CISO MAG

beyond cybersecurity

Volume 1 | Issue 3 | November - December 2017

CLOUD FORECAST: THUNDERSTORMS AND LIGHTNING

RAPID7

From the CISO Perspective to Cloud Security Assessments

Learn How to Make the Leap With Confidence

The secret is out:
Enterprises large and small have moved to the cloud, and more are making the move daily. Whether you're an early adopter or you've been battling that persistent strain of nephophobia going around, it's important to thoroughly understand and evaluate potential cloud vendors, instilling confidence for your organization and your customers.

Download our Cloud Security Toolkit to help you evaluate potential cloud vendors.

http://bit.ly/2ivU4I9

Get insight into how other companies are approaching cloud opportunities, and instill confidence across your organization today.

INDEX

BUZZ
Space Wars: The Last Frontier 06

UNDER THE SPOTLIGHT
Few Minutes with Kevin O'Leary 12

COVER STORY
Cloud Forecast: Thunderstorms and Lightning 18

INSIGHT
M&A Cyber Due Diligence: A Critical Factor during Transactions 26

VIEWPOINT
MSSP Shopping: Use Your Corporate AMEX Wisely 30

KNOWLEDGE HUB
Cybersecurity Talent Gap: Is There One? 36

TABLE TALK
Interview with Richard Rushing 40

IN THE HOTSEAT
High-Profile Appointments in the Cybersecurity World 46

KICKSTARTERS
Startups Making Waves in the Cybersecurity World 50

INFOSEC PARTNERSHIPS
Famous Collaborations in the Cybersecurity World 56

EVENT FOCUS
A Curtain Raiser to Second Fintech Security Summit 62

IN THE NEWS
Top Stories from the Cybersecurity World 64

PROFILE
Global CISO Awards 2017 70

TECH TALK
Shadow IT: Blending Innovation with Risk 74

EDITOR'S NOTE

The world is witnessing a paradigm shift in terms of data storage. As each day passes, organizations are exploring new ways to exploit cloud storage solutions, leveraging IaaS, PaaS, and even SaaS mediums. The adoption rate at present is at an all-time high. The number of organizations gaining competence and advantage through cloud utilization has doubled in the past couple of years and is expected to skyrocket in future. Cloud storage solutions are touted to be advantageous in terms of usability, bandwidth, accessibility, cost savings, and even disaster recovery.

But a wide open network perimeter has given chief information security officers sleepless nights. In the last couple of months, we have all read about poor configuration in S3 buckets resulting in massive leaks. In our cover story, we explore the hurdles faced by CISOs in handling security in a cloud environment, as well as exploring cloud bursting opportunities.

In our Buzz section, we discuss the impending threat of space hacking, where satellites orbiting around the planet turn into threat vectors. We also discuss several scenarios that have already occurred and how several state-sponsored actors are honing their skills in this new realm.

We have Kevin O'Leary, CISO of GE China, Under the Spotlight for this issue. O'Leary shares his insights about the new and controversial China Cyber Law and how seriously the nation is taking cybersecurity. We also interviewed Richard Rushing, CISO of Motorola Mobility. Rushing, who is also known as a 'Wi-Fi Guru', speaks about Wi-Fi security and other cybersecurity issues.

Tell us what you think of this issue. If you have any suggestions, comments or queries, please reach us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief

CISO MAG
beyond cybersecurity

Volume 1 | Issue 3
November - December 2017

Editorial
International Editor
Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

Senior Feature Writer
Preeti Panwar
preeti.p@eccouncil.org

Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Design Head and Visualizer
MSH Rabbani
rabbani@eccouncil.org

Designer
Jeevana Rao Jinaga
jeevana.j@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Senior Director,
Compliance & Governance
Cherylann Vanderhide
cherylann@eccouncil.org

Marketing & Sales
General Manager
Meghana Vyas
meghana.vyas@eccouncil.org

Marketing Manager
Jinu Francis
jinu.francis@eccouncil.org

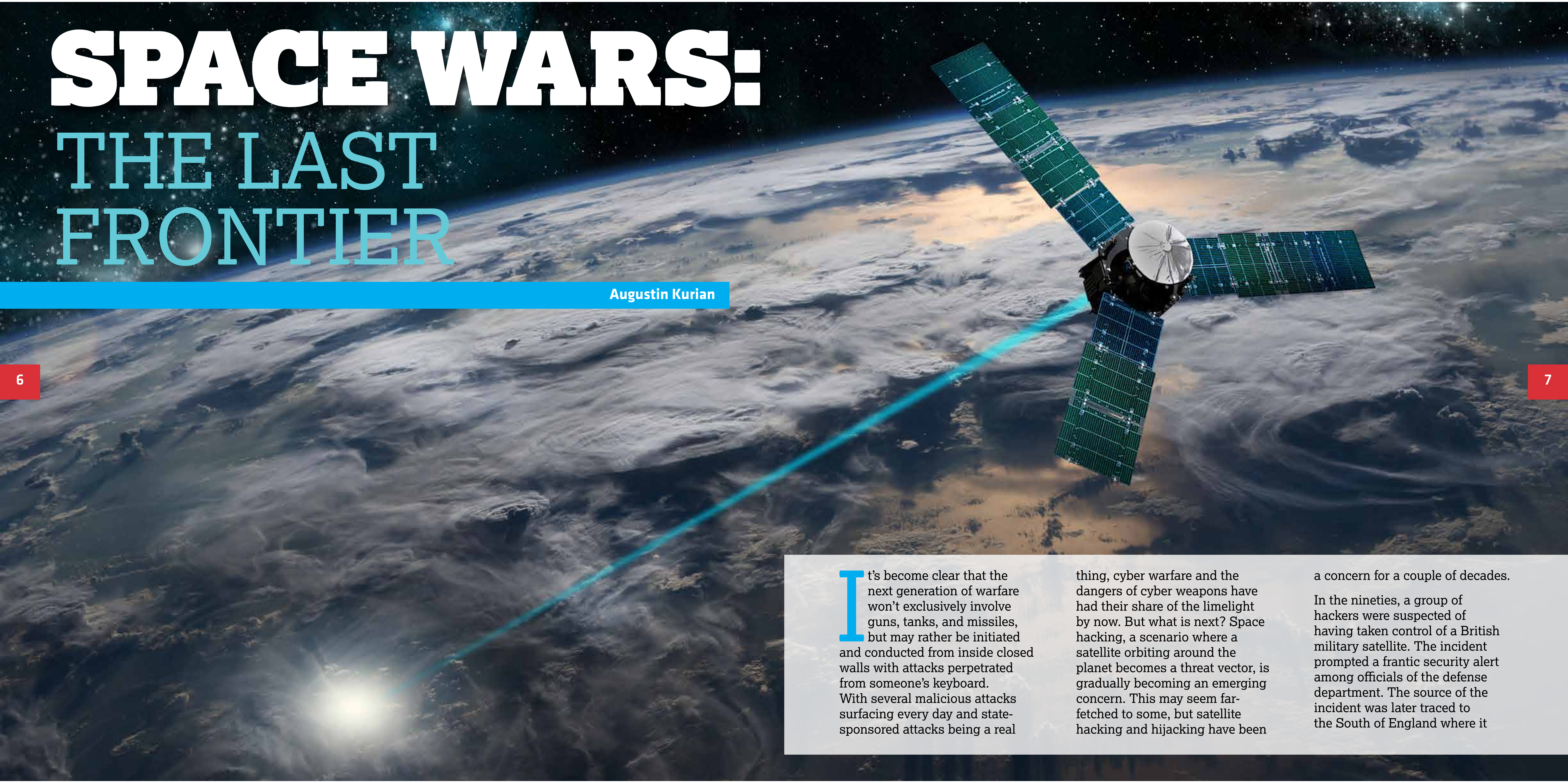
Sales Manager - India
Basant Das
basant.das@eccouncil.org

Sales Manager - North America
Jessica Johnson
jessica.johnson@eccouncil.org

Technology
Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Rahul Arora.

The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & may not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged.



SPACE WARS: THE LAST FRONTIER

Augustin Kurian

It's become clear that the next generation of warfare won't exclusively involve guns, tanks, and missiles, but may rather be initiated and conducted from inside closed walls with attacks perpetrated from someone's keyboard. With several malicious attacks surfacing every day and state-sponsored attacks being a real thing, cyber warfare and the dangers of cyber weapons have had their share of the limelight by now. But what is next? Space hacking, a scenario where a satellite orbiting around the planet becomes a threat vector, is gradually becoming an emerging concern. This may seem far-fetched to some, but satellite hacking and hijacking have been a concern for a couple of decades.

In the nineties, a group of hackers were suspected of having taken control of a British military satellite. The incident prompted a frantic security alert among officials of the defense department. The source of the incident was later traced to the South of England where it

was found that hackers found a way to control the satellites and change “the characteristics of channels used to convey military communications, satellite television and telephone calls.”

During an interview with *NBC News*, Jeff Matthews, Director of Venture Strategy and Research at the Space Frontier Foundation, said, “Space allows for some very unique business-use cases and opportunities, and when done right, can really go a long way to protecting communication interests and national infrastructure. However, we have to be very aware about the information security side up in space and down here.”

> Space allows for some very unique business-use cases and opportunities, and when done right, can really go a long way to protecting communication interests and national infrastructure. However, we have to be very aware about the information security side up in space and down here.

A recent Chatham House paper pointed out that cybersecurity in space has remained unrecognized as a potential vulnerability. According to the paper, there is an “increasingly blurred line between ‘offensive’ and ‘defensive’ activities in cyber and space, given that, technologically, the offence is easier and more cost-effective than defence.” It further stated, “More advanced countries are increasingly vulnerable to attack from less developed states, and from terrorist groups and other actors such as organized criminals. In addition, the technologies for the space sector are developed and sourced from all over the world; the space supply chain can, therefore, be considered a truly internationalized business environment that is not yet well regulated with cybersecurity in mind.”

While the approach of many governments to cybersecurity is becoming more effective, the paper warned that “the conjunction of cyber and space remains vulnerable to exploitation in the context of complex and internationalized supply chains and space-related infrastructure.”

Reports have also suggested that hacking a satellite is a rather easy task. At the Chaos Communication Camp (a security conference) in 2015, hackers Sec and Schneider demonstrated “how to eavesdrop on Iridium pager traffic using the Camp badge” in their presentation titled ‘Iridium Hacking: please don’t sue us.’ The Iridium satellite network, developed by Motorola, consisted of 66 active satellites in low Earth orbit and was a highly vulnerable vector. The hackers said “The problem isn’t that Iridium has poor security. It’s that it has no security. With just the radio and an onboard PCB antenna, you can collect 22 percent of all the packets you can receive with a proper Iridium antenna. You just load the software on your PC, you attach the radio and you can start receiving Iridium pager messages.” They also pointed out that the largest user of the Iridium network was the Pentagon.

Satellite hacking has caused enough uproar that former Chief Information Security Officer of NASA, Jeanette Hanna-Ruiz, prioritized cyber attacks as one of the agency’s top concerns. “It’s a matter of time before someone hacks into something in space. We see ourselves as a very attractive target,” she stated in an interview with *Bloomberg*.

Among her key concerns was a rogue agency or a hacker group trying to disrupt communication between NASA and its spacecraft that transmits research data. “There could be a company that wants it, there could be a nation-state that wants it,” Hanna-Ruiz said. The challenge, she said, is, “How do I harden these streams and communications flows?” She was clearly worried about a direct cyber attack on a satellite that would allow adversaries to commandeer the controls of the satellites. The apprehension is also among the military. Even though the U.S. Air Force and Missile Systems Center is confident that its own spacecraft are securely encrypted, its major concerns are about the “vulnerability of commercial satellites that host military payloads.”

The agencies have also contracted Innoflights, a company that specializes in information security for spacecraft. Innoflights have subcontracted with commercial satellite firm SSL to “develop a high-fidelity simulation environment for testing the security of hosted payloads on commercial satellites," as reported by *Spacenews*.

According to Al Tadros, Vice President of Space Infrastructure and Civil Space at SSL, the project might be a major opportunity for the government to increase the deployment of commercial space technology as well as meeting with the standards of military-level cybersecurity. "The government wants a level of security for payloads that are hosted on commercial satellites. It's a reasonable thing. But it hasn't been developed previously," Tadros said. "Security is one element of resilience, and hosted payloads are part of the solution for increased resilience."

According to experts, the main problem is that space observers often assume that the threat to satellites comes from a direct kinetic attack. But the most probable assault would be through jamming satellite signals. This brings us to the next challenge in space warfare: Global Positioning System (GPS). This technique came to fore after reports emerged that Russia might be testing systems that can interfere with GPS signals by overriding them with fake ones.

It all began on June 22, 2017 when the master of a ship off the Russian port discovered that his GPS had pointed him 25 nautical miles inland near Vnukovo Airport. He reported to the U.S. Coast Guard Navigation Center. When the coast guard contacted other nearby ships, it was found that all their automatic identification system (AIS) pointed to the same location at the Vnukovo Airport, affecting nearly 20 ships traversing the Black Sea.

This was not the first time when GPS spoofing was effectively deployed. In 2013, students of University of Texas sent an $80 million yacht off course by using a custom-built GPS spoofer. The students, with owner's permission, misdirected the yacht by mimicking the GPS signal. "The yacht's on-board navigation system detected the (fake) signal and used it as a triangulation point; no alarms were triggered, and the crew obeyed their computer and changed course," stated a report in *The Verge*.

At present, space may seem like an untouchable realm. But what many fail to understand is that the systems that we have in place are outdated, and that means they are increasingly vulnerable to cyber threats.

Hackers are evolving their methodologies, creating a future in which the possibility of hacking a satellite and crashing into specific targeted locations is a real threat. It's an urban legend that if you drop a penny from the top of The Empire State Building it can kill a person below, but a three-ton satellite crashing down from outer space could become a very real scenario. It would be nothing short of a weapon. For now, that may seem implausible, but there is an impending threat and it needs to be addressed.

