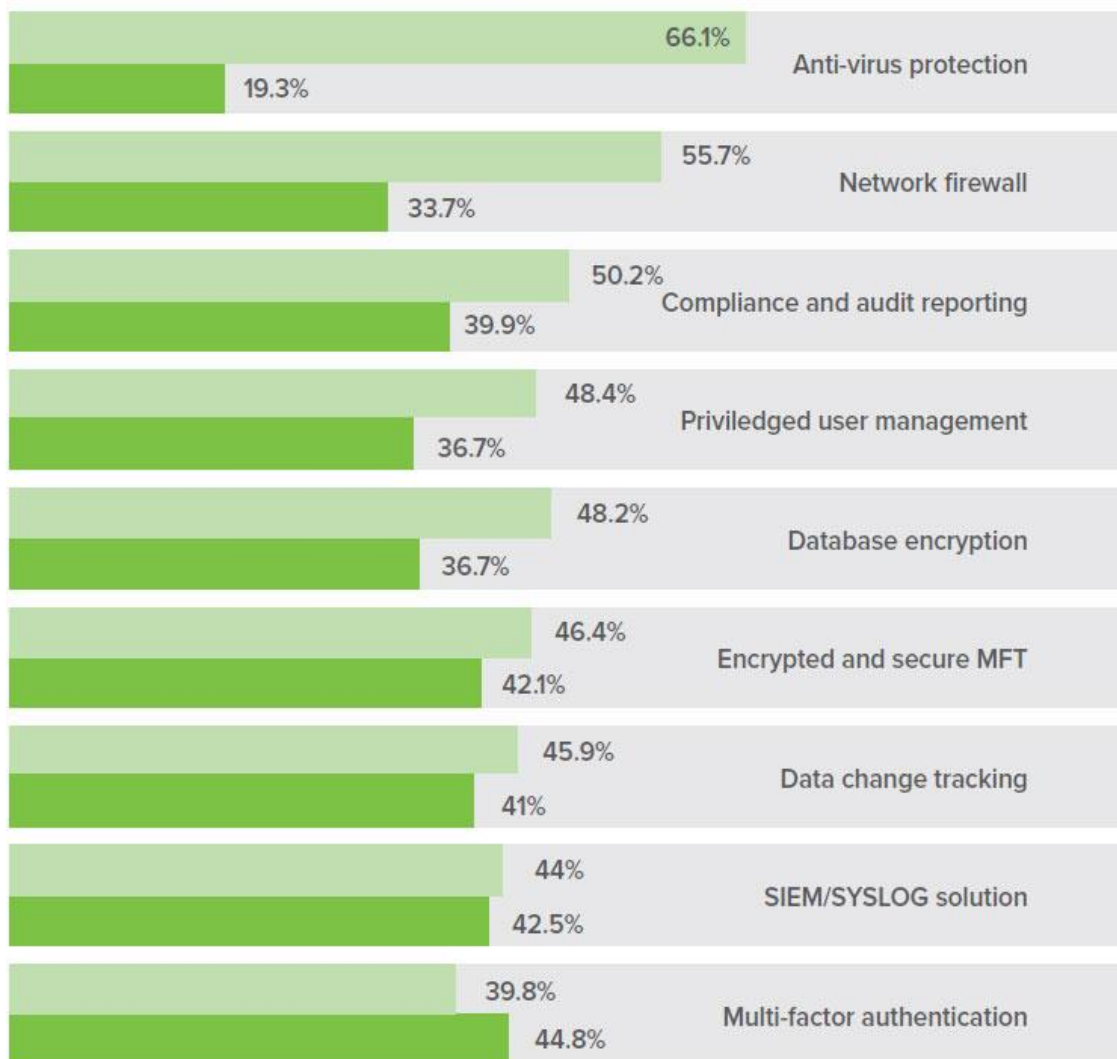


The good news is there is an array of powerful security solutions available, and IT professionals are either using or planning to implement many of these technologies in their AIX environments. When looking at solutions currently deployed, 66.1 percent have adopted anti-virus protection, 55.7 percent use network firewalls, and 50.2 percent use compliance and audit reporting tools. Many respondents noted plans to implement security solutions, with multi-factor authentication leading the pack at 44.8 percent followed by SIEM/SYSLOG solutions at 42.5 percent, and encrypted and secure managed file transfer at 42.1 percent.

Interestingly, there is a notable relationship between the number of IT security staff and plans to adopt new security applications. Organizations with two or fewer resources devoted to security are much more likely to forego technology in this area. For example, more than 27 percent have no plans to implement anti-virus protection, privileged user management, or multi-factor authentication. By comparison, companies with more than 10 security personnel reported 90.2 percent have or plan to implement anti-virus protection, 99.1 percent have or plan to add privileged user management, and 95.2 percent have or plan to use multi-factor authentication.

What security solutions do you have in place or plan to put in place across your AIX servers?

■ In place today ■ Planning to implement

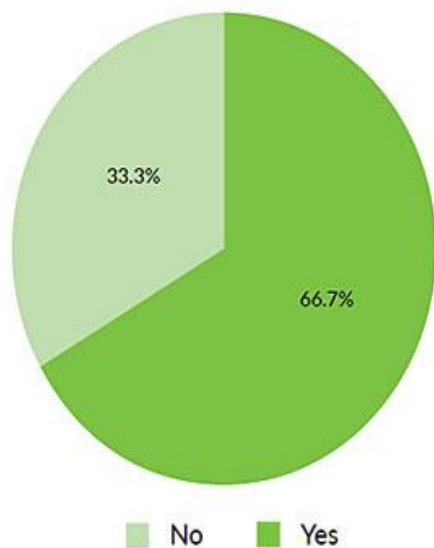


Staying Current

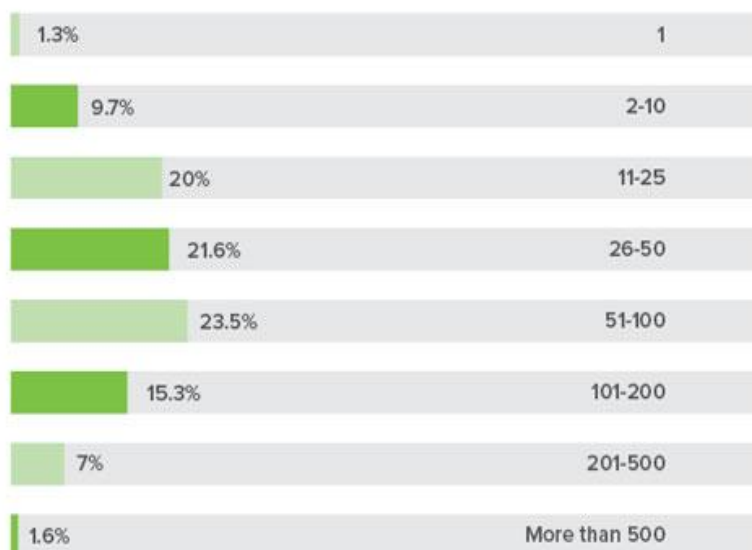
AIX users are staying reasonably current with their hardware and software. Nearly 87 percent of those surveyed are either on AIX 7.1 or 7.2. Only 24.4 percent are using POWER6® technology, although some respondents that use this older version also have POWER8® and POWER7® servers. Almost 90 percent of AIX users have 11 or more partitions of AIX in their environments. As IBM lowers the cost of hardware while increasing the power of the server, we will see more and more partitions in this operating system.

It is also interesting to see that 66.7 percent of survey respondents run Linux or IBM i operating systems on the same servers they use to run AIX. The adoption rate for this is much higher than expected but shows consolidation has occurred even across the various OS offerings. When an organization hasn't updated to a new OS level, it is generally a reflection of budget, the applications that need to run on the server, or a lack of necessity for adding an OS level or hardware.

Are you running AIX on the same frame as Linux and/or iOS?



How many total partitions of AIX do you run?



AIX continues to be a highly valued operating system for IT professionals across many industries with more than half of those surveyed planning to increase or maintain their AIX footprint. Pressure on IT teams also continues to mount regarding challenges such as high availability/disaster recovery, cybersecurity, and data management. Regulatory requirements are driving adoption of new security technologies, although companies with smaller cybersecurity teams are less likely to implement common solutions such as anti-virus and multi-factor authentication. Keeping ahead of changing cybersecurity threats means IT experts need to stay abreast of the most cost-effective method of protecting sensitive data and what makes the most sense in their environments.

About the Author



Tom Huntington is Executive Vice President of Technical Solutions at HelpSystems, and has been with the company for nearly 30 years. He works with business alliances, acquisitions and large customer relationships and ensures that the HelpSystems software works with other major software and hardware vendors worldwide. He is the author of the [HelpSystems IBM i Marketplace Survey](#) and was named an IBM Champion in 2016, 2017, and 2018 for over three decades of advocacy and thought leadership on the IBM i platform. Tom can be reached online at [@tjhuntington](#) and at <http://www.helpsystems.com/>.


itsa 2018
India
 India's IT Security
 Expo & Conference
www.itsa-india.com

NÜRNBERG MESSE


Detect. Analyse. Secure.
 Join the IT-Security Revolution.

Bombay Convention & Exhibition Centre
 Mumbai, India | 24-25 May 2018



Powered by:



Supported by:



Knowledge Partner:



B2B Connect Partner:



Partners:



PENTESTER SYNDROME

MAKING THINGS APPEAR WORSE THAN THEY ARE

by Alex Haynes, Information Security Manager, CDL

If you work in Enterprise security or in any technical domain you may have at one point had the pleasure of reading a report from a recent penetration test (otherwise known as 'pentesting'). These tests are usually conducted against websites or exposed infrastructure to simulate a real life attacker and are genuinely useful at evaluating your security posture at a particular point in time. That being said, there are also many misinterpretations of pentesting as an activity and pentesting results and reports that leads to a skewed perspective on risk in the Enterprise as a result of pentesting itself. I'll cover off the main downsides to pentesting and how to compensate for these in an Enterprise environment so you don't fall victim to 'pentester syndrome' yourself and get the best value out of your pentests.

Pentests are frozen in time

One of the major downsides of pentesting today is that they don't match the speed of development of modern applications. Most companies pentest annually but rarely will you now find an application or website that is only updated once a year. In today's environments, applications and websites are updated frequently, sometimes once a day, and occasionally even more than that. Like I mentioned earlier, a pentest is a *snapshot of your security posture at a particular point in time*. That's it. Once you've updated your website or application, those findings are potentially out of date, as you may have already introduced new configuration changes into your environment, which means potential new vulnerabilities.

Hear ye, my pentest begins today

As a pentest is supposed to be a simulation of a real-life attack, it's always interesting to note the number of companies I've seen announce to all and sundry that they are beginning a pentest. This eliminates one of the primary advantages of the test – *simulating a real life attack*. Telling everyone in advance of a test means everyone will discount logs, reports and alerts generated by that test, effectively robbing you of a simulated incident response scenario. It's a surprising discovery that once you stop announcing your pentests, no one detects them. If you cannot even detect a legitimate pentest with your current enterprise security setup, then it's unlikely you'll be able to detect a malicious attacker doing the same.

Time-limited

Pentesters don't have the luxury of time in any engagement. A website pentest may go from 3-5 days, plus an extra day or two to write up the report. Because of this limitation, pentesters will gravitate towards low-hanging fruit – vulnerabilities that are easy to find, especially with automated tools. Vulnerabilities that required complex custom scripting or time investment won't be looked at in depth simply because they don't have time and this is completely normal. Attackers today don't have any such time constraints so can spend as long as they like focusing on a single asset, dredging up obscure but nonetheless critical vulnerabilities that would require more time investment than a pentest can provide.

Pentester syndrome

Pentesting companies often have to prove their value to their customers – after all, they are paid lucrative rates to provide a niche service. Unfortunately for many, the 'value' derived from the point of view of the customer has been degraded to how many vulnerabilities were found. After all, if a company uses two different pentesting companies in a row, but one of them found more of them than the other company – are they not better?

This is where 'pentester syndrome' occurs – making things worse than they appear. I've had the pleasure (or misfortune – depending on your point of view) of having written or read hundreds of pentesting reports in my career. When a pentester doesn't find any vulnerabilities of note, it becomes the norm to 'talk up' issues that can be classed as 'informational' to vulnerability status. This is damaging for many reasons, the first being, that you are being given a false assessment of your security posture. If you aren't experienced or technical enough to translate these findings into quantifiable risk, you will then spend resource and time blindly chasing down remediations for these 'vulnerabilities' that have absolutely no bearing on your security posture and will never cause you any trouble. I've listed the kind of findings you don't really need to spend too much resource on unless you need a very hardened security posture.

What kind of findings don't I need to be worried about?

So a bit of a caveat: I don't know what your risk profile is, so these might not all be applicable to you. What I can tell you, is that no one has suffered breaches due to the below by virtue of the fact that they only aid an attacker in very specific contrived situations, and then only for a specific kind of vulnerability or require a man-in-the-middle positioning which is, despite what you may hear, difficult to achieve.

No HSTS headers, any kind of SSL/TLS issues

A common one that finds itself onto pentest reports. If you have HSTS then client side certificate errors will always be fatal (the user can't click through the warnings) and that

side can only be negotiated in HTTPS. What this means if someone tries to man-in-the-middle you, well they can't. This also means it's hardly likely to affect many users since a man-in-the-middle position for an attacker is hard to get. You can lump all SSL/TLS issues into this bucket, so things like weak ciphers and outdated versions of SSL are here. As the attack vector is identical (you need man-in-the-middle) these are never likely to affect a great number of individuals at once.

Lack of Secure/HTTPOnly flags on cookies

This one's another common culprit. The lack of the HTTPOnly flag on cookies will only ever help an attacker who's found a cross-site scripting vulnerability and is only leveraging it to extract the cookie itself. As now we have things like the browser exploitation framework (BEEF) and many other vectors to exploit cross-site scripting apart from cookie theft, it is of limited use and is effectively 'hardening' – it's even less useful if they find no cross-site scripting vulnerabilities on your site. The 'secure' cookie only implies cookies can only be sent over HTTPS, so it also falls into 'hardening' like the HSTS issues above

Use of a vulnerable library

I see this one a lot – usually affecting things like out of date third party libraries in products (things like jquery, reactjs, etc.). A vulnerable library only indicates a method in a specific library is vulnerable if it is used and then only in a specific way. If it's not used, no way you can be vulnerable. If you see this in a pentesting report, just ask for a proof of concept, and the finding usually gets taken off the report.

And many more

Lack of x-frame-options header, user or account ID enumeration, lack of CAPTCHA, lack of password complexity requirements, inadequate SPF/DMARC/DKIM configs are all things which may appear but which will rarely cause you any trouble since they are not 'vulnerabilities'.

Getting the most out of your pentests

So now that we've exposed the issues with pentesting today, how can we make them better. Some of them are down to pentesting being the incorrect tool for the job but a lot of it can be improved by engaging with your pentester provider a bit more.

Challenge them

Even if you are not a technical individual or feel out of your depth when people start talking about XXE's and Cross-origin resource sharing, you can always ask the pentester for proof of concept, especially if he's written 'X is vulnerable because of Y'. Pentesters will provide this by default for major vulnerabilities but may sometimes gloss over this part. Feel free to challenge the reports and have them modified. If they can't provide proof of concept, then you can have it removed from the report.

Don't announce them

To get the 'simulation' get prior approval to stop announcing to the world when pentests are occurring. The data you gather will be more valuable and if your incident response procedures and operational teams detect them, that data can be fed back into a virtuous cycle of improvement. This is just as valuable if they *aren't* detected. What failed? Why?

Match them to major functionality improvements and updates

When your application or website has a new functionality added or improved, try and cycle the pentest to coincide right after this. Now, this will largely be budget dependent. Alternatively if you have frequent functionality updates, consider switching to crowdsourced security to replace some or all of your pentests, as this will mitigate the main weakness of pentests – that they occur at a single point in time.

Cycle pentesters

One pentester will see vulnerabilities that a previous pentester missed, and this is entirely normal. To remedy this the best practice is to cycle your pentesters, be it by asking the vendor you use to send a different individual each time, or by just picking a different vendor each time. As offensive security skills are at a premium this will sometimes backfire and you'll end up with the same pentester at a different company (this happens more often than you think). Switching to a crowdsourced security model remedies this entirely, as your pool of testers inflates so you have dozens if not hundreds of people testing your application.

Just another tool

Finally, pentesting is just another tool in your arsenal. You cannot get by with *just* a pentest, nor can you really get by without one. They are useful tools, but are a complement to your arsenal, not the only thing. Whether you preach holistic security or ascribe to a defense in depth model then pentesting is just another aspect of that model. Just make sure you get the most out of it.

About the Author



Alex Haynes is Information Security Manager at CDL.

He has a background in offensive security and is credited for discovering vulnerabilities in products by Microsoft, Adobe, Pinterest, Amazon Web Services, IBM and many more. He is a former top 10 ranked researcher on Bugcrowd - a vulnerability disclosure platform with over 200 vulnerabilities to his name.

Alex can be reached online at alex_haynes@outlook.com

EC-Council

20th March 2018
Royale Chulan
Kuala Lumpur | Malaysia



Collaborating for Cyber Security

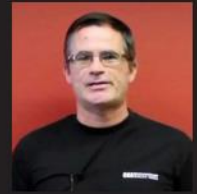
LIVE CLASS ROOM TRAINING

Dates: 19th-22nd March, 2018

ECSA

EC-Council Certified Security Analyst

MASTER TRAINER



Kevin Cardwell

EXPERTS AT THE SUMMIT INCLUDE



Jay Bavisi
President & CEO
EC-Council



Dato' Dr. Haji Amirudin Bin Abdul Wahab
CEO
CyberSecurity Malaysia



Dato' Arif Siddiqui
Former CIO
Standard Chartered Bank
Malaysia



Abdul Fattah Yatim
Chairman
National Standards Committee
on Blockchain and Distributed
Ledger Technologies



Dr. Gajendran Kandasamy
Chief Information Officer
MatchMove Pay Pte. Ltd



Peter Leong
Head of Group Technology,
Kenanga Investment Bank Berhad
Malaysia



Taufik Nordin
Head of IT Security
SME Bank



Dr. Mingu
Chief Information Security
Officer, JPKN Sabah
Malaysia



Jason Lim
Vice President - Cyber Security
Wiki Labs



Vicknaeswaran Sundararaju
Head, Group Information Security
PETRONAS



Jasmine Goh
Head of Information Security
EPF



Han Ther LEE
Digital Security Advisor
REA Group - Asia



Andrew Martin
Senior Board Member
Asia Online Publishing Group



Murari Kalyanaramani
Head of Information Security
Standard Chartered Bank



Shanmugasilan Anantan
Information & Cyber Security
PwC



Solomon Wesley Sua
President & CEO
Pacific Cyber Security Academy



Maninder Pal Singh
Executive Director
EGS

Supporting Partner



Gold Partners



Silver Partners



Official Oil & Gas Solutions Partner



Exclusive Media Partners



Exhibitor



Associate Partner



Media Partners

Speaking Opportunities

JYOTI PUNJABI

+91-99636-54422

jyoti.punjabi@eccouncil.org

Sponsorship & Exhibiting

BASANT DAS

+91-96526-14411

basant.das@eccouncil.org

Training & Delegate Registrations

RENALDO HOWELL

+91-79955-64887

renaldo.h@eccouncil.org

www.eccouncil.org

IMPORTANCE OF “THE GENERAL DATA PROTECTION REGULATION” IN CYBER SECURITY WORLD

A MILESTONE IN PERSONAL DATA PROTECTION

by Yagiz Atmaça, CTO and Co-Founder, Zemana

HOW MUCH DO WE SHARE ON INTERNET?

Technology keeps on changing with every new day. The way we communicate and how we handle everyday tasks have dramatically changed.

It is almost impossible for us to imagine a day without Internet. We use it for almost anything we need: sending emails, sharing documents, paying bills, purchasing goods... When we do this, we enter our personal details online without giving a second thought.

Our credit cards information, contacts, addresses, social media posts, and even our IP addresses are all stored digitally.

So, what happens to all that data? What if our personal details go to the wrong hands?

HACKERS NEVER SLEEP

We all need to be aware that our virtual world is full of cyber criminals who are jumping at every chance to take down companies' websites, steal customer's personal data, and even more.

The fact is that hackers never sleep. Their motivation can vary but the result of their attacks is always the same - causing damage to companies and individuals. This damage can have important impact on the finances and the overall reputation of the company.

As you probably know, the most popular attack methods that are used by cybercriminals are malwares, DDoS attacks, email fraud, Domain Infringement and Hijacking.

Even though hackers are constantly looking for new and improved methods, there is a way to stop them in their attempts of stealing personal information.

In my opinion, EU has found an effective way in preventing cyber criminals from obtaining confidential data. They called it [“The General Data Protection Regulation” \(GDPR\)](#).

WHAT IS GDPR?

We have already heard talks about GDPR. It is a European privacy regulation that is going to be implemented on May 25, 2018, across the entire EU and EEA region. In my opinion, the most positive aspect of implementing GDPR is providing citizens with better control over their personal data and giving them certainty that their information is being protected.

They will have an insight to how their data is used, and they will know who has access to their data. Every gathering of data by companies will be possible only if an individual has been informed about it. If a company (and clients' data) becomes threatened by an external influence, one has the right to be notified within 72 hours.

Will it be difficult for companies to adjust to these requirements?

I believe that for many companies it will be difficult. However, they will have to adjust because EU has set up very tough penalties for all those companies that do not comply – a fine of 20 million euros.

GOING A STEP FURTHER

Years ago, when I was a student, I was carefully studying viruses. I was deeply researching and testing behavior of various malware samples when I realized that, instead of just updating a virus database with known virus variants, the most effective way in fighting malware is developing security solutions based on behavioral characteristics.

What I am trying to say is that all suspicious processes/activities should be blocked automatically. On the other hand, virus databases were only capable of detecting known viruses, but they were unable to detect and fight against new zero-day malware.

Such newly created malware presented an enormous threat for personal data. Therefore, today most of software solutions incorporate behavioral characteristics together with keystroke encryption into their technology.

I see that GDPR even goes a step further and promotes the encryption of pseudonymizing data. These solutions provide prevention and protection in two

directions: making the data unreadable to the unauthorized user or masking the data to remove its ability to identify an individual.

To do this, companies should constantly invest in their technology to improve their security against cyber-attacks, rapidly detect and respond to malicious threats, and

FINAL THOUGHTS

The GDPR will give people more power over their personal data. On the other hand, it will decrease the power of some organizations who collect and use such data for monetary gain. Even though GDPR does create challenges and efforts for companies, it also creates opportunities.

In my opinion, it is important for companies to understand that if you show to people that you can protect their personal data, they will trust you more and there are better chances that they are going to want to work with you.

Companies who show that they are protecting individuals' privacy, who are transparent about how their data is used, who invest in new and improved ways of handling customer data will for sure, build trust and acquire new customers and clients.

About the Author

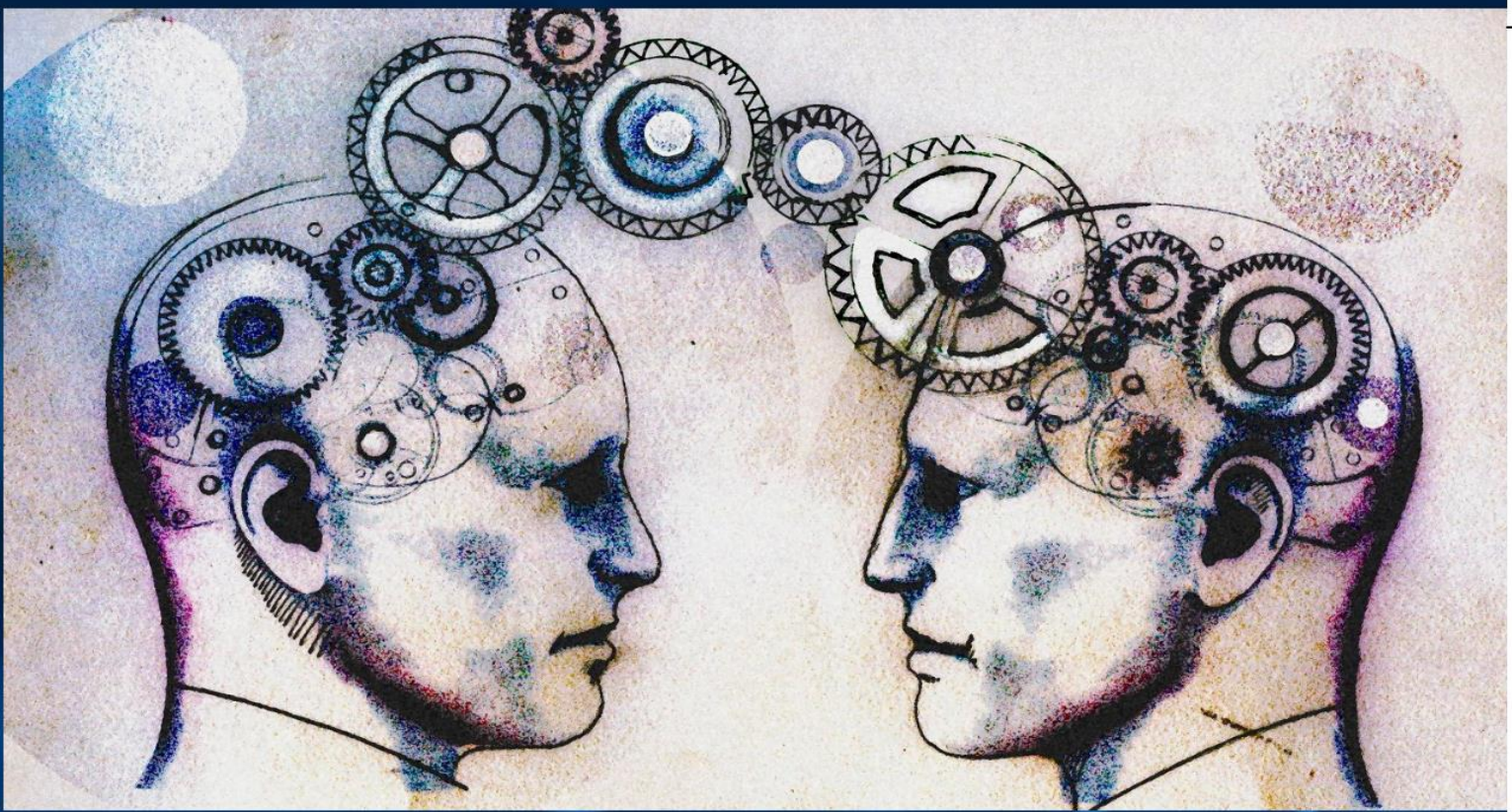


Yagiz Atmaca, Zemana

Yagiz Atmaca is CTO and Co-founder of Zemana, mainly working on long-term product development strategies while guiding and pursuing company's overall strategies and vision.

Yagiz can be reached online at yagiz.atmaca@zemana.com

and at our company website <https://www.zemana.com/>



**World Congress on
Computer Science, Machine
Learning, and Big Data Analytics**

**AUGUST 30-31, 2018
DUBAI, UAE**



<https://computer-science.enggconferences.com/>

HOW WE CAN SECURE THE ENERGY GRID AND THE SMART HOME OF THE FUTURE

by Uri Kreisman, COO, Bluechip Systems

On August 15th, 2012, the Saudi Arabian group Saudi Aramco [suffered a malware attack](#) called “Shamoon” that damaged about thirty thousand computers. The state-owned group runs the entire nation’s oil production, and the attack sent the nation’s entire economy into disarray. In total, eighty-five percent of Saudi Aramco’s hardware was compromised.