FEW MINUTES WITH KEVIN O'LEARY, CISO, GE CHINA

Rahul Arora

On June 1, 2017, the People's Republic of China ushered in a new cybersecurity law that requires companies to store user data within the country and submit to regular spot-checks on their network operations. While the Chinese government endorsed the law as a milestone in data privacy regulations, critics feared that the new regulations were vague and would leave multinational companies vulnerable to industrial espionage.

Five months later, CISO MAG tries to understand how the new law impacted multinationals in China and the efforts these companies are putting in to complying with it. We got in touch with Kevin O'Leary, Chief Information Security Officer, GE China, who gave us some insight into the law and its effects.

In his role at GE China, O'Leary advises the global and local leadership on security and risk as aligned to business strategy within China and other growth regions globally. As the new cybersecurity laws came into effect in China, O'Leary was asked to update the GE board on the implications for GE's operations in the country.

> This is a brand new law that is just beginning to be understood by China itself. There will be constant changes in the future and updation that will happen. So there is still a lot to be done. From operations point of view, we have been continuing to work in China like we used to do, but we are also looking on the kinds of effect it will have on the future

Tell us a bit about your role and responsibilities in GE Digital.

I actually don two hats when it comes to GE. I am the Chief Information Security Officer for Greater China and Mongolia. I also serve as the GE Regions leader, which basically means that I have a team that spans the globe from Tokyo to Sao Paulo and everywhere in between excluding the United States.

We are the regional face of GE cybersecurity. Because of the vastness of GE, we have an IT security organization that manages cybersecurity from several locations in the world. We don't have IT security personnel in every country, but certainly at a regional level, we need to have some sort of a presence, and because China is such an enormous market, GE regards it as a region.

The Regional Cyber Security Officers for GE act as the frontline in our respective regions for local IT risk and cyber issues and regulatory affairs. We are here to ensure that our security toolset is properly applied across the globe and protects GE.

The second part is really for our business units, in terms of their product security and how they sell product within their particular region. We are able to meet with customers locally at their headquarters to discuss with them any concerns they might have with respect to cybersecurity. So, we act as a support function for business units when it comes to cybersecurity on the ground in the regions if this is something a customer wishes to examine with GE.

The third part is in terms of the OT security products that we sell. GE works extensively within the domain of the industrial internet of things and the convergence between traditional IT, OT, and industrial control systems. The manner in which these are becoming increasingly unified and integrated is something GE has been considering for many years now.

Let us talk about the National Cyber Law that was implemented in the country in June 2017. Did it have a direct impact on GE? What did GE do to prepare or comply with the new law?

I think it makes more sense to talk about this in terms of how any multinational firm trying to operate within the Chinese market is having to adjust. It is having an impact, at least on the planning and strategic point of view, as it would have been for any other multinational firm here. In terms of complying with the law, I think we have to understand how it is being implemented. Even though it came into effect in the beginning of June, the real implementation has been quite a soft implementation, and the government has really been working through the practicalities surrounding enforcing the new laws.

In terms of compliance for multinational companies, there hasn't been an immediate impact. We have been preparing for well over a year and a half on what might be affected due to any change in regulation that came about by reviewing the early drafts of the cyber law that came out last November. And throughout this current year, we have been driving a deeper understanding of the effects of the law and how it would be applied.

I think the effect now is how we prepare for the gradual implementation of the law, and the actual enforcement. There are a few key stages to that, in terms of the timing and we have some indications from discussions with the testing agencies engaged by the government in terms of what they are looking for with regards to compliance. Because of this, we have been able to plan accordingly in terms of the localization and certification of data.

So, look at it this way, this is a brand new law that is just beginning to be understood by Chinese companies and institutions themselves, add to that the possibility that there will be adjustments to the regulations over time. From an operations point of view, we have been continuing to work in China as normal, but we are also looking to the future and the operational changes we may have to make.

From outside of the country, it feels like there is not much awareness of the law among companies. Did the Chinese government ensure that there was enough awareness of the law before it came into effect?

The way it works in China is that any new regulation or any new law is sent out for consultation to Chinese and foreign businesses operating here, often through the different chambers of commerce. GE was engaged and well aware of the law as it went through this notice and comment phase.

I think the issue is not if the message was well circulated, it is more about the nature of the early drafts of the law, it was really a framework and the details such as the definition of private information, sensitive information, etc. These weren't well defined in the early drafts of the law and are only now really beginning to crystalize.

The regulatory bodies for the different business sectors are beginning to come out with detailed regulations a requirements that fall within the framework of the cybersecurity law and this has clarified how these elements of the law should be interpreted.

I think it is at three levels: One, which is the protection of the Chinese citizens on their personal data and information; second is in terms of sensitive information for national security, and then the third part is data, operations and security of companies that is important to them.

Are there any frequent operational hurdles or additional costs that companies face due to the new law?

What we are focusing on are data flows into and out of China, and what are the operational impacts in terms of localizing some of that work. Because as a multinational, we depend on global supply chains much of the infrastructure surrounding that includes the movement of data across borders. However, the most important thing is to operate transparently with the Chinese government.

Through building transparency, you have an opportunity to look at it pragmatically in terms of what is really important for the Chinese State and Chinese citizens, and our obligations as a responsible international company to abide by the laws of the countries where we operate.

Before the law was implemented, there was a concern that Chinese will soon have a strong legal basis to access foreign companies' data. How real is this concern now?

Whether to do with legal basis or not, I believe the government here is really concerned with transparency, whether it is commercial or otherwise. We all need to accept that this is now law. I think the law formalizes something that was more ad hoc previously.

Does this make it harder for international companies? I don't think it makes it any worse for the security of data that we hold in our networks. I think it has made it harder and costly simply because of the need to localize data. But that was the consequence and not the aim of the law. And this concern and approach is not unlike other countries.

Do you think the law is unfair to non-Chinese companies?

You have to look in two ways. On one side, a lot of laws that are implemented in here are not any different from what India has implemented, or Malaysia or any other country for that matter. In a way, you can say that the government of China has every right to implement these laws. On the other hand, what many don't see is that many Chinese companies find it hard to break into global markets and as a consequence, they already operate within the Chinese state and don't face the same issues with regards to localizing data, etc. This operational change and investment probably doesn't hit them the same way as it does international companies.

But I don't think that is done intentionally. You have to look at it in terms of sovereignty. If the government and people want to protect their data then that is what it is going to do and that is we have to deal with accordingly.

The Chinese government is ensuring sovereignty of data – this is not unique to China and we can see many other countries acting in the same way.

Do you think setting of cybersecurity standards should be government driven or industry driven?

I think there needs to be a benchmark, and that benchmark should be established by the government. But what really drives the development of cybersecurity is the bottom line. It is what customers and business partners demand. So, if a customer wishes to engage GE, then they want to be certain that we have a minimum of cybersecurity standards in place. It is what is expected by partners and customers, and rightly so. In short, we need government regulation and business drivers to drive excellence in Cyber together.

What are the long-term effects of the law you can foresee?

There is going to be a financial impact for multinationals operating in China. This will be both on OpEx and CapEx. Companies will need to invest capital in the initial compliance with the law and factor ongoing certification maintenance costs into their operating budgets. Beyond that, once the corrections have been baked into the operating model, things should normalize. The need for cybersecurity and compliance teams within Chinese companies will grow, and this is a positive impact of the new law.

CLOUD FORECAST:

THUNDERSTORMS AND LIGHTNING

Augustin Kurian

If the cloud is the ultimate data storage solution remains a hot and widely debated topic. Each day, more organizations are unplugging their data centers and moving to cloud storage for various reason that include cost reduction and security. But cloud itself can also pose several major vulnerabilities and may at times be a threat vector itself, with problems originating from home devices and hard disks. These may be regular system vulnerabilities that can be fixed with basic IT processes, and cloud may also help organizations recover data from accidental deletes and overwrites. If history has taught us anything about new technology, it is that migrating to the cloud poses very real challenges.

In the past few years, several high-profile breaches of cloud providers have been reported. One of the notable ones is the Distributed Denial of Service (DDoS) Mirai botnet attack on Dyn, a company that controlled several domain name system (DNS) infrastructures. Experts called the breach “likely the largest of its kind in history.” Vulnerabilities in cloud security have also become a huge ordeal for companies. For example, the string of ransomware attacks on MongoDB databases left roughly 27,000 servers compromised. The incident occurred after older databases were left in default configuration settings.

Unfortunately, in the latter incident, most victims were not able to get their data back. “There is only 1 out of the 8 MongoDB ransom groups that actually “SAVES” your database to another host - We only don’t know WHO from the 8,” tweeted cybersecurity expert and Chairman of GDI Foundation Victor Gevers post the incident. The GDI Foundation also tracked close to 175,000 cases of misconfigured software and services on the cloud this year. These cases and incidents highlight the need for security in the cloud and the challenges in implementing them.

The cracks

One of the key security challenges of the cloud is the multiple entry points to a network and devices. The inherent vulnerability of the cloud lies in the way the app codes are designed. In most cases, cloud apps are designed for usability with security as an afterthought. Additional risks come from third-party APIs.

Advanced Persistent Threats (APTs) are another concern in the cloud security space. APTs remain undetected and move laterally through the network, blending with the regular Web traffic by using advanced techniques to penetrate the framework.

Compounding the problem is the fact that there is a huge gap between CXOs and the reality of the cloud in their organizations. According to Symantec's Internet Security Trends Report, CIOs and CISOs have lost track of how many cloud apps are used inside their organizations. When asked, most assumed their organizations use up to 40 cloud apps when in reality, the number nears 1,000. “This disparity can lead to a lack of policies and procedures for how employees access cloud services, which in turn makes cloud apps riskier. These cracks found in the cloud are taking shape. Symantec predicts that unless CIOs get a firmer grip on the cloud apps used inside their organizations, they will see a shift in how threats enter their environment,” stated the report.

The bigger concern was that 75 percent of the data is shared externally, increasing its risk of exposure. And three percent of this “broadly shared” data is compliance related and contains sensitive information.

The thunderstorm

Keeping critical data assets within an organization's premises is a difficult task. An immediate solution is to hand off the responsibilities of setting up, hosting, and scaling back-end architecture to third-party public cloud vendors like Amazon Web Services (AWS), Google Cloud, Microsoft, Azure, Cloudstack, and others. But often public cloud platforms are vulnerable. According to a recent survey by Intel Security, nearly 62 percent of companies store sensitive data on public cloud platforms. Even here, 52 percent of respondents tracked malware to a cloud Software-as-a-Service (SaaS) application, resulting in slowing down the cloud adoption rate.

One of the reasons that may be attributed to the downward trend in cloud adoption is the series of configuration glitches in AWS Simple Storage Service (S3) buckets which have been in the limelight lately. Among the earliest data leaks this year was at Verizon when the company confirmed that data from nearly six million customers was leaked due to a poorly chosen security setting. After this, a Republican data firm accidentally leaked personal details of nearly 200 million American voters. The leak, dubbed as the “largest ever of its kind,” was attributed to a poor S3 configuration. Dow Jones continued the trend with more sloppy configuration resulting in exposing names, addresses, and partial credit card numbers of millions of their customers. Earlier this September, thousands of resumes and personal information of U.S. veterans, many with top-secret clearances, were left exposed by a recruiting vendor… again due to configuration problems. And most recently, media conglomerate Viacom was notified over a misconfigured S3 bucket. “Researchers found a wide-open, public-facing misconfigured AWS S3 bucket containing pretty much everything a hacker would need to take down the company's IT systems,” suggested a report on the Register.

Takeaways for CISOs:

1. Configure security controls and understand the baskets. Don't' leave any configuration glitches for hackers to find.
2. Secure your cloud with APIs and monitor user access.
3. Use IAM to secure and restrict user access to data and services.
4. Set up a central body to control outsourced information technology vendors and third parties in compliance with internal access control policies.
5. Make sure all security perimeters are met while cloud bursting.

Detectify Labs has taken a deep dive into ‘AWS S3 access controls – taking full control over your assets’ on a blog. It notes that “If you are vulnerable, attackers could get full access to your S3 bucket, allowing them to download, upload and overwrite files.” It points out the S3 bucket name is most often not a secret. Once an attacker knows the name of the bucket, he can leverage multiple misconfigurations to access or even overwrite data, “leading to three different scenarios.

By using the AWS Command Line to talk to Amazon's API, the attacker can: Get access to list and read files in S3 bucket; write/upload files to S3 bucket; change access rights to all objects and control the content of the files (full control of the bucket does not mean the attacker gains full read access to the objects, but they can control the content).”

According to the research firm, the company may not even find out that the attacker has full access to S3 bucket. The key solution is to change privileges of your buckets. “AWS are aware of the security issue, but are not likely to mitigate it since it is caused by user misconfigurations,” it adds.

The oncoming flood

Security concerns will continue to be a problem for consumers and corporations. In one of its security predictions, Gartner stated that through 2020, 95 percent of cloud security failures will be the fault of customers. "Only a small percentage of the security incidents impacting enterprises using the cloud have been due to vulnerabilities that were the provider's fault," the report said. "The characteristics of the parts of the cloud stack under customer control can make cloud computing a highly efficient way for naive users to leverage poor practices, which can easily result in widespread security or compliance failures. The growing recognition of the enterprise's responsibility for the appropriate use of the public cloud is reflected in the growing market for cloud control tools." Gartner also predicts that by 2018, nearly 50 percent of organizations with more than 1,000 users will move to the cloud, with cloud security brokers monitoring and managing their data.

Cloud bursting

With security concerns in both on-premises and public cloud platforms, organizations are looking at the third option: hybrid cloud or cloud bursting. It is often seen as a compelling solution for long-standing problems. It is also recommended for high-performing applications which would not suffer any latency hurdles during the migration process. But even these come with similar predicaments as it involves moving a certain amount of data to the public cloud for effective management. Keeping critical and sensitive data within the organization and migrating the less important data to the cloud may seem like a sensible approach. But then, there are other hurdles here, like compliance and regulations with regard to the kind of data that is moved. Also, if there is a breach, how would your insurer treat the incident? Other challenges include cross-cloud policy management, infrastructure policy, firewall rules, IPS signatures, user identification/authentication, and data encryption.