Shamoon highlights how a cyberattack on an energy entity could cripple an entire nation. Indeed, it’s this potential for such damage that makes them an attractive option for cyberterrorists.

Smart grids being an attractive target for cybercriminals points to a larger trend. The internet of things (IoT), powered by smart devices, gives cybercriminals the opportunity to hack devices previously unheard of even a decade ago. Since more and more homes are now attached to the smart grid through IoT, the need to secure these networks is becoming more and more vital.

All of the internet connected devices in your home that have cameras attached to them - smartphones, smart TVs, video game consoles, baby monitors, laptops -- can be hacked and exploited to monitor and spy on residents and execute powerful botnet attacks all without your knowledge.

There is now an increasing need to be able to secure IoT devices that were never built to be secured in the first place. Instead of relying on manufacturer software updates, I believe that a hardware-isolated solution is the future. If you embed a low-power, highly flexible, hardware-isolated computational and storage container that isolates data inside the host architecture, you can secure data and processes independently of the host’s operating system or networking protocol and make them virtually impervious to attack; an innovation that will change cybersecurity as we know it today.

IOT PERVADES THE ENTIRE UTILITY AND NETWORKING GRID

As of today, there are 8.4 billion IoT devices currently in use: one device for every living person on the planet. This number is set to keep growing, especially as our homes become “smart” via their connection to the internet. Since the house of the future is pre-loaded with an ubiquitous number of these devices -- Alexa, Google Home, Smart Fridges, smart cars, smart thermostats, automatic locks and so on -- hackers can monitor and access our information when we are at our most vulnerable.

Even if you “unplug” your home and refuse to install any IoT devices, you’re still vulnerable as smart buildings are on the rise. McKinsey & Company expect the IoT installed base in smart buildings to grow by 40% until 2020. Where you work, commute and go to the gym could be exposed to hackers and used to monitor or harass.

Cyberattacks on the entire grid are becoming increasingly more common. In December 2015, three electric companies in Ukraine [were targets of a cyberattack that resulted in power outages for two hundred twenty five thousand customers](#). Even after power was bright back several hours later, control centers still weren’t fully operational two months later.

According to ICS-CERT statistics, energy is the second-most targeted sector. Energy companies oftentimes rely on Industrial Control Systems (ICS), which have become attractive targets for cyberterrorists for several reasons, including:

- Their longevity means information on how to program (and, by extension, hack) is readily available online.
- Many ICS protocols were developed with availability and control in mind, not security, leaving systems with innate vulnerabilities.
- Many systems are decades old. Security updates and patches are often pushed off due to fears that they would cause power outages.
- The emergence of smart grids have increased the attack surface of hacking activities

HARDWARE ISOLATION IS THE KEY TO SECURING IOT NETWORKS

Software updates and best practices may have worked for one or two of the breaches in the history of IoT, but these tactics are no match for a more sophisticated solution that exploits the device firmware or hardware. Indeed, cybersecurity experts have increasingly been partnering and working together with IoT industry leaders to find out the ways in which we can harden devices that were never built with security in mind.

The only viable defense is one that relies on the inherent security of hardware isolation. By shifting all of the IoT processes to another processor, hardware solutions effectively sandbox important data and make them simply inaccessible from the IoT device itself.

I believe that the future of IoT security rests in the power of embeddable microchips and the power of process isolation. By inserting a linux-powered computer into the architecture of a non-secure IoT device, you will be able to create a Hardware Root of Trust that completely seals any endpoint from man-in-the-middle attacks, effectively preventing weaponization of such endpoint as a source of future DDoS or Mirai attacks.

This new approach to cybersecurity aims to protect an IoT device by changing the whole paradigm: if you store away data on a hardware isolated container, it cannot be accessible to an attacker. Adding an isolated self-contained layer of hardware and software protection is of paramount importance to protecting our smart energy grid and our smart homes in the future from infrastructure-level cyber attacks.

About the Author



I'm Uri Kreisman, the COO of Bluechip Systems - we're building hybrid hardware and software cybersecurity solutions for IoT and mobile.

With more than 20 years of experience in the industry, I write on emerging trends and technology in cybersecurity.

You can find me on [LinkedIn](#) and at our company website: <http://www.bluechipsys.com/>

EC-Council

present

MENA

CISO SUMMIT

18th - 19th April 2018 | Dusit Thani Dubai

UNITING EFFORTS TO CREATE A SECURE CYBERSPACE

EXPERTS AT THE SUMMIT INCLUDE



Anson Zeall
Chairman ACCESS
The Singapore Cryptocurrency and
Blockchain Industry Association



Adv. Prashant Mali
Cyber Law & Cyber Security Expert
High Court Lawyer, India



Abdullah Mutawi
Partner
Baker Botts, UAE



Chandra Shekhar Jajware
Group Chief Information Officer
Khimji Ramdas Group, Oman



Sanjay Khanna
CIO RAK Bank



Serdar Güner
Director
Supervision
Dubai Financial Services Authority



Venu Sriraj
Group Chief Information
Security Officer
UAE EXCHANGE



Rohan Roberts
Innovation Leader
GEMS Education



Parthasarathy P
Group Chief Security Officer
First Abu Dhabi Bank



Saqib Chaudhry
Chief Information Security Officer
Cleveland Clinic Abu Dhabi



Bruno Fonseca
Chief Information Security Officer
AXA



Charles (Chuck) L. McGann
Jr. COO
McGann Consulting Group, USA



Mohamed Roushdy
Experienced CIOFinTech |
Digital Transformation | CXO Advisor

Gold Partner



Silver Partner



Exclusive Media Partners



Exhibitor



Media Partners



Speaking Opportunities

JYOTI PUNJABI

+91-99636-54422

jyoti.punjabi@eccouncil.org

Sponsorship & Exhibiting

BASANT DAS

+91-96526-14411

basant.das@eccouncil.org

Training & Delegate Registrations

HEMALATHA LOKAVARAPU

+91-8341 589 697

hemalatha.l@eccouncil.org

www.eccouncil.org

CLOUD CLOUD & THE CHINESE AGNOSTIC

by David Nagrosst, Entrepreneurial Leader and CISSP Qualified Cyber Security Expert



All three of the world's largest hosting companies – Amazon, Alibaba Group, and Microsoft – have achieved their positions by offering relatively low-cost cloud computing resources.

How did Aliyun go from China based Cloud solution to an International player and should buyers beware?

NATIONAL TO INTERNATIONAL

Accessibility and ease of use plays an important part in the success of a hosting provider and Aliyun (Alibaba cloud service) had some fundamental limitations that held back its earlier growth. Most notably, its virtual machines could only be hosted in China, which meant that they could not be bought by many customers outside China, and it was unsuitable for hosting websites that had an international audience.

Any customer who wanted to buy a virtual server at Aliyun had to go through an identity verification process that required them to be a national of China or one of a few other Asia-Pacific countries, or to represent a Chinese company. Also, all websites hosted in China were – and still are – required by law to obtain an ICP licence.

Flaky cross-border internet connectivity, along with potential interference by the Great Firewall of China, also made China a poor location to host any website that has an international audience. The aliyun.com website itself was also hosted in China, resulting in a very poor user experience from outside China – many international requests were slow and some did not succeed at all.

By opening overseas data centres and hosting the international version of its website – alibabacloud.com in Singapore, Alibaba solved a few connectivity issues. Singapore has numerous submarine cables that provide links throughout Asia, Australia, the Middle East, Europe and the US. This connectivity results in faster, more consistent international response times, with very few requests failing.

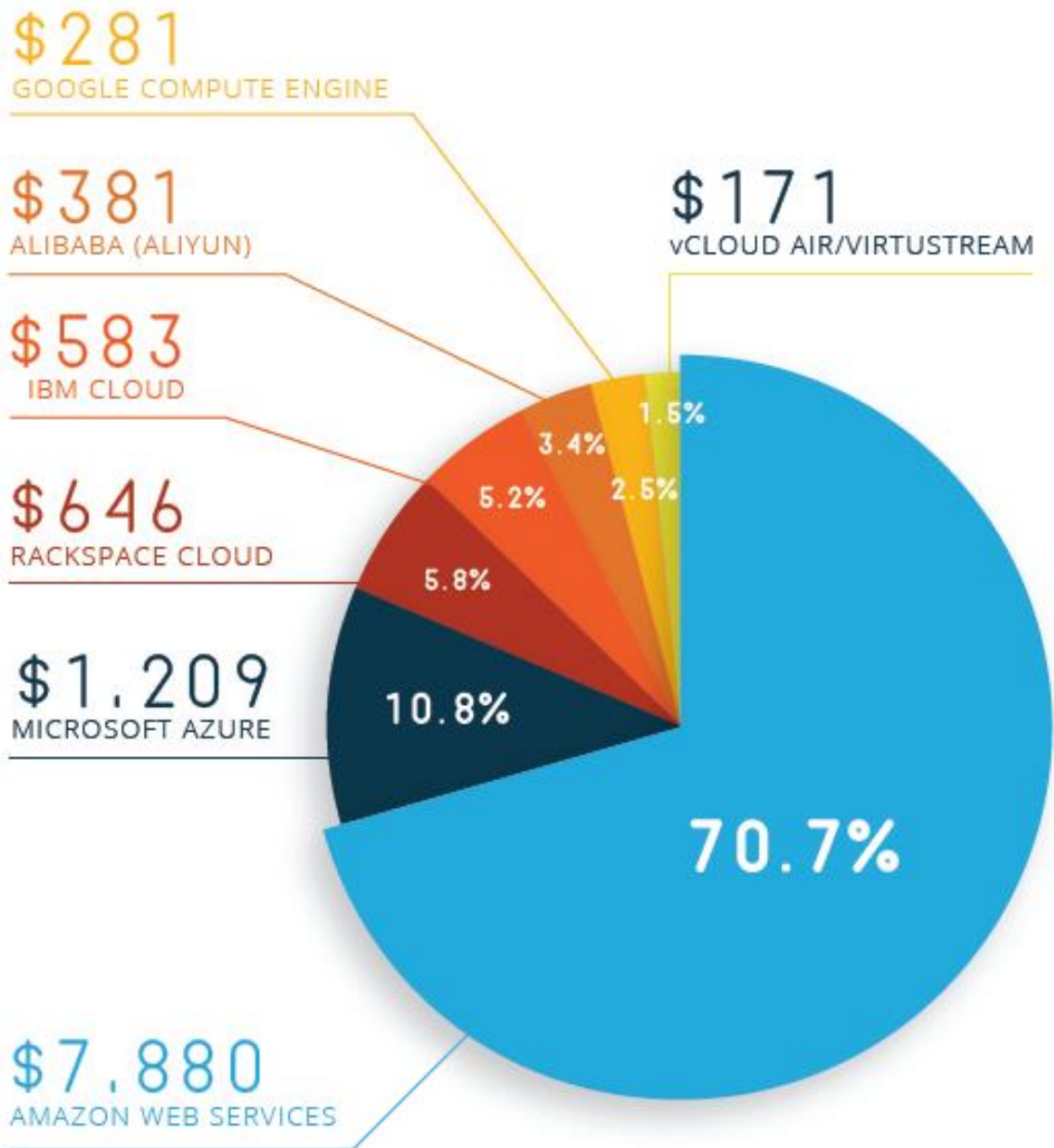
In addition to its six data centers in mainland China, Alibaba Cloud now operates several others located in Hong Kong, Japan, Singapore, Australia, Dubai, Germany and the United States (Silicon Valley and Virginia). It is also planning to open more in India and Indonesia by March 2018. With partnerships with Nvidia and Cisco on cloud data center technology, Alibaba and NXP semiconductors announced a strategic partnership to enable development of secure smart devices for edge computing applications and have plans to further develop solutions for the Internet of Things (IoT).

To facilitate growth in the world market, Alibaba Cloud now automatically presents international visitors with an English-language version of the site. Logged-in users can control their products via an international version of Alibaba Cloud's control panel and a ticket-based support system is also available in English, where previously it was only available in Chinese.

WHO USES ALIBABA CLOUD?

Chinese companies are still the most prominent users of Alibaba Cloud given that most of its web-facing computers are still hosted in China.

Although Alibaba has the second largest number of web-facing computers, it has a relatively low presence among the world's top million websites – only 6,560 are hosted by Alibaba, compared with 79,800 at Amazon.



Some of the highest ranked websites hosted in Alibaba's US data centers – and therefore more readily accessible by an international audience – belong to Alibaba Group companies. This includes several hostnames used by its AliExpress online retail service, which allows Chinese retailers to sell to international customers. Customers in mainland China are not allowed to buy from AliExpress; instead, they use Alibaba's Taobao marketplace, which is hosted in China.

IAAS, SAAS & ALIBABA

Globally, Alibaba is the No. 3 infrastructure-as-a-service (IaaS) public cloud vendor, according to Gartner's latest numbers. Compared to public cloud leader AWS (44 percent) and No. 2 Microsoft Azure (7 percent), Alibaba trails behind with only 3 percent of the global market share for 2016. But its growth — almost 127 percent from 2015 to 2016 — far outpaces its top two competitors.

Software-as-a-service (SaaS) has grown 10 times faster than traditional, on-premises software among Chinese enterprises, so there seems to be a huge incentive for U.S.-based software companies to sell to the Chinese market and run on Alibaba Cloud.

As U.S. companies go to China through those programs, synergy the benefit for Alibaba is two-fold. One, they will eventually be able to host the same SaaS in the Alibaba Cloud in the U.S. And second, they will be able to more quickly deploy their services in the U.S. While the company's IaaS business is strong, it doesn't have significant platform-as-a-service (PaaS) or SaaS offerings. However, Alibaba's IaaS is still light-years behind AWS in terms of market share.

ALIBABA – THE GLOBAL PLAYER AGNOSTIC OF THEIR CHINESE HERITAGE?

As a Chinese cloud provider there are data protection issues – the lack of enterprise-grade offerings of AliCloud, most companies are reluctant to upload mission-critical workloads into AliCloud or sensitive data. With a team of more than 100 security specialists who focus on product development and provides security products directly customers, there are still niggling doubts and worries over security from International consumers - they may simply be put off by the fact that Alibaba Group is a Chinese company where the Chinese government is notorious for censoring internet content. There may be fear and uncertainty over whether such control could also extend to customer content hosted by Alibaba in other countries.

Apart from Alibaba, Tencent, the owner of WeChat is now the largest Internet company in China, has plans to significantly increase their cloud offerings overseas. The primary uptake is Chinese companies expanding in overseas markets in Europe and the US, but they also have their eye on serving international companies. Will they draw a truly international client base despite being Chinese owned or does it even matter for it to get on the global market share board? Does the China growth story even need International customers in the short term to grow in their global market share or will enough domestic Chinese companies leverage this platform to grow their presence overseas?

It will be interesting to see how Chinese cloud compares in 2018 and how successfully they will be in acquiring new international customers. I for one to think their Chinese Internet growth is in the near term helping to fuel domestic growth and access to foreign markets and It should be noted that I am long Tencent and Alibaba as an investment.

About the Author



David Nagrosst is an Exceptional International Leader and CISSP Qualified IT Security Expert with 20 years+ demonstrable experience in business, sales and providing IT Security, Cloud, and Datacenter Solutions to Organizations from Start-up to Fortune 150. He provides outstanding strategic, operational, business (PNL) and sales leadership to high-performing teams in sales, pre-sales solutions, consulting, engagement and bid management, leading senior teams in Singapore, Hong Kong, China, India, Japan & Australia.

David is also an international keynote & workshop speaker and a member of AmCham Singapore. David has talked in major events like 6th Compliance Summit Asia, DCD Zettastructure, DCD Converged Hong Kong, and CenturyLink APAC Sales Kickoff. He is committed to developing, testing and continually creating new methods to drive efficiency, cost saving, growth and profit

alongside innovative technical expertise. He is eager to support international Security companies operate and develop in Asia.

He has held senior positions in Consulting, Software, Telecom, and Startup companies with expertise in Financial Services and knowledge and experience in many other industries such as E-commerce, Education, Construction, Retail, Internet Advertising and Publishing.

More about David can be found on his LinkedIn:

<https://www.linkedin.com/in/davidnagrosst/>



SMART CITIES EXPO WORLD FORUM

7th-8th May 2018, Toronto, Canada

SPEAKERS HIGHLIGHTS 2018



Marc Trouyet
Diplomat (UN & Development), Town-Planner, Consulate General of France in Toronto, Canada



Shawn Slack
Director Information Technology and Chief Information Officer
City of Mississauga



Michelle Holland
City Councillor, Chief Advocate For The Innovation Economy,
City of Toronto, Canada



Ray Boisvert
Provincial Security Advisor,
Government of Ontario
Canada



Mike Williams
General Manager, Economic Development & Culture
City of Toronto, Canada

SPONSORS & PARTICIPATING COMPANIES

At Smart Cities Expo World Forum 2018



Register at www.smartcitiesexpoworldforum.ca/registration/

GDPR PRIVACY LAWS: RAMIFICATIONS AND POSSIBLE INTERDICTIONS FOR OPEN SOURCE SECURITY VULNERABILITIES

The Data Protection Directive 95/46/EC, adopted in 1995, was an attempt by the European Union to create a unified set of data privacy rules for all member countries. In 1998, the U.S. legislation enacted the Health Insurance Portability and Privacy Act (HIPPA) to provide significant data privacy and security provisions. This was followed in 2003, by the state of California's bill SB1386, which established mandatory privacy laws in the U.S. As each new set of regulations were implemented, multinational businesses were required to adjust their data privacy and protection practices.

In less than two months, on May 25th, the E.U. will enact its landmark General Data Protection Regulation (GDPR) that was approved in 2016. Not only will the GDPR will affect any organization located or doing business in the E.U., it will also impact organizations processing data of EU individuals, regardless of their own geographic location. Just as multinationals had to address their privacy and data protection activities in order to do business in California, so too will they will have to adjust their practices in order to comply with the new, and more stringent, data privacy and protection policies in the E.U.

So what is the GDPR?

According to the official GDPR website [www.eugdpr.org], it is a law to “protect all E.U. citizens from privacy and data breaches in an increasingly data-driven world.” Its reach is broad, “it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.” And, the penalties are non-trivial, “organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).”

The GDPR includes the E.U.'s Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (95/46/EC). The GDPR contains these guidelines, and several more, and has turned mere directives into law, with stiff penalties for non-compliance.

The Equifax data breach of 2017, illustrated the issues surrounding the use of open source code, or code elements, and data protection. The credit giant could have avoided the breach had it installed the version of an Apache Struts software that had

fixed the security vulnerability for which the warning was issued. This update had been available for months prior to the outbreak.

Had the GDPR been in place at the time of the Equifax breach, the fines would have been significant. Based on estimated Equifax 2017 income, which has been delayed in reporting, 4% of its approximately \$3 billion in revenues is \$120 million. The days of sweeping security vulnerabilities under the rug in the E.U. are over.

Proliferation of Open Source and Its Vulnerabilities

More than 90 percent of the software written these days integrates open source code. Such code is used in operating systems, network platforms and applications. This trend will only continue to grow because, by leveraging open source, developers can lower assembly costs and quickly add innovations.

Whether software code is proprietary or open source, it harbors security vulnerabilities. Because of its transparency, open source code tends to be better engineered than a comparable piece of proprietary code. And thanks to its flexibility, open source code is extensively used. This means that a security vulnerability in a piece of open source code is likely to exist across a multitude of applications and platforms. Consequently, open source software vulnerabilities become a “low hanging fruit” for hackers to target and attack.

The mission to secure outward-facing, software infrastructure systems has become incredibly chaotic, thanks to obstacles that include the proliferation of open source, a poor accumulation of institutional software memory, unknown software components delivered in third-party binaries and a very low-level priority placed on engineering debt.

So what can businesses do to mitigate their potential data losses and E.U. fines from open source software vulnerabilities?

Open Source Software Vulnerability Cyber Security Insurance Interdiction

Many businesses are finding that their software infrastructure becomes increasingly challenging to secure every year. Some organizations have turned to purchasing cyber security insurance to mitigate their financial losses from this trend. PwC estimates that by 2020, businesses will spend \$7.5 billion for cyber security insurance. [\[https://www.technologyreview.com/s/603937/insurers-scramble-to-put-a-price-on-a-cyber-catastrophe/\]](https://www.technologyreview.com/s/603937/insurers-scramble-to-put-a-price-on-a-cyber-catastrophe/)

Many legal and insurance pundits have commented about the limitations of cyber security insurance as it relates to GDPR. For example, a November 2017 contribution by Shoosmiths LLP in Lexology, see: <https://www.lexology.com/library/detail.aspx?g=25c7cefc-e438-48cd-82a3-639611506656>, a resource of free-to-access legal updates and analysis, posits that organizations will find it tremendously difficult to secure an insurance company willing to face and underwrite a policy covering 4% of global turnover in this day and age, when cyber-attacks are becoming daily occurrences.

Effective Vulnerability Remediation Interdiction

Another method of addressing open source vulnerabilities is for businesses to know exactly what open source code elements hide in their software – before and after they procure it. This can be a challenge given that open source code elements are not well documented due to software procurement trends and intellectual property issues.

Fortunately, there are new types of fingerprint-based binary code scanners that alleviate this challenge. These solutions enable companies to scan their software and firmware in binary code, without recreating the source code through the somewhat inaccurate and time consuming practice of reverse engineering – and then scan it for composition.

By knowing exactly what open source code elements reside in the current or prospective code, IT departments can assess their investment risks and take proactive measures to ensure that they are up-to-date with the latest open source component versions. The implementation of an effective open source update model should be of utmost priority to ensure data security and mitigate potential corporate losses.

Open source software development and use are irreversible trends in today's business. And given the undeniable importance of the E.U market, organizations must adapt to comply with the GDPR. It is prudent for software development and IT teams to investigate and reevaluate, in-depth: the ramifications of GDPR, their client data and privacy procedures, the short-term risk mitigation potentially offered by cyber security insurances and their plans and practices for finding and responding to open source security vulnerabilities.

About the Author

Tae Jin "TJ" Kang is a technology industry executive and entrepreneur. He is the president and CEO of Insignary. In addition to founding a number successful technology startups, Mr. Kang has held senior management positions with global technology leaders that include Korea Telecom and Samsung Electronics, among others.

Mr. Kang can be reached online at tjkang@insignary.com and at our company website www.insignary.com





LOOK TO THE SOURCE. PSST. WE'RE OVER HERE.

Having a go-to is great. A go-to friend. Go-to café. And now, a go-to cybersecurity resource.

At RSA Conference, we play host to the industry's top minds, addressing what's relevant in cybersecurity. And what's coming your way. Our global events are filled with expert-led keynotes, tutorials, and everything else you'll need to be on your professional toes.

But don't be fooled, there's more to us than just great events and really smart people. From podcasts to virtual sessions, we also create content to keep you in the loop 365 days a year. And when you subscribe, we've even been known to throw in an exclusive deal or two. You know, just because we like you.

Experts. Smart content. Insider savings. There's a lot waiting for you here. And no reason to wait.

Subscribe to greatness today: www.rsaconference.com/CDM

RSA[®]
Conference

Where the world
talks security

Follow us on: #RSAC     

TECH AND IT COMPANIES ARE DRIVING CLOUD SECURITY INVESTMENTS

NEW SURVEY SHOWS HOW COMPANIES IN DIFFERENT REGIONS AND INDUSTRIES DEAL DIFFERENTLY WITH CLOUD SECURITY RISKS

by Michael Fimin, CEO and Co-Founder Netwrix

Regardless of how long organizations have used the cloud, how much sensitive data they entrust to cloud providers and how regulated their industries are, they share the same cloud security concerns. Most of these concerns are directly attributed to human factors and stem from insufficient awareness about activity in the cloud environment.

Netwrix recently conducted an in-depth report on cloud security, which supplements the [2018 Netwrix Cloud Security Report](#). The report unveils survey findings specific to various industries and regions. Overall, 853 organizations shared their feedback for the survey, conducted in November 2017. All organizations are public or hybrid cloud users.

Key findings include:

- 80% of technology & IT organizations get support from top management for cloud security initiatives — more than any other industry surveyed.
- Malware is most feared by health care organizations (61%) and government entities (60%), though it is the number two concern for all industries surveyed.
- 62% of educational institutions perceive their own employees to be the biggest threat to cloud security, the largest share among the industries surveyed. This result is explained by the education sector also having the lowest visibility into user activity in the cloud: Only 18% of the institutions are completely aware of their IT staff activity and just 7% have complete understanding of business user activity.
- Financial organizations outdo other industries when it comes to visibility into IT staff activity: 47% of them claim to have complete visibility. They are also the most active cloud users; 96% of financial organizations already store sensitive data there.
- The retail & wholesale sector sees the biggest threat as hackers (48%), rather than employees (27%). This also is the only industry that cited denial-of-service attacks as one of their major concerns.
- Organizations from JAPAC are more enthusiastic about broader cloud adoption (54%) and adopting a cloud-first approach (44%) than companies in other regions.
- To strengthen IT security, the majority of North-American (57%) and European (57%) organizations are planning to improve employee training, while the most popular measure planned by Asian companies is the purchase of vendor security solutions (49%).

The majority of organizations across all the industries and regions surveyed believe in the power of staff training and security policy enforcement as two top measures to improve cloud security. However, these measures will work only if you have complete visibility into user activity in the cloud.

You can download the full cloud security report at www.netwrix.com/go/2018cloudsecurityindepth.

About the Author



Michael Fimin is the CEO and Co-Founder of Netwrix. He joined Netwrix in 2007, bringing more than a decade of IT industry experience, management practices and innovation. Prior to joining Netwrix, Michael held several key positions at Aelita Software (later acquired by Quest Software), driving the company's top-selling security and compliance product. Michael lives in Monarch Beach, California. For more information, visit www.netwrix.com

Michael can be reached online at (@TrueCalifornian) and at the Netwrix website www.netwrix.com.

Don't miss the world's leading event in Intelligent Transport Systems & Services



Early Bird Registration now open!

17 – 21 September 2018
Copenhagen, Denmark
www.itsworldcongress.com

A unique opportunity to:

- Exchange information and network with 10 000+ stakeholders and decision makers
- See the latest mobility solutions
- Share experiences and lessons learned
- Monitor progress and measure results of implementation and deployment
- Exhibit and experience cutting-edge technologies and innovative products and services
- Enter business and partnership opportunities

Organised by:



Co-organised by:



Hosted by:



Supported by:



DON'T GET CAUGHT BY RANSOMWARE

by Aarij Khan, Vice President of Marketing, Securonix

As businesses increasingly rely on digital systems, networks, and data for operations, the value of maintaining the integrity and availability of these resources becomes more critical. According to the Ransomware 2017 Report by Cybersecurity Insiders, 80% of cybersecurity professionals surveyed considered ransomware as a threat ranging from moderate to extreme.

Ransomware infections are particularly concerning for Security Operations Center (SOC) analysts because there is usually little to no advance warning. Unlike advanced persistent threats (APT), that rely on low-and-slow techniques, ransomware instead uses shock-and-awe techniques. Once it starts, an attack is capable of encrypting large numbers of files within minutes. For individuals this can be the contents of their computer. For companies, where employees often have access to multiple shared files and databases, ransomware can spread quickly to shared drives, bringing business to a standstill. When it comes to organizations such as hospitals, critical infrastructure, or transportation systems, a ransomware attack can even be potentially life threatening. Thirty nine percent of security professionals surveyed estimate that it would take anywhere from a couple of days to a few weeks for their organization to recover from a ransomware attack.