The umbrella

One of the biggest issues of cloud security is identity and access management. A recent survey from the Cloud Security Alliance showed that nearly 22 percent of respondents linked a data breach to compromised credentials. One key area to focus on is Identity and Access Management (IAM) policies for cloud apps. Companies embracing big data solutions also must adopt more perimeter and identity security solutions. The first step must begin with ensuring a proper verification process that can defend the systems from modern-day hackers and their techniques. There must also be continuous testing of security solutions already in place.

Another key area of concern should be the internal access control policies as these must be extended to outsourced information technology vendors and other third parties, and there must be a central body that controls these aspects. "The corporate IAM policy needs to be extended to encompass the cloud apps that you have identified, and then combined with alerting mechanisms that can report on unusual logon activity on cloud services. By undertaking this process, it reduces the likelihood that credentials can be stolen and misused without the organization being aware," suggested a report in Tech Target last year.

The necessity for cloud adoption varies from company to company. And in most cases, the benefits of cloud computing depend on the kind of business the organization is. Just like with any tool, organizations ultimately must consider their risk profiles, staffing and access, resource allocation, and regulatory policies within the organization, and risk appetite before making a decision about cloud storage.

EC-Council

010
001
110

STORM

Mobile Security Tool Kit

TAKE YOUR HACKING BY STORM

The Storm Mobile Security Toolkit is mobile training on a versatile, portable Raspberry Pi-based, touchscreen, tailor-made system. It is a customized, customizable*, fully-loaded pen test platform!

The Storm comes equipped with a customized distro of Kali Linux and the course of your choice (or 2) on the device.

RETAIL $749 | DISCOUNT $699

Use code **CISOMAG** at checkout to get your discount.

TOOL KIT CONTENTS

- ✓ 64Bit - Quad Core Mobile System
- ✓ 1GB RAM
- ✓ 7” touch screen display
- ✓ 64GB MicroSD - Preloaded w/Custom Linux Hacking OS
- ✓ 100Mb Ethernet port
- ✓ 4 USB ports
- ✓ 802.11n wireless
- ✓ Bluetooth 4.1
- ✓ Combined 3.5mm audio jack and composite video
- ✓ Camera interface (CSI)
- ✓ Display interface (DSI)
- ✓ VideoCore IV 3D graphics core
- ✓ Full HDMI
- ✓ USB Micro Power Cable
- ✓ Rollup water resistant keyboard
- ✓ Field Case Organizer for all your gear

WIRELESS HACKING
WIRED HACKING
RF HACKING

BUY NOW

* Customize at your own risk. You assume the responsibility for your device. No warranty is implied or given.

M&A CYBER DUE DILIGENCE: A CRITICAL FACTOR DURING TRANSACTIONS

Nitin Kumar, CM&AA, CMC
Senior Managing Director - Technology, Media & Telecom, FTI Consulting

Digital is the buzzword of today and organizations are scrambling to establish or consolidate their positions in the digital world. Many are taking the non-organic route [i.e., mergers and acquisitions (M&A)] to acquire digital capabilities and assets.

The transition to the digital economy also brings cybersecurity to the forefront of evaluating these target companies and the security posture of their digital assets. Today, ransomware and the weaponization of sensitive data are very real threats as malicious actors use sophisticated techniques to attack organizations, heightening the need for due diligence.

In the past, traditional due diligence exercises have focused on the quality of earnings, operational assessments, legal risks, and, at times, IT in some form (with cyber being a bullet-point under IT).

With cybersecurity issues capable of disrupting the flow of operations, executives should now realize the potential risks to their brand, customer confidence, insurance premiums, valuation, incident remediation costs, and, eventually, investor confidence. These factors are contributing to the rise of cybersecurity due diligence becoming part of the mainstream body of assessment.

UNDERSTANDING M&A CYBERSECURITY DUE DILIGENCE

Assessing the posture of a target company's security requires thinking beyond traditional checklist assessments used to evaluate compliance and canned, tool-based scans. The short due diligence timeframes, low cybersecurity acumen of management and issues with quality and completeness of data create additional challenges during the M&A due diligence of a target company.

There are three flavors of cybersecurity due diligence and acquirers can decide the level of assessment they undertake toward evaluating risks.

RED FLAGS REVIEW

The quick and dirty version of a cybersecurity due diligence typically includes requesting high-priority information and reports from the target company and validating them through analysis, management interviews, and corroborating it with the team's prior assessment of similar target companies.

The next step is to quickly document "red flag" issues and initiate further drill-down on those specific areas in a surgical manner.

TEST REVIEWS

This level of review typically encompasses the detailed assessment of multiple areas of cybersecurity and can even include running intrusive scans if the information submitted by the target does not meet expectations. Characteristic areas of technical assessment include data-center security, network security, storage controls, end-user posture, applications, third-party risks, data controls, etc. It is also a good practice to interview key personnel and understand the level of security awareness in the organization. More details are provided in the article.

LANDSCAPE REVIEW

The highest level of review usually entails a detailed scan of the target company's entire threat landscape for existing, new, and emerging threats, and documenting the risk level associated with each vector. One way to do this would be to assess the landscape to understand whether malicious groups could access the infrastructure, applications, or data of the target. This step also includes evaluating the attack vectors, points of vulnerability, mechanisms and speed of response, cost of controls/response teams, or risks due to the lack thereof. Landscape assessments should also factor in the change of location due to integration of the two companies.

TYPICAL AREAS OF M&A CYBERSECURITY DUE DILIGENCE INCLUDE:

CYBERSECURITY STRATEGY

Understand and document the overall cybersecurity strategy and its alignment levels with the overall business strategy, IT strategy, and the company's product portfolio. Typical gaps arise when the cybersecurity strategy is skewed too much into IT or gets very compliance-centric. Make sure the gaps due to the strategic direction are captured well.

GOVERNANCE

Document the governance posture of the company (e.g., who is involved in direction setting, defining priorities, ensuring level of alignment, making decisions, level of rigor, reporting, etc.). Assess the impact of the governance posture of the organization on the cyber-risk posture of the company.

ORGANIZATION

Evaluate the cybersecurity organization, including structure, size, skill sets, and staffing by functional area. Assess the leadership and the culture of the cybersecurity organization to assess the fit. Identify and analyze the value/impact of existing third parties in use to provide cost-effective or specialized services. Document the risks due to skills, staffing levels and structure, etc. Understand the level of security awareness and acumen in the organization and assess human weaknesses in the overall security posture

INFRASTRUCTURE

Evaluate the risk posture associated with the core IT infrastructure components, including data center, network (WAN/LAN), desktops, hardware, and office automation tools (e.g., messaging, file and print, etc.). Identify potential business risks and/or improvement opportunities.

APPLICATIONS

Evaluate the security and privacy posture of major business systems providing automation and support to the core operating processes. Understand the financial impact associated with the confidentiality, availability, agility, and integrity of each of them. Assess the ability to log, monitor, track, and report timely and accurate cybersecurity-related metrics and information.

DATA

Understand key data flows through the organization, ensure no PII data-related risks are assumed, and that appropriate controls are in place. Review data creation, data acquisition, data modification, data transmission, data storage, and data disposal; make certain they are well understood. At each phase of the data cycle, the controls should reflect the value and risk of data with respect to the organization and the threat landscape.

OPERATIONS

Review all policies and procedures in place. Assess whether they are aligned with the cyber strategy, the compliance needs of the organization, and if there is a consistency of awareness with respect to policies and procedures such as authentication, access control, business continuity, passwords, incident response, etc. Document the ability to enforce, manage, monitor, track, and report across multiple areas, locations, and controls. Document any possible risks and gaps.

PRIOR HISTORY

Review prior incident history including breaches, outages, audit reports, etc. Understand root causes, response procedures, mitigation plans, and continuous improvement. Review all existing and prior vulnerability assessments, IT audits, and penetration testing reports to ascertain the rigor and discipline of testing to document all risks and opportunities.

SPEND AND BUDGETS

Analyze overall cybersecurity expenditure plans and budgets (both capital and operating expenses) with respect to strategic objectives and risk profiles. Understand historical spending levels with respect to industry trends, benchmarks, and best practices.

KEY INITIATIVES/ PROJECTS

Identify and profile significant, capital-intensive cybersecurity projects as plans or in process. Evaluate the status, strategic value (with respect to management's objectives), feasibility of cost and timelines, and potential business/execution risks.

INTEGRATION PLANNING

Assess the overall cybersecurity integration strategy, identifying synergy opportunities associated with consolidating environments, infrastructure, redundant controls, locations, vendors, contracts, licenses, and organizations. Understand the key integration projects and initiatives, including the one-time costs, timing, and level of effort. Understand factors such as the new regulation compliance, probability of success, resource constraints, and conflicting projects that could impact cost/timing of synergy realization or assume new risks attributed to the changed threat landscape.

Always analyze the full stack i.e., data center, network, storage, end user computing and applications, etc. Document risks across each layer and impact on other layers. The target company is only as vulnerable as its weakest link. The Yahoo and Equifax like scenarios are only going to grow unless acquirers give adequate importance to cybersecurity due diligence.

The opinions expressed within this article are the personal opinions of the author. The facts and opinions appearing in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

MSSP SHOPPING:

USE YOUR CORPORATE AMEX WISELY

Chris Roberts
Chief Security Architect, Acalvio Technologies

It's worth noting that many of the Managed Security Service Providers (MSSPs) out there have their own take on what you should look for when selecting one, however, almost all of them require you to register on their site before they end up telling you to select their services with the exceptions being IBM, Trustwave, and Digital Guardian. These providers happily hand over their selection criteria without demanding your name, rank, and serial number.

So, let's set the scene. The following are questions I find useful in guiding companies through a solid MSSP selection process. I have learned to ask many of these questions by working with clients through the horror of migrations-gone-bad.

Have you conducted an extensive evaluation of your security requirements?

- Garbage in, garbage out. No MSSP is going to be able to untangle your mess if you don't even know what you have AND where it is. Get organized BEFORE you commit.
- If it's not being logged in your environment, the MSSP isn't going to miraculously find and deal with it.
- No, they are not going to work out that Gladys in accounting has a local XLS spreadsheet with all the credit card numbers on it. Find ALL your data before you say "I do."
- No, they wont protect you from stupid. MSSPs are not going to be a silver bullet; they are another pair of hands that WILL help you, but you must still help yourself otherwise the relationship is doomed.

Do you understand the security measures with which you must comply?

- Handing over the controls does not mean "passing the buck" in the realm of compliance. At the end of the day, if the worst happens and you are breached, it is you, not the MSSP, that's on the stand giving testimony as to what went wrong.
- Whatever you are required to have in place, your MSSP also must have in place – at a minimum. MSSPs really should have more given that they are a consolidation of everyone's data and, therefore, much more of a target.
- If your compliance is due to an auditing or governing body in Q1 and your MSSP leaves it until March 31st to get you a letter of compliance (or something similar), it's not going to work. Setting realistic goals and deadlines for how your MSSP reports compliance is crucial – especially if you have deadlines to adhere to. Remember, a lack of planning on your part will not constitute an emergency on theirs.

Have you established a reliable governance model?

- What happens when the MSSP finds something? Who is on point, who is on triage, who is going to get the call at 3 AM and which one of you is going to call the lawyer, the compliance officer, and presumably the spin doctors?
- How much does your MSSP have to declare? If you've got someone inside the organization breaking the law and they find the evidence, who calls law enforcement?

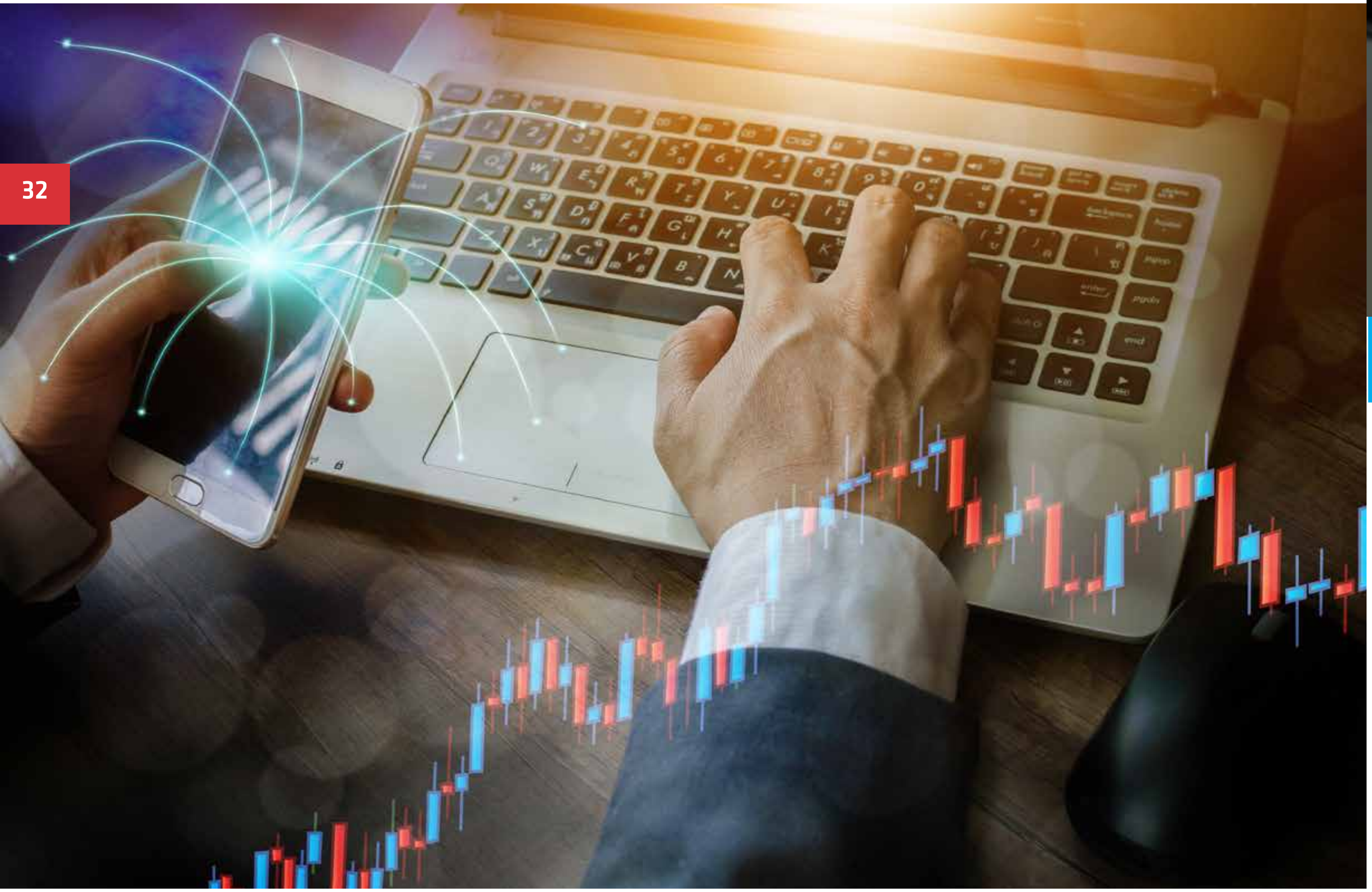
Have you determined which security requirements you expect the MSSP to put in place?

- Just because you managed to get rid of your logs, your alerts and your local SOC/NOC it doesn't mean you are off the hook…how far does your MSSP take an issue, are they simply first line support, are they a 1-2-3 tier SOC/NOC or what's the limitations of their capabilities?
- Do they know who to wake up in the DBA team at 4 am when root's just dumped the HIPAA database out to an FTP server in Brazil?

What are your criteria for success?

- Security maturity. Does having the MSSP in place advance your security maturity across any of the core criteria? (If you are looking at this and wondering what the heck a security maturity model is then we probably need to talk). If you can, by integrating an MSSP into your solution stack, increase the overall maturity from "repeatable/defined" to something like "managed," then this is something worth considering doing.
- If you are looking at stability within the enterprise environment and consolidating the various logging and monitoring solutions, then again, this is something that should be considered. But, as we've pointed out earlier, an MSSP is not going to come in, wave the magic wand, and rid you of all your legacy logging gear overnight. The migration project and the integration of THEIR chosen solution will take time and effort so make sure you plan, plan again, ask more questions, check the plan, and only then, sign on the dotted line. The age-old saying of "measure twice, cut once" is very relevant when it comes to any forms of outsourcing.

Now we've established that you (hopefully) know what you are protecting and how you want it protected, and you have a plan in place for evaluating your future MSSP. Let's go shopping with the corporate AmEx.



The Seven Ps of MSSP

Broad portfolio of security services:

This might be one of those rare instances when you do want to put all your eggs in one basket. That sentence hurt to write but it's going to be essential to find an MSSP that can consolidate your mess into something cohesive and usable. What you don't want to do is add another layer of detachment into an already complex environment. It goes without saying that having a different MSSP for different areas within the enterprise is not going to work well, so compromise on things you can, select the MSSP that has the best overall architecture, solution, and services, and work with them across the entire spectrum.

Highly respected security intelligence and research professionals:

Part of the logic for getting an MSSP to look after you is that they do allow you to sleep at night, but the only way that happens is if they are one step ahead of things. "One step ahead" doesn't mean one step ahead of the bad guys, because we have a long way to go before we get there. What they should be are your eyes, ears, and early warning system, and for that they need good people—not just in the NOC/SOC watching your stuff, but good people with their finger on the pulse of the digital world. So select your MSSP accordingly.

Sophisticated back-end technology:

Your corporate AmEx is going to be a hit for the proverbial "six", therefore, make sure you are getting your money's worth. You want to make sure that your MSSP has not only the latest and greatest technology, but also a balance of reactive and predictive, proactive, preventative technologies to ensure the integrity of your environment as best as possible. And for once, give open source tools a chance here. Just because your MSSP has Oracle or IBM at the back-end, it doesn't mean they are any good. Heck I'd go with a MicroCentre H/W with Hadoop and HBase any day if the coding and algorithms for detection and analysis were better, their client services shone, and they cared about you. Choose carefully and involve someone to help you ask all the nasty questions. Oh, and find an MSSP that works with multiple vendors, suppliers, partners, and solutions. That way you have the best-of-breed mentality at all times. The bottom line is to remember that the answer is not always Cisco or Palo Alto.

Excellent reputation:

This counts for a lot, but the focus here should be on satisfied clients. Don't focus just on the ones they feed you but ones you can go out on your own and find. Time to brush off the OSINT skills and see who's using them! Hit the conferences, hit the shows, and do your research. Yes, there will be unhappy customers, there always are. Keep in mind that a lot of them are unhappy probably because they believed in the magic wand. But do you own validation. This covers another point: reference clients. Find not only the happy ones but the annoyed ones, work out what is good, bad, and ugly before you do damage to the corporate budget.

Broad security infrastructure expertise:

This one almost goes without saying, but it's in here because some clients have not done all their homework and get an MSSP to look after their log management, monitoring, and archiving, and then work out if they need a different MSSP to do their compliance, oh, and a third MSSP to do vulnerability assessment and remediation work. That's never going to work. Best case, you have so much stuff going in so many different directions that you sink into TPS reporting hell. Worst case, the vendor blame game happens when each of your MSSPs blames the other for whatever the problem du-jour is. Find an MSSP that can cover most or all your requirements, simple as that.

Robust, web-based management tool to improve visibility and intelligence:

Ok, so you've handed over all your data, your management, and basically given the front door keys to your chosen MSSP. How do you keep tabs on them, how do you now gain visibility into their world? What management, access, and controls do you and your team have? How easy is it to interface with both the humans and the chosen technology that is now protecting you? And, above all, when leadership and the board ask you to "justify and provide metrics" for your money, how are you going to do that with your new MSSP?

Financial stability:

Let's keep this one simple. I don't care if they are small up-and-coming or too-big-to-fail, everyone has a weakness when it comes to financial stability. Do your own risk analysis and go from there. You want your MSSP to be around longer than you are.

Your data is in their hands. How safe are they?

This is your data, it's your a** on the line if it goes missing or ends up on a .RU website, so be aware of that when talking to your prospective MSSP. What PPCs do they have in place, what background checks, how often, what do they do with the people, the processes, the technology, how do they respond when you ask them all the nasty questions about how they keep people like me our of their systems? These days, attackers increasingly focus on vendors, partners, and third parties as often they are easier and softer than walking through your front door.

Customer focused:

Nobody cares which restaurants or golf courses they took you too when the chips are down. The measure here is on a Sunday night over a holiday when all the red blinky lights start flashing, will you be able to get hold of enough people to keep you functioning, will you be able to recover inside the SLA timeframe and will your MSSP go above and beyond, not just because you have the biggest checkbook, but simply because to them you are more than just a number?

Global coverage (for that nice 24/7/365, even if Yellowstone goes critical type of coverage)

I'll never understand why companies choose to put all their trust in an MSSP that has one data center 100 miles or less from Yellowstone or somewhere in California on a fault line or in the Gulf of Mexico etc. You get the idea. I told you to put everything in one place, but that one MSSP has to be distributed for your sakes. Get out the map, brush off the geography and geo-political analysis tools, and work out where your data's going to be when the zombie apocalypse hits.

So, now you have the criteria for both analyzing what you want vs. need, what you can integrate vs. hand over, and who's going to work best for you without relying on the magic-8-ball, i.e. Gartner. Good luck, may the force be with you, and reach out to me if you have questions!

One last thing, and this one's a doozy. When you've read this, ignored all the bullet points, and chosen your MSSP based on which golf course they took you to, then 18 months later you want to exit them, I hope you previously worked out who owns "your" data when you leave.

The opinions expressed within this article are the personal opinions of the author. The facts and opinions appearing in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

CYBERSECURITY TALENT GAP

IS THERE ONE?

Renee Brown,
CEO, Cyber Human Capital, and Author, *Magnetic Hiring*

From Equifax to Deloitte to Yahoo, there is nonstop discussion on how and why these companies were breached and how to mitigate a problem that is here to stay. There is almost always an element of the talent shortage that plays a role in these conversations. There is no lack of statistics about the security skills gap and the lack of talent in the industry. Some of these articles suggest recommendations for solutions to the problem — more university degrees and technical school programs, more cyber boot camps, certifications, and trainings overall. The real question is why is it taking so long to fix this problem? It would seem logical that if there are good, high paying jobs available, supply would eventually catch up to demand.

Let's, for a moment, consider the career paths of many CISOs, the highest-ranking security professionals at any organization.

Prior to information security degree programs, formal trainings, and cybersecurity boot camps, there were computer science and engineering degrees and on-the-job training. Since the security field is a relatively new industry, any seasoned CISO with a decade or two of experience likely has grown into his or her role in this way.

There are many paths to becoming a CISO and most CISOs transferred into security from another area of IT or another field altogether. Some earned a bachelors or master's degree at the start of their careers but many CISOs are self-taught career changers. Many accomplished this by earning certifications and degrees while they transitioned into the profession. Others have transferred into security from the military.

So, why aren't more CISOs taking a model that has proven successful for them and scaling it to fill the security talent skills gap at their organizations? Why aren't there more formalized programs to support IT professionals wanting to become security professionals? Below are some possible explanations.

TENURE

According to Gartner and the Poneman Institute, the average CISO tenure is four years and two years, respectively. With such a short duration of time in such a demanding role, it may seem impossible to implement a task-force to train entry-level workers and support career-changing talent. You will need to get them up to speed quickly enough to be able to reap the benefits while you're still at that company. Some Fortune 500 companies have been successful at quickly training staffers who have no formal security experience and turning them into security professionals through boot camps and on-the-job training. Implementing early-career rotational programs is another method that has proven successful.

INTERNAL MOBILITY POLITICS

Internal mobility is one of the fastest ways to re-recruit and retain talent. If there are talented professionals in other areas of IT or across the organization who have the aptitude to learn specific areas of cybersecurity, they should be one of the company's first sources of talent. This could come with some internal political challenges since IT leaders will feel that the CISOs are poaching their best talent. Talent sharing should be a win for all parties and the company overall, since the top request from technology professionals is to stay at the forefront of technology in their careers.

RESOURCES

Specifically Human Resources. It is a fact that HR professionals, especially the corporate recruiters representing your organization, need education on the nuances of security to effectively and efficiently present candidates who could be a fit for open positions. One solution could be to provide your company's HR business partners with a security analyst liaison who can field security questions, so the HR contact is educated when approaching external candidates. Each role needs to have an employee value proposition to provide candidates with highlights that would make your projects and assignments attractive to them. Implementing a rotating project like this that is part of someone's responsibilities could be a great stretch assignment for someone in the security group who is eager to help you build the team.

One of the biggest complaints that security professionals share when being recruited is that they are frustrated when trying to move from one area in security to another. The biggest challenge faced is that they can't get through the HR red tape or applicant tracking systems because their resumes don't match the roles exactly. An organization will want to train its leaders to consider candidates with growth opportunity for roles and not only people who have done this work at a prior employer. It's not feasible to do this for every role but there are opportunities that should be explored.

UNDER-EMPLOYED/ EVER-EVOLVING SECURITY PROFESSIONAL

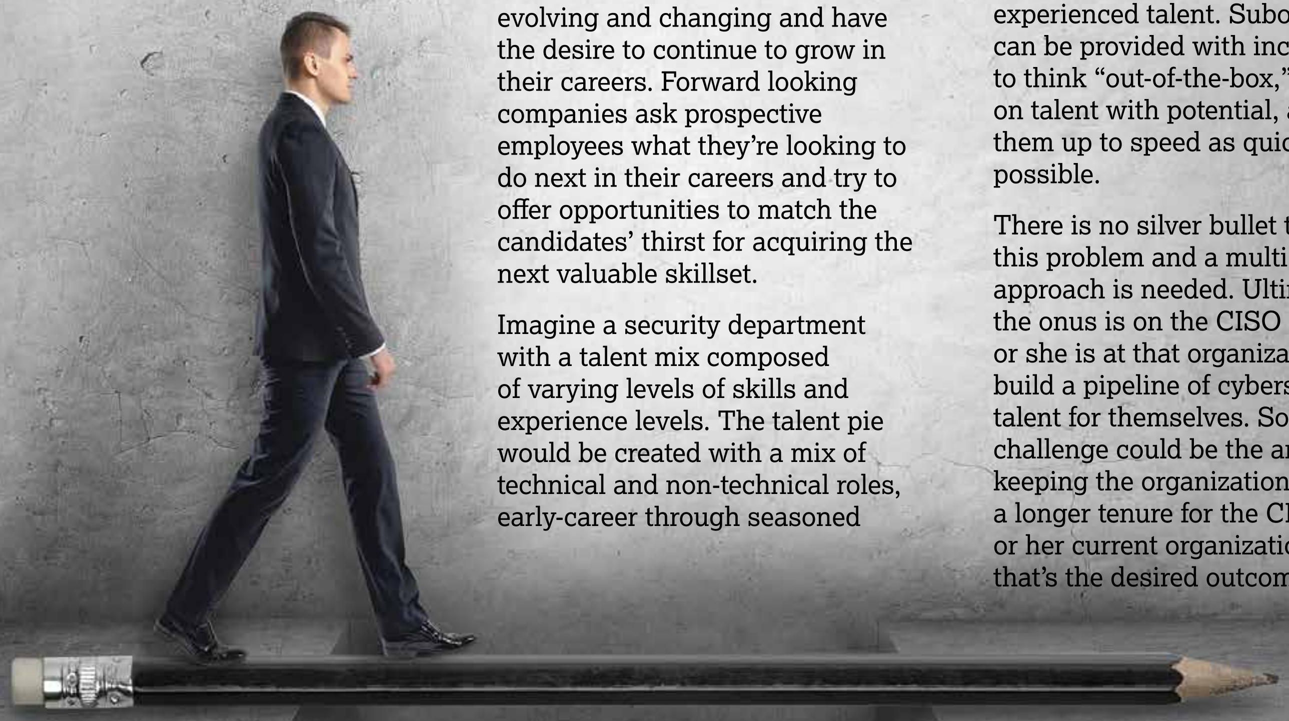
Although statistics and countless articles show that there is zero percent unemployment in cybersecurity, there are quite a number of security professionals that are in transition or looking to move from one area of security to another. Unbelievably, many recent college grads with degrees in cybersecurity, especially from community colleges and technical schools, struggle to break into the industry. There is constant complaint from this talent population that the entry-level jobs available to them come with poor salaries and even then it is difficult to get their foot in the door. Like the security landscape, the best professionals are ever evolving and changing and have the desire to continue to grow in their careers. Forward looking companies ask prospective employees what they're looking to do next in their careers and try to offer opportunities to match the candidates' thirst for acquiring the next valuable skillset.