Ransomware is likely to remain a popular form of attack as long as it remains profitable to attackers. While only 23% of security professionals surveyed say that their company is even slightly likely to pay a ransom demand, 3% of companies have already set up a bitcoin account to prepare for a future attack. Combined with high-profile news of large payouts, ransomware isn't likely to disappear any time soon.

There are many methods hackers use to spread ransomware. The most common method is through malicious email attachments, often as part of a phishing campaign. Victims are sent an email that appears to come from a trusted source and are enticed to open the attachment. This could be an Adobe PDF, Microsoft Excel or Word document, or even an image file, and is infected with the malicious ransomware. The second most common vector for ransomware attacks is visiting malicious websites that exploit common software vulnerabilities to spread ransomware to visitors. Other attack vectors include social engineering, where an attacker poses as a trusted individual, or even removable media, where attacks can spread through infected USB drives.

Given all of this, how can you protect your organization from falling prey to a ransomware outbreak? A comprehensive approach to ransomware requires three things: people, process, and product.

First, train people across your organization. Teach users how to spot and avoid phishing campaigns. Encourage good “cyber hygiene” practices including keeping devices up to date, learning how to identify and avoid suspicious public WiFi access points, and maintaining regular backups of important files. All of these practices help reduce the risk of infection and minimize the impact of a successful attack.

Second, create a process that ensures that, in case of a successful ransomware attack, the number of users, devices, and amount of data compromised is minimal. Automated incident response (IR) triage actions, when well defined and quickly executed, are a critical first step. Automation is particularly important given the speed with which ransomware attacks occur. When a user is infected by malware, quickly informing the IT security team, shutting down the user’s network connection(s), and powering off the device are all steps that can prevent a massive impact. Additional IR processes executed by security analysts can ensure that the ransomware does not spread across the organization or across shared resources.

Third, leverage available product technologies to detect and respond to ransomware attacks, minimizing impact, and speeding recovery. Organizations have historically relied on perimeter, network, and endpoint security products to prevent attacks. However, point products often create security data silos, leaving SOC teams to struggle with overall visibility and intelligence. To close the gap between point products, consider a next generation machine learning and AI-based security analytics solution that collects data from across your enterprise, adds wider context, and intelligently cuts through the noise to identify the alerts that can indicate a ransomware infection. Organizations that deploy an advanced security analytics technology, train their users appropriately, and implement effective triage and recovery processes will be much better prepared to defend against ransomware attacks.

About the Author



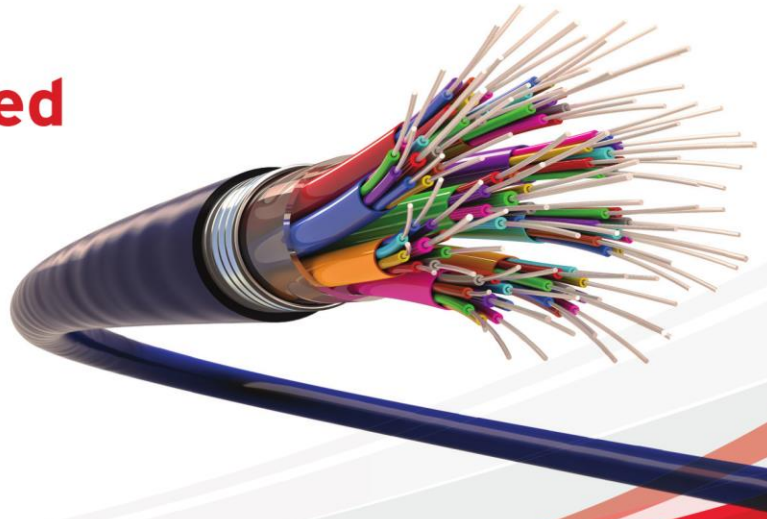
Aarij is the Vice President of Marketing at Securonix.

He brings a deep understanding of the security market and buyer combined with over 15 years of marketing leadership at high growth, innovative security vendors.

Aarij can be reached online at aarij.khan@securonix.com and at www.securonix.com



Detect and prevent breaches at wire speed



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

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

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



Proven capability

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

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

Industry leading threat intelligence



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

www.trendmicro.co.uk/xgen-cyber

by Thomas MacIsaac, Cybersecurity Strategist, SSH Communications Security

Cybercrime is as old as the internet, which means there has always been a need for cybersecurity. One of these bits of security is the Secure Shell (SSH) protocol, designed by Tatu Ylönen more than 20 years ago to protect communications between computers. Its main function is to circumvent man-in-the-middle attacks that can steal data in transit by establishing a kind of shell—an encrypted tunnel—to facilitate secure communication between two points. It gained widespread adoption such that today, SSH comes pre-installed in every Unix, Linux, Mainframe, Mac and most network devices.

Dangerous Complacency

The success of SSH is a two-edged sword. It effortlessly arrives on servers and devices, so most organizations put no further effort toward it. They do not have any group or individual responsible for monitoring SSH activities. In fact, most businesses make the leap that SSH equals encryption and encryption equals security. In this day and age, who doesn't want more encryption and security?

The premise that encryption alone negates the need for vigilance and oversight of SSH use is dangerously flawed. Here is why: SSH does encrypt communication, but the real formula of SSH is best represented by a more accurate equation of SSH equals access. SSH access comes in two variants: interactive (Human to Machine) and non-interactive (Machine to Machine). Furthermore, access to critical resources and data needs to be managed, monitored and controlled. Thus, closing the SSH responsibility gap should be a Tier 1 priority for an enterprise.

Who Holds the Keys?

As with other encryption protocols, SSH works by creating key pairs consisting of a private and a public key. To understand the function of these keys, it's best to use an analogy: A public key is similar to a lock on a door, whereas a private key is similar to a physical key you keep in your pocket. Presenting a matching private key to a public key grants an encrypted connection.

There are certain aspects of SSH that engender risk:

- **Tunnel vision** – SSH tunneling enables traffic to traverse routers and avoid being blocked.
- **Self-provisioned keys** – It is a disquieting thought that SSH keys allow any employee or consultant access to critical applications.
- **SSH keys are good forever** – Even a key pair created decades ago still works today.
- **Security work-arounds** – Security solutions don't work on SSH encrypted traffic, effectively creating a security blind spot.
- **Deep-level access** – SSH can provide root (command)-level access to systems and data.
- **Sharing the wealth** – Because people often copy and share SSH keys, it is impossible to know who did what when.

It's clear to see how SSH keys, if used with malicious intent, grant the ability to do all sorts of nefarious things that cannot be detected within this security blind spot created through SSH.

Guidelines for SSH

However, all is not lost. Effective, consistent SSH key management and risk prevention are possible with the implementation of industry best practices. One best practice is to create usage procedures that include periodic access reviews, documenting and disseminating security policies and standards, and implementation of required IT controls.

Another is to create and implement hardening configuration and to set up a timetable to regularly review the configuration. Consider automated tools to manage the configuration and apply integrity control checks and monitoring over critical files. Make sure to define roles and responsibilities as well, so that SSH key management does not fall through the cracks again.

Because there could ultimately be tens of thousands of keys in play, automation is critical for the success of SSH key deployments. Make sure to put automation in place. Standardization is required, and access restrictions are key. Finally, inventory of keys and usage tracking is necessary as part of the overall provisioning of users and accounts.

Encrypted communications are a great asset – until they aren't. Cybercriminals are determined and innovative and will use whatever they can find to steal data. SSH in the wrong hands can be disastrous, granting root-level access to the network. Encrypted traffic can cause a security blind spot, so SSH must be properly and consistently managed. Use these best practices now to get started on the path to greater overall security.

About the Author



Thomas Maclsaac is a cybersecurity strategist and currently serves as VP Eastern US, Canada and Federal Markets for SSH. Thomas has spent over 22 years in the high-tech industry representing many of the foundational and cutting-edge technologies of our time. Thomas regularly consults with Fortune 500 businesses and government agencies in the area of security on topics of data at rest and in transit, identity and access management, APIs, and SIEMS, and is a sought-after speaker for audit, compliance, and security events.

First Name can be reached online at our company website <https://www.ssh.com/>

THIRD-PARTY PATCHING

A VENDOR-NEUTRAL FRAMEWORK FOR ADDRESSING THE OTHER 85% OF VULNERABILITIES

by Duncan McAlynn, Cybersecurity Consultant

If your organization is like most, you likely have clearly defined processes in place for deploying newly released Microsoft security updates each month. If not, you should. We've only had 15 years to hone the process, dating back to when Bill Gates dropped the hammer following the massive "Melissa, I Love You" VBScript outbreak. The result of the worm was a halt to all new product development and an immediate review of existing code sets across all Microsoft products, as well as sending over 7,000 developers to security training.

In the following year, this Trustworthy Computing Initiative gave birth to what we have all come to know and love (or hate) as Patch Tuesday. This cyclic schedule of software update releases on the second Tuesday of each month has allowed us to align our internal resources to assess applicability, test compatibility and deploy those updates in a structured manner, including obtaining any required change management board approvals.

In short, "We got this!"

But, do we have a handle on it? Do you believe your company has a solid grasp on its patch management? Let's look at the facts.

Per data obtained from cvedetails.com, no more than fifteen percent (15%) of all the known vulnerabilities reported over the past three-year period have affected the Microsoft platforms. By that I mean all Microsoft operating systems (both desktop and server versions), Office, Internet Explorer, Skype, Visual Studio, SQL Server, SharePoint, BizTalk, you name it. If it has had the software giant's name associated with the vulnerable executable, it has only ranged between 8%-15% of all the reported vulnerabilities.

So, what about the other 85%? That is where all the third-party applications and non-Microsoft operating systems come into play. In most corporate environments, you're going to have these applications like PDF readers, Internet browsers, Java-based applications, networking tools, graphic programs and the like. These software applications have update releases for new versions or security patches for existing versions. And, as the cloud becomes more and more a part of our daily lives, it becomes increasingly more important that we're applying these third-party product updates in a timely and consistent manner to protect the attack surfaces that they are introducing because of the applications being connected to the Internet.

When I'm giving conference and user group presentations on this topic throughout the country, I tend to ask the audience "Why are you not being as diligent with patching your third-party products as you are your Microsoft updates each month?", I hear the same reasons repeatedly. See if you can relate to them:

1. "We don't have the time"
2. "We don't have the resources"
3. "We don't have the right tools"

This is the recurring theme that I am constantly faced with and I completely understand where they are coming from. In a large-scale enterprise environment with global operations and tens of thousands of endpoints, just handling the Microsoft updates can be a vicious, never-ending cycle requiring *at least* one full headcount administrator to manage the pilot, user acceptance and production deployments. To illustrate this point, here is a typical approach such an organization might take for patching *just* Microsoft products each month:

Patch Release Cycle

© 2017, WindowsSecurity.tips

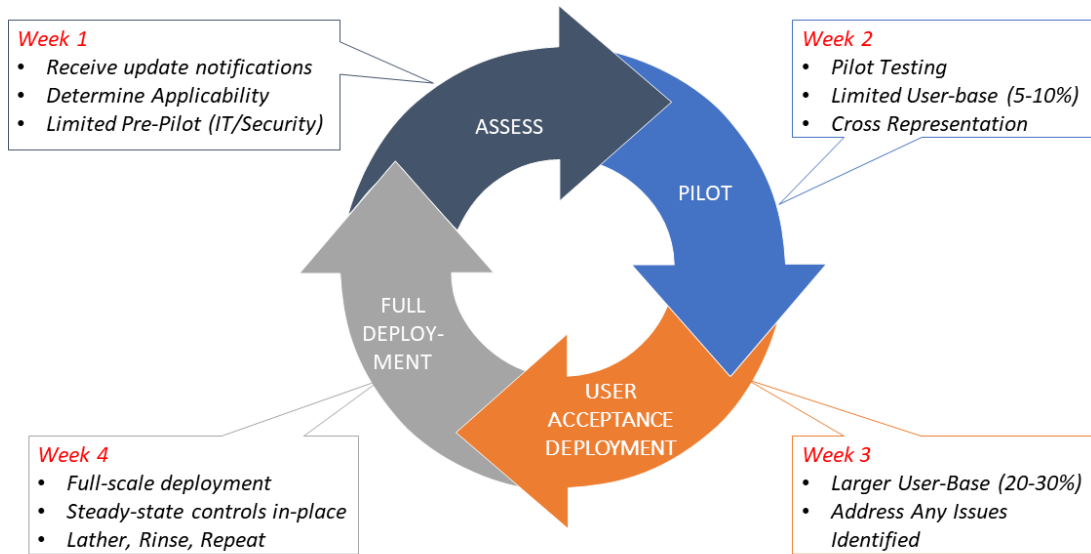


Figure 1 - Patch Release Cycle

As you can see from the figure above, by the time one can get through the deployment cycle of a month's batch of updates, the next month's worth is already upon them. It's a relentless onslaught and quite often a thankless task for the poor soul that is charged with it.

So, what is the solution for our poor SecOps engineer? An integrated solution that can help them with addressing the other 85% percent by utilising the existing investments the organization has made in their patch management framework.

Today, most corporations worldwide are using Microsoft's Windows Server Update Service component to be able to push out the products from Redmond. Windows Server Update Service (WSUS) is a capable solution but has its limitations. For SMBs, it's a perfect fit – just synchronise it with WindowsUpdate.com, approve your updates and let it go. Through group policy, the endpoints receive their updates and report back their patch compliance status. Done!

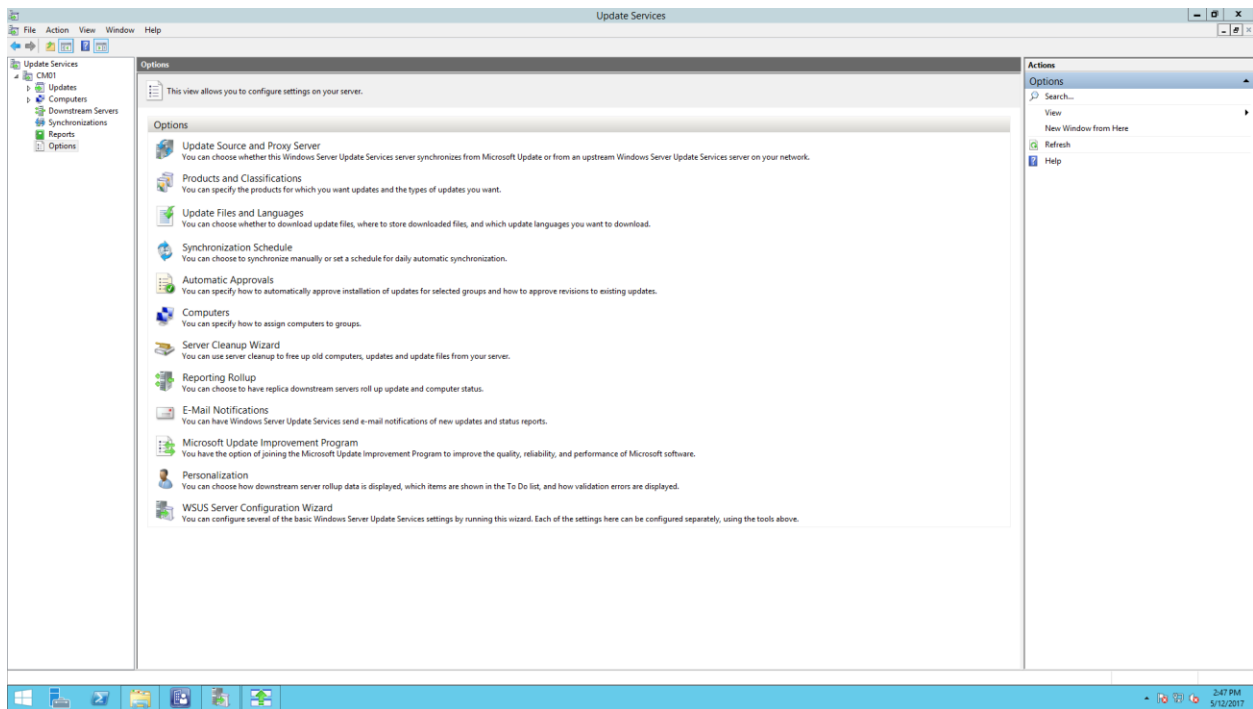


Figure 2 - Windows Server Update Services

For larger, more complex corporate environments requiring more granularity of control, time of deployments, network utilisation and better reporting, WSUS can be integrated into their System Center Configuration Manager (SCCM) product to extend and enhance WSUS. It will use all the existing infrastructure investments in SCCM to improve the scalability of WSUS, provide much more control over to whom and when patches are deployed and much more comprehensive reporting capabilities.

But, back to the point of our poor SecOps guy tasked with also updating Java, Adobe Reader, Chrome, Notepad++ and the like, how is he to integrate these third-party updates into WSUS or SCCM? Thankfully, Microsoft has provided an entry-level solution accelerator named [System Center Updates Publisher](#).

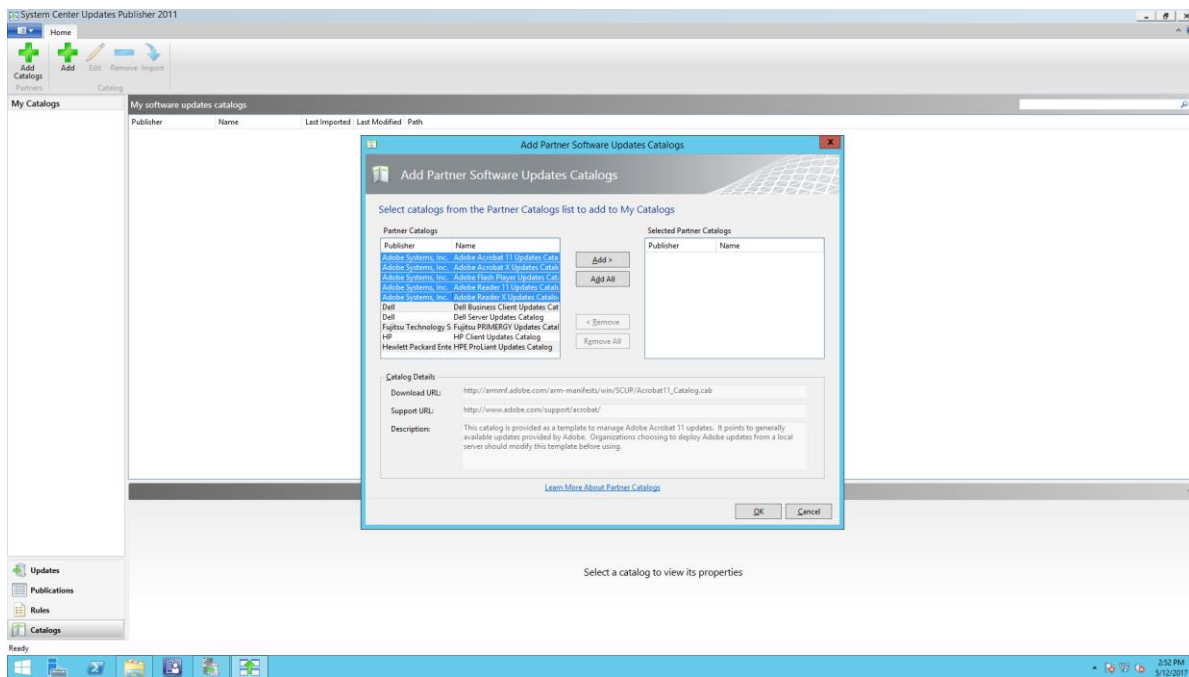


Figure 3 - System Center Updates Publisher

Despite its name, System Center Updates Publisher (SCUP), the product actually first synchronizes its catalogues from the third-party vendor's website into WSUS, and through WSUS' native functions, will then synchronize with SCCM. So, regardless of whether you have SCCM deployed or not, you're able to use SCUP to integrate the following vendor update catalogues into your WSUS/SCCM environment(s):

- Adobe Acrobat 11
- Adobe Acrobat X
- Adobe Flash Player
- Adobe Reader 11
- Adobe Reader X
- Dell Business Client Updates
- Dell Server Updates
- Fujitsu Technology Solutions
- HP Client Updates
- Hewlett Packard Enterprise

Now as you may have already noticed, the list of available products is pretty slim. The reality is that Microsoft hasn't really seen the independent software vendor (ISV) support that they had hoped to with SCUP. In fact, Adobe is the *only* ISV to get on board with it. The other three vendors are all hardware, providing firmware and driver updates.

So, how is one to go about fully addressing the problem at hand with the other 85%? That is a void Microsoft has intentionally left to the partner community to fill. Over the past several years a few key players have emerged to help organizations patch third-party applications by natively integrating into WSUS, SCCM or both.

What should an organization look for in a third-party patch management solution? The following table includes a list of items that I would include in any assessment or proof-of-value project for third-party patch management. I hope it will be of use to you during your evaluation process.

Table 1 - Patch Management Solution Selection Criteria

Third-Party Patching Solution Selection Criteria	Critical	Optional	Not Required
General Features			
The solution is dedicated and specialized for patching the 3 rd -party applications via Microsoft WSUS/SCCM.			
It is scalable and can grow with Microsoft WSUS/SCCM without restrictions.			
True plugin-based and seamlessly integrated into Microsoft SCCM environment without requiring additional software components or separate agents to be installed.			
Provides automation of recurring administrative tasks, including automatic import, download, publishing and synchronization of patch catalogs/contents.			
Leverages WSUS/SCCM deployment features (including interfaces, mechanisms, wizards, etc.) and doesn't change the administrator experience or require			

additional training.			
Also leverages WSUS/SCCM reporting engine and templates thus providing consistent compliance reporting across all content.			
The solution provides 'normalized' content where different content from various vendors as well as the native content provided by WSUS/SCCM itself are all treated in the same way, and don't require custom modification or scripting. This results in all content to be viewed, deployed and reported on in a consistent fashion.			
It covers patch content of the most vulnerable/targeted and most common 3 rd -party applications in corporate networks. This includes (but not limited to) content from Adobe, Apple, Citrix, Oracle, VMware, Google, Mozilla, etc.			
Provides enhanced content with powerful applicability detection rulesets.			
Includes enhanced security metadata with detailed description of content.			
Provides enhanced content with information about what updates are superseded by any particular package.			
The solution provides enhanced content with the vendor security identifier information (vendor convention of content bulletin IDs, labelling and serialization)			
Provides enhanced content with reference information about any industry-standard CVE metadata associated with any particular package (i.e. MITRE, NIST, etc.)			

It includes a user-friendly configuration wizard that helps administrators configure the solution as well as select the desired patch content.			
The solution provides flexible controls for synchronization scheduling.			
Provides the ability for automatic subscriptions on product level, where any new content for the selected product(s) is automatically retrieved once released by the vendor(s).			
Includes access to multiple versions of software update content (not only the latest version) for more convenience and meeting corporate/enterprise needs. This also avoids unintended version upgrades that can result in unwanted or negative outcomes.			
Incorporates alerting templates to notify on common events (including new updates availability, failed synchronization, license issues, etc.).			
Provides mechanisms for admins to subscribe to alerts so they will receive emails when a selected alert has been triggered.			
Retrieves the content in protected manner via secure and validated communication channels.			
The solution uses native role-based access controls and security scopes to define whom can push security updates to which systems.			
The solution can seamlessly integrate into Automatic Deployment Rules (ADRs) to enhance process automation as it relates to establishing a patch management framework.			

The solution can quickly and easily be utilized for creating security-centric configuration baselines for compliance reporting and alerting.			
--	--	--	--

Have I missed something? Let me know. I love hearing from my readers. Otherwise, happy patching! And, patching... and patching!

About the Author



Duncan McAlynn is an award-winning InfoSec professional with 20yrs experience consulting Fortune 500s on enterprise management & security posturing. He is a published author, editor, industry columnist public presenter and has obtained a number of certifications and awards over his 20yr career, including MS-MVP, MCITP, MCSE, Security+ & the coveted CISSP.

McAlynn is also an active member in his local ISSA, ISACA & InfraGard chapters. His community project is helping small business owners work through the challenges of cybersecurity. And, most recently, he has successfully completed a comprehensive Harvard University Cybersecurity Risk Management program.

He can be reached on Twitter using [@infosecwar](https://twitter.com/infosecwar) or by secure email with SudoMail at infosecwar@sudomail.com



**TRANSPORT
SECURITY &
SAFETY EXPO**
DETER / PROTECT / RESPOND

co-located with



Gold Sponsor
WATERFALL
Stronger Than Firewalls

Silver Sponsor
nccgroup

June 11-12, 2018
Hilton, Washington D.C.

SECURITY AND SAFETY FOR MASS TRANSPORT IN THE DIGITAL AGE

11%+
CAGR of the global
transport security
technology market
from 2017 to 2022*

*Source: GYReports



“Understanding how to better safeguard operations and protect critical networks and infrastructure from damage is paramount. Opportunities like TSSX that bring the industry together for training and solutions are welcomed by SANS.”

Doug Wylie, Director, Industrials & Infrastructure Portfolio, **SANS Institute**

Contact Tim Edwards, Event Director to see how you can get involved:

tim@transportsecurityworld.com
+44 (0) 207 045 0945

Please visit www.transportsecurityworld.com for more information.

produced by



**TRANSPORT
SECURITY
WORLD**
DETER / PROTECT / RESPOND

AHEAD OF THE 2018 US MIDTERMS, HOW CAN WE RESPOND TO FOREIGN VOTING INTERFERENCE?

By: Brent Whitfield, CEO at [DCG Technical Solutions Inc.](#)

Whether the attempts of foreign agents to affect the 2016 presidential election had a significant effect or not, many eyes have since been opened to the need to secure the integrity of our voting system.

With the mid-term elections rapidly approaching, this article looks at the current state of our cyber defenses and what work is left to do in the coming months to secure them.



WHAT DID THE 2016 ELECTIONS REVEAL?

The first inkling that voting interference was more than just a paranoid theory was in the summer prior to the 2016 elections when Democratic National Committee emails were leaked. Cybersecurity experts traced the cyber-attack to two Russian intelligence groups.

Donald Trump then went on to voice his concerns that the election would be rigged against him, claiming that lax voter ID processes would lead to repeat voting.

In the months leading up to the election, further reports revealed that voter databases had been probed with some being hacked. It has since been found that the databases kept by 41 States are outdated.

There is little evidence that actual hacking of the voting system itself has occurred. However, this is hardly surprising since a large number of voting machines do not have a parallel paper trail against which the results could be audited.

In the wake of Trump's election victory, evidence has emerged of more pervasive attacks targeting the hearts and minds of the US electorate. These include the spreading of disinformation (so-called 'fake news') and the buying of online ads by foreign bodies. These have been facilitated by social media platforms which enable individuals and interest groups to wield greater influence than ever before.

Research has revealed that foreign organizations spent \$100,000 on 3,000 ads and created 470 fake social media accounts during the presidential campaign. Russian bots and trolls have also been active in spreading the Nunes memo, a document exposing 'illegal' activity by the FBI in obtaining a FISA warrant against Trump adviser Carter Page in the Russian interference investigations.

HOW VULNERABLE IS THE VOTING SYSTEM?