Imagine a security department with a talent mix composed of varying levels of skills and experience levels. The talent pie would be created with a mix of technical and non-technical roles, early-career through seasoned professional, and leadership roles. 10-15% of each category would have "transition positions" for candidates with great aptitude and training but not the actual experience. And this would be mirrored across all experience levels — not only early-career talent but more seasoned professionals as well. This could be a solution to your talent gap challenges.

EMPOWERING YOUR SUBORDINATES

Many times a CISO's vision is completely aligned with hiring talented individuals with potential who have aptitude and transferable skills but may not have the specific experience requested for some positions. However, their subordinates may feel the pressure to hire skilled, experienced talent. Subordinates can be provided with incentives to think "out-of-the-box," bring on talent with potential, and get them up to speed as quickly as possible.

There is no silver bullet to solve this problem and a multi-faceted approach is needed. Ultimately, the onus is on the CISO while he or she is at that organization to build a pipeline of cybersecurity talent for themselves. Solving this challenge could be the answer to keeping the organization safe and a longer tenure for the CISO in his or her current organization — if that's the desired outcome.



The opinions expressed within this article are the personal opinions of the author. The facts and opinions appearing in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

RICHARD RUSHING
CISO, MOTOROLA

Rahul Arora

As the Chief Information Security Officer for Motorola Mobility LLC, Richard Rushing has seen his company through targeted attacks, emerging threats, and enough technological innovation to fill a book. In an exclusive interview with CISO MAG, he talks about managing cybersecurity risks efficiently while covering aspects such as Wi-Fi security and 5G technology.

Can you tell us how Motorola Mobility is committed to cybersecurity? What are the cybersecurity practices that Motorola Mobility follows?

From a general standpoint, we've always been a strong practitioner of cybersecurity and privacy all around the world from the beginning, and that has continued till this day. As an organization, you can consider cybersecurity almost like a recipe that has some key ingredients. So, some of those key ingredients are your policies, your processes, your technology, your management of assets, how you recover from issues, and how you would respond. How you mix those together really depends upon the kind of organization that you are and what you're actually trying to protect and kind of the data that you're protecting.

I think that's one of the key areas that we have addressed in a mature manner. We really have not changed, even though the industry around us has kind of changed and the technology has kind of changed, the underlying pillars of this have not really changed in the past of how we do business, how we conduct ourselves, how where we look at data, how we manage data, how we work with the business groups, etc.

Do you think companies are overlooking the basics and probably have their priorities at the wrong place when they go for really advanced tools and technologies?

I don't want to say that they have the wrong priorities, I think they have too many priorities and some basics get forgotten. The biggest examples I've seen time and time again are having problem with things like patches. We're not even talking about vulnerability remediation or anything else, just patching. And we saw that with WannaCry and some of the other recent breaches.

We can create technologies that solve patches, or pay companies that have patch management capability. A process still has to be there and people are required to do that. You know, you can automate a lot of it, but there still needs to be someone who is making choices.

I think, unfortunately, there's always reluctance to change and not just in security. It's like we see patching as being part of security, but it is not yet considered that important. What they don't realize is that patching is probably going to make things much better. I think that's a historical perspective.

No one remembers the 36 versions when we pushed patches and nothing went wrong. They will remember the one time when everything went wrong.

Let's move our focus to something else. These days, 5G is a trending topic. What, according to you, are the new requirements the 5G would drive when it comes to cybersecurity?

So, 5G is when you started looking at the speed at which the Gs are coming. Between 1G and 2G, there was a 10-year gap. There are currently no standards that have been generated for 5G technology. This time IoT is playing a role as well. Service providers want to provide multi-megabit data sets for your phone, mobile devices, and everything else that are around along with gigabit speeds.

From a cyber perspective, your mobile devices are going to do more. They will use a massive amount of data. The other side of it is, you think about the draw of connectivity. So, I use my work networks and Internet connection because in all likelihood, it's faster. Now, if I can have super-fast Internet by just connecting through another side of it, I am going to have the idea of flip flopping from one network to another. I now move from a protected information network that has all my corporate firewalls and all my corporate cyber assets to going out to the Internet.

In a lot of organizations, the PC is not really designed to do self-healing, self-protection, and to stand on its own. You have to VPN to get data connection. And that whole philosophy is going to have to change when 5G becomes prevalent across the area, because you are going to have higher speed networking. It's going to be just a flip of a switch away from your PC, from your mobile device and etc. The other area that you always get into is the number of IoT sensors and everything else. That's going to be easy to access and bandwidth will have multiple sensors running on it.

The bandwidth can only support so much now. 5G has the potential to support even more, but if a cell crashes, those sensors are not going to be able to transmit data. If these sensors are taken away, what happens to everything? We're very much caught up in the work of IoT and using mobile devices for all sorts of things from lights to cameras to other things. If that fails, what will then happen?

Motorola Mobility was acquired by Lenovo last year. What were the cybersecurity challenges that came up before, during, and after the acquisition?

Motorola has gone through actual acquisitions and selling out portions of the company and everything else. If you're doing merger and acquisition kind of stuff, there's always lots of complexity. And then there's the business side of the equation which is always, "we would either like to keep everything separate and figure out a way to share data, or we want to try to converge the data together, or we want to try to move the data from one system to the other system."

You can see it with the transitional service agreements that everybody that's done acquisitions has used. The way to start the process is to say "Here are our key ingredients. Do they match up to yours? Are the security policies the same? What are some of your requirements? What are our requirements? Do you have processes around all of these? Do you have procedures around them? Do you have people around them?"

Some organizations have centralized cybersecurity and other organizations have dispersed it. Some organizations have moved the product security group to the cyber group, while some organizations have big, virtual teams and dedicated resources. One of the bigger areas here is the policy and procedures. Is someone getting together all the people and putting those together through a framework? That's kind of like phase one.

The second phase is how you put this into a functioning team. The format of two organizations may not be the same. It's great if both formats mirror each other because then it becomes seamless. If not, then it becomes difficult to put things in order.

There are lots of differences in how organizations work, but the main thing to think about is where security is in parts of the organization. Is it scattered or central? I think those are the biggest challenges you run into.

Your LinkedIn profile mentions you are a Wi-Fi Guru. How do you go about securing a Wi-Fi connection for users?

Wi-Fi is an issue just because of the pervasiveness of it. If you think about it, wireless is a physical layer. Its use is the problem. There are a lot of other things that go along with it. If my computer is connected with a cable going to the connection in the wall, I know my computer is connected to this. Now, behind that it could be connected to anywhere. But let's just assume that it's connected to the right port in the right switch that is going to the right location. It's there – you have to physically break into my building to do some other things or have malicious intent to violate the physical presence of that.

In a wireless environment, I have no idea where my phone is actually connected to for Wi-Fi. In other words, even though it says you're connected to this hotspot at this location, it may not be that hotspot. How do I know it's good? How do I know that's the right one for the location? I don't have like Wi-Fi eye glasses where I can see my signal and say "Yeah that's the right access point."

> In a wireless environment, I have no idea where my phone is actually connected to for Wi-Fi. In other words, even though it says you're connected to this hotspot at this location, it may not be that hotspot.

As far as security goes, I think it boils down to that you should always encrypt your data and have the highest levels of all of authentication that you can put onto it, whether it's at home or anywhere else, because once I'm on your connection and once I'm connected to you, I can potentially change the DNS or something else.

The other side that you get into is dealing with is when you're connected at hotels, coffee shops, other free environments – and I think that is probably the biggest issue that you run into because everybody does that. I walk in. OK! let me connect here and see what it's actually there. And usually it's just a splash screen. It's the terms and conditions page and you're off and running. The likelihood that that is something fake or not is we think about because you walk into the coffee shop or library or through the airport and there are 30 other people on laptops and I'm like "OK, which one is the bad guy?" It's really hard to tell. And so that's where you really have to be careful.

According to you, what is the future of cybersecurity? Where do you see it, say, five years from now?

I think we're getting better. At the same time, there are more issues, more problems, and it's kind of 80/20 thing. We kind of solve about 80 percent of the problems in cybersecurity and there's always that outlined 20 percent that are really hard to solve. But, I think that instead of that being fixed, it's a sliding platform. We solve a problem and then five years later, it comes back.

There has to be an understanding that there is no perfection in cybersecurity and you're not going to be able to magically say we can cover 100 percent of this stuff because the bad guys are going to come up with something. And it's useful to think of security as hurdles you're putting in the bad guys' way to slow them down and give yourself breathing room to go repair the damage and prepare for next time. We would really love to be done with something and be able to put this here and not have to worry about it again but that's simply not the case.

What would be your advice to a budding information security professional? What can he/she learn from Richard Rushing?

I love security. I love the passion of the people. And I love the sharing of the technology community. I tell people when they start looking into a career in security, their biggest problem will be choosing where to focus. Because I think that's the biggest problem in security is that it's so big. When I started, it was narrow and focused, but is so big now. You need to experience a lot of different venues.

I think security is one of those few areas where you can really like to do something and you can do it for the rest of your life. And I do and I really mean this is not going to be solved. So, if this is what you're going to do, you better like what you're doing.

> So, if this is what you're going to do, you better like what you're doing.

In a business landscape characterized by dynamic trends and events, change is the only constant. Many organizations often bring about a change in their leadership to achieve the desired results from a new direction, to create and disseminate a vision, or just to breathe new life into the corporate structure. The field of information security is no different. In this segment, we take a look at some of the new appointments in the information security domain.

CISO MAG staff

DHS MAKES TWO IMPORTANT APPOINTMENTS

The United States Department of Homeland Security made two important appointments in the month of October. Deputy Chief of Staff Kirstjen Nielsen was appointed as the Secretary of the Department of Homeland Security, and Dr. Barry West was named the next Deputy Chief Information Officer (CIO).

Nielsen takes over from Elaine Duke, the acting DHS secretary. Nielsen has the task of helping coordinate the federal response to potential cyber attacks that target elections. West will be replacing acting DHS CIO Steve Rice, who was elevated from the deputy CIO role in August when then-DHS CIO Richard Staropoli resigned.

In the White House, Nielsen was responsible for carrying out White House Chief of Staff John Kelly's orders on who gets access to the president. A close and longtime aide of Kelly, Nelson is widely viewed as a competent, experienced, and non-partisan security professional. It was reported that Kelly made a personal appeal to Trump for nominating Nielsen after the president reportedly rejected several contenders for the job.

Nielsen has experience in handling cybersecurity-related issues, as she has worked at a cyber-think-tank at George Washington University and is considered well-versed in some of the more technical missions at the department, such as sharing cyber threat information with the private sector. She is a former marine general and a lawyer.

Prior to his appointment, West was serving as a senior advisor at DHS as well as a senior accountable official for risk management. In his previous position, West worked to align DHS with the Trump administration's policies surrounding cybersecurity.

West has vast experience in the CIO role for various government agencies, including roles as the CIO at the Federal Deposit Insurance Corp., Pension Benefit Guaranty Corp., Commerce Department, Federal Emergency Management Agency, and the National Oceanic and Atmospheric Administration.

He has also been a part of senior leadership in information technology companies Mason Harriman Group and Strategic Enterprise Solutions. The appointment of CIO does not require Senate confirmation.

AUSTRALIAN STATE VICTORIA APPOINTS ITS FIRST CISO

In a bid to strengthen the cybersecurity infrastructure in the Australian state Victoria, the Andrews Labor Government appointed John O'Driscoll as its first Chief Information Security Officer (CISO). The appointment was a part of the 23-point Cyber Security Strategy that was released by the Victorian Government in August 2017. O'Driscoll focuses on assessing, monitoring, and responding to cyber risks across the Victorian government's departments and agencies.

While making the announcement, Special Minister of State Gavin Jennings said, "John O'Driscoll's extensive experience working across information technology and cybersecurity make him ideally suited to be Victoria's first Chief Information Security Officer, as we seek to secure government services. As organized crime and others become more sophisticated in hacking and disrupting digital services, it's crucial government steps up to better protect our public services and information – John will help us do just that."

With 20 years of experience,

Driscoll is a former senior manager of information and technology risk at Australia and New Zealand Banking Group, where he worked till 2011. Prior to that, he held senior security positions at AMP and Commonwealth Bank of Australia.

KROLL APPOINTS STACY SCOTT AS MANAGING DIRECTOR IN CYBERSECURITY DIVISION

Kroll, a risk consulting firm, named Stacy Scott as Managing Director in Cyber Security and Investigations Practice in Dallas. A veteran of 16 years in the industry, Scott has served in high-profile roles with a leading cybersecurity consulting firm, a Big Four accounting firm, and the largest not-for-profit healthcare system in Texas. She also owns her own consultancy firm.