To test just how vulnerable direct-recording electronic voting machines (DREs) could be, Princeton professor Andrew Appel bought a Sequoia machine online. It was an AVC Advantage model used in some jurisdictions of Louisiana, New Jersey, Pennsylvania and Virginia. Within seven minutes, Appel and a graduate helper, Alex Halderman, had broken into the casing and switched out the unsoldered circuit boards for modified versions.

This was just the latest of a string of hacks Appel and his Princeton colleagues had carried out on voting machines over more than a decade. They even managed to obtain keys for some of the machines via eBay and to turn one machine into a Pac-Man arcade game.

In addition to the technical vulnerabilities revealed by the Princeton hacks, there is an underlying constitutional weakness. This is because elections are regulated on a state-by-state basis and there are no overarching Federal bodies in charge of running them.

According to the president of voting transparency advocates Verified Voting, Pamela Smith, there are five states which operate digital only voting machines. These are Delaware, Georgia, Louisiana, New Jersey and South Carolina. A further ten use hybrid systems with voters in some parts of Arkansas, Florida, Indiana, Kansas, Kentucky, Mississippi, Pennsylvania, Tennessee, Texas and Virginia also relying on technology alone.

Of those States, three (Florida, Pennsylvania and Virginia) are considered perennial swing states. Two of these, of course, switched from blue to red in the 2016 election. Although there are no serious suggestions that fraudulent votes played much – if any – part in this, it does raise a red flag that can't just be ignored.

The voting machines are supplied by seven companies: Avante (who supply Warren County, New Jersey only); Danaher; Dominion Voting Systems (which acquired Premier, formerly Diebold, and Sequoia); Election Systems and Software; Hart InterCivic; MicroVote and Unilect.

ONLINE STRATEGIES FOR CYBER PROTECTION

It is clearly important for any solutions to include protecting the election infrastructure itself. Some national security experts have insisted that the top IT consultants/professionals available need to be brought in to secure registration systems, voting machines, tally systems and election night reporting systems while others have called for paperless DRE machines to be replaced completely and to ensure that a voter-marked paper record is always retained.

The voting machine vendors will have to play a key role themselves in rolling out more secure technology.

In order to fund the changes, the Democrats have introduced an Elections Security Act which would make \$1 billion of grants available for States to pay for paper-backed voting machines, hire security personnel and carry out proper risk assessments. The bill was referred to the subcommittee on Cybersecurity and Infrastructure Protection on 28th February 2018 but has no Republican co-sponsors.

OFFLINE STRATEGIES FOR CYBER PROTECTION

The Elections Security Act is just one piece of legislation that has been introduced as lawmakers seek to shore up our cyber defenses. Others include the Secure Elections Act, Paper Act, Honest Ads Act and DISCLOSE Act of 2017.

- The Secure Elections Act (introduced December 2017) proposes the elimination of paperless voting machines.
- The Paper Act (introduced September 2017) looks at developing best practices for States to use to protect the integrity of elections and to make grants available to implement this.
- The Honest Ads Act (introduced October 2017) proposes extending transparency over ad purchasers and content to the online space.
- The DISCLOSE Act of 2017 (introduced July 2017) seeks to put further restrictions on foreign-owned companies to prevent them funding political movements.

None of these bills have yet made it to the Houses and each have a poor enactment prognosis.

The indictment of 13 Russian agents in February 2018 is another attempt by the government to disrupt and call out electoral interference although some have called for tougher sanctions against Russia itself.

Aside from these legal and political actions, some national security experts have called for both parties to dilute the impact of fake news by educating the American public in how to recognize it and stop its spread.

Whatever measures will see the light of day in the next few months, it seems clear that only a two-pronged, multi-agency Cybersecurity offensive can plug the holes in our voting system and restore trust in the democratic system that forms the foundation of the United States.

About the Author

Brent Whitfield is CEO of [DCG Technical Solutions Inc.](https://www.dcgla.com) DCG provide a range of IT consulting and related IT services including cyber security, security assessments, breach prevention, security training, internet content filtering, disaster recovery and dark web monitoring. Brent has been featured in Fast Company, CNBC, Network Computing, Reuters, and Yahoo Business. <https://www.dcgla.com> was recognized among the Top 10 Fastest Growing MSPs in North America by MSP mentor. Twitter: [@DCGCloud](https://twitter.com/DCGCloud)



COMEX 2018
HIGHLIGHTS

WWW.COMEX.OM

FOCUS INDUSTRIES

 MANUFACTURING	 TRANSPORT & LOGISTICS	 HEALTHCARE
 EDUCATION	 OIL & GAS	 TOURISM

FEATURED ZONES

- | | | |
|---------------|--------------------|---------------------|
| • AR/VR | • Digital Learning | • Cloud & Big Data |
| • IoT | • Digital Commerce | • Digital Health |
| • 3D Printing | • Cybersecurity | • Digital Marketing |
| • Robotics | • Smart Homes | • SMEs & Start-ups |

-  Network with C-Level tech executives at **TECH EXECS VIP CLUB**

-  Focus on 'Internet of Things' and 'Artificial Intelligence' at **TECH SMART CONFERENCE**

-  Knowledge-sharing seminars & demos at **TECH TALKS WORKSHOPS**

-  Smart Homes & Tech Wars at **COMEX SHOPPER**

-  Pre-registered meetings at **COMEX MATCHMAKING ZONE**


**BOOK
YOUR SPACE
TODAY!**

Organiser



Ashit I Barnes - Exhibitions Director
☎ +968 9934 1687 ✉ barnes@oite.com

Ahmed Farag - Sales Manager
☎ +968 9411 3434 ✉ a.farag@oite.com

Supporting
Associations



Media Partners



ATTACKERS ON RAMPAGE

LACK OF KNOWLEDGE CAN COST YOU ALOT

by Charles Chipiliro Chioko, IT Security Compliance Officer, NICO Technologies Limited

Gone are the days where people gets worried about viruses which can just cause disruption to services or denial of services to different systems. Attackers have now taken a step further stealing information and data with an aim of getting money. Recently we heard about different types of Malware which hit many companies across the globe. A lot of companies have paid to money in form of bitcoin to get back their encrypted data to continue with their businesses. Right now, bitcoin is now a currency which companies or organizations have known apart from the usual known currency we know (dollar, Euro, etc.) Companies and organizations are now busy looking for ways on how they can secure their data and information. Some companies and organizations have migrated their data to the cloud and some have increased their Security by upgrading their Security infrastructure. Although this can be done nothing can be 100% secure, it doesn't mean migrating data to the cloud its safer than keeping it on your own, attackers nowadays are also targeting those Companies which are providing Cloud based Storage Services.

It should be noted that there is no "one size fit for all solution" in order to protect company or organization data. Its high time now for Company owners or Organization owners to realize that protecting Information and data is expensive, they should be willing to pay more to protect their data or information. A lot of Company managers or decision makers think that just having Computers with Antiviruses installed on them is safe to run their business but this is totally wrong.

This lack of knowledge from top level management is the one which can cost the company to lose valuable data if no proper decisions are made. As I have already said there is no "one size fit for all solution" in order to protect company data, there are several things which top level management needs to do to protect their data. Apart from the usual password management, software updates and patches, access control, installation of anti-virus software and updating of operating system, the following can also be added to the list of the actions which organizations can take to reduce the probability of being victims of attack.

Management buy in: Top level management should understand that having their data and information or their infrastructure on internet is risky, as such they should be willing to spend or invest on IT infrastructure, User training and IT processes. They should also have a proper risk management system in place to manage the risks which might come along the way.

IT Security Awareness training: Everyone including the top-level management should be trained on IT Security issues as they can also become victims of different attacks due to lack of knowledge on how to perform their day to day duties on internet. These awareness trainings should be done frequently and should be mandatory to all the users including top-level management.

Security Operating Center (SOC): with the current attack trend, Companies or organizations needs to build their own Security Operating Center, this will help IT Security analyst monitor the network, detect intrusion and manage threats as they occur. Security Operating centers will have an added advantage to the organizations as they will be exposed to various tools which can be used in monitoring and preventing threats.

Frequent Vulnerability Assessments: Security has passed the stage of having an Anti-virus installed nowadays, there is a need to perform frequent vulnerability network or systems assessments, this will help the IT team to identify weaknesses in their systems which can be exploited if not well managed.

New Infrastructure: It is better for organizations or companies to purchase very high performance, intelligent devices than having a lot of old or out dated devices like switches or routers. CISCO provides a wide range of intelligent devices which can be used to monitor the network, detect for intrusion and prevent malware into the system.

Effective Backup Policies: There is a need for organizations and companies to adopt strong backup policies and procedures, backups need to be tested frequently and check for inconsistencies. Dry run tests need also to be done to simulate an event of data recovery should a catastrophic event or an attack take place. Companies need to have Disaster recover sites which should be 24/7 operational and should be secured and monitored always and data or information kept on these sites need to be tested for integrity.

Encryption: Much as encryption will not prevent data or infrastructure from being lost or stolen, Companies need to make sure that their data is encrypted to prevent data being manipulated or changed in any way, all the medium which can be used to transfer data

from one point to another need also to be encrypted. This ensures integrity should a device is lost or stolen, e.g. an external hard drive, a laptop, a tablet etc.

In conclusion, as attackers are advancing in the way how they are exploiting vulnerabilities, Companies need to wake up and try all the best to combine a number of mitigation techniques to prevent being victims of attacks, as I quote a statement by Robert Mueller, FBI director in 2012 and I quote “There are only two types of companies: those that have been hacked and those that will be.”

About the Author



Charles Chipiliro Chioko is an IT Security Compliance Officer at NICO Technologies Limited. He is a Certified Cisco CCNA Cyber Ops Security Analyst and a Microsoft Certified Professional He has worked in the IT industry for more than 12 years. He is focused on Cyber Security and Network Security. He has worked for a couple of IT Companies which exposed him to different types of Systems. He is experienced in Network Security, Database Management, Systems Administration and Systems design. He started his career in 2005 when he was doing Management Information Systems then later pursued with a BSc Degree in Information Technology. For more information visit <https://www.nicottechnologies.com/>

CYBER RESILIENCE & INFO SECURITY **CRIS 3.0** CONFERENCE

11 & 12 APRIL 2018
8:00AM - 5:45PM
SETIA CITY CONVENTION CENTRE
SHAH ALAM



SECURING YOUR IOT IN INDUSTRIAL REVOLUTION 4.0

Join us in this seminar filled with security experts that will help you secure your organisation

WHAT YOU WILL GAIN FROM THIS SEMINAR?

Inspiring thought leader

Connects together with the best and brightest speakers in CyberSecurity, Cloud Computing, IoT and Big Data

Security challenges ahead of industry 4.0

Preparing for industrial revolution 4.0, by exploring current security challenges and trends in the era of digitalization..

Real-life hack demo

Witness real-life hack demo of how hacking works and explore solutions to protect your organization from cyber breaches.

Real-life case study

Learn first-hand from CyberSecurity experts and IT C-levels of large corporations regarding cyber breaches

Incredible networking

Spend time connecting with ICT peers, our sponsors, partners and friends and share applicable knowledge.

Post-event session

Interactive, personalized follow-up sessions for selected participants after the completion of the first series, where CRIS 3.0 speakers will conduct a catch-up for recent updates of the industry.

COME AND LEARN FROM THESE INDUSTRY EXPERT



WONG WING KEONG
Wired Realm
Sdn Bhd



SAURABH SARAWAT
Across Verticals



FAISAL YAHYA
Bina Nusantara University



FONG CHOONG FOOK
LE Global Services
Sdn Bhd



PREETHKARAN J
KPMG in Malaysia



RODNEY LEE
DNex Technology
Sdn Bhd



A.J. MINAI
Tomorrow Academy
Sdn. Bhd.



DR. MOHAMMAD SHAHIR MAJED
Ernst & Young Advisory
Services Sdn. Bhd.



PETER LEONG
Kenanga Investment
Bank



MELVIN FOONG MUN HOE
Titan System Integration
Sdn. Bhd.



LEE HAN THER
REA Group ASIA



SYAHRIL AZIZ
Mycrypto Sdn Bhd



Alan Yau
Sysarmy Sdn. Bhd



Raj Kumar Kunhiraman
Cyber Intelligence Sdn Bhd

SECURE THE CYBER SPHERE OF YOUR ORGANISATION NOW!
newhorizons.my/events/cris2018

CALL US:
603-2287 1829

EMAIL US: cris@newhorizons.my
benjamin@peoplelogy.com



COMPUTER BUG HISTORY – NOTABLE PESTS FROM THE LAST 30 YEARS

by James Smith, Bugsnag CEO

Over the last three months, the media including Cyber Defense Magazine has reported what seems to be one computer bug after another, including the Meltdown and Spectre Intel CPU bug, the Apple 'chaiOS' bug that crashes the Messages app, crypto-currency mining infections, and the latest uTorrent bug that lets websites control computers to steal information.

Let's face it. The technology we rely on for business and pleasure today has bugs. While overall code quality has improved, with better programming practices and automated quality assurance testing, there is so much more software now than there was even five years ago that it is almost inevitable that some bugs will make it out of development into production.

Those with the biggest impact will inevitably grab headlines, but many of us are responsible for applications that are critical for our organizations and customers, and we are not immune to this trend. So it is important for every software professional to ensure that robust systems are in place to catch bugs in development as well as in production.

Over the last several decades, computer bugs have been responsible for major data breaches, privacy issues, and crashed rockets and trains. One class of bugs with security holes that malware exploited led to the explosion of "bug bounties." Last year, just one company, Google, offered to pay \$1 million to external researchers to find security bugs within their code.

But just as important are bugs that cause software to behave in unexpected ways, or to crash altogether. These bugs can slip through QA tests, especially when they involve new devices, interactions between humans and the software, or unintended usage that has not been tested for.

As a reminder of just how far-reaching these threats are, let's take a step back and remember how long computer bugs have been an issue and take note of some of the major havoc they've caused.

Many people don't remember that the first recorded computer "bug" was an actual moth discovered in 1943 by Grace Hopper stuck in between the relays of the Harvard Mark II computer. Her notes of the encounter involved the very first use of the term "debugging" in relation to computers.

Since then, software bugs have been a fact of life. Here are four of the most notorious and costly bugs of the last 40 years in terms of money and lives.

Therac-25 causes radiation overdoses

One of the most tragic software bug stories involves the Therac-25, a machine meant to deliver radiation therapy to cancer patients. In 1985, concurrent programming errors caused the machine to mistakenly deliver an overdose of radiation hundreds of times greater than normal, killing three patients and causing debilitating injuries to at least three others.

The previous model of this device had both hardware and software controls to ensure the correct dose of radiation, but the Therac-25 model removed the hardware controls under the false assumption that the software controls were sufficient. It turns out there was an error in the software controls that when combined with human interaction could lead to a deadly overdose. The new device was never fully tested with the software-only controls. The only indication that something was wrong was an ambiguous error code that did not state the severity of the error and did not block the operator from continuing to administer a fatal dose.

A 64-bit software bug squeezes into a 16-bit processor to crash the first Ariane 5 rocket

To the horror of onlookers and European Space Agency employees, a software bug caused the first Ariane 5 rocket to flip 90 degrees and explode shortly after liftoff on June 4th, 1996. The ESA used the Ariane 5 to deliver payloads in space for low Earth orbits. The cost of the crash exceeded \$370 million.

The fault was identified as a software bug in the rocket's Inertial Reference System used to determine whether it was pointing up or down based on a 16-bit integer. Again, this software was a holdover from the previous generation rocket, which reported velocities using a 16 bit integer. The new Ariane 5 was faster and more sensitive, and used a 64 bit floating point value for its velocity reports. This mismatch between the two systems proved to be disastrous.

For the first few seconds of flight, the rocket's acceleration was low, so the conversion between these two values was successful. However, as the rocket's velocity increased, the 64-bit variable exceeded the capacity of the 16 bit integer in the IRS software. Suddenly, the rocket thought it was pointed in the wrong direction, and the software overcorrected, essentially flipping the rocket in mid flight leading to failure.

Mars Climate Orbiter burns up in space

On Sept. 23, 1999, NASA lost its \$235 million Mars climate orbiter spacecraft because of two software teams using two different units of measurement, imperial units of pounds-seconds, and metric units of newton-seconds. In an unfortunate fluke, at distances close to the earth, the units looked nearly identical numerically, and the differences were not caught in pre-flight testing.

Larger deviations as the mission progressed were attributed to solar wind or dust particles affecting the orbiter speed, which were expected and manually corrected. But by the time the orbiter approached Mars, the accumulated error was too much, and the time lag between Mars and Earth left no time for corrections when things started to go wrong. The incorrect calculation of the spacecraft's trajectory led it to burn up in the Martian atmosphere.

This story is a good reminder to make sure software teams are working closely, to test the full range of anticipated conditions before releasing, and to not make assumptions about the source of errors before correcting them.

Knight Capital Loses \$460 million in 45 minutes

On Aug. 1, 2012, Knight Capital deployed a new software update to its production server. What they did not notice is that someone had accidentally reactivated in the production software defunct internal testing subroutine that was last used in 2003. This subroutine was designed to stress test the software for trade volume, generating a high number of trades without regard to whether they were good trades or not.

Just 45 minutes into trading that day, the misconfigured, outdated program generated more than 4 million faulty trades resulting in losses. This was compounded by other trading systems detecting these seemingly bizarre trades and amplifying them for their own gain. Ultimately, these 45 faulty minutes cost the financial firm more than \$460 million on behalf of one of its retail investors and later resulted in an SEC fine of \$12 million.

An SEC report later determined the problem was based on a lack of formal code reviews and quality assurance processes that might have identified and removed the dead code that produced the error.

History has shown that computer bugs can come in a variety of forms – from the outside by cyber criminals or from the inside due to lack of oversight and inadequate programming processes, bad assumptions and human error.

Robust quality assurance systems and automated testing tools can help reduce errors released to production. Bug bounty programs, both external and internal, can be helpful in identifying security bugs and performance issues in production as can the judicious use of ethical hackers. Tools such as APM and logging can help identify performance issues in production that are caused by infrastructure issues or by software inefficiencies. And production error monitoring tools can capture live errors from production for analysis, prioritization, and resolution long before trouble tickets and support calls identify such issues.

With these systems in place, organizations can be proactive about security, performance and stability of their applications and instill a culture of quality and end-to-end ownership of the application. At the end of the day, it all comes down to prevention and early detection.

KEEP HACKERS FROM BOARDING YOUR NETWORK WITH A CYBER NO-FLY LIST

By Hugh Njemanze, CEO, Anomali

According to a recent report from the [Online Trust Alliance](#), 2017 marked another “worst year ever” for cyberattacks. Businesses across every sector experienced nearly twice the amount of attacks over the previous 12 months, with major breaches hitting sectors like healthcare, heavy industry and even election and government security. At least one [research report](#) estimates that the cost associated with attacks will total more than \$6 trillion by 2021.

With digital transformation well underway across numerous industries, more data than ever before is headed from behind company firewalls and into the cloud. Data that most people couldn't imagine sharing even five years ago – credit card numbers, banking information, social security numbers, medical records, confidential documents – are being transacted over the Internet. The lucrative nature of cybercrime and availability of tools and data continue to lure new criminals to the cyber world. Security leaders are under more pressure than ever to ensure that they have a constant view into their networks to identify when and how these bad actors strike. Breach reporting requirements make this challenge even greater. This is an immensely difficult task.

One way companies can better contend with cyber threats in their networks is to build a dynamic, thorough threat intelligence framework from which they can cast a larger cyber security net. In taking a page from the government's anti-terrorism playbook, we call this the Cyber No-Fly list.

The No-Fly List

One of the government's better known anti-terrorism tools, the “No-Fly List,” is a list maintained by the FBI's Terrorist Screening Center. The No-Fly List identifies individuals who are deemed too much of a national security risk to be allowed to fly. The list pulls information from several different databases to identify bad actors, their associates, backgrounds and the risk level they bring. Although the No-Fly List is only one tactic the US uses it in the fight against terrorism, since its inception, there have been no successful aircraft-focused attacks on U.S. soil. The FBI even asserted that the watch list “...is one of the most effective counterterrorism tools for the U.S. government.” The effectiveness of the No-Fly List on physical security makes this

intelligence-based approach to defense worthy of consideration by all organizations that are regularly targeted by cyber threats.

As rates of cybercrime and cyber terrorism continue to rise, it only makes sense for enterprises to implement a similar system – one that identifies bad actors and their IP addresses, malware signatures and tell-tale techniques, and then flags when they try to penetrate a network. The TSA's machines, checkpoints and rules work to a similar end as the tools enterprises use to detect and keep out threats, like network monitoring tools, firewalls and endpoint management systems.

The Cyber No-Fly List

Establishing a Cyber No-Fly List is no easy feat. Enterprises currently enforce checkpoints and controls to reduce the odds of being compromised, but, like any rules, they can be circumvented by a crafty interloper. To really crack down on malicious traffic, enterprises must catch threats before they even enter their systems. To do this, cyber security professionals need to draw from massive quantities of threat data, and more importantly, threat intelligence.

At the root of the Cyber No-Fly list is data sourced from a variety of different data feeds and arriving in disparate formats. To even begin looking for threat indicators, a company must have the infrastructure to collect, cleanse and normalize the data. This is where automation can help. Given the shortage of trained cyber security professionals and the exponential increase in threats, software solutions can help optimize and integrate this data into threat intelligence – the deep context that security leaders can use to make decisions.

This threat intelligence is what drives the Cyber No-Fly list. In a typical business day, a large enterprise will easily record over 1 billion network and system events, all of which need to be checked against the list of threat indicators. Putting a Cyber No-Fly List to work means analyzing all that digital traffic in close to real-time and determining who to keep out — a major undertaking, even with today's computing power.

Real-Time Updates

Perhaps even more important than establishing the list itself are updates to the list, i.e. the newly discovered cyber threats. Every day researchers identify thousands of new malicious cyber indicators. It's not enough to just start looking out for these new bad actors. As soon as new threat data is available, organizations need to know if their networks have already been infected.

This means looking over months or even years of historical traffic to identify breaches. To draw on the analogy of the actual No-Fly list, this would be like identifying a new terrorist and then diving into their entire life's worth of travel records, identifying whether they have already entered the country, where they went and how they got there. Unlike humans, cyber actors can quickly and easily change "fingerprints" – using different IP addresses, domains, malware, etc. More sophisticated actors will even monitor public threat lists as well to find out if they've been detected.

It Works

Because all companies have unique characteristics and threat landscapes, there is no definitive or "master" cyber No-Fly List. However, for those companies who take the time to cultivate and maintain a list, it works.

A recent study of 1,000 cyber security experts found 80% utilize threat intelligence in their daily security operations. Recent events like the WannaCry and Petya attacks demonstrate the need for rapid intelligence. Within hours of the Petya outbreak, subscribers to threat intelligence providers began receiving specific, actionable threat indicators – the fingerprints of the attacker – so they could put in place safeguards like firewall blocking rules and network monitoring alerts.

The Cyber No-Fly List approach leverages one of the most effective tools in warfare — intelligence. The Cyber No-Fly list allows companies to proactively keep tabs on their potential and current foes, ensuring that they never get through the gates in the first place.

GLOBAL CYBER SECURITY IN HEALTHCARE & PHARMA SUMMIT 2018



The Global Cyber Security in Healthcare & Pharma Summit 2018 will bring together high-level representatives from around the globe to create a cyber security roadmap for the future.

Over two days, the congress will cover topics in healthcare, medical devices and pharmaceuticals.

To book your place visit:

www.global-engage.com/event/cyber-security-summit/#register

SPEAKERS INCLUDE:



JIM JACOBSON
Chief Product and Solution
Security Officer, Siemens
Healthineers, USA



DENISE ANDERSON
President, National Health
Information Sharing and Analysis
Center (NH-ISAC), USA



JASON MEDEIROS
Senior Vice President, Hosting,
American Well, USA



**ATHANASIOS
DROUGKAS**
Officer in Network and
Information Security, European
Union Agency for Network and
Information Security, Greece

TOP 5 WAYS TO COMBAT INSIDER THREAT

by Dr. Eric Cole

I've been talking about insider threat for nearly 10 years and advocating the position that compromising an insider is a lot easier for an adversary than breaking into an organization from the outside. A [study](#) that I recently authored for SANS Institute (co-sponsored by Dtex Systems, Haystax Technology and Rapid7) illustrates that attention to the problem of insider threat is still well below where it needs to be.

In particular, while 40% of survey respondents rate insider threat as the most damaging threat vector they face, nearly the same percentage (38%) say they don't have an effective way to detect insider threat, and fewer than 20% don't have a response plan in place to mitigate damage from an insider incident.

Yet, there are some relatively easy ways to protect the organization from both the malicious insider and the unintentional insider. Here are my top five:

- 1) Control or eliminate email attachments and links – emails are the primary attack vectors in use today, and while the message itself isn't dangerous, links and attachments are. Today's security product vendors are offering real-time malware assessment of links and attachments that will quarantine a suspicious attachment or prevent connection to a dangerous link.
- 2) Properly manage and control access to data and critical systems – role-based permission and the principle of least privilege are your friends. Work with your HR team and line of business managers to understand user roles and the types of application and data access they need to do their jobs. Then, assign only that access level, no more.
- 3) Know where your data is – an important corollary to point 2 is knowing where mission-critical and sensitive data resides in the system so that you can lock it down with appropriate permissions. If you don't know where it is, how can you protect it with the right level of access?

- 4) Monitor employee behavior and look for anomalies – this can occur at many levels, including action monitoring software. It's not intrusive to look for excessive data dumps or repeated attempts to look at files or directories that are not permitted – it's good business. But it also makes sense to educate employees to be on the lookout for behavioral changes in their coworkers – what are the signs of financial or emotional distress that could lead to an attack on company systems...or worse.
- 5) Raise security awareness – last but not least is the need for ongoing security awareness training that is an integral part of company culture – not an afterthought or a “checklist” item. A company that partners with employees to ensure security awareness will do better than one that forces compliance or just performs training to check a box.

Finally, getting back to the survey, I'll leave you with this important point.

It is easy, while evaluating attack vectors, researching competitors and gauging the threat from organized crime or foreign adversaries, to conclude that external attacks should be the primary focus of defense. This conclusion would be wrong. The critical element is not the source of a threat, but its potential for damage. Evaluating threats from that perspective, it becomes obvious that although most attacks might come from outside the organization, the most serious damage is done with help from the inside.

Dr. Eric Cole is CEO of Secure Anchor, former CTO of McAfee and Lockheed Martin, member of the Commission on Cyber Security for President Obama, the security advisor for Bill Gates and his family, and author of a new book, [Online Danger: How to Protect Yourself and Your Loved Ones From the Evil Side of the Internet](#). For more information, please visit, www.onlinedanger.com and connect with Dr. Cole on Twitter, [@drericcole](#).



CONFERENCE
2nd – 3rd
MARCH

2018

TRAINING
27th Feb' - 1st
MARCH

NULLCON INTERNATIONAL SECURITY CONFERENCE GOA 2018

TALKS HIGHLIGHTS:

Haroon Meer (Keynote)

The founder of Thinkst, the company behind the Thinkst Canary

Rajeev Chandrasekhar

Member of Parliament, Rajya Sabha

Eva Galperin

Director of cybersecurity, Electronic Frontier Foundation (EFF)

Leonid Evdokimov

Developer at OONI and TOR Project

IN ADDITION:

- 13 Security Trainings
- Workshops & Villages
- CXO Panels
- Exhibition Area
- Job Fair
- on-the-spot CTF challenges
- BlackShield Awards
- HackerHoly Party

VENUE

HOLIDAY INN RESORT, GOA

FOR MORE INFORMATION : INFO@NULLCON.NET

WWW.NULLCON.NET

Cybersecurity expert Will LaSala, director of security solutions for [VASCO](#), recaps five of the hottest trends of 2017, and takes a look ahead to what we can expect in the coming year

The Internet of Things (IoT)

By far the top technology trend of 2017 was the continued adoption of IoT. Thus, IoT security will receive more attention in 2018 as the number of IoT devices increases. Should these devices be compromised, it will take some time for the security patches to be developed and installed, because consumers likely aren't thinking or worried about the security of their in-home devices like smart appliances and televisions. The recent [KRACK](#) attack has affected many wireless access points in consumer's homes and there is a danger that the same will happen with IoT. To mitigate the KRACK attack, the consumer needs to go to the website of the manufacturer of the access point, download software and install it on their router.

The number of IoT devices will only increase and, given their known vulnerabilities and the fact that the Reaper botnet alone has harnessed more than a million devices, we will most likely see more large scale Distributed Denial of Service (DDoS) and Destruction of Service (DEoS) attacks. If we look at the trend from recent attacks, we went from Wanna Cry to NotPetya, we saw motivation shifting from getting money to destroying systems. Malware will also be more mischievous as it looks to see what it can destroy and break the ability to restore by looking up an organization or consumers' backup capabilities and erasing data.

There will be an increase of random hacks and attacks because the tools are easy to find and use, as well because of all the unsecured IoT devices – [Gartner](#) says there are 8 billion connected things in 2017 and expects 20 billion connected devices by 2020. Anyone can go onto the dark web and start using available malware code, not to mention the hacking, malware- and ransomware-as-a-service that can all be hired for next to nothing. It's very easy these days from someone with little knowledge to launch a sophisticated attack and there's incentive – in the last three years business email compromise alone made \$5.3 billion.

We will also start to see a shift in IoT technology as it relates to identification. For example, cameras or detectors in a room are able to identify a person with a lot of parameters, the technology is making the identification that consists of a low level of energy use, capturing all the data points from your devices and your signals. IoT is there to build intelligence around your virtual identity and that's why IoT devices will be more important as data collectors rather than as intelligent devices.

The need for stronger encryption will become more important because of the communication between IoT devices, humans and the cloud. The more data we have in the cloud, the more secure it has to be. We are currently researching biometric fusion algorithms and the impact it has on encryption. For example, with biometric authentication (face, fingerprint, voice and behavior) using each as an independent authentication option creates a false positive rate, however if you combined any of these methods, there's a decrease in false positives and through machine learning, you can create an almost eliminate the amount of false algorithms.

Machine Learning and Artificial Intelligence (ML/AI)

In the next five years, different levels of AI will emerge along with some clear leaders. Those leaders will provide incredibly advanced AI solutions, likely as a service, and become the next Google and Apple.

AI will emerge as a usable capability to mitigate fraud for online and mobile, and will become a major focus area for banks. Machine learning will also become fruitful and the capabilities held now only by larger providers will become more widespread.

We've entered the age of artificial intelligence, machine learning and robotics, and use the data collected to gain insight, secure applications and channels. But if we have the technology, then so do fraudsters. That's why in 2018, we will see more malicious software with AI capabilities, more automated attacks and more intelligent (spear) phishing campaigns. With the help of machine learning, fraudsters will be able to scan the web in an automated way, requiring little or no human intervention, and requiring fewer resources to create more devastating attacks.

Mobile App Security

One of the biggest threats against mobile were overlay attacks, especially in the U.S. and Europe. In the past, these attacks were only spotted in Russia, but we've seen the first examples in Europe and the U.S. and we expect there will be more next year. These overlay attacks are a type of malware that also takes advantage of the user, who has to enter his credentials into the overlay window. The combination of malware detection and Runtime-Application Self Protection is the strongest way to protect mobile applications today.

In 2018, mobile platforms will be the biggest attack platform. We will still see attacks on browsers for online banking, this will not go away. What we will see is an increase in mobile banking attacks next year—because more and more banks are providing mobile banking apps, and there is a shift by the users themselves from PC online banking to mobile banking. Additionally, more than 50 percent of banking transactions are taking place on a mobile device in the EU. One major reason why the U.S. often lags so far behind in mobile banking usage is because many banks have been so preoccupied with meeting new compliance obligations and rebuilding their reputations.

The recent news of the WiFi WPA vulnerability and the potential for attacks is greatest on the fractured versioning system of the Android device space. Along with this attack, the rise in social engineering with mobile application repackaging and app distribution is on the verge of explosion. Combine these monster holes with where the mobile app industry is headed, businesses should be aware and take extra precautions next year to secure their mobile offerings.

Banks will continue to push into the mobile space and bring new services to the channel as social engineering attacks increase and hackers work to find ways to exploit the new mobile services. With the recent news of ATM malware being sold on the black market, I believe we could see bigger retail attacks in 2018, while corporate attacks will continue to rise as they have been previously. Point of Sale and payment-related attacks in the U.S. where the broken Chip and PIN systems are rolled out, will lead to easy attacks on which social engineers will prey. Corporate banking and core banking will continue to see advanced persistent threats, and hackers that are well-funded and well-organized.

We'll continue to see a rise in Synthetic Identity fraud which is costing businesses a fortune in losses. Cybercrime networks are making it really easy to get the information and assemble it to build a realistic identity. Javelin Strategy & Research estimates new account fraud, with many accounts being synthetic, will soar 44% between 2014 and 2018, rising from \$5 billion in annual losses to a projected \$8 billion.

GDPR

Companies are going to pull out of Europe rather than deal with the cost and hassle of GDPR compliance. For non-European companies, as soon as you host or process any data about EU residents, you're subject to a lot of legal obligations with how you process data, what you do with it, where it gets stored, and the level of transparency you give to individuals whose data you are gathering.

This is the biggest piece of privacy legislation in the last 20 years and it requires organizations to reengineer how they process information and how they work. Given the compliance date is less than a year away, this one will be a struggle for many organizations.

Banking/Fraud

The banking world is facing increasingly intricate fraud schemes. Each year statistics show that instances of online fraud are rising, while customers are placed at risk from new attack scenarios on a near daily basis. As a result, banks will deploy more sophisticated solutions that combine risk analysis with machine learning, authentication, mobile security and orchestration to dynamically and in real time, apply the proper level of security for each unique transaction based on a risk score. Banks will also demand

that these solutions provide simple integrations with a variety of fraud tools/platforms to ensure future requirements are easily incorporated.

2018 will be an exciting time as we will see new defenses and technologies paving the way to mitigate fraud and risk. Two years ago, we were all excited because Bank of America set no limit on security spending in an effort to thwart cyber criminals. However, [research](#) is finding banks are still falling further behind as they try to keep pace with today's fraud schemes. If banks are already moving as quickly as they can on security issues but can't keep up with fraudsters, then it's time to turn to new solutions based on AI and machine learning that speed up the ability to detect fraud, enabling banks to not only keep up but get ahead on reducing the losses to fraud and defending against attacks.

2018 will be the year of zero login. You will just click and open, everything will happen in the background. AI will also emerge as a usable capability to mitigate fraud for online and mobile, and will become a major focus area for banks.

YOU HAVE TRIED THE REST. TRY THE BEST!  

PC



www.trymyantivirus.com

SECURITY AWARENESS TRAINING (VERSION 4.9)

Inspired eLearning offers a complete security awareness training solution designed to build and maintain a security conscious culture over the long term. Our solution is more than just a group of courses, it's a complete awareness platform that includes professional services and support. We offer continuous reinforcement of the learnings through phishing campaigns, short burst videos and supplemental materials such as digital signage and posters.

Our PhishProof Simulated Attack Solution allows you to immediately identify weak spots in your employee base and gives users training when it is most effective — the moment they click. As the only provider in the industry with a mobile application, employees can train on their schedule by simply downloading the courses and training whether they are on the road, on a plane, or away from the desk. Combining these capabilities with our business analytics, you can analyze the results at all steps along the process, and communicate to the learners about new threats, relevant safety steps and best practices. Our goal is to help leaders take control of their security, empower their employees to identify threats, and transform the organization into one that is safe and protected from external threats.

Our team of experienced instructional designers leverage well-established learning methodologies to plan and build out our content to be instructionally sound. We use a combination of positive and conversational script which respects the user's intelligence and doesn't make light of information security. We utilize adult learning theory, high quality production, and engaging interactivities to not only focus the attention of the user but push information retention.

Each of our courses are updated regularly to reflect the current threat landscape and security trends. Our cybersecurity subject matter experts keep an ear to the ground on just what issues and concerns are top of mind with CISOs and organizations. They regularly review our course material and our instructional designers make sure that the information is clear and easily understood by the typical employee. We always strive to have a conversation with the user in a relatable tone, as opposed to just dictating the information to them.

Security Awareness - A Day in the Life

<https://upload.inspiredelearning.com/PM/MDC/John/s-173/demo/index-video.htm?lang=en&mode=1>

Information Security for Executives

<https://upload.inspiredelearning.com/john/Course.Development/Awards/S-114/v16.1.0/index-video.htm?lang=en&mode=1>

Internet of Things “IoT” and Home Security

<https://upload.inspiredelearning.com/john/Course.Development/Awards/S-161-HS/v15.0.8/index-video.htm?lang=en&mode=1>

Business Email Compromise (BEC)

https://upload.inspiredelearning.com/PM/MDC/Courses/Documents/Videos/BEC/BEC_Microvid_VO_FINAL_LOW2017.mp4

by Stewart Kantor, CEO and co-founder of Full Spectrum Inc.

Interconnectivity has become a norm in today's society, with everything from your smartphone to your increasingly automated home and vehicle. Experts predict that there will be 50 billion connected devices by 2020 and with this ever-growing expansion, the Internet of Things (IoT) is progressively making its way into the industrial sector. But, as the classic Spider-Man quote goes, "With great power comes great responsibility" and this is especially true with the continued push for internet connectivity within industrial applications. The Industrial Internet of Things (IIoT) poses emerging security concerns in which mission-critical sectors in particular must find different solutions to mitigate these risks.

The benefits of accessing information and remotely controlling thousands of industrial devices are unparalleled to what was available just a decade ago, helping to save time, effort and money. Many critical sectors including the electric, natural gas and water utilities, military & defense and transportation industries have begun to leverage automation in one way or another and are already benefitting from the interconnectivity of the IIoT. However, as our systems become smarter and more interconnected, the likelihood of a significant cyber threat increases.

While the IIoT becomes more advanced, so do the hackers who are constantly targeting mission-critical operations and looking to cause damage that could be far more devastating than a simple hack on your laptop or smartphone. As a result, mission-critical entities are focusing on one of the key components of cyber security, establishing a secure network to create a customized defense for IIoT technologies. To do this, many operators are leveraging separate and private wide area wireless network technology.

Where Automation Has Led Us

With the ever-increasing growth of the consumer IoT, wireless connectivity has grown from 2G to 3G to 4G and now with the rollout of 5G to enable faster speeds and greater capacity. This growth has been great for the consumer, but industrial sectors are finding serious concerns in using the same public cellular data networks for industrial

applications as these networks fail to meet the capacity and reliability demands of mission-critical applications.

The public wireless data networks from AT&T, Sprint, Verizon and T Mobile have been engineered for much greater downlink capacity to enable streaming video and other data intensive services. Industrial applications, on the other hand, require greater coverage, capacity and reliability in the uplink given the information is located at the grid or network edge (in the “fog” vs the “cloud”). This includes SCADA and sensor data for industrial applications that are often latency sensitive.

This lack of predictable capacity and coverage in the uplink from the major wireless carriers has led some mission critical operators to leverage unlicensed spectrum technology in order to meet capacity and quality demands. This approach, while it may seem like a ‘quick fix’ solution to the capacity problem, ultimately creates a new concern in the lack of security for these operations – opening up more access points for hackers and threats from interference.

We’ve seen these threats continue to emerge for critical infrastructure operations that are connected to the public internet or that leverage unlicensed spectrum. In December 2016, we bore witness to one of the largest attacks on a nation’s [power grid in the Ukraine](#), after hackers took down an electric transmission station north of Kiev and blacked out a fifth of its total capacity. Hacks have also occurred in the transportation sector including targeting passenger rail.

In the wake of these emerging security threats, mission-critical entities have faced a difficult choice, prioritizing either security or capacity, both of which are of the utmost importance to maintaining operations. To overcome this, some have sought out other options, outside of the traditional public or unlicensed networks in order to establish networks designed specifically for industrial applications.

A New Standard to Bolster Industrial Wireless Connectivity Needs

To create a better data communications solution capable of meeting security, reliability and capacity demands, associations including the Electric Power Research Institute (EPRI), the Utilities Technology Council (UTC), and over twenty of the industry's leading utilities along with key technology providers set out to develop a new licensed wide area wireless standard. Published in October 2017, the new IEEE 802.16s standard leverages underutilized licensed VHF and UHF spectrum in a variety of channel sizes ideal for industrial internet applications. The expanded spectrum options and channel flexibility allows industrial providers to obtain licensed spectrum without having to compete with the consumer wireless operators.

802.16s networks can be built to an operators exact requirements ensuring high security, low latency, prioritized capacity and reliability in an industrial wide area network. For example, in the power grid, where the integration of renewable energy requires the use of multiple, automated, interconnected smart devices, utilities can build a network specifically to meet those capacity demands, meanwhile an oil & gas operator, wary of cyber threats, can build a network separate from the public internet with layered security protocols on top of it. The flexibility of the standard gives mission critical operators the option of purchasing multiple licensed frequencies to add capacity if needed.

As IIoT emerges, so do the options for increased network connectivity, which can be either beneficial or detrimental depending on which option is selected. The new 802.16s standard is an ideal solution for the Industrial IoT allowing for separate private and secure wide area wireless networks.

11 | 13_04_2018
PRAGUE, CZ



CyberCentral

ONE OF EUROPE'S MOST EXCLUSIVE
INFOSEC EVENT

Speakers from:



FBI



Tinkoff
Bank



GAMES

WEFIGHTFRAUD

SONY

SANOFI



..and more

For more information:

CYBERCENTRAL.EU

IS C-LEVEL SECURITY TALK RESULTING IN ACTION?

EXECUTIVES SAY SECURITY IS TOP OF MIND, BUT SEARCH DATA PROVES OTHERWISE

by Ben Lorica, Chief Data Scientist, [O'Reilly](#)

From media headlines to industry surveys, most business executives across industries are continually naming security as one of their highest priorities. After the myriad of globally destructive breaches that 2017 brought us, from Equifax to WannaCry, it makes sense that organizations are trying to convince consumers and employees alike that they value the safety of their data and are doing all they can in the fight against hackers. But is all of their talk actually resulting in action?

According to new data from O'Reilly's online learning platform, Safari, it's not. To find out what organizations are really focusing on, O'Reilly analyzed search data from Safari's user base of more than two million business and technology professionals. It found that despite the grave importance of cybersecurity in business and technology today, there's a concerning lack of activity in this area when it comes to what skills and trends professionals are searching for – and, therefore, what they're prioritizing.

Along with the increasing sophistication of cyberattacks and the consequences of becoming the victim of one, the gap between the number of qualified security professionals and the number of open security positions is becoming even wider. As legacy systems are being replaced by hybrid cloud environments, it's imperative that organizations across industries start taking security seriously. Without impenetrable security, these organizations will suffer a loss of not only funds, but also customers (let alone their reputations).

What Security Search Data Tells Us

Despite its priority claims, “security” ranked 47th on the list of Safari's top search terms. “Hacking” came in at #127 and Wireshark, an open source packet analyzer tool, took the 141st spot. It is possible that security activity is included in other development work or hidden within other search terms. It's also possible that organizations could be moving to the cloud and therefore adopting the security features offered by their cloud providers, as noted by the popularity of cloud-related search terms, such as “Amazon Web Services” and “microservices.”

Whatever the case may be, security is an essential and incredibly broad area that deserves higher activity and ongoing attention from professionals across all industries. In our age of frequent and increasingly sophisticated cyberattacks that are capable of shutting down global operations within seconds, it's no longer enough to have an

educated, security-savvy C-Suite. The whole organization must be paying attention to security policies and best practices. The smartest organizations are the ones pursuing “baked-in security,” woven into the tools and structure of an organization, rather than “bolted-on security,” implemented after a product or process is already complete.

How To Improve Your Organization’s Approach to Security

In order to start taking best security practices head-on, you’ll need a baseline understanding of where your organization stands. Here are some of the key questions to ask as you begin your own security audit:

Does your organization’s leadership team know what the security policies are? What about the other employees?

Although it might seem like having an educated C-Suite is enough, today, every employee an organization has influences its security posture. Every employee is accessing the organization’s network through their own unique identity, which means that every employee can be used as a pathway to compromise the network. Certainly, some employees have a much larger bearing on security than others, such as those who wield the widest access to the company’s most sensitive data. For this reason, you should start security education with those who present the highest risks and build out from there. For example, while business leadership definitely comes to mind as among those who should be immediately and most thoroughly educated on organizational security, what about administrative assistants? Do they have access to everything that your C-Suite has access to? Chances are they do *and* that they’re less security-aware. If this is the case, simple (and common) attack vectors such as phishing and social engineering could easily lead to serious consequences. And don’t forget about passwords. Although they may seem like a basic component of security, their impact can be huge. Employees reusing passwords or leaving default passwords in place can quickly create problems. In fact, London-based consultancy [Wills Towers Watson](#) found that 66 percent of breaches in 2016 were caused by “employee negligence or malfeasance.” Making sure that every employee, from the CEO to the summer intern, is thoroughly educated on security hygiene and basic policies, as well as why they should care about following them, can help address many of these issues.

How distributed is your technology stack?

The more distributed your technology stack is, the more challenging it becomes to secure it – and the more important it becomes that security controls are set correctly from the beginning. Sprawl presents a lot of access points that need to be protected. In addition to the increased security challenges, maintaining flexibility and agility while ensuring all of those access points are protected can be especially difficult. If your organization does choose to implement a distributed technology stack, making sure that employees are educated on every tool they’ll use and how to protect the sensitive information each contains is essential.

Does your organization have a plan for how it will stay strong amid the growing cybersecurity skills gap?

Even if your organization's security force is one to be reckoned with right now, consider how it will be in ten years. Evolving technology, advanced cyberattacks and a lack of qualified professionals to help protect against them are inevitably in every organization's future. Consider this: cybersecurity has the highest demand as well as the largest gap between demand and supply, with 68 percent of organizations reporting high demand for cybersecurity skills and only 43 percent reporting proficient cybersecurity skills already present in the organization, according to a recent report by [Capgemini](#). The near future is not looking much better – the [Information Systems Audit and Control Association](#) predicts a global shortage of two million cybersecurity professionals by 2019. Unfortunately, it's likely that your organization is going to face the challenges that stem from this shortage, including having to rely on your existing security staff more. Planning accordingly by prioritizing a “baked-in” security strategy is a more sustainable model. It also means that the security resources you can procure will be used more efficiently and effectively by the whole organization.

With rising cyber-risks and a lack of skilled security staff to help organizations figure out how to protect themselves, it's understandable that security is an area some employees find it preferable to ignore. However, it's imperative that professionals across all industries start paying more detailed and frequent attention to security, and that organizations and their security teams prioritize a “baked-in” approach that will help carry them through all the changes technology brings. In addition to efforts from the security team, every employee should take a moment to ensure they know how to do their part in protecting against cyberattacks – and, if not, peruse all the resources they have available to educate themselves.

About the Author



Ben Lorica is the Chief Data Scientist at O'Reilly Media, Inc. and is the Program Director of both the [Strata Data Conference](#) and the [O'Reilly Artificial Intelligence Conference](#). He has applied Business Intelligence, Data Mining, Machine Learning and Statistical Analysis in a variety of settings including Direct Marketing, Consumer and Market Research, Targeted Advertising, Text Mining, and Financial Engineering. His background includes stints with an investment management company, internet startups, and financial services. Ben can be reached online at [@bigdata](#) and at our company website, <http://www.oreilly.com>.

THE SECURITY BEHIND E-SIGNATURES

by **Tommy Petrogiannis, President, [eSignLive by VASCO](#)**

E-signatures have been helping enterprises transform their operations for 25 years. Companies in both the public and private sectors deploy e-signatures for customer onboarding, consumer loan applications, employee performance reviews, contract negotiations, recruiting and much more.

The benefits of e-signatures continue to be quantified, including: 99% customer adoption rates at over 1,700 OneMain Financial branches; \$8 million paper savings annually at Royal Bank of Canada; and 70% reduction in the processing time for employee performance reviews at the U.S. Census Bureau. Yet with the increasing incidents of data breaches and hacks worldwide, it's worth revisiting exactly how e-signatures provide the security so critically needed today.

To ensure a trusted experience between an organization, its employees and customers, e-signature solutions should meet these top three requirements:

- Use digital signatures to protect documents from tampering
- Embed detailed audit trails for regulatory compliance
- Verify the signer's identity through appropriate levels of authentication and attribution

Digital vs. Electronic Signatures

Document and signature security are at the heart of any electronically signed document. The way to achieve the highest level of trust and security is to require the document and *each* signature to be secured with a digital signature. Digital signatures ensure the document is rendered tamper-proof and that signatures cannot be copied and pasted.

The term "digital signature" is often confused with "electronic signature." An electronic signature, like its paper equivalent, is a legal concept. Its purpose is to capture a person's intent to be legally bound to an agreement or contract.

A digital signature, on the other hand, is a security technology. Based on public/private key cryptography, digital signatures are used in a variety of security, e-business and e-commerce applications.

When used within an electronic signing application, digital signature encryption secures the e-signed data. If an e-signed document is modified or tampered with in any way, digital signature technology will detect it and invalidate the document. Unlike paper-based contracts and signatures that require careful attention to detail and that rely on the human eye for verification, e-signed contracts with digital signatures will automatically flag any errors or alterations.

Digital signatures are the foundation of any reliable electronic signature and a core requirement for a trustworthy solution.

Comprehensive Audit Trails

Audit trails play a key role in documenting each step of the transaction, ensuring compliance with state and federal regulations and helping foster consumer confidence. A comprehensive audit trail should include the date and time of *each* signature in the document, and the audit trail should be securely embedded in the document and linked to each signature. By embedding this information in the document, the authenticity can be verified independently in the future, no matter which e-signature solution you use. In addition, the record can securely travel through any email, storage or archiving system without being compromised or requiring additional programming.

Identification and Authentication

E-Signature laws don't say much when it comes to security techniques and technology, but the legal definition of an electronic signature always includes language around signer identity. This means organizations need to take steps to identify and/or authenticate users prior to e-signing, and they need to tie that authentication to the e-signature and e-signed record.

Authenticating users and transactions are top priorities for banks and other organizations conducting business online and via the mobile channel. When evaluating how to identify new customers over the web, consider how this is accomplished in other remote channels, such as call centers and by mail. These processes often identify first time applicants using two types of personal information - personally identifiable information (PII), and non-public personal information.

The customer's information is typically verified through a third-party identification service (e.g. Experian, Trans Union, Equifax). Financial service providers, for example, frequently use third-party services, since they are often already accessing credit databases as part of loan applications and other processes. In this case, look for an e-signature solution that integrates with third-party identity verification services.

Once a signer's identity is verified, organizations often issue electronic credentials to facilitate future digital transactions. In the case of existing customers, it is highly recommended to leverage credentials you may have already issued (e.g. logins for online banking). Not only are such credentials generally reliable if they have been used over time, it saves the customer the hassle of having to create and remember yet another password.

In addition, organizations in certain geographies or in sectors that deal with high-value, high-risk transactions often use strong, multi-factor authentication services at any point during the process. This reinforces trust in the transaction and creates a secure environment so that identities, data and digital lives remain protected. In this case, look for an e-signature solution that can easily integrate with authentication services throughout the e-sign workflow.

Attribution

Signature attribution is the process of proving who actually clicked to apply an e-signature. Questions of attribution often come up when looking at processes where staff interacts with customers in a face-to-face environment using the click-to-sign method on a shared device.

Consider the use case where a signer is asked to click a button to e-sign on an agent's laptop. The challenge becomes how to prove who was holding the mouse when the e-signature was applied. There are two proven approaches for establishing attribution in these circumstances: affidavits and the use of SMS passcodes sent to personal mobile phones.

Affidavits are the most cost-effective and the easiest way to establish attribution. Just before handing over control of a laptop or tablet to the customer for signing, your employee or representative would be presented with affidavit text affirming they are handing control over to the signer. This transfer of control would be captured as part of the audit trail.

Another option is to use the signer's personal smartphone. Signers can be sent a one-time passcode via SMS text that they would use in order to gain access to the e-sign session.

While there are many secure and user-friendly options for identifying signers online, ultimately the choice of authentication method depends on the risk profile of the process being automated and the underlying digital transaction. The key point here is to authenticate users without diminishing their experience.

Trust and Security Are the Foundation of E-Signatures

Providing a secure digital experience is a top priority for any e-signature deployment. Not only should it be easy to use, it should assure the user that the underlying integrity of the signature and the security behind the technology is solid. The most trusted e-signature solutions should utilize a digital signature, embed comprehensive audit trails and properly identify and attribute each user. With these key security features, your organization is on track to successfully digitize its business processes, while providing customers with a trusted and secure experience, no matter the use case, channel or geography.

International Conference on Mechatronics & Robotics

October 15-16, 2018 | Helsinki, Finland

Theme: "Unfolding Knowledge with a Delineate Technical World"

Mechatronics and Robotics 2018 warmly welcome all the researchers, developers, experts, students from the field of mechatronics & robotics to attend International Conference on Mechatronics & Robotics during October 15-16, 2018, Helsinki, Finland. The Conference will be composed around the theme "Unfolding Knowledge with a Delineate Technical World".

Sessions related to Mechatronics & Robotics 2018

1. Mechatronics and Robotics
2. Design and product development
3. Materials Science
4. Materials and Manufacturing
5. New Approaches in Automation and Robotics
6. Computational Vision and Robotics
7. 3D Scanning
8. wearable robots
9. Medical Robotics and Computer-assisted Surgery
10. Industrial Automation
11. Autonomous Technology
12. Sensor Networks
13. Intelligent Machines
14. Automotive and Vehicle Technology Systems
15. The Coming Future of Artificial intelligence
16. Power storage

This will be the best common platform to learning and offer new thoughts, create a network amongst the Technologist, Professionals, Industrialists, Researchers, Innovators and students from the area of Technical as well as Non-Technical background.

For more details: <https://robotics-mechatronics.enggconferences.com/>

For Queries

Contact: Kevin Mathew

Program Manager | Mechatronics & Robotics 2018

Mail: mechatronicscongress@enggconferences.com

Office Ph: +1-702-508-5200 Ext 8122

Toll No: +1-800-216-6499 (USA & Canada)

<https://robotics-mechatronics.enggconferences.com/>



The cybersecurity threat landscape is now more fraught than ever. New revelations on the [scope and severity of 2017's Equifax hack seem to roll out by the day](#). The IRS has just released a number of [tax scam-related warnings](#) well ahead of schedule. And [Uber](#), breached in 2016, is still running the gamut of reputational damage control in the face of its customers' potential data exposure.

Yet what is most shocking about these cyberattacks, scams and data breach reports is that they now scarcely seem to shock us at all. Many businesses appear to have adopted an attitude of learned helplessness where these attacks are concerned. Indeed, while [75% of executives](#) report that their greatest risks come from bad actors on the digital front, only 19% consider themselves adequately prepared to mitigate these threats.