Lauding her achievements, Jason Smolanoff, Senior Managing Director and Global Cyber Security Practice Leader for Kroll, said "Stacy brings a wealth of information risk management experience, with particular expertise in cyber risk management, security program development, and regulatory compliance, especially in the healthcare sector."

Scott has worked as the president and founder of Wisterwood Advisory Services where she was HIPAA Security Rule subject matter expert. She also served as the Director, Enterprise Architecture and Security, for Baylor Scott & White Health, a not-for-profit healthcare system in Texas.

Scott, who won Woman of the

Year award by the National Association of Professional Women in 2012, holds a Bachelor of Business Administration degree in Information & Operations Management from Texas A&M University along with a number of certifications, such as Information Systems Auditor and HITRUST Common Security Framework Practitioner.

INSURANCE PROVIDER HISCOX HIRES ROBERT HANNIGAN AS ADVISOR

Lloyd's of London insurer Hiscox has hired former spy chief Robert Hannigan to advise on emerging cyber threats and new criminal techniques. Hannigan was Director of GCHQ, the United Kingdom's largest intelligence and security agency, from 2014-17. He is known for developing the UK's first cybersecurity strategy and setting up the National Cyber Security Centre.

At Hiscox, Hannigan is responsible for providing market intelligence, training cybersecurity professionals, and assisting in the development of new and existing cyber products.

On January 23, 2017, Haanigan had made headlines when he abruptly stepped down from GCHQ citing "personal reasons." Hannigan, who joined GCHQ in November 2014, was succeeded by Jeremy Fleming. He is credited for bringing transparency and openness to GCHQ, advising several international companies on issues related to cybersecurity, cyber conflict, and the application of technology in national security.

Hannigan has also been writing regularly since the 1990s on cyber issues in multiple media houses. He was awarded a CMG by Queen Elizabeth for services to national security and the US Intelligence Distinguished Public Service Medal.

On his appointment, Hannigan said "the risks that cyber criminals pose, both to businesses and individuals in the UK, are significant and sophisticated. Insurers must evolve their understanding and defense against cyber crime."

ALAN FEELEY APPOINTED AS CHIEF CYBER SECURITY OFFICER OF SIEMENS GAMESA RENEWABLE ENERGY

Siemens Gamesa Renewable Energy (SGRE) in September 2017 appointed Alan Feeley as its new Chief Cyber Security Officer. Feeley, who is already serving as Chief Information Officer, works in conjunction with the technology and product security departments, corporate security, and human resources.

According to a statement by the company, Feeley is responsible for expanding and managing "the company's operational framework for cybersecurity." He also consolidates the security developments in the context of the digital transformation of SGRE after the merger of Gamesa and Siemens Wind Power.

A SGRE spokesperson said, "Cybersecurity vulnerabilities and threats present tangible risks and challenges to companies and to the operations they support for their customers. The complexity of this topic requires coordination and orchestration across many parts of large companies, including IT, Product Design, Security, and Data Protection, to name a few."

With cybersecurity gaining more importance than ever, cybersecurity startups have become a huge attraction for venture capitalists. The cybersecurity market has seen tremendous growth despite the slowdown in the global economy with many companies inking record-breaking funding deals with venture capital firms. The influx of money has driven innovation and solutions to important security challenges. In this section, we look at some emerging companies making waves in the information security domain.

CISO MAG staff

BROMIUM

Founded in 2010, Bromium is a venture capital–backed startup that restores trust in computing. Led by Ian Pratt (President) and Simon Crosby (CTO), the Bromium team claims to have created a new technology called micro-virtualization to protect end users from threats like viruses, malware, and adware.

What sets Bromium apart: Micro-virtualization and AI-based threat detection and analysis.

Market Adoption: For most companies, it seems that micro-virtualization and AI-based threat detection and analysis are not thought of as standard, must-haves quite yet. Early versions of the technology caught the attention of the market but usability and scalability were problems. While these have been solved with recent versions, first impressions are hard to overcome, which could explain some market resistance to the product. With recent endorsements by Microsoft for Windows 10 and HP integrating a version of the technology into a line of laptops, the stars may be aligning for Bromium. What's standing in their way now could be cost. They may be cheap for what they do at $75 per device per year, enterprises aren't comparing them against other companies that do what they do – they are comparing them to standard antivirus software, which is significantly less expensive.

CYBERLYTIC

United Kingdom-based Cyberlytic International Limited uses Artificial Intelligence (AI) to provide advanced web application security solution, real-time risk assessments, and actionable intelligence.It deals with Intelligent Web Application Security that applies cognitive machine learning and risk analytics to detect, prioritize the workload of security teams, prevent web attacks such as SQL injection and cross-site scripting (XSS), and reduce response times from cyber-attacks.

Headquartered in London, Cyberlytic works closely with the Centre for Secure IT, part of Queen's University Belfast, and is recognized as the Government Communication Headquarters Cyber Academic Centre of Excellence.

What sets Cyberlytic apart: Their focus on identifying cyber risk using artificial intelligence and machine learning, which not a new idea, is only being used by a small number of security startups. Cyberlytic's focus on risk distinguishes them from the field.

Market Adoption: It initially developed its techniques for the UK Ministry of Defense and is now available to SMEs to help them counter increasingly complex cyber threats. They are currently still in funding rounds to bring their technology to the private sector.

FUGUE

Founded in 2013, Fugue is a venture-backed software that that develops infrastructure-level operating systems for managing cloud-based workloads. It eases public and private sector compliance burdens and automates operations by building, enforcing, and optimizing cloud infrastructure. Fugue runs on a virtual machine (EC2 instance) inside Amazon Web Services accounts and uses cloud APIs to build, update, and enforce infrastructure.

What sets Fugue apart: According to Gartner's Cool Vendor in Cloud Computing 2017 report, "Fugue has created a declarative programming language to optimize the rapidly increasing complexities of cloud orchestration and configuration."

Market Adoption: This year, the firm reportedly raised $75 million in overall funding. The company plans to utilize newly-raised funds to fuel its market strategy and accelerate product development to meet the requirements of enterprise customers but one of the drawbacks of the product is that it runs on its own unique language called Ludwig. This means their customers will have to buy the language to use the product. This could be a problem as another vendor could offer similar services without requiring customers to invest in and learn a new language. Fugue is also limited by its sole focus on AWS.

INFISECURE

InfiSecure Technologies Pvt. Ltd is focused on bot detection and fraud protection. Their web security platform is built to give organizations control over bot traffic on their sites and therefore protects them from threats like content theft, web scraping, price scraping, account hijacking, carding fraud, and form and comment spam.

What sets InfiSecure apart: Their focus on bots is an interesting take on the typical web protection model. “Bot protection is an emerging space and we believe has a large global market potential. We are very impressed with InfiSecure team and are happy to partner with them in this journey”, said Venkatesh Peddi, Executive Director, IDG Ventures India.

Market Adoption: Within a year of its launch, Infisecure raised $600,000 in seed funding from IDG Ventures and Axilor Ventures and utilized those funds for research, technology investment and overseas expansion. The Indian-based company claims that the U.S. is its key focus market and it also plans to explore Australian and United Kingdom market in next few years.

EVIDENT.IO

Evident.io was founded in 2013 with an aim to make cloud infrastructure security easier and accessible to organizations of all sizes in all industries.

Evident.io’s leaders have worked at some of the biggest names in security and cloud computing including Adobe, Netflix, McAfee, and Trend Micro.

What sets Evident.io apart: The Evident Security Platform (ESP) is an agentless, API-centric platform that combines detection and analysis of misconfigurations, vulnerabilities, and risk, providing a continuous global view and the actionable intelligence needed to rapidly remediate and secure the client’s entire public cloud. ESP claims it can be deployed into even the most complex environments in minutes.

Market Adoption: Evident.io recently announced a partnership with intelligence community investor In-Q-Tel. Evident.io hopes this partnership will open the door for U.S. intelligence agencies to maintain Federal Risk and Authorization Management Program compliance while transitioning to Amazon Web Services.

Earlier in 2017, they finished a $22 million round of funding which they put toward building platforms to support other infrastructures. Their competitors include Dome9 and CloudPassage, among others.

RISKIQ

RiskIQ, founded in 2009, is a cybersecurity company that deals in external digital threat management defense with an objective to provide organizations with unified visibility and control over threats beyond the firewall. It is a single platform for security operations, hunter, defender, and brand protection teams to automate a diverse range of detection, triage, monitoring, and response tasks. RiskIQ monitors advertising networks against malicious content such as malvertising and spyware, and provides mobile app security services.

Based in San Francisco, California, RiskIQ is a member of the Cloud Security Alliance (CSA) and Information Systems Audit and Control Association (ISACA).

What sets RiskIQ apart: The firm claims to detect zero-day threats by addressing four critical problem areas: web scanning, mobile app security monitoring, brand and trademark protection, and malvertisement prevention. In 2015, a study by RiskIQ uncovered that one out of every three content theft sites exposed users to malware.

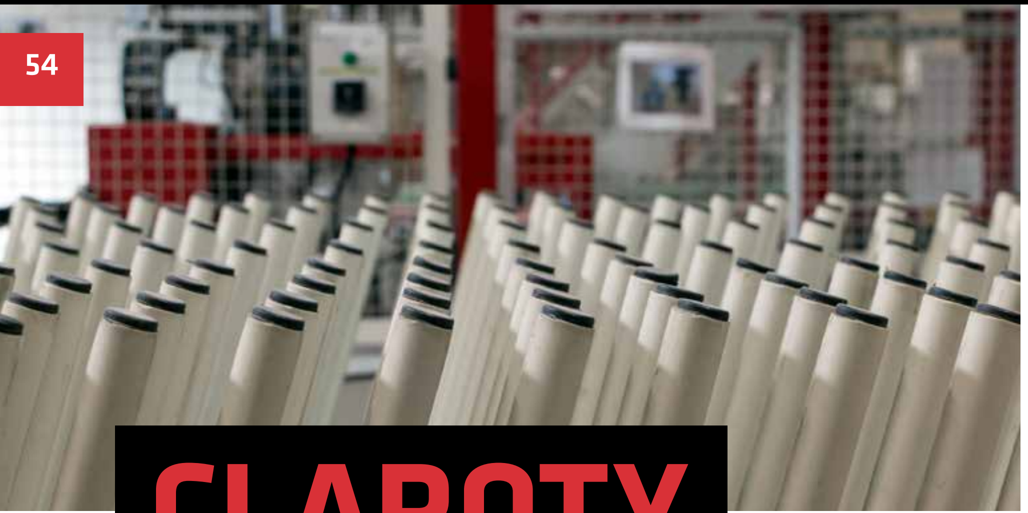
Market Adoption: The company works with Fortune 500 companies, security-savvy enterprises, and growing community of over 20,000 security professionals.

ZONEFOX

ZoneFox focuses on user behavior and behavior analytics to detect insider threats. ZoneFox has a hosted platform to monitor data no matter where it ends up, including tracking file uploads and downloads from a user's endpoint to any network location, including other computers on the local network, computers across the internet and websites or services such as Google Drive. ZoneFox combats the risk of the insider threat by identifying and alerting on anomalous or suspicious activity by monitoring user behavior and data movement, both on and off the network. This includes activity such as file transferring, data loss or theft, writing IP to removable media, tunneling data through the dark web, ransomware and malware files entering the network and unauthorized or suspicious file access.

What sets ZoneFox apart: ZoneFox's claim to monitor and alert on user behavior without drowning you in data is intriguing. They claim to present "No logs, no policies only the insights you need, when you need them so you can focus on the important stuff."

Market Adoption: In March, ZoneFox secured a £3.6m funding boost from Scottish business angel investment syndicate Archangels. Their goal is to have 30 employees by the end of 2017 and set up an office in London to house their expanded sales and technology teams.



CLAROTY

Claroty provides Industrial Control Systems/Critical Infrastructure cybersecurity solutions. The company was recognized as One of the 10 Most Innovative Companies of the Year at RSA 2017. The Claroty Platform is a suite of integrated products specifically designed for ICS environments. It provides continuous threat monitoring and anomaly detection, enables secure remote access for third parties, and provides deep, context based alerts which enable Security and Engineering teams to rapidly respond to identified events.

What sets Claroty apart: The Claroty Platform requires no agents, no plant down time, no complex setup, and no ongoing signature development and tuning. The Claroty Platform is a passive deep packet inspection (DPI) engine and advanced protocol dissector for visibility into ICS networks and protocols. It automatically discovers network assets and communication patterns and builds a very high-fidelity baseline model.

Market Adoption: Claroty products have been running in large-scale, global production environments, at multiple customers, across multiple continents and industrial segments for over two years – including oil/gas, chemicals, mining, manufacturing, food and beverage, and more.

INFOSEC PARTNERSHIPS

In an age where cyber threats are increasingly frequent and the information security business landscape is evolving, it is imperative for CISOs to take a strategic leadership role and adopt a collaborative and inclusive approach. An acquisition or a collaboration can serve several purposes for organizations, from propelling them into new markets to strengthening their critical IT infrastructure to sharing information for turning knowledge into action. These partnerships can be difficult, challenging, or chaotic events, but can represent the positive change for a business. In this segment, we take a look at some notable collaborations and acquisitions in the cybersecurity domain.

CISO MAG staff

SINGAPORE AND JAPAN FINALIZE PACT TO STRENGTHEN CYBERSECURITY COOPERATION

On September 18, during Singapore's International Cyber Week (SICW), Japan and Singapore signed a Memorandum of Cooperation (MoC) to strengthen cybersecurity cooperation.

The signing ceremony between David Koh, Chief Executive of the CSA, and Dr Ikuo Misumi, Deputy Director General of Japan's National Center of Incident Readiness and Strategy for cybersecurity (NISC), took place at The St. Regis Singapore Hotel.

In a statement, Singapore's cybersecurity agency (CSA) said "the agreements related to cybersecurity will promote closer cooperation between the two countries in addition to information exchanges, collaborations to enhance cybersecurity awareness, joint regional capacity-building efforts, and sharing of best practices."