All this comes even as [most experts now regard data breach not as a possibility, but an inevitability](#). Over the past five years, the wave of cyber breaches hitting businesses has [nearly doubled](#) in size. And with the Internet of Things projected to expand to [20.4 billion devices by 2020](#), these risks will only grow.

With the threat of data breach escalating at fiber optic speeds, businesses cannot afford to respond at a dial-up pace. Nor can they content themselves with partial measures or fortify only one stronghold of cyberdefense.

Too often, companies dedicate their resources to preventive efforts alone, imagining that if they turn their attention to retroactive measures, they are preemptively conceding defeat. Yet rather than view breach prevention as an isolated set of tactics apart from breach response and recovery, businesses need to see it as just one component of a comprehensive, customized cybersecurity strategy—one that integrates readiness, response and retrospective measures into a fluid, strategic framework.

Businesses must start by differentiating between their internal and external vulnerabilities and preempt each one accordingly. One of the largest factors in securing company data involves properly training employees in how to open, handle and store sensitive information. Too many cyber breaches occur when unsuspecting personnel expose company systems through downloading unsolicited email attachments or clicking on suspicious links.

Because these errors can instantaneously subject an entire network to malware or ransomware, early and continuous employee education is critical. Routine cybersecurity drills and debriefs should not merely consist of running through a generic list of best practices, but instead take into account workplace- and department-specific strengths and weaknesses. Strong breach readiness requires a trained workforce well-versed in its unique threats and individual protocols for dealing with them.

Organizations must also conduct ongoing screenings of end-user and external networks. The number of these networks varies by company and by sector, with healthcare organizations among the most frequent to engage with end-users. (Lately, healthcare organizations have also been some of the organizations [most vulnerable to data exposure.](#))

Un- or under-secured external networks are a surprisingly common way for companies to expose sensitive information to malicious third parties; both Equifax and FedEx, in fact, were breached because of their flawed external network security measures. By contrast, excellent breach readiness involves securing end-users and external networks through routine network scans and regularly searching third-party platforms, like the Dark Web, for company data. At this stage, the groundwork of breach readiness becomes the cornerstone for a solid breach response.

Ultimately, a company's internal incident response team is the first line of defense in cases of a data breach or cyberattack. For this reason, while specific incident response team roles and procedures will differ by organization, a number of characteristics should remain consistent regardless of company sector or size.

At the helm of every effective incident response team is a company executive with decision-making authority and, if applicable, contact with a company's Board of Directors. The rest of the team should comprise personnel from multiple departments throughout the organization, including IT, finances, compliance and account management. At least one member, preferably from the company's HR or communications department, should serve as the breach response "spokesperson" and be charged with overseeing all media and external communications.

In cases of small or service-industry businesses that do not have different expert departments in-house, incident response teams can incorporate trusted external resources, like outside legal counsel familiar with cybersecurity and disclosure laws. By highlighting strengths and weaknesses within a company's existing defense strategy, and by developing a rapport with local resources in advance, businesses can go a long way in making sure their incident response team is ready to spring into action at the first sign of a breach.

Companies must be prepared to communicate frequently with key stakeholders in the aftermath of a data breach. Here, it can be wise to draft sample emails and other communications detailing the nature of and company response to the breach in advance. During and after a breach, when energy is scattered and emotions are high, having immediate access to a number of pre-vetted templates for engaging with the public can save a company time and effort and will often reduce the risk of client or regulatory fallout.

After a breach has been arrested, assessed and adequately reported, retrospective occurs. During this stage, companies should turn to patching whatever loopholes allowed the breach to occur, restoring business operations and discussing areas where its breach strategy was effective as well as what could be improved.

According to the 2018 Global Risks Report, cybercrime is expected to cost U.S. businesses 8 trillion dollars over the next 5 years, affecting small businesses disproportionately. If a breach does occur, minimizing its impact starts with these conversations. As the risks and costs of cybercrime and data breach continue to rise, so should an organization's level of awareness, preparedness and expertise.

About the Author



Jerry Thompson is senior vice president of Identity Guard, provided by Intersections, Inc., which since 1996 has protected more than 47 million consumers. Learn more about Identity Guard by visiting Jerry online at <https://www.identityguard.com/>.

"Asia's Premier Counter-Terrorism and Internal Security Exhibition and Conference!"

CTA

COUNTER TERROR ASIA EXPO 2018

4 - 5 DECEMBER 2018

**Marina Bay Sands,
Singapore**

Co-located With:



An International Conference on
Counter-Terrorism and Internal
Security

www.counterterrorasia.com

For more info, contact us:

Phone: (+65) 6100 9101 | Email: sg@asiafireworks.com

Organized by:



Fireworks Trade Media Pte Ltd

MISADDRESSED EMAILS WERE THE #1 DATA SECURITY INCIDENT REPORTED IN 2017

Tim Sadler comments on the alarming statistic released by the Information Commissioner's office stating that misaddressed emails were the number form of data loss in 2017. Tim Sadler is CEO & Co-Founder of [Tessian](#), a next-generation email security platform using machine intelligence to analyse email networks and automatically prevent highly sensitive emails being sent to the wrong people with minimal end-user disruption.

by Tim Sadler, CEO & Co-Founder, Tessian

With emails forming the main artillery of communication in most organizations, it is perhaps not surprising that email data breaches were the main cause of critical data loss in financial, legal and professional firms in the UK in 2017.

Today's rapidly evolving cybersecurity landscape is creating a sea change for how enterprises run their business. Impending changes to data protection legislation via GDPR law, coupled with daily news stories about cyber attacks in every form, have left many organisations scrambling to put a plan in place that will effectively shield their business against risk.

Common Perceptions of Cybersecurity

Often when people talk about cybersecurity, what they're *really* referring to is external cyber threats like malicious hackers. The incidence of attacks on companies of all sizes and sectors from these sources has increased sharply in the last 12 months. In 2017, the number of ransomware attacks increased by 36% and an estimated 6.5% of people fell victim to identity fraud. This type of cyber risk is at the forefront of everyone's mind and the top of every Board's cybersecurity agenda.

We are currently living in an era where the trials, scandals and downfall of companies that once might have remained behind closed doors have become media fodder. This is especially true of high profile cases of cyber attacks and security breaches on enterprises and governments. Attention-grabbing headlines about malicious attacks create a climate of fear, which actually distorts the reality and severity of the some of the far less sensational challenges around cybersecurity.

For businesses and governments, this is problematic in assessing risk and accountability. It gives a false impression that in order to eliminate risk, they must build an impenetrable fortress around their enterprise that no attacker can enter. But this is not the case.

95% of all security incidents involved human error - IBM

A quick look at the data security incidents reported to the Information Commissioner's Office last year tells a different story about risk to the one we hear in the media.

In 2017, the number one digital data security incident reported to the ICO was not credential phishing, ransomware scams or anonymous hackers. It was data loss due to misaddressed emails. To be specific, the ICO details the most reported digital data security incident as:

“Data sent by email to the incorrect recipient or failure to use bcc when sending email.”

So despite how high businesses build those walls to insulate themselves from external attacks, the more prevalent problem is accidentally leaking sensitive information through an open window.

Human error is an enterprise-level threat that businesses and governments must address and be held accountable for. According to research by IBM, 95% of all security incidents involved human error. Unfortunately, human beings are capable of wrecking complete havoc on enterprises without malicious intent. Luckily, there is only a minority of people who are in charge of dealing with missiles as part of their daily job. But for everyday businesses, sensitive data loss via misaddressed emails is the most common cyber risk. In the pantheon of cyber risks, misaddressed emails may not be as newsworthy or as scandalous of a threat as malicious hackers, but it is a serious, ubiquitous risk.

The Impact of Human Error on Businesses and Governments

Emailing is such a familiar part of our daily lives that we don't consider it to be as harmful as it can be. It is the main artery of communication for enterprises and governments, used to share the most highly classified and the most trivial of information.

Given the huge volumes of sensitive data traded every day by governments and businesses such as law firms, hedge funds, banks and medical clinics, the consequences of just one of these emails ending up in the wrong hands are extremely damaging.

In the case of the legal industry, there was an 173% increase in the number of legal sector information security incidents reported to the ICO in Q1 of 2017 alone. If a law firm were to accidentally leak confidential project information to the wrong client or third party, to a member of the press or to a personal email account that was later hacked, that law firm could face the loss of that client and potentially others whose faith in the firm was ruined, loss of income and serious reputational damage if the incident was reported in the media.

Not to mention the serious financial penalties of personal data breaches. As of May 2018, when new GDPR legislation is enforced, organisations can be fined up to 4% of their global annual turnover for data breaches. In forcing businesses and governments to take accountability for the data they must protect, GDPR law also states that any personal data breach must be reported no later than 72 hours after becoming aware of it.

Not acknowledging personal data breaches - or failing to prevent them from happening - will no longer be an option for businesses and governments. Organisations must have a clear-cut way of monitoring and preventing sensitive data loss, especially via misaddressed emails, in order to demonstrate accountability.

Tessian is an award-winning email security platform that helps enterprises counteract human error and prevent misaddressed emails. Using advanced machine intelligent technology, Tessian analyses email networks and automatically prevents highly sensitive emails being sent to the wrong people. Some of the world's leading organisations across the legal, financial, professional services and technology sectors rely on Tessian as a critical component of their cybersecurity framework.

Despite the notions we have of cyber risk, it is the threat of human error that must become a bigger part of the cybersecurity agenda. It is impossible to remove the presence of human error from an organisation entirely, but businesses and governments must mitigate and take accountability for this risk by identifying internal risk and using smart cybersecurity software to counteract it. UK companies are realizing the importance of investing in cyber security technology not just to prevent, but also to detect and report, any emails that could have been sent to the wrong person. Given the current climate and impending changes to UK data law, having control and peace of mind that confidential client data will remain confidential is a critical priority for all businesses in 2018.

Tessian, formerly CheckRecipient, is a next-generation email security platform that helps enterprises counteract human error and significantly reduce the risk of data loss. Tessian uses machine intelligence to analyse email networks and automatically prevent highly sensitive emails being sent to the wrong people with minimal end user disruption. Some of the world's leading organisations across the legal, financial, professional services and technology sectors rely on Tessian as a critical component of their cybersecurity framework.

The rebrand comes after a year of triple-digit growth for the company which also saw the team expand from 7 to 45. 2017 kicked off with Tessian CEO, Tim Sadler, being named on the Forbes 30 Under 30 list in Technology and over the course of the year the company picked up other high profile awards such as Best Innovation in Data Protection and Privacy (CogX), Best Security Startup (Info Security Products Guide) and the UK's Most Innovative Security Startup (Dept of Culture Media and Sport). Tessian is backed by the world's best venture capital firms and raised a \$2.7 million funding round led jointly by Accel and LocalGlobe. Others participating include Winton Ventures, Amadeus Capital Partners and Crane.

To find out more, visit www.tessian.com.

About the Author

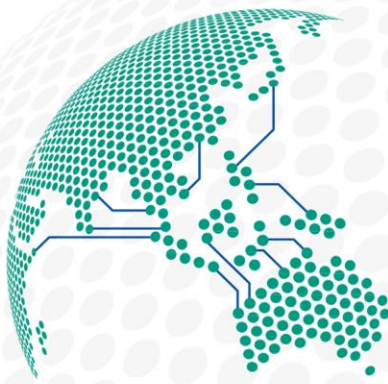


Tim Sadler, is the CEO & Co-Founder of Tessian. Tim is the CEO and co-founder of Tessian, a next-generation email security platform which uses machine learning to predict when emails are being sent to the wrong people. Some of the world's largest organisations across the financial and legal sectors are using Tessian and in the past 6 months, the company has been crowned "Best Security Startup" by WIRED, "Best Machine Intelligence Startup" by Legal Geek and "Best Startup - Gold Category" by Info Security Products Guide. Tim holds three Masters degrees in design, engineering and innovation from Imperial College and formerly worked in

HSBC's Global Banking division -- Tim was also listed as one of Forbes "30 Under 30" in European Technology for 2017. Tim Sadler can be reached online at:

<https://www.linkedin.com/company/tessian> and <https://twitter.com/tessian>

and at our company website: <http://www.tessian.com/>



SMTC SINGAPORE MARITIME TECHNOLOGY CONFERENCE

24-26 APRIL 2018
MARINA BAY SANDS
SINGAPORE

The 3rd Singapore Maritime Technology Conference and Exhibition (SMTC) 2018 is organised by the Maritime and Port Authority of Singapore and will be held in conjunction with Singapore Maritime Week 2018.

Powered by the world's top ship owners, terminal operators and Government authorities, SMTC 2017 set the bench mark with unrivalled information, peer to peer networking and an accompanying exhibition of new and upcoming technology products.

SMTC 2018 AT A GLANCE

PRE CONFERENCE

Tuesday 24 April 2018

Singapore Maritime Institute Seminar

MAIN CONFERENCE DAY 1

Wednesday 25 April 2018

Digitalisation Strategy

Plenary Day

- The Digital journey for Shipping
- Digital innovation trends

MAIN CONFERENCE DAY 2

Thursday 26 April 2018

Tools, Systems and Applications of Digital Technologies

Track 1 - Smart Technologies

Track 2 - Strategy and Business of Digitalisation

350+

Total Participants

160+

Companies

70+

Speakers

20+

Countries

"SMTC is very useful in sharing of various technology innovations, implementation and case studies from ship owners, technology companies and various others in the eco system. It is a very good conference to align maritime industry with the digital revolution."

Jessica Chen Jinzhu, Wilhelmsen

www.smtcsingapore.com

Organised by:
Maritime and Port Authority
of Singapore



Managed by:
IBC Asia (S) Pte Ltd



COULD OUR WEB DEPENDENCY COST US A LOT?

by Milica D. Djekic

What is in common to the DDoS and any ransomware attacks? We could confidently say it's their ability to get used as the sabotage weapons. If we have in mind how time consuming and expensive, say, ransomware or even DDoS could be, it's quite obvious why we should get concerned if those tools get in hands of the bad guys. The greatest fear here could be if we focus on communications system being the part of some web infrastructure. In many practical cases – when you vitally depend on the communications, you would realize how slowing down the web traffic or locking the systems or files could be threatening. The role of this article is to provide a short insight how these powerful weapons could get applied in order to cause the catastrophic impacts.

Through this effort, we would mainly talk about the terrorist-organized attacks and give some everyday examples how cyber solutions could serve as a critical weapon. As it's well known, the threats are getting more and more sophisticated and sometimes it may appear as quite challenging handling all those risks. So, let's try to explain why it's so concerning if anyone tries to threaten your systems being vitally dependable on communications. The good instance of such a system is the ground control station either being civilian or military. In so many cases, these facilities could suffer the well organized and synchronized cyber breaches that could get applied in order to run the DDoS or ransomware attacks.

For that reason we would ask in our title if our web dependency could cost us greatly. The answer to this question could be quite embarrassing to many people. Just try to imagine how frustrating it could be if the terrorists would take control over some ground control station either being in some urban area or on the battlefield. Such an operation could get conducted so simply taking into account how vulnerable IT infrastructure could be.

The next step in this explanation would be to attempt to figure out what could occur if, let's say, the aircraft is flying from Europe to the US and on its way to the final destination when the crew is getting ready for the landing – the pilot loses the contact with the ground control. Also, try to realize that the terrorists could choose a day with the heavy weather conditions like show, ice, fog or thunderstorm are. Losing contact with the ground control while you are in the air trying to land could be the big shock to the pilot and his crew. In such a case, he should count on his experience and get prepared to handle such a situation.

The main risk is that the crew could lose control over the situation and the aircraft could crash on that urban area. The similar scenario could happen to the army ground and communications control stations.

In conclusion, we would make some recommendations how such a situation could get overcome. For instance, it's so important to check out the airport IT infrastructure from cyber breaches as well as raise some awareness within the civilians and army people how to behave in such a case if it even occurs. The pilots should receive some training how to deal if they lose contact with the ground and the ground control folks should learn how to cope with such a situation directing the aircraft to the safe place and promptly repairing the flaws within their IT systems.

About The Author



A Frequent contributor to Cyber Defense Magazine, Milica Djekic is a talented cybersecurity expert.

Since [Milica Djekic](#) graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia.

She also serves as a Reviewer at the Journal of Computer Sciences and Applications and. She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

connect:ID | 2018

5th
Edition

Walter E. Washington Convention Center, Washington, DC, USA

Conference: April 30–May 2, 2018

Exhibition: May 1–2, 2018

CONNECT WITH A WORLD OF NEXT-GENERATION IDENTITY SOLUTIONS

1,400

industry leaders, specialists
and senior decision makers
attending.

3

conference streams with in-depth
analysis of digital ID ecosystems,
fintech, border management,
biometrics, future ID and more.

80+

speakers, hand selected to
inform, inspire and prepare
attendees for future challenges.

100

exhibiting companies showing
the latest in identity solutions
plus a new Start-up Zone.

2

free seminar theaters,
offering a wealth of free
content to attendees.

Countless

opportunities to learn,
meet new contacts, and
do business.

Event powered by

WWW.CONNECTIDEXPO.COM



As fast as cyber criminals adapt to work their way around security defences, new techniques and tactics for preventing hacks, infections and data breaches come into play. While the size of the average data breach increased by nearly 2% last year, the global average cost is [down 10%](#) on previous years to \$3.62million – and by keeping up with the latest cybersecurity updates, businesses can help to keep that number falling.

Certain weaknesses and challenges are likely to come into play for all businesses, if they haven't already. But there are new trends set to help fight cybercrime, and a few key facts to remember this year.

1. The Internet of Things increases vulnerability

The growing trend for internet-connected devices is showing no sign of slowing, with everything from TVs to refrigerators getting hooked up to the web. But the Internet of Things is a serious weak point in online defences, with smart devices often not made with even the most basic security features. An estimated [8.4 billion 'things'](#) are now connected to the internet worldwide, and while this level of connectivity comes with plenty of benefits, it also brings increased cybersecurity risks.

Many connected 'things' – such as security cameras and baby monitors – are left to rely on default passwords that grant hackers easy access. Those that aren't left on default passwords are often still woefully under-defended, and easily accessed by hackers looking to create [Botnets](#) and carry out huge spam attacks.

Listed by security provider AVG as one of the [top 10 points of entry](#) for hackers to access your network, the Internet of Things is not just a problem in the sense that devices can be used to form attack networks or for hackers to co-opt devices for their computing power, it's also possible to access private information or simply cause a nuisance.

That means devices like security cameras can be viewed and switched off, posing serious physical security risks as well as digital ones. In January 2017, hackers [locked a dozen guests out of their rooms](#) at the lakeside Alpine hotel in Austria after accessing the electronic key system, holding the hotel's managing director to ransom.

As the mobile office and IoT becomes increasingly prevalent in day-to-day life, the need to find ways to secure the Internet of Things is only going to increase for SMBs and their staff.

2. AI and machine learning can boost cyber defences

Cyber criminals move quickly, and machine learning grants us the ability to [predict and accurately identify attacks](#) faster than ever before so that we can keep up. A recent [survey by Avast Business](#) found that 46% of respondents were worried about problems with Artificial Intelligence affecting their security, but the reality is that AI and machine learning are fast becoming a crucial tools for cyber security.

A prime example of this can be seen in PayPal. To increase its cybersecurity, PayPal now uses 'deep learning' AI to spot possible fraudulent activity in customer accounts. Users who might have fallen victim to phishing scams can be protected thanks to detailed, real-time behaviour analysis by [artificial intelligence systems](#). Many other companies are also beginning to implement similar techniques.

The key obstacle stopping widespread acceptance of AI is that, in theory, any computer system can be compromised. Super intelligent machine learning can outrun the criminals, but if they catch up, many fear that the damage that could be done with a hacked super AI could be far worse than anything that has come before. Machine learning can absolutely assist in improving security classifications, recommendations and reinforcements. Network traffic analysis, intrusion detection, database firewalls and anti-malware layers can all be strengthened through the use of machine learning – something that can protect a lot of data and save a lot of money.

3. Worms may begin to outrank other forms of malware

Some of 2017's major cybersecurity headlines were the result of WannaCry and Trickbot – a pair of attacks which both used [worm functionality](#) to spread malware and cause almost immeasurable damage. This kind of malware tactic can affect a huge number of victims in very little time, which is why an increasing number of malware families are expected to attempt this technique throughout 2018 and beyond.

In 2017 a new type of malware emerged [every 4.2 seconds](#), and in the past worms have been some of the most destructive infections – the infamous [ILOVEYOU worm](#) successfully infected 10% of the worlds internet-connected computers in less than ten days.

Worms are much like viruses in that they replicate copies of themselves but differ in their ability to execute and propagate without a host program or human help. They can be defended against using locked down firewalls and other security measures that are nothing out of the ordinary, but without these in place, systems lie open to major corruptions and data loss.

Total defense and security can feel impossible but making sure that the basics are in place will greatly lower the risk of a hack or infection. To help establish this way of thinking, SMBs should develop a security mantra to make sure that their business is prepared to tackle new threats. Simple protections that are often forgotten, such always updating software with the latest patches, installing a reputable anti-virus and keeping it

up to date and ensuring employees get regular security training are the most effective way to minimize the risk of worms, trojans and other malicious programs from reaching your businesses' computers and devices.

About the Author:

As Avast's VP of Engineering, Greg Mosher leads product management and R&D for all Avast Business products. Greg brings nearly 20 years of experience in the anti-malware industry, starting in the early 90s when he created his first antivirus engine as both developer and researcher.



comex

AN ICT INDUSTRY EXHIBITION & CONFERENCE

COMEX TECHNOLOGY WEEK

23-28 APRIL 2018

Business & E-Oman: 23rd- 25th April 2018

Shopper & Smart Homes: 24th- 28th April 2018

Oman Convention & Exhibition Centre, Muscat

Under the Patronage



e.oman



COMEX 2018 HIGHLIGHTS

WWW.COMEX.OM

FOCUS INDUSTRIES



MANUFACTURING



TRANSPORT & LOGISTICS



HEALTHCARE



EDUCATION



OIL & GAS



TOURISM

FEATURED ZONES

- AR/VR
- IoT
- 3D Printing
- Robotics
- Digital Learning
- Digital Commerce
- Cybersecurity
- Smart Homes
- Cloud & Big Data
- Digital Health
- Digital Marketing
- SMEs & Start-ups



Network with C-Level tech executives at **TECH EXECS VIP CLUB**



Focus on 'Internet of Things' and 'Artificial Intelligence' at **TECH SMART CONFERENCE**



Knowledge-sharing seminars & demos at **TECH TALKS WORKSHOPS**



Smart Homes & Tech Wars at **COMEX SHOPPER**



Pre-registered meetings at **COMEX MATCHMAKING ZONE**

BOOK YOUR SPACE TODAY!

Organiser



Ashit Barnes - Exhibitions Director
 ☎ +968 9934 1687 ✉ barnes@oite.com

Ahmed Farag - Sales Manager
 ☎ +968 9411 3434 ✉ a.farag@oite.com

Supporting Associations



Media Partners



SHINING A LIGHT ON THE DARK WEB

UNDERSTANDING THE MYSTERIOUS WORLD OF THE DARK WEB

by Chris Cowen, Cyber Security Expert, US Dept. of Defense

So what is this Dark Web everyone is talking about?

So in order to understand the Dark Web we need to put it within the content of the larger web. There are basically three parts to the world wide web. They are as follows the surface web, the deep web, and the Dark Web.

The surface web is everything that's publicly available and accessible through search or by typing a URL into your browser. The deep web, also known as the invisible web, is all the content on the web that is not indexed by standard search engines, such as email clients, online banking websites, or pages that are inaccessible to crawlers (software that indexes the web for search engines). Some of those pages can still be accessed if you have the URL while others require you to have login credentials. According to expert estimates, the deep web is 500 times larger than the surface web.

The Dark Web, however, is a totally different beast. The Dark Web is a tiny fraction of the web that is only accessible through specialized software such as the Tor browser. However, the term "Dark Web" is also often used to refer to the darknet, the overlay networks that are used to anonymize communications and obfuscate both the origin and destination of internet traffic.

So now that we know what the Dark Web is who uses it?

The main characteristic of the Dark Web is its anonymity, which makes it appealing to a number of actors. Like all innovative tools, the Dark Web is an instrument to shady and illegal activities, such as child pornography and the sale of drugs, firearms, and stolen credit card numbers.

One of the most famous cases that involves the Dark Web is that of Silk Road, the first modern online black market that was created on the Dark Web. The website was shut down in 2013 and its founder is serving a life sentence in prison. Naturally, many other similar websites have sprouted in recent years. Earlier this year, AlphaBay, another Dark Web marketplace claimed that it made \$600,000 and \$800,000 a day, but has since been shut down by law enforcement.

However, the Dark Web is also being used for many other activities that are mostly legitimate (though not necessarily legal, depending on your perspective). Edward Snowden, the famous whistleblower who exposed the U.S. government's mass

surveillance program, used the Dark Web to send information to reporters and media outlets. Journalists and activists also use the Dark Web to avoid being traced by autocratic governments or other actors that might want to harm them. In countries where the government restricts access to specific websites and social media networks such as Facebook, twitter, and YouTube, Dark Web tools can help circumvent censorship.

So how do people access the Dark Web?

The most famous tool to get on the Dark Web is the Tor browser. With Tor, you can access websites whose address ends with the .onion extension. These are websites that are exclusively available on the Dark Web and can't be accessed through normal browsers. Tor enables you to access all the other surface and deep websites with the added benefit that it anonymizes your browser traffic by encrypting it and deflecting it across several computers called Tor nodes before sending it to its destination.

However, there are several things you should know about Tor:

- Tor's browsing experience is considerably slower than normal browsers because of the anonymization technique.
- Some websites block traffic coming from Tor browser.
- While Tor protects you from eavesdropping and surveillance, it won't protect you from websites that contain malicious content.

Navigating the Deep Web and Dark Web

Traditional search engines often use "web crawlers" to access websites on the Surface Web. This process of crawling searches the web and gathers websites that the search engines can then catalog and index. Content on the Deep (and Dark) Web, however, may not be caught by web crawlers (and subsequently indexed by traditional search engines) for a number of reasons, including that it may be unstructured, unlinked, or temporary content. As such, there are different mechanisms for navigating the Deep Web than there are for the Surface Web.

Users often navigate Dark Web sites through directories such as the "Hidden Wiki," which organizes sites by category, similar to Wikipedia. In addition to the wikis, individuals can also search the Dark Web with search engines. These search engines may be broad, searching across the Deep Web, or they may be more specific. When using Tor, website URLs change formats. Instead of websites ending in .com, .org, .net,

etc., domains usually end with an “onion” suffix, identifying a “hidden service.” Notably, when searching the web using Tor, an onion icon displays in the Tor browser.

Tor is notoriously slow, and this has been cited as one drawback to using the service. This is because all Tor traffic is routed through at least three relays, and there can be delays anywhere along its path. In addition, speed is reduced when more users are simultaneously on the Tor network. On the other hand, increasing the number of users who agree to use their computers as relays can increase the speed on Tor.

Tor and similar networks are not the only means to reach hidden content on the web. Other developers have created tools such as Tor2web that may allow individuals access to Tor-hosted content without downloading and installing the Tor software. Using bridges such as Tor2web, however, does not provide users with the same anonymity that Tor offers. As such, if users of Tor2web or other bridges access sites containing illegal content, they could more easily be detected by law enforcement than individuals who use anonymizing software such as Tor.

Government use of the Dark Web

Law Enforcement

Just as criminals can leverage the anonymity of the Dark Web, so too can law enforcement. Law enforcement may use this to conduct online surveillance and sting operations and to maintain anonymous tip lines. While individuals may anonymize activities, some have speculated about means by which law enforcement can still track malicious activity.

Military and Intelligence

Anonymity in the dark web can be used to shield military command and control systems in the field from identification and hacking by adversaries. The military may use the dark web to study the environment in which it is operating as well as to discover activities that present an operational risk to troops. For instance, evidence suggests that the Islamic State (IS) and supporting groups seek to use the Dark Web’s anonymity for activities beyond information sharing, recruitment, and propaganda dissemination, using Bitcoin to raise money for their operations. Military and intelligence agencies can monitor these activities and employ a variety of tactics to foil terrorist plots.

Conclusion

Because of the anonymity provided by Tor and other software, the Dark Web can be a playground for nefarious actors online. There are also many researcher and law enforcement/intelligence agencies that also navigate the Dark Web to protect the public for which they serve. But if you are not within either the law enforcement and or intelligence community it is better stay out of the dark web. But by understanding the Dark Web you can understand this shadowy world and the danger that lurks within it. As always I would tell to protect your personally identifiable information so that you do not become a victim of one of the bad actors within the Dark Web.

About the Author



Chris Cowen is a currently the Cyber Security Subject Matter Expert with the US Department of Defense (DOD). Mr. Cowen has worked within Information Technology for over 20 years within both the corporate and government space. He is currently focused in area of enterprise security and researching emerging trends within the information security space. Prior to working for US DOD Mr. Cowen worked for the United States Capitol Police where he coordinated multijurisdictional events that required working closely with other domestic and international law enforcement agencies, these events included The President's State of the Union Address and multiple United States Presidential

Inaugurations. Mr. Cowen is a Certified Information Systems Security Professional (CISSP). He is also a Certified Ethical Hacking (CEH) and a Certified Information Security Manager (CISM). He has been a featured speaker at conferences around the world this includes speaking in Qatar, Kazakhstan, Estonia, Ukraine, United Kingdom, Kingdom of Jordan, China, and India.

Are Your Data Transfers PCI DSS Compliant?

Don't let a PCI DSS audit surprise you.

One important aspect of achieving PCI DSS compliance is securing data in motion and at rest. If audited next month, would your organization's transfers pass the latest PCI DSS requirements?

With GoAnywhere MFT's Security Settings Audit Report, you can test over 60 security settings in your GoAnywhere environment to see how they perform against PCI DSS. Quickly learn which settings need improvement and receive recommendations on those that failed.



GO ANYWHERE[®]
Managed File Transfer

See the Report in Action. Request a Demo.
www.goanywhere.com/demo



INFECTION MONKEY'S CONTROLLED CHAOS IN NETWORK ENGINEERING

GUARDICORE'S OPEN SOURCE SELF-PROPAGATING SECURITY TESTING TOOL

by Ofri Ziv, VP Research, GuardiCore

Chaos engineering is a rising concept in software engineering built around simulating extreme conditions and observing how the system performs. There is growing interest from the cybersecurity community to apply these same principles, the idea being to bring “controlled chaos” into network security. By constantly simulating breaches into random parts of your network—public or private cloud or any mix thereof—you can test how well your security controls work - all the time. Practitioners should assess the resiliency of their private and public cloud environments to post-breach attacks and lateral movement, and ultimately be better prepared to defend critical organizational assets.


Through continuous simulation of breaches into random parts of a customer's network the customer can test how well their security controls work at any time. The [Infection Monkey](#), developed by [GuardiCore Labs](#), provides detailed information about the specific vulnerability exploited and the effect vulnerable segments may have on the entire network. This actionable information gives security organizations the insights they need to make informed decisions and enforce tighter security policies.

We recently [announced](#) a new version of our Infection Monkey, an autonomous, self-propagating testing tool designed to assess the resiliency of private and public cloud environments to post-breach attacks. Infection Monkey v1.5 now includes support for the AWS, Azure and Google Cloud Platform environments, and has expanded support for Debian Linux and Windows MSI, enabling broader security assessments across hybrid cloud and data center environments. The v1.5 release also adds support for Docker containers used by developers to build software applications.

Infection Monkey v1.5 highlights:

- **New user interface design:** The Infection Monkey UI has been completely redesigned, enabling fast deployment and easier, continuous use.

- **Evaluating your security posture in 3 easy steps:** Launch the Monkey from any given machine, let it simulate an attacker and act on its findings and recommendations.
- **Visual map display:** The Infection Monkey features a dramatically improved Infection Map that visualizes lateral movement inside the network with details of successful and unsuccessful attack attempts, all from the Monkey's eyes.



Infection Monkey

- 1. Run C&C Server ✓
- 2. Run Monkey ✓
- 3. Infection Map ✓
- 4. Security Report ✓
- Start Over


Configuration

Log

Powered by GuardiCore License

The Network from the Monkey's Eyes

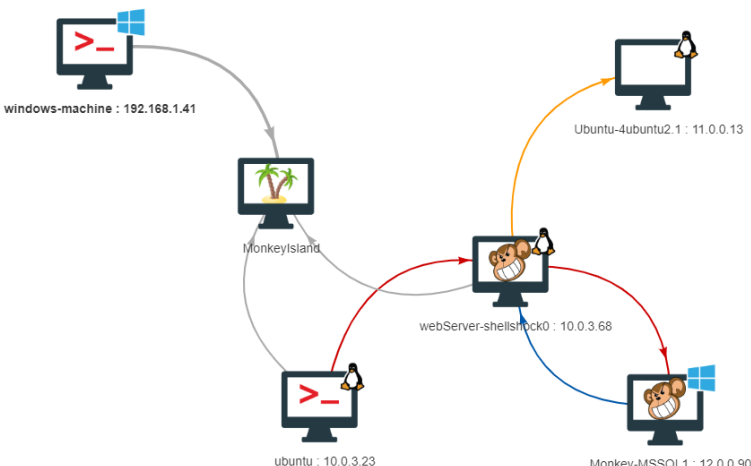
The Monkey discovered 5 machines and successfully breached 2 of them.



40% of scanned machines exploited

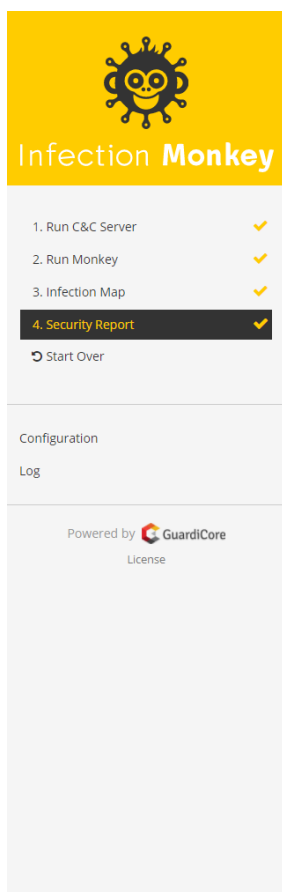
From the attacker's point of view, the network looks like this:

Legend: Exploit — | Scan — | Tunnel — | Island Communication —



The diagram illustrates a network topology with five nodes: windows-machine (192.168.1.41), MonkeyIsland, ubuntu (10.0.3.23), webServer-shellshock0 (10.0.3.68), and Ubuntu-4ubuntu2.1 (11.0.0.13). A grey line connects windows-machine to MonkeyIsland, and another grey line connects MonkeyIsland to ubuntu. A red arrow (Exploit) points from ubuntu to webServer-shellshock0. A blue arrow (Tunnel) points from webServer-shellshock0 to Monkey-MSSQL1. A yellow arrow (Scan) points from webServer-shellshock0 to Ubuntu-4ubuntu2.1. A grey arrow (Island Communication) points from webServer-shellshock0 to ubuntu.

- **New exploits:** The Monkey detects SambaCry and Elasticsearch vulnerabilities and attacks on Windows machines using the pass the hash hacking technique.
- **Security report:** We now provide an elaborate security report at the end of every Monkey session. The report features immediate threats, security issues and actionable recommendations on how to resolve them.
- **Expanded platform support:** This release adds support for Docker containers plus AWS, Azure and Google Cloud Platform environments, and has expanded support for Debian Linux and Windows MSI.



- Machines are accessible using passwords supplied by the user during the Monkey's configuration.

Potential Security Issues

The Monkey uncovered the following possible set of issues:

- Weak segmentation - machines were able to communicate over unused ports.

Recommendations

- **Monkey-MSSQL1**
 1. Change **Administrator**'s password to a complex one-use password that is not shared with other computers on the network.

[Read More...](#)

The machine **Monkey-MSSQL1** (**11.0.0.90**) is vulnerable to a **SMB** attack. The Monkey authenticated over the SMB protocol with user **Administrator** and its password.

2. Use micro-segmentation policies to disable communication other than the required.

[Read More...](#)

- **webServer-shellshock0**

1. Update your Bash to a ShellShock-patched version.

[Read More...](#)





The machine **webServer-shellshock0** (**10.0.3.68**) is vulnerable to a **ShellShock** attack. The attack was made possible because the HTTP server running on TCP port **80** was vulnerable to a shell injection attack on the paths: **/cgi-bin** .

The Network from the Monkey's Eyes

The Monkey discovered **5** machines and successfully breached **2** of them.

 40% of scanned machines exploited

From the attacker's point of view, the network looks like this:

Legend: Exploit  | Scan  | Tunnel  | Island Communication 

• Infection Monkey availability and support

The Infection Monkey is free and can be downloaded [here](#). Source code is available from the [GitHub](#) repository. For questions, suggestions and guidance we encourage you to join the [Infection Monkey](#) Google Group.

About the Author



Ofri Ziv, VP of Research at GuardICore, is the head of GuardICore Labs which conducts ongoing research to discover new cyber threats and help strengthen the security community. Ofri is a veteran of the Israel Defense Forces (IDF) Intelligence Corps, where he led groups of security researchers and was in charge of the IDF's elite cyber security training program. Ofri holds MSc in Computer Science from the Tel Aviv University. He is the author of several papers and has over 10 years of cyber security research experience. Ofri can be reached online at ofri@guardicore.com, [@OfriZiv](https://twitter.com/OfriZiv) and at our company website <http://www.guardicore.com/>



LOOK TO THE SOURCE. PSST. WE'RE OVER HERE.

Having a go-to is great. A go-to friend. Go-to café. And now, a go-to cybersecurity resource.

At RSA Conference, we play host to the industry's top minds, addressing what's relevant in cybersecurity. And what's coming your way. Our global events are filled with expert-led keynotes, tutorials, and everything else you'll need to be on your professional toes.

But don't be fooled, there's more to us than just great events and really smart people. From podcasts to virtual sessions, we also create content to keep you in the loop 365 days a year. And when you subscribe, we've even been known to throw in an exclusive deal or two. You know, just because we like you.

Experts. Smart content. Insider savings. There's a lot waiting for you here. And no reason to wait.

Subscribe to greatness today: www.rsaconference.com/CDM

RSA[®]
Conference

Where the world
talks security

Follow us on: #RSAC     

Multifactor authentication is the undisputed wave of the future when it comes to identity authentication and access management. But, what does multifactor authentication entail? Here is a basic breakdown of the various MFA options.

Multifactor Authentication

What makes multifactor authentication so useful? Throughout history, those who needed to keep people or things secure would never use a single layer of security. Think of a bank, which may have locks on the doors, security guards and then a sealed vault protecting the most precious valuables. The idea behind MFA is the same.

A standard multifactor authentication system uses two of three methods of authentication, which can be classified as something you know, something you have and something you are. The old process of cybersecurity, where all that is required is a single password or PIN code, does not provide a sufficient level of security for valuable assets. This is because not only are passwords or PIN codes easy to figure out or steal, but enterprising hackers can use a brute force approach to guess such access control methods.

With multi-factor authentication, even if an unscrupulous person gets access to a working password, they will not have access to the other method(s) of authentication required to make them work.

What Are Common Multifactor Authentication Options?

As we mentioned above, there are three typical "layers" to multifactor authentication, including:

- **Something You Know:** The first layer of multifactor authentication comes with what you know. Your options here include a password, a PIN, a security question or a pattern you input. The challenge with these knowledge-based authentication factors is that if they are simple enough for a user to remember, they are usually easy enough to hack. Typically, a security question or a long-form password the user has already committed to memory will be most effective.
- **Something You Have:** There are two main options here; a physical token or an app. A physical object could be something like a key card or a FOB. The system could be designed with a reader primed to accept this item's code, along with your login or password. The second option is an app, which is where the push notification comes in. An authentication app turns your smartphone or other enabled device into the second layer of authentication. Once you enter your login or password on a computer to get into the system, this type of MFA sends a

notification to your enabled device. You must confirm your attempt to access the system on that device. If you don't have the device, you can't get in.

- **Something You Are:** Many companies are also opting for a biometric verification protocol, either instead of one of the other layers or in addition to it. This segment requires you provide some physical proof of who you are to access the system. The most common biometric verification is a fingerprint. Your fingerprint is unique and simple to present in fact, most modern smartphones already have fingerprint readers. A popular alternative is a retinal or iris scan, which would essentially require you look into an eye reader for verification. Like a fingerprint, your retinal pattern and iris are unique, easy to provide and hard to steal. In the future, other biometric options may gain favor, such as voiceprints.

Why Agentless SSO?

To explain Agentless SSO, we must first understand SSO, or single sign-on.

SSO is easily achieved in an environment where you are a domain-joined Windows client and access only Kerberos based resources that are a part of that same active directory (A.D.) forest. However, even domain joined resources, like SQL Server has the ability to be its own directory silo---requiring an additional login. Inside the firewall, there may exist hundreds of applications, many requiring their own user account and password. In the past, administrators and developers have compromised security by trying to enable 'SSO' scenarios by trying to allow the user to use their same password in disparate applications through a number of possible insecure 'workarounds.'

To enable a more secure SSO experience inside the firewall, some software vendors would require their proprietary software agent to sit on one of the application servers (sometimes a domain controller) and intercept and channel the requests to their proprietary server/application for an SSO experience. The advent of internet web based applications, extranet applications and mobile apps provide a challenge to the proprietary software agent model because the applications exist outside your firewall. Each of your end-users authenticate to scores of web applications. Administration of thousands of end-users and their numerous accounts would be a prohibitory administrative burden. Decentralizing this administration burden is one of the things that Federation Services offer. Federation aware applications use a standards-based approach to enable SSO securely.

Federation basically sets up an authentication handshake between a trusted authority, usually referred to as an Identity Provider (referred to as an IdP or sometimes as a 'broker') and a Service Provider (SP). This allows the user to leverage a single identity against numerous federation aware and supported applications (SPs). For the most part, modern federation aware applications, like web apps and SaaS apps require no software agents.

Non-Federation aware 'legacy' apps require some level of 'intervention' to support SSO. Most legacy applications inside your firewall can be made federation aware, and offer

SSO convenience to your end-users. There are a couple ways to enable this scenario--- only a few vendors support a clean, non-invasive agentless SSO solution.

Software agents in your network provide several challenges. Software agent-based solutions include additional deployment considerations, supportability ramifications to the application and the vendor of the proprietary software agents, versioning issues, the privilege model that the software agents usually need to run in, the fact that they access highly sensitive information and that they are closed solutions that you can't see in to.

Done properly SSO, especially combined with access policies and multifactor authentication (MFA) can give you a highly secure solution that provides nearly no administrative overhead or burden as well as the most productive end-user experience that both global enterprises and small businesses can leverage.

Instead of installing a software agent on the provider environment, customers of an agentless single sign-on system rely on already established communication protocols between the application and the Federation Broker. Therefore, there are no software agents to deploy or maintain and no changes to application servers.

About The Author



Mark Foust is Director of Worldwide Technical Sales for Optimal IdM. Mark has over 20 years experience in Identity & Directory Services. Previously, Mark spent 16 years working for Microsoft on various teams including the Active Directory Product Group, Microsoft Consulting and Microsoft Premier Support Group. He also performed technical sales at Microsoft for the largest commercial and government accounts in the southeast of the United States. Mark has authored and co-authored 3 technical books and has contributed to numerous technical articles. Mark has also worked for American Airlines

(SABRE), Delta Airlines, Whitman-Hart/marchFIRST and Novell. He holds his MCSE and CISSP certifications and is a frequent speaker at industry events.

About Optimal IdM

Optimal IdM is a global provider of innovative and affordable identity access management solutions. Optimal IdM partners with clients to provide comprehensive, fully customizable enterprise level solutions that meet the specific security and scalability needs of their organizations. Optimal IdM offers its solutions both on premise and in the cloud as a 100% managed service offering. Optimal IdM was recently featured on the Best Identity Management Solutions list of 2018 by PC Magazine, positioned by Gartner, Inc. in the Niche Players quadrant of the Magic Quadrant for Access Management, Worldwide, named a Leader in the KuppingerCole Leadership Compass Identity as a Service: Single Sign-On to the Cloud Report, and awarded Best Multifactor Authentication Solution in the 2017 Government Security News (GSN) Homeland Security Awards (HSA) Program under the Cyber Security Products and Solutions category.

INFOSEC MANCHESTER

Developing information and cyber security strategies in the North West

NEXT EVENT



Meet our Publisher...

Gary S. Miliefsky, CISSP

THINK LIKE A HACKER, ACT LIKE A CISO:
ADOPTING RISK BASED METHODOLOGIES

Date	Wednesday 25 April
Venue	Principal Manchester Hotel, Oxford Street, Manchester, M60 7HA
Agenda	18:00 Welcome drinks reception 18:30 Speakers 20:00 Networking drinks and canapes reception 21:00 Finish



DON'T LET VULNERABILITIES WIN: PATCH IT SO IT HOLDS

by Jessica Dore

When it comes to car maintenance, we know how to keep ourselves safe on the road: have your breaks checked at regular intervals; get an oil change as recommended by the manufacturer; and if you have a hole in your tire, get it patched before it becomes a flat.

IT patches are similar in nature—essential repairs that keep your company's infrastructure up and running safely. Without them, computers and other devices are ticking time bombs, susceptible to data breaches, viruses and malware. Similar to a driver with a hole in their tire, IT security professionals should apply computer software patches to repair flaws and keep hackers out.

Even the most seasoned IT professionals should have a plan in place to keep up-to-date on patches, and keep their IT environment safe and secure. Here are four steps to get started.

1. Define your patch process

A variety of tools are designed to help track available patches for your operating system and third-party software. These tools will help you establish how often to patch, determine how to execute patches and even deploy the patches. Windows Server Update Services is commonly used to track patches for Windows operating systems, while SolarWinds is a popular tool for third-party software patches.

In outlining your patch process, you should also determine if you plan to conduct internal and external vulnerability scans. Vulnerability scans identify bugs in software. At Rehmann, we often run both internal scans—determining potential harm a disgruntled employee could cause, and external scans, taking on the role of an outsider who could try to access devices from the perimeter.

Determining a regular cadence for patch implementation is important, too. At the very least, patches should be implemented within 30 days of their release. Major software providers, like Microsoft, offer monthly roll-outs of available patches, while other providers may release patches once per week. Again, the tool you utilize to track patches will be critical in identifying what's available.

2. Prioritize your patches

Once your patch process has been developed, you should immediately work to identify any critical security patches. Providers will often share patches in order of importance and will even break protocol by issuing an immediate patch update for those of critical nature. Stay up-to-date on important patches and other issues top of mind in the industry by subscribing to and reading IT security publications. You may also choose to consult with an outside expert to make sure critical patches are always implemented in a timely manner.

3. Implement your patch process

With critical patches underway, it's time to put your patch process to the test. With any new patches, it's helpful to test them first to make sure they don't conflict with—or even break—any other programs on the network. Many organizations have test environments designed with this process in mind. If you do not have resources to conduct a trial run with patches in a test environment, research the patch online to see what issues may have already been identified by other users. Many IT professional forums exist as well and are a great resource on all aspects of the patch process.

4. Deep-clean your IT environment

Finally, you should deep-clean your IT environment. If you have any XP systems, Server 2003 systems or other obsolete equipment, it should be removed immediately. Systems like these, which are end of life, no longer receive patches and therefore present tremendous vulnerabilities to your entire IT infrastructure. Replacing obsolete programs can require a large monetary investment, but the system compromise that could result from not doing so is often far greater.

If you partner with an external IT provider, make sure they are conducting proper patching. Do your own spot-checking to make sure everything is as it should be, and even ask your provider for monthly reports, so you always know the status of critical patches.

This is also a good time to utilize your previously-identified vulnerability scan. You should also conduct a malware scan. While malware scans extend beyond the realm of patching, they're another asset to address any issues that could compromise the system. Available tools will clean the malware from your system.

Hackers work hard to find vulnerabilities in the systems we rely on every day, but it is possible to get out in front of them with the right patch process in place. Roll up your sleeves, take a look at your capabilities, and chart the path forward. Once you do, you'll be well-positioned for any potential compromises that come your way.

About the Author



Jessica Dore leads Rehmann's Technology Risk Management Group, overseeing cyber security assessments, information security assessments, vulnerability and penetration testing, social engineering testing, information security training and Sarbanes-Oxley Act (SOX) 404 consulting engagements for publicly-traded companies. Jessica provides information technology (IT)

consulting and security services to a wide range of clients.



RSA[®]Conference2018

San Francisco | April 16 – 20 | Moscone Center

At [RSA Conference 2018](#), [Cyber Defense Magazine](#) will be celebrating our 6th year as a media partner.

Thank you to the RSA Conference team.

Thank you to CDM readers!

“See you at RSA...”



HOW WILL THE 2018 GDPR CHANGES WORK?

From May 2018, EU member states will adopt new data privacy legislation known as the General Data Protection Regulation (GDPR), which will standardise and improve the regulation of data protection across participating member states. Here's a simplified guide to how data protection in the EU is set to change.

BACKGROUND TO THE GDPR CHANGES



The GDPR is a new piece of legislation which will be formally implemented in EU member states in May 2018, when it replaces all existing data protection law within participating countries.



The main reason for its implementation is the requirement to update existing data protection legislation, most of which has been in place long before social media became prevalent and the volume of data stored by businesses grew exponentially.



The GDPR changes are intended to give consumers greater control over how their data is used and it is hoped that consumer trust in the digital economy will be enhanced.



The changes will ensure a consistency across all participating EU member states regarding data protection legislation.

WHAT ARE THE 10 GDPR CHANGES?



TERRITORIAL SCOPE

The GDPR will now apply to any organisation which engages in data processing or control activities involving subjects within the EU, even if the organisation is based outside the EU, e.g. Far Eastern online advertisers targeting EU consumers.

ONE-STOP SHOP

The GDPR introduces a 'one-stop shop' where multinational companies are mainly regulated by the supervisory authority of their primary establishment, but other concerned authorities could also be involved in handling complaints against the company.



INCREASED PROCESSOR OBLIGATIONS

The GDPR imposes direct statutory obligations on data processors and subject to direct enforcement by supervisory authorities. Processors will be held liable for data protection breaches if they act outside the instructions of controllers.



IMPROVED RECORD KEEPING

Data processors will be required to keep detailed records of all processing activities and present these records upon request from the relevant supervisory authority.



TRANSPARENT PRESENTATION OF DATA

The GDPR will require data processors to present a greater deal of personal information to data subjects and to present it in a manner that is fully accessible and easily understandable.



DECREASED RELIANCE ON CONSENT

The GDPR raises the bar of consent from data subjects in that it must now be fully explicit, making consent less reliable as a legal basis for data collection. Data subjects can withdraw consent at any time and it must be easy for them to do so.





ENHANCED INDIVIDUAL RIGHTS

Data subjects will have enhanced rights, such as greater control over the processing of their personal data and a right to data portability.

BREACH NOTIFICATION

Data controllers must now notify the relevant supervisory authority of a data breach within 72 hours, unless the breach is unlikely to threaten the rights of data subjects. Processors are only obliged to report breaches to data controllers.



INTERNATIONAL DATA TRANSFERS

The GDPR removes the need for international data transfers to be pre-approved. It has also removed self-assessment as a basis for transfers, a move which is intended to improve uniformity across all participating members.

IMPOSITION OF STRICT FINES

The GDPR enables supervisory authorities with the power to impose severe fines for non-compliance with legislation – a potential €10 million or 2% of total global annual turnover for 'serious' offences and double that for 'very serious' offences.



WHAT HAPPENS NEXT?



The GDPR changes will be imposed into legislation effective as of 25 May 2018. From this date, the existing Data Protection Directive will be annulled.



While the GDPR will have a direct effect in all member states, national laws will need to be amended to regulate aspects such as the position of data protection authorities, transitional rules and the enforcement of additional regulations where granted by the GDPR.

Some nations (Germany, Netherlands, Poland) have already drafted national laws with necessary legislative changes incorporated.

Companies across participating countries are currently moving towards compliance with the GDPR changes, carefully taking stock of how it could impact on national data protection laws.

HOW CAN ORGANISATIONS PREPARE FOR THE GDPR CHANGES?



Implement clear policies and procedures so that they can react swiftly to data breaches.



Establish a framework for accountability by appointing a data protection officer, implementing clear policies and forging a culture of strict data monitoring.



Make privacy a core aspect of all processes within the organisation.



Establish the legal basis on which personal data is used – is there a heavy reliance on the consent of data subjects?



Ensure that data policies are transparent and easy to understand.



Anticipate dealings with data subjects over their rights such as data portability and erasure.



Check existing contractual documentation to see if it needs to be revised to include new obligations for data processing.



Ensure that there is a legitimate basis for transferring personal data to jurisdictions where data protection laws are inferior to that of GDPR participants.

REFERENCES

www.independent.ie/datasec/general-data-protection-regulation-gdpr-what-why-where-when-35519585.html

www.algoodbody.com/media/TheGDPR-Top10KeyChanges1.pdf

www.williamfry.com/newsandinsights/news-article/2016/06/08/key-impacts-of-the-eu-general-data-protection-regulation

www.allenoverly.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf



exigentnetworks.ie

CASE STUDY: NEIL DANIELL, INFORMATION SECURITY SPECIALIST AT PEOPLE'S BANCORP

Cyber attacks on the banking industry are growing more sophisticated, frequent, and dynamic. This includes risks from distributed denial-of-service (DDoS) attacks, viruses and malware, phishing, internal threats, exploitable vulnerabilities related to online and mobile device banking, and potential hacking breaches to obtain sensitive financial information.

It is therefore critical that banks and other financial institutions protect their networks, systems, and information from unauthorized access or disruption.

However, even today, most of the available cybersecurity offerings do not deliver the primary item on every information security checklist - true, continuous monitoring of all assets in real-time, without burdening the network.

“When you are responsible for cybersecurity for the banking industry, you always have to be concerned about what is coming next,” says Neil Daniell, Information Security Specialist at Peoples Bancorp. “We can try to be as preventative as possible, but for those things we don’t know are coming, we have to have resources available immediately ensuring our customers and employees are not affected.”

Cybersecurity Product “Noise”

Over the years, Daniell says cybersecurity has become an industry in which there is a tremendous amount of “noise,” with competing products and services making similar claims about the comprehensive nature of the protection provided.

A more realistic assessment of the available options is that for the most part, there are a handful of products and service categories that exist. Among these are traditional endpoint monitoring solutions, including SIEM (Security Information and Event Management) systems, along with other less comprehensive cybersecurity solutions.