Speaking at the opening of the ASEAN ministerial conference,

Koh said "before this, Singapore and Japan had already been working closely together on various cybersecurity initiatives at both the bilateral and multilateral levels, and the deal will serve to bring our cooperation and relations a step further."

Yaacob Ibrahim, Singapore's minister for communications and information, called for "a coherent, coordinated global effort" that would facilitate a "confident exchange of information among states and execution of joint operations to effectively respond to trans-boundary cyber threats."

In 2018, Singapore is planning to further their cybersecurity agenda by introducing a cybersecurity bill in parliament to facilitate information-sharing and empower the local authorities to work closely with affected parties to resolve cybersecurity incidents.

ENGILITY BAGS CONTRACT WORTH $28 MILLION FROM DEPARTMENT OF DEFENSE

On October 10, Engility Corporation received a five-year contract worth $28 million to provide cybersecurity services to help safeguard technologies from foreign exploitation to the Department of Defense (DoD) Acquisition and Weapons Systems. The contract contains a one base year and four option years.

In a statement, Engility Holdings said "the contract supports DoD's Damage Assessment Management Office and Joint Acquisition Protection and Exploitation Cell. This effort seeks to help protect the government throughout the manufacturing supply chain and defend the military's acquisition programs and technologies from foreign adversaries".

According to the contract, Engility will work with agencies across the counter intelligence, intelligence, and law enforcement communities to assess existing information exploitation in the U.S. defense systems, address vulnerabilities and mitigate future attacks.

Small business Systems Planning and Analysis (SPA) will act as subcontractor. Founded in 2012, defense and space industry Engility Corporation serves a variety of customers with varying degrees of security requirements.

CISCO, CB BANK, NEX4 ENTER INTO TECHNICAL COLLABORATION

Cooperative Bank and Cisco Systems, a U.S. based-multinational technology conglomerate, entered into a collaboration to transform Cooperative Bank's data center and core network infrastructure and to enable core banking applications, digital banking, and international services to be delivered to its customers and partners in a secure manner. The signing ceremony took place at Melia Hotel in Yangon on September 26.

CB Bank has engaged the Cisco Advanced Services team to maintain the highest standards for the design. For the implementation of this project, Cisco Advanced Services team has partnered with NEX4 ICT Solutions.

US ARMY TIES UP WITH IBM FOR CLOUD SERVICES

IBM recently announced that the U.S. Army's Logistics Support Activity (LOGSA) awarded IBM a contract to continue providing cloud services, software development, and cognitive computing, constituting the technical infrastructure for one of the U.S. federal government's biggest logistics systems.

The 33-month, $135 million contract represents a successful re-compete of work that LOGSA signed with IBM in September 2012. Under that managed services agreement, the Army pays only for cloud services that it actually consumes. The efficiencies created by this arrangement have enabled the Army to avoid about $15 million per year in operational costs.

In addition to continuing to provide managed services as part of this new contract, IBM will also help the Army focus on:

- improving cybersecurity by applying risk management framework (RMF) security controls to LOGSA's IT enterprise. RMF is the unified information security framework for the entire U.S. federal government; it replaces legacy IT security standards.
- incorporating cognitive computing that enhances readiness by anticipating needs.
- speeding application modernization.

As part of this new contract, IBM will also help the Army predict vehicle maintenance failures from more than five billion data points of on-board sensors that will be stored within this environment. In addition, the Army is adopting Watson IoT services and a new Watson IoT Equipment Advisor solution that analyzes unstructured, structured, and sensor data directly from military assets.

In addition to private cloud deployments, IBM manages five dedicated federal cloud data centers, including a cloud environment accredited up to impact level 5 (IL-5). These were built to meet Federal Risk and Authorization Management Program (FedRAMP) and Federal Information Security Management Act (FISMA) requirements for government workloads.

SIEMENS PARTNERS WITH ISA TO IMPROVE AWARENESS ON INDUSTRIAL CYBERSECURITY

Catering to the changing landscape of industrial cybersecurity, the International Society of Automation (ISA) has entered a global partnership with Siemens to improve awareness on industrial cybersecurity. The partnership aims at broadening the cybersecurity understanding in industries, establishing best practices, and the adoption of updated methodologies to combat cyber attacks and incidents.

"Cybersecurity needs to be addressed by industrial companies as recent global ransomware attacks have demonstrated the possible

impacts in the last weeks. Our customers need to adequately manage the associated cyber risk, arising from the vulnerabilities of IT technology combined with the increased connectedness in our digital age," said Henning Rudolf, Global Head of Siemens Plant Security Services.

The organizations will also develop procedures for standardizations in the industrial cybersecurity domain by sharing expertise in protecting automation environment based on ISA Security Compliance Institute (ISCI)'s ISA/IEC 62443 cybersecurity standards.

"ISA is committed to providing high-quality technical resources covering all areas of cybersecurity. Within our brand family, we have the entire spectrum of cybersecurity education and advocacy covered, from the development of the world's only consensus industrial cybersecurity standard, to critical education on the topic, to compliance programs that help companies certify products and systems," said Jennifer Halsey, ISA Director of Marketing & Communications.

The two organizations will also co-sponsor events, webinars, and other educational activities intended to raise awareness on cybersecurity. The first activity in the pipeline will be two live webinar sessions titled "Cybersecurity for Control Systems in Process Automation" with Siemens Plant Security Services Product Solution and Security Officer (PSSO) Robert Thompson and ISA 99/IEC 62443 Committee Co-Chair Eric Cosman.

BT OPENS NEW CYBERSECURITY HUB IN AUSTRALIA

Telecommunications provider BT and the New South Wales government recently announced the opening of a new global security hub in Sydney, Australia. The new facility, which is BT's first R&D facility outside of the UK, will help in research and development in cybersecurity, machine learning, cloud computing, big data engineering, data science analytics and visualization, among others.

To build the center, BT invested AU$2 million ($1.6 million) and the New South Wales government invested AU$1.67 ($1.34 million). It will create 172 new jobs over the next five years and will be among BT's 14 global security operations centers.

"This cutting-edge operation will help keep Australia's best cybersecurity talent here in NSW while nurturing our next generation of specialists to ensure we remain a regional leader in this fast growing industry. As well as creating 172 jobs, including 38 jobs for skilled graduates over the next five years, BT will also make a $2 million investment in capital infrastructure and a further multi-million-dollar investment to employ cybersecurity specialists at the hub," said Matt Kean, minister for innovation.

FINTECH SECURITY SUMMIT 2ND EDITION

Preeti Panwar

An initiative by EC-Council, the second edition of the Fintech Security Summit is based on the theme of “NextGen Cybersecurity for Finnovation.” The event, to be held from December 3, 2017, to December 7, 2017, in Abu Dhabi, UAE, will be an opportunity for insightful speakers to provide international solutions to cybersecurity and technology-related woes and other pressing issues facing the cybersecurity world. The event will also host C|CISO training from Dec. 3 to Dec. 6 followed by a Business Summit on Dec. 7.

The 2nd Fintech Security Summit is expected to be attended by over 200 experts from the Middle East and across the world to speed up with the dynamic financial technologies market. The event will be attended by cybersecurity influencers, thought-leaders, innovators across India, USA, Singapore, Malaysia, Indonesia, Hong Kong, Nepal, and Philippines.

The highlights of the event will be international keynotes, special addresses, 12 focused sessions, panel discussions, networking, and a startup “Launchpad” session, among many others.

The Summit will showcase innovations in the financial technologies space and address cybersecurity dynamics involved in the digital era.

Abu Dhabi was chosen for the event venue because of its emergence as a financial technology hub in the Middle East market. Recently, a few key events in Abu Dhabi have changed the industry. First, the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM), and the International Financial Centre in Abu Dhabi sent out its approach to Initial Coin/Token Offerings (ICOs) and virtual currencies under the Financial Services and Markets Regulations (FSMR. Also, on October 11, ADGM and Yes Bank entered a collaboration to enable FinTech innovators from the Middle East region and India to apply into YES FinTech programs and the ADGM’s Regulatory Laboratory to have the opportunity to expand into each other’s markets.

The agenda of the Fintech Security Summit will focus on providing a safe environment for banking and financial technologies services from the ever-growing threats of cybercrimes. Compliance synergies, disruptive technologies, artificial intelligence, cyber vulnerabilities, and cloud migration are the some of the topics that will be addressed.

The much-awaited event gathering will commence with a welcome address by Mr. Jay Bavisi, the CEO & President of the EC-Council.

The first keynote is entitled “Understanding the Road Towards Digitization and Building the Necessary Security Infrastructure for It.” The talk will cover topics such as the role of accelerator programs, testing and developing innovative concepts in a regulatory-lenient but controlled environment, and Fintech self-regulation.

The special address will be all about “Decoding the Regulatory Framework for Fintech Startups in the Region” and will cover the role of international cooperation, favorability of the UAE to become the Fintech hub of the MENA region, and the UAE’s National Innovation Strategy.

The panel of astute speakers includes:

- Anshul Srivastav, Chief Information Officer & Digital officer, Union Insurance, UAE
- Abdullah Mutawi, Partner, Baker Botts, UAE
- Ahmed Baig, Co-Founder, CISOCONNECT
- Alexander AA Director, Cyber Intelligence & Fraud Investigations, VISA, UAE
- Charles L. McGann Jr. COO McGann Consulting Group, USA
- Hock Lai Chia, President, Singapore Fintech Association, Singapore
- James Greenwood, Chief Technology Officer, BankCLEARLY, UAE
- Malikkhan Kotadia Mentor, The FinLab Pte Ltd, Singapore
- Rajesh Kumar, Director, Compliance Risk Control – AME Standard Chartered Bank, UAE
- Saleem Ahmed, Senior Vice President-Head of Information Technology, Sharjah Islamic Bank

The second keynote address will be “Cyber Security in the Age of Regtech” and will include issues such as intersecting regulation with innovation, mitigating risks using disruptive technologies to combat cybersecurity, fraud detection, regulatory reporting, risk data aggregation and stress testing, managing compliance challenges, and improving data management while reducing costs.

A panel discussion about “Blockchain, Cloud and Artificial Intelligence: Modern Innovations are Rethinking the Future of Cybersecurity” will follow. The session will be chaired by Anshul Srivastav, Chief Information Officer and Digital Officer, Union Insurance, UAE and panelists will include Charles L. McGann, Jr. COO McGann Consulting Group, USA.

The second half of the event will be chaired by Malikkhan Kotadia, Mentor, The FinLab Pte Ltd, Singapore and panelist Rajesh Kumar, Director, Compliance Risk Control – AME Standard Chartered Bank, UAE. It will feature discussions on the following topics:

- With the importance of cloud computing for growing your business, how prepared are you to combat the security and scalability challenges?
- With security as the basis, how is the Middle East financial services sector transforming with Blockchain?

Four slots have been reserved for technical addresses before the closing panel discussion on “Addressing Cyber Security Vulnerabilities in the FinTech Era,” with panelist James Greenwood, Chief Technology Officer, BankCLEARLY.

Due to the ongoing, high-profile data breaches in 2017, cybersecurity is a trending topic in all kinds of media. It is imperative that information security executives are updated about the incidents around them. Read on for the 10 most important cybersecurity stories of the last two months.

CISO MAG staff

canada/home/en_ca_b/
EQUIFAX
PERSONAL
Business
About Equifax
Products
Education Centre
Credit Report Assistance
Update on Equifax Cybersecurity Incident
Equifax Canada is providing additional information to Canadians that may be
cybersecurity incident announced last
you do?

EMBATTLED EQUIFAX ON A TIGHT ROPE AFTER MASSIVE HACK

One of the three major credit reporting agencies, Equifax Inc., was left embarrassed when an enormous data breach affected 145.5 million of its customers.

The attack: Equifax discovered the security breach on July 29, 2017, but waited until after the close of trading on September 7, 2017, to disclose the breach to consumers and investors. The breach that took place between May and July of this year compromised personal data including customers' names, social security numbers, addresses, credit card numbers, and other financial details that could be used by criminals to steal identities for financial gain.

Analysts at Morgan Stanley Capital International (MSCI) warned Equifax in August 2016 that it was not well-equipped to protect the personal data of its millions of customers. A Baird Equity Research report revealed that the data breach suffered by Equifax seems to be due to a vulnerability in the open-source Apache Struts Framework. However, the firm neither publicly confirmed nor denied that the flaw in Apache Struts is the root cause of the incident, though the company admitted that a Web application vulnerability may be the reason behind the breach.

The investigation: The Department of Justice in Atlanta and the Federal Trade Commission initiated an investigation into the data breach. The credit reporting giant now faces more than 20 private breach-related lawsuits nationwide and began its own internal investigation with FBI officials.

On October 4, Equifax announced that the cybersecurity firm Mandiant has completed the forensic portion of its investigation of the breach to pinpoint the consumers potentially impacted.

The effect: On September 26, 2017, the San Francisco Superior Court sued the credit reporting firm for failing to protect the personal data of 15 million Californian residents. The lawsuit was filed on same day as Equifax's CEO Richard Smith "stepped down" following the company's chief security officer and chief information officer also retiring.

The current situation: On October 12, Equifax lost a fraud prevention contract worth $7.25 million with the Internal Revenue Service that it had been awarded on September 29.

Zimbabwean activists reject Ministry of Cybersecurity

Several human right activists, war veterans, and opposition parties are protesting the newly established Ministry of Cyber Security of Zimbawe, stating that the ministry poses a threat to the nation's freedom of expression.

The reaction is due in part to President Robert Mugabe's comment that "the abuse of social media (is) a threat to the country's security" and said the new ministry of cybersecurity was being set up to control this.

According to President Mugabe Spokesperson George Charamba, the action comes against the backdrop of recent critical supply-shortage of basic commodities, which he says was because of panic-buying due to false rumors spread on social media. According to him, the incident had triggered a 'sense of panic in the economy.'