Furthermore, traditional endpoint monitoring solutions often sell security consulting services with the software to maintain the system, interpret reports, and prioritize remediation. This drives up the overall cost and is a key profit center for the provider.

Daniell says that in the past 5-10 years he has seen many cybersecurity companies acquire others to fill in holes in their product offerings.

“A lot of companies realized that they didn’t have an all-encompassing security product, so they began acquiring other companies in the hopes that they could fill loopholes in their existing product offering and gain market share,” says Daniell.

Peoples Bancorp Continuous Monitoring

In business in excess of 115 years, Peoples Bancorp Inc. (NASDAQ: PEBO) is a diversified financial services holding company with \$3.6 billion in total assets with 75 sales offices including 66 full-service bank branches and 73 ATM’s in Ohio, West Virginia, and Kentucky.

In addition, the company operates retail, commercial, trust & investment services, and the Peoples Insurance Agency, LLC.

From an Information Technology (IT) perspective, the challenge is finding a way to incorporate the various disparate systems. According to Daniell, Peoples Bancorp is acquiring 8 additional locations in the next quarter that will need to be integrated into the existing systems. The challenge will always be incorporating all of the systems to work harmoniously as one.

For cybersecurity protection that extends to all these locations, Peoples Bancorp utilizes AristotleInsight from Sergeant Laboratories.

The comprehensive IT and security management platform combines several IT and security functions behind a single-pane of glass to provide insights, actionable items, and the data needed to properly manage and audit configurations, assets, user behavior, threat analytics, and risk.

Perhaps most importantly, the software meets the requirements of Continuous Diagnostics and Mitigation as outlined by the Department of Homeland Security.

The Continuous Diagnostics and Mitigation (CDM) program is the government’s approach to fortifying the cybersecurity of government networks and systems. This includes tools that identify vulnerabilities and risks on an ongoing basis, prioritizing those risks based on potential impact, therefore enabling network cybersecurity personnel to mitigate the most significant problems first.

“It is critical to have real-time monitoring to see exactly what is going on at any time,” says Daniell. “The software allows one to, at any moment, observe everything from keystrokes, to who is downloading information, or installing software. This is very important from an information security viewpoint.”

“If someone downloads a virus, that is not something you want to find out about on tomorrow’s report,” he adds.

The product collects security metrics down at the kernel level. There is so little burden on the network that, in fact, the system is typically not even noticed by network security or virus scanners while operating.

“What is unique about AristotleInsight is it is essentially an all-inclusive product that provides a lot of different functionality, gathers a lot of information, and has a relatively small footprint that doesn’t impact user access or response time,” says Daniell.

Within 24 hours of installation, the program is able to determine what is happening on the network, even with tens of thousands of computers involved. Within 48 and 72 hours, it will be clear if the network has been breached, if there has been illegal access, or if other issues exist.

Reporting and Remediation

One of the challenges, when a breach is suspected, is the ability to sift through the mass of information available. Therefore, the priority is to utilize a security platform that effectively analyzes, prioritizes and presents information in organized, understandable reports.

The AristotleInsight software prioritizes vulnerabilities and risks and then walks network administrators through the steps to remediate the problem.

The data is organized into an accounting double entry system developed in 1494 by Luca Pacioli, which provides forensic auditing capabilities. A unique Bayesian Inference Engine and data linking techniques are then used to interpret and prioritize the data.

The information is organized into 3-tiers of logical layers using a top-down approach. Specialized knowledge, training, or the help of security consultants is not required.

The reports are presented in an understandable format for management, while also providing more detailed information for security and compliance professionals to protect their organization.

“You can have 10 layers of information, but if no one is looking at the logs, it’s useless,” says Daniell.

Instead, he appreciates the ability to apply filters to the data to hone in on the most relevant information along with the ability to set alerts.

“The dashboard provides real-time information. Alerts and reports can also be set to trigger emails immediately or routinely (i.e. hourly/daily/weekly/monthly), depending on the type of issue or concern,” explains Daniell.

According to Daniell, Peoples Bancorp’s security posture has improved significantly since the software was implemented.

“Protecting our customer’s and company’s information is the top priority,” says Daniell. “AristotleInsight gives us peace of mind that we have implemented the necessary controls to help identify and resolve any issues that need to be addressed.

For more information about AristotleInsight call 866-748-5227; e-mail info@aristotleinsight.com; visit www.aristotleinsight.com; or write to 200 Mason St. #15, Onalaska, WI 54650.

SITELock RESEARCH: BUSINESSES SEE MORE EFFECTIVE WEBSITE ATTACKS IN Q4 2017

by Jessica Ortega, SiteLock

Throughout 2017, cybercriminals became increasingly sophisticated, expanding their craft to more complex and sneakier malware. In deploying more attacks that flew under the radar of unsuspecting website owners, they achieved their goal of maintaining access to infected sites for longer periods of time.

This isn’t good news for business owners as we move into 2018. Cyber threats are only going to increase in sophistication, so it’s imperative businesses understand today’s cybersecurity landscape and current website security trends in order to avoid falling victim to a breach.

Attack effectiveness is on the rise

According to the [SiteLock Website Security Insider Q4 2017](#), which analyzed more than 6 million websites, there was a 25 percent decrease in website attack volume from Q3 to Q4 2017. That should be good news, right? Wrong. Despite the decrease in attacks, sites still experienced an average of 44 attacks per day, or a whopping 16,000 attacks per year.

A decrease in attacks might make business owners think their website is more secure and their security efforts are paying off. However, this couldn't be further from the truth. Cybercriminals are constantly refining old tactics while exploring new ways to break into websites. As our research shows, this means cybercriminals are getting more effective and increasing their attack success rates. Now more than ever, businesses need to evaluate their current security practices and ensure they have both the right technology and a response plan in place should an infection occur.

Starting with the basics, like updating plugins and patching site vulnerabilities, is a solid first step to reducing the chances of a successful attack. However, updates alone aren't enough. Using more advanced tools, like a web application firewall, can help prevent attacks in real time.

Don't rely on search engines to catch malware infections

Malware is one of the biggest threats to websites, and too often business owners leave their fate in the hands of search engines to find the malware for them. While popular search engines perform basic website scans to protect users from malware-infected websites, the scans fail to flag most instances of malware. This is no fault of search engines, as the scan is done as a courtesy for website owners. Without knowing that search engines err on the side of caution when blacklisting websites, many website owners assume search engines will alert them if malware is found. Unfortunately, if a search engine finds malware on your site before the owner does, it means the site has been blacklisted and removed from search results.

According to our latest report, search engines only notified and blacklisted 19 percent of infected websites in Q4 2017, down three percent from the previous quarter. The report also found that 1 percent of the sites sampled were infected with malware each week. While this might seem like a small number, globally this means roughly 18.5 million websites are likely infected with malicious content at any given moment.

The ongoing challenge facing today's small businesses, is cybercriminals are using a variety of new and increasingly complex methods to infect websites. In Q4 2017, 51 percent of malware was encoded or randomly generated, which means these files were difficult to decode, but still detectable. Additionally, file manager and administrative shell scripts made up 6 percent of malware found, backdoor files accounted for 13 percent of cleaned files, and phishing kits accounted for 3 percent of malware during Q4.

As websites continue to be targeted from virtually every angle, business owners need to be prepared on all fronts to protect their website and their visitors. This means investing in the right tools to prevent and detect when an attack occurs.

No matter the size of the business or website, cyberattacks can happen to anyone. You might not think your website is a valuable target to cybercriminals, but even the smallest website can be targeted for its traffic, data, or to further the spread of malware. As the cybersecurity landscape continues to evolve with increasing more complex, sophisticated and effective attacks, website owners need to be proactive and take the necessary security precautions.

About the Author

*Jessica Ortega is a Product Marketing Specialist and Technical Writer at [SiteLock](#). She has over 10 years of experience in the website hosting and security fields, including two years as a SiteLock Security Analyst where she was responsible for cleaning malware infections and writing malware detection tools. She also co-hosts the cybersecurity podcast, *Decoding Security*.*

SMART HOME CYBER SECURITY



Smart homes are homes connected through the so-called Internet of Things (IoT). They have a number of smart devices and appliances that are connected to the internet, to each other, that can be operated remotely, or through smartphones and tablets.

This level of automation and technological upgrades of our houses and everyday lives has also improved our comfort levels and convenience in life. We tend to depend on technology a lot, and the number of smart homes and available gadgets is constantly growing.

This has, however, brought about new kinds of threats to our homes – cyber threats and risks, such as hackers. How exactly is your smart home at risk and what can you do to ensure proper cybersecurity for it? Find out and make your home security a top priority.

CYBERSECURITY RISKS: THE SOURCE OF THE PROBLEM

THE MARKET

When it comes to the security of all the smart, high-tech gadgets, devices and appliances that are released practically daily, it is not very often a top priority. The first source of the problem, therefore, would be the market itself.

The basic principle of any kind of market is supply and demand. It supplies as much as it can of what is currently in demand. And in that highly competitive process, sales rates and making a profit is what matters the most. So, the manufacturers and the market appeal to the consumer with the aesthetics of the product, its convenience, and many functions. Very often, they neglect to point out their level of security and safety.

Unfortunately, more often than not, security is not manufacturer's top priority. Making the products cyber secure is not what attracts consumers, and it is not what will sell the product. This leads us to the other part of the problem.

THE CONSUMER

As consumers, buyers of these [smart devices](#), we are a part of the market, as well as a part of the problem. We focus on the less important details of the product too often. Of course, design and functionality are very important, but security should always come first. As our way of life upgrades and changes, so do the security risks. They change and adapt to the circumstances.

The responsibility of the consumer is to ask a question and get informed about the product. You need to pay attention to details and get 'deeper' into the product. You need to know how secure it is or how to properly secure it against potential cyber

threats once you install it in your home. It should be specified on the product, or you can ask the salesperson.

WHAT CAN BE AT RISK AND HOW?

When making [home improvements](#) while moving, renovating or upgrading your home, the focus is nowadays primarily on making it a smart, connected and convenient home. Everything within reach, or better to say within a click, easily managed and controlled.

But there is another side to it as well. Everything that is connected to the internet, to your Wi-Fi, and that can be remotely controlled, can be a cybersecurity risk. Here are some examples of smart homes devices or appliances that can become a cybersecurity risk, and that may not have crossed your mind in this context.

SMART TELEVISIONS

Smart television sets can be used for some serious invasion of privacy. If hackers manage to get through to it, they can use the camera on the front of your TV, if you have one, and see everything that is going on inside that room. They can basically get a free live stream video of your movements and your house, which can lead to some more serious crimes.

SMART CARS

[Smart cars](#) are experiencing a surge in popularity in recent times. As with any other smart product, they bring about more convenience and functional upgrades. But they can also be in danger of cybersecurity threats.

When an increased number of the car's functions and commands is automated or connected to the internet, it makes it more vulnerable to hacker attacks. They can take over your system or commands and put you and your vehicle in great danger. That's why it is very important to protect your smart devices as much as you can.

HOW CAN YOU PROTECT A SMART HOME?

1. START WITH THE BASICS

The first thing you should do is get informed about the product before you buy it, research its security settings or ask the salesperson at the spot. Make sure to know

what the risks are, how you can prevent them if you can upgrade your security and how to use it safely.

Add passwords to all of your devices and controls, and make sure that they are strong and not something obvious such as birthdays. Always change the product's default password, the one that is preset by the manufacturer.

2. SECURE YOUR NETWORK

Securing your Wi-Fi network to which everything in your house is connected is very important because it protects your private information. Your network is best protected by the WPA2 (Wi-Fi Protected Access II) encryption protocol, so make sure to activate it. The most common protection protocol is still the Wired Equivalent Privacy (WEP), but it is weaker and more easily breached.

3. CREATE MULTIPLE NETWORK IDENTITIES

If you can, and depending on your router's capabilities and your gateway, it is recommended to create two or more network identities, or SSIDs. If you don't know how to do it yourself, ask a friend with a bit more expertise. You can then use one identity for all the online and banking transactions, and the other for the rest of the devices and more general online activity.

4. INSTALL FIREWALL AND SECURITY SOFTWARE

[Firewall](#) is what protects your network from outside threats by restricting incoming connections that may harm you or steal your information. Every network should have one. It is recommended to set it up in the way that it allows traffic only on ports that are specific to your devices.

Apart from that, make sure you always have the latest security software on all of your smart devices, as well as the control devices such as phones and tablets. This makes it harder for the hacker to take control.

CONCLUSION

As much as we deem important to keep up with the latest trends in technology, it is as important, or even more so, to keep up with the possible cybersecurity risks. Information is key here, and knowledge is power. To know how to defend yourself and provide the best security for your home, it is important to know what you are faced with. If you follow

these tips, take proper steps and precautions, you can enjoy all the benefits a smart home brings while being safe and secure.

About the Author



Matthew James is a freelance writer specialized in home improvement, smart technology, architecture & design.

He has a love of outdoors and spending time with his dog Cooper. You can reach him on [Facebook](#) and [Instagram](#).

DEMYSTIFYING THE SOURCE CODE VS. BINARY DEBATE

by Taylor Armerding, security consultant, Synopsys

Is exposure of software source code disastrous enough to merit a meltdown?

Based on a couple of incidents in the last few weeks, you might think so. The first was portrayed as major tech companies handing tools to the Russians to spy on the US. The other was termed by one researcher as, “the biggest leak in history.”

But those views are not unanimous. Other voices in the IT security community are declaring that everybody ought to take a chill pill.

Both events generated plenty of media coverage, however. It started with [Reuters reporting a couple of weeks ago](#) that major tech companies have allowed Russian authorities to inspect the source code of their software – the same software used by at least a dozen US government departments including Defense, State, NASA, the FBI and other intelligence agencies.

The second round came this past week, with word that an anonymous “someone” (later reported to be a former Apple intern) had posted the “iBoot” source code from Apple’s iOS 9 on the open-source code repository GitHub – a disclosure that Jonathan Levin, author of several books on iOS and OSX, [told Motherboard](#), qualified as, “the biggest leak in history.”

Which seems a major stretch. Bigger than the [breach of the US Office of Personnel Management \(OPM\)](#), that compromised the personally identifiable information (PII) of

more than 22 million current and former employees? Bigger than the [Equifax breach](#), which exposed the PII and credit history of about 145.5 million people?

Perhaps a “leak” is considered different from a “breach,” but for there to be a leak, there first has to be a breach, even if it’s committed by an insider.

So, let’s take them one at a time. Reuters reported that tech companies – SAP, Symantec, Micro Focus and McAfee – had permitted Russian authorities to inspect their source code before using their products.

According to the companies, Russia just wanted to make sure the code didn’t have backdoors or defects that could allow hackers into their systems. They added that those inspections were done under tightly controlled conditions, with not even a pencil allowed in the room.

Still, US government officials and several security experts said that allowing a prospective customer to inspect software source code put the US at risk.

A [Dec. 7 letter from the Pentagon](#) to Sen. Jeanne Shaheen (D-NH) said that allowing governments to review the code, “may aid such countries in discovering vulnerabilities in those products.”

But Gary McGraw, vice president of security technology at Synopsys’ Software Integrity Group, branded those warnings “ridiculous.”

McGraw, who initiated a [lengthy debate on Twitter](#) about the issue, says he is not advocating handing over proprietary source code to anyone who wants to inspect it, because it would put intellectual property (IP) at risk.

But he said when it comes to defects that can be exploited for cyberattacks or espionage, access to the source code is no more dangerous – likely less so – than access to the binary code, which is created from the source code and is sold along with the commercial product that results.

“You sell them (customers) the binary,” he said, which means all customers can inspect it for exploitable defects at their leisure.

McGraw contends that the source code scare is simply unwarranted FUD – fear, uncertainty and doubt – that has tended to reappear every few years for the past two decades.

“The myth is that having source code out there is somehow way more dangerous and exposes you to attackers in a way that having binary out does not,” he said.

“Software exploit can be and is accomplished with binary only all the time. In fact, some attackers, and white-hat exploit people, argue that having a binary is better than having source when it comes to exploit development.”

The Reuters story didn't even mention binary. But McGraw said the confusion between the two allows, "unscrupulous vendors to produce FUD and get coverage.

"The programs that the Russians were reviewing were programs whose binary is widely available commercially," he said. "The fact that it was the source code being reviewed doesn't put any other customer, including the US government, at any greater risk."

So, does that same logic apply to Apple and users of its older iPhones? Should they just chill, since they aren't at any increased risk from the GitHub post? As has been reported extensively, the leaked code is old – from two versions ago.

That was the basic message from Apple itself, which issued a statement to Motherboard that, "old source code from three years ago appears to have been leaked, but by design the security of our products doesn't depend on the secrecy of our source code.

"There are many layers of hardware and software protections built in to our products, and we always encourage customers to update to the newest software releases to benefit from the latest protections."

Security researcher Patrick Wardle essentially agreed. [He told Mashable](#) that having access to code does not necessarily make a well-designed OS less secure, noting that Linux is quite secure despite being totally open-source.

And, like McGraw, he added that good hackers, "don't need access to source code – they can reverse a binary and find bugs."

Still, the leaked code is the part that is responsible for ensuring a trusted boot of the operating system. And, obviously, it wasn't exposed only to selected people who weren't even allowed to bring pencils into a room. It was out there for anyone to grab.

While Apple issued a takedown order under the Digital Millennium Copyright Act (DCMA) hours after the Motherboard story appeared, about the only thing that did was confirm that the code was legitimate. By then it had spread far beyond GitHub.

Another reality is that not everybody updates their software. According to [Apple's own estimate](#), about 7 percent of iPhone and iPad owners may be using iOS 9 or earlier. And with about a billion devices out there, that means a potential attack surface of 70 million devices.

Still, it seems that if anybody is at risk in this case, it would be Apple itself, since the source code is its proprietary IP, and access to it might make it easier to jailbreak the OS and use it on non-Apple devices – something the company ferociously tries to prevent.

That is McGraw's take. "The thing that makes this story interesting is that it's a bit of an embarrassment for Apple who has guarded their IP so rigorously," he said. "And yes, it could make jailbreaking easier."

John Kozyrakis, research engineer at Synopsys, said that access to the iOS source code might also make it a bit easier for those looking for defects in the binary code.

“Unlock mechanisms are used by three main groups,” he said. “For legitimate forensic tools, malicious exploit tools for targeted attacks and jailbreak tools.

“The release of this source could help ongoing efforts to use iOS on generic, non-Apple hardware or emulators, which has not been possible so far, and is restricted by Apple.”

But Amit Sethi, a senior principle consultant, also thinks the leak, “should have little impact.”

He said even if it does expose some defects in Apple iOS source code, “we’ll end up with more secure devices in the long term, as Apple fixes the discovered vulnerabilities.”

For customers and users, he said, it should be a reminder that, “people should design and implement systems – especially client-side components – so they don't rely on their source code being secret.”

Beyond that, as McGraw has been saying for more than a decade, the threat of exploits from the exposure of source code can be minimized by building security into it from the start.

“During development, source code can and should be reviewed by a static analysis program,” he said. “When you find a bug in source code, it is easier to fix, since you know where in the code it is.”

About the Author

Taylor Armerding is an award-winning journalist who left the declining field of mainstream newspapers in 2011 to write in the explosively expanding field of information security. He has previously written for CSO Online and the Sophos blog Naked Security. When he's not writing he hikes, bikes, golfs, and plays bluegrass music

About the Synopsys Software Integrity Platform

Synopsys offers the most comprehensive solution for building integrity—security and quality—into the software development lifecycle and supply chain. The Software Integrity Platform unites leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop personalized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in application security testing, is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. For more information, go to www.synopsys.com/software.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.



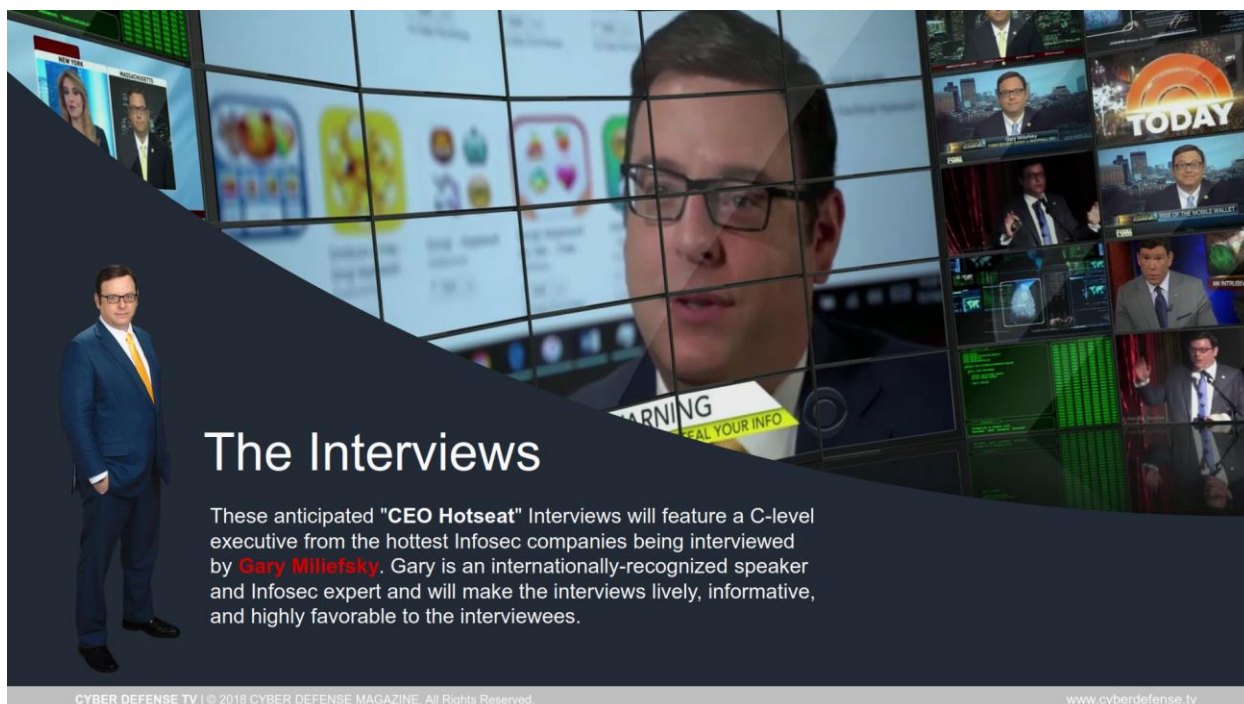
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

You asked, so we're doing it! Coming in Q2, 2018, we're launching CyberDefense.TV

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

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



The Interviews

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

CYBER DEFENSE TV | © 2016 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

TYPES OF DDOS AND HOW TO PREVENT FROM DDOS ATTACKS

In today's world, the volume of cybercrime has been increased significantly. The biggest challenge most individuals and companies are facing is, how to fight against DDOS attacks? For the sake of security, there are thousands of DDoS in the market to accommodate this issue and help the victims wisely. The Whole big slot has been categorized into few parts to make it short, simple and concise.

There are few different types of DDoS attacks that will be cover over here. As far as their characteristics are concerned, they are similar but at the same time slightly differ from each other. By considering their characteristics and features, all are now fall under mainly three parts or categories that are going to discuss:

1. Volumetric Attacks:

It is one of the most common category among the other two ones. According to [Arbor Networks](#), its percentage rate is about 65% of the total. In it, the attacker send millions of traffic on the website so that it stops running its functions properly for few seconds. As a result of this, the user will be unable to access the website hence, the server goes down.

2. Portal Attack:

First of all, the attacker is in hunts to find the weakness or flaws in layer 3 and layer 4 of protocol stack and after that he consumes all processing capacity of the target or audience. Ultimately, the audience will not be able to reach on the website.

3. Application Attack:

Among all, it is one of the most sophisticated as well as most challenging one to recognize. Firstly, the attacker figure out the deficiency in layer 7 by creating a connection with targeted audience and then over-exercise the specific feature. Due to this act, the function becomes disable and stop working. In this way, drive benefit from it.

This is how hackers take revenge from you and sometimes in return they get nothing but just the satisfaction of revenge, whereas, sometimes they get paid from the rivals. All in all, the victim will ended up with significant loss in different manners including monetary and non-monetary aspects.

Nowadays, the competition is so high in terms of technology, the need of protection is arises so that survival can be done correctly. By considering the fact, most of companies offering basic level of DDoS protection to the website of their customers. But one size doesn't fit all, just like one basic level of protection is not appropriate for all websites. Few websites have less traffic whereas as few have more. Now the question has been arises that how to cater it successfully? Well, it's easy, just need to know the procedure and do accordingly. The first step is, need to know the average amount of traffic a website has then design a protection of DDoS attack accordingly. The edge you will get is to avoid extensive downtime and other stuff.

There are a number of ways to prevent DDoS attack from hackers, few of them are listed below:

- Implement the filters so that the noisy or unusable messages get filtered out.
- You should disabled your network services when there isn't required.
- You need to maintain your backups so that if any mishaps occur you will be in a position of cope up.
- Use the best ddos protected protected [VPN](#).

- Use password policies to secure even more.
- If you find some hints of DDoS attacks then there is a high chance to [effects your ISP provider](#), so make a call and confirm it before the situation gets worse or out of control.
- Always prepare with incident resource plan.
- You must have the systems who detect any sort of attack.

About the Author

Susan is a small business owner, traveler and investor of cryptocurrencies. She is just another creative writer helping to create the kind of information that young people want.

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.](#)



CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY OPERATIONS

eMAGAZINE

IN THIS EDITION:

NEVER STOPS GIVING

IT'S FREE

SUBSCRIBE TODAY! NO STRINGS...

InfoSec Thoughts for 2018
Network Traffic Insecurities
Endpoint Security Best Practices
Vulnerability Equities Process

CELEBRATING 5 YEARS OF PUBLICATION

DECEMBER 2017 MORE INSIDE!

MARKETING AND PARTNERSHIP OPPORTUNITIES

BANNERS, E-MAILS, INFOSEC AWARDS, DOWNLOADS, PRINT EDITIONS AND MUCH MORE...



CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY OPERATIONS

ANNUAL EDITION - RSA Conference 2018

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY OPERATIONS

2018 PREDICTIONS

CYBERSECURITY TRENDS

REQUIRE YOUR IT BODILY TO PREPARE FOR THE FUTURE

Download

MediaKIT
Special Annual Edition
RSA Conference 2018

Email: marketing@cyberdefensemagazine.com
Call us Toll Free (USA): 1-833-844-9468
International: +1-603-280-4451 M-F 8am to 6pm EST

CDM | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefensemagazine.com

Copyright (C) 2018, Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC. PO Box 8224, Nashua, NH 03060-8224. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com Cyber Defense Magazine, CDM, Cyber Defense eMagazine, Cyber Defense Test Labs and CDTL are Registered Trademarks of STEVEN G. SAMUELS LLC. All rights reserved worldwide. Copyright © 2018, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

JOB OPPORTUNITIES

Send us your list and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

PO Box 8224, Nashua, NH 03060-8224.

EIN: 454-18-8465, DUNS# 078358935.

All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

Our New Office Addresses coming soon: **NEW YORK** (US HQ), **LONDON**, **HONG KONG**

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 03/30/2018

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION



**MEET OUR PUBLISHER:
GARY S. MILIEFSKY
@ RSA CONFERENCE 2018**

CYBERSECURITY EXPERT - FREQUENT SPEAKER - MEDIA TALENT