"They can't turn Zimbabwe into a North Korea. For your information in North Korea, they don't have social media itself. They can't pull back social media at this stage, so it's completely unfortunate and uncalled for," the leader of Transform Zimbabwe Jacob Ngarivhume said. According to him, social and political activism is what the government is actually trying to curtail.

US bans Russia's Kaspersky software over security issues

Following allegations that Russian hackers interfered in 2016 U.S. elections and amid fears that it could jeopardize national security, the Department of Homeland Security banned the Moscow-based multinational cybersecurity firm Kaspersky Lab in September, citing concerns the company may be linked to the Kremlin and Russian spy agencies.

Recently, the U.S. National Security Agency contractor came under scanner, whose personal computer was equipped with Kaspersky anti-virus software and confidential details were shared with the Russian company. The unidentified NSA contractor had reportedly downloaded a cache of classified information from his workplace, even though he was aware of the consequences that moving such a classified and confidential data without approval is not only against NSA policy, but it also falls under criminal offence.

Elaine Duke, the Acting Secretary of DHS, had given federal agencies a 90-day deadline to get rid of all Kaspersky software from their networks. Shortly after the ban, Best Buy, America's largest electronics retailer, pulled all Kaspersky products from its shelves and website. On July 11, the federal General Services Administration, the agency in charge of government purchasing, also removed Kaspersky from its list of approved vendors.

Kaspersky Lab has repeatedly denied that it has any unethical ties to any government and said it would not help a government with cyber espionage or offensive cyber efforts. It also highlighted that more than 85% of its revenue comes from outside Russia. It maintains that it has no connection with Russian intelligence but it is registered with the Federal Security Service.

To restore people's and government's trust again, Kaspersky on Oct 23 allowed to have his company's source code audited independently by "an internationally recognized authority" in the first quarter of 2018, as part of "comprehensive transparency initiative." Founded in 1997, Kaspersky plans to open three "transparency centers" across United States, Europe, and Asia by 2020.

Deloitte hack: Iranian hackers 'honey trapped' cybersecurity employee

Deloitte, one of the 'big four' multinational accountancy and consulting firms, discovered a breach in March of this year. The incident led to an embarrassment for Deloitte as it is one of the world's best cybersecurity consulting firms. The first alarm bell rang after Deloitte hired the U.S. law firm Hogan Lovells on special assignment to review a possible cybersecurity incident earlier this year.

Iranian hackers were said to be behind the hack, which was executed with the help of a seriously convincing fake Facebook post. The hacker crew known as OilRig created "Mia Ash," a fictional female, to execute its plot. The perpetrators penetrated Deloitte's systems back in July 2016 after Mia's puppeteers targeted a Deloitte cybersecurity employee, engaging him though the social network in conversations about his job. After sending messages on Facebook from July 2016 to February 2017, Mia Ash disappeared from the social networking site. She somehow managed to convince the Deloitte staffer to open a file purportedly containing some of her photos on a work laptop. The account only required a single password login that gave them "access to all areas" of Deloitte's global email server.

To investigate the incident, an internal inquiry team, codenamed Windham, was set up. The team's conclusion was that the data of only six clients had been compromised. However, sources said data from as many as 350 clients including four U.S. government departments, the United Nations and some of the world's biggest multinationals, were compromised. The case is now being investigated by Eric Schneiderman, New York State's Attorney General.

Yahoo 2013 data breach: All 3 billion user accounts hacked

Internet Service company Yahoo! confirmed that during a major data breach in August 2013, three billion of its user accounts were affected. This new figure is triple of its December 2016 claim that only 1 billion accounts were compromised. The company, that took three years to discover and disclose the breach, on October 3 said it is sending email notifications to additional affected user accounts.

One of the biggest data breaches ever reported, the hacked data exposed some of the most personal information of users including their names, email addresses, usernames, telephone numbers, dates of birth, encrypted passwords, unencrypted security questions and answers, and even backup email addresses used to reset lost passwords.

Yahoo! was hit by another enormous cybersecurity breach in late 2014 that impacted 500 million accounts and was disclosed in September 2016. Due to the severity of two cyber attacks, U.S. telecom firm Verizon lowered its original offer to acquire Yahoo! by $350 million and finalized the deal at $4.48 billion in June 2017. Yahoo! is part of Verizon's digital media company Oath.

The Yahoo! 2013 intrusion is being investigated by the U.S. Securities and Exchange

Commission (SEC). The investigators suspect that the Russian government may be behind 2013 breach.

In March 2017, the Department of Justice charged four men, including two Russian intelligence officers and two hackers, in connection with the 2014 breach. Once the Internet giant, Yahoo! now faces 41 consumer class-action lawsuits in the U.S.

Domestic companies to be preferred for Indian government's cybersecurity procurements

With a vision to promote domestic technology and to prevent data theft, the Indian Ministry of Electronics and Information Technology (MeitY) announced that Indian companies will now get preference in their government's cybersecurity procurements. The new policy is part of the country's "Make In India" program and includes both hardware and software solutions.

The announcement issued by the Department of Industrial Policy and Promotion (DIPP) stated "Preference shall be provided by all procuring entities to domestically manufactured/produced cybersecurity products as per the order. The Government has issued public procurement order to encourage "Make in India" and to promote manufacturing and production of goods and services in India with a view to enhancing income and employment."

As per the policy, a cybersecurity product means a product or appliance or software manufactured or produced for the purpose of maintaining confidentiality, availability, and integrity of information by protecting computing devices, infrastructure, programs, data from attack, damage, or unauthorized access.

The notification defined a 'local supplier' of domestically manufactured or produced cybersecurity products as a company incorporated and registered in India. It also mentioned that resellers, dealers, distributors, and support service agencies of foreign-developed products and services who have limited rights to a product's intellectual property are exempted from the tentative mandate. A preliminary list of affected cybersecurity products includes 20 items such as big data analytics, secure access products and services, Web security products and services, antivirus and antimalware products and services, and mobile payment products and services, among others.

Singapore ranked as the top attacker

Singapore has been ranked number one when when it comes to leading the world in launching cyber attacks. The island nation outstrips superpower nations such as the U.S., the UK, Russia, Cyprus, Italy, France, China, Germany, and the Netherlands, a report revealed.

Eying Wee, Asia-Pacific spokesperson from Check Point, the firm behind the report, told *The New Paper* that even though the attacks are launched from computer systems in Singapore, the perpetrators behind these attacks hijack the vulnerable systems remotely. She explained that the high volume of Asia-based business traffic and massive computing power of the country makes it favorable for the hackers.

However, in the past, Singapore also witnessed cyber attacks on its government agencies, universities, and companies.

Simultaneously, the list of top ten "Target Countries" was also released that features Colombia on top followed by India, Saudi Arabia, Ecuador, and Taiwan. Earlier this year, a survey by United Nations International Telecommunication Union (ITU) revealed that Singapore has the best cybersecurity approach in the world. Also, Singapore recently allocated S$1.5 million ($1.1 million) to train incident responders and operators to tackle cyber threats. The move was a part of ASEAN Cyber Capacity Building Program (ACCP) that endeavors to develop technical, policy, and strategy-building capabilities within ASEAN member states.

Facebook fined $1.4 million by Spanish data regulator

Spanish privacy regulator AEPD imposed a fine of 1.2 million euros ($1.44 million) on Facebook for failing to protect users' data that the company allowed to be accessed by advertisers. According to the regulator, the personal data of users collected by Facebook "does not adequately collect the consent of either its users or non-users, which constitutes a serious infringement."

The regulatory body stated that the data collected include political ideology, sex, religious beliefs, personal tastes, and browsing history, but the users remain unaware of Facebook sharing the data with advertisers. Facebook is also accused of using cookies to track user activity on the web, including on non-Facebook sites. Additionally, the agency claims that the users' site navigation information and personal data are retained by Facebook beyond the period of its stated purpose.

"When a social network user has deleted his account and requests the deletion of the information, Facebook still keeps the information for more than 17 months, through a deleted account cookie," AEPD stated.

AEPD further claimed that the privacy policy of Facebook contains "generic and unclear expressions" which can only be accessed by users after many levels of navigation.

Saying that Facebook should obtain "unequivocal, specific and informed consent" from their users, the enforcement agency found one "very serious" and two "serious" issues.

North Korea hacks U.S and South Korea joint war plan

North Korean hackers stole a vast cache of highly classified military documents from South Korea, involving its U.S. ally. South Korean lawmaker Rhee Cheol Hee told *Chosun Ilbo*, a Korean daily newspaper, that the hackers had broken into South Korea's military network in September 2016 and gained access to 235 gigabytes of sensitive data.

Rhee was quoted saying that "Operational Plans 5015 and 3100" and a contingency plan containing the South Korean military's plan to remove North Korean leader Kim Jong Un, referred to as the "decapitation strike" plan, were among the leaked documents.

"80 percent of the leaked documents that were compromised is yet to be identified", Rhee added.

According to the South Korean government, Pyongyang has a 6,800-strong unit of trained cyber-warfare specialists. In May this year, North Korea had reportedly hacked into Seoul's military intranet, but it wasn't revealed what was leaked.

Recently, U.S. President Donald Trump tweeted saying that diplomatic efforts with North Korea have consistently failed, adding that "only one thing will work."

Poland to set up cybersecurity infrastructure

Poland Prime Minister Beata Szydło announced that a new department of cybersecurity will be set up in her office. "I have decided to create a department, which is currently being set up at many offices of the EU's prime ministers, whose task will be analyze, monitor, and serve as my network of experts," she said in a statement.

While acknowledging that cybersecurity is among the most important challenges for the modern world, Szydlo said "This is about the economy, security, it's a question of stability, but also — I think we all realize — of peace."

The head of the government also said that an expert team was needed in her chancellery in order to meet the challenges of the present day and to have a modern PM's office.

Antoni Macierewicz, Polish defense minister, added, "Poland is going to have a "cyber army" of at least 1,000 soldiers within several years capable of waging warfare in cyberspace."

"We are aware of how much responsibility falls on Poland because of the key role it plays on NATO's eastern flank" he said. In June this year, it was reported by Kosciuszko Institute that Poland may become a global leader in the cybersecurity sector.

Juliusz Brzostek, Director of Poland's National Cybersecurity Center, at an earlier event stated that "Computer Emergency Response Teams (CERT) Poland is one of the most active teams in the world and has very experienced researchers." Also, Poland's digital affairs ministry had earlier released the draft cybersecurity strategy for the 2017-2022.

GLOBAL CISO AWARD 2017

CISO MAG staff

In a black-tie ceremony, EC-Council honored leaders in information security by recognizing finalists and winners in seven categories. The CISO Awards preceded both Hacker Halted, EC-Council's largest annual cybersecurity conference, and the Global CISO Forum, EC-Council's premier executive-level event. EC-Council's CISO Awards recognize leaders making an impact by implementing security programs and security awareness programs that break the mold and address the root problems of modern breaches. These awards are decided by a committee in an anonymous voting process.

The first award given was the Presidential Award for Excellence to Nitin Kumar, the Senior Managing Director of Technology, Media & Telecom for FTI Consulting where he manages innovations in security across multiple industries. Kumar is a founding member of the Certified CISO Executive Board and has helped shape the CCISO program and initiatives since its very inception.

The next category was the Innovative Security Project of the Year, wherein EC-Council recognizes a CISO for a specific effort that made a lasting impact to his or her business. The winner, Jorge Mario Ochoa Vasquez, is the CISO for Tigo Guatemala and he focused his innovative project on an area critical to the success of a security program — end user awareness. After a thorough measure of the demographics of his company, adjustments were made to the communication strategy that led to drastically improved outcomes for participation, comprehension, and phishing incidences.

The next award was the Most Improved Security Program of the Year. This award was designed to recognize CISOs who have been able to make huge strides in their programs in a short time. Nominations outlined where their programs started, the changes implemented, and the improvements realized. The runner-up for the award was John Young, IT Security Manager, for his work with the People's Postcode Lottery security system.

The winner, Hemant Dusane, Chief Information Security & Risk Management Officer of Rage Frameworks, focused improvements for his program on reducing the delays caused by information security measures to product development, thereby reducing project teams' hesitance in involving security as early in the project as possible.

The third award is for the CISO of the Year and is EC-Council's chance to look out at the industry and acknowledge a distinguished professional making a difference in the security of not just their organization, but the world at large. The finalists for the awards were John Christly, Global CISO at Netsurion and EventTracker; Heath Renfrow, CISO at US Army Medicine; Sumit Dhar, Senior Director & Head, Information Security & Risk Management; Tim Callahan, SVP, Global Chief Security Officer at Aflac; Ashvin Parankusha Narasimha Murthy; Risk and Compliance Leader at IBM; Aneesh Nair, CIO at NDTV Worldwide; and Youseff Elmalty, Global Cybersecurity Architect at IBM.

The winner, Heath Renfrow, CISO of Army Medicine, oversees a vast network of military healthcare entities. He has helped guide his teams to executing the Risk Management Framework and NIST standards throughout not only the enterprise, but also with the medical devices and their vendors. He oversees a complex and vast worldwide cybersecurity program, which not only includes the security of the enterprise, but the manpower recruitment, training programs, budgetary management, and many other complicated duties as well.

The final award was the Certified CISO of the Year. The Certified CISO program has been in place since 2011 but has seen an explosion of growth around the world in the last two years. Finalists included Favour Femi-Oyewole, CISO of the Nigerian Stock Exchange; Vijay Haripal, Director, Solutions Architecture for Optiv; Bob Van Graft, Director IT/CISO for Vrije Universiteit Amsterdam; Cory Mazzola; CISO of the Las Vegas Sands Corp; Sean Walls, Senior Director of Information Security for Presidio; Mike Santos, Director of Security and Information Governance; Syed Ovais Irfan, ISM South Asia Region SSC, IT Manager, BGV Pakistan Pvt. Ltd; Patric Versteeg, CISO at Novamedia; Craig Goodwinn, Vice President, Chief Security Officer (CSO) at CDK Global; Marco Pacchiardo, Senior Enterprise Security Architect EMEA at Akamai; and Blake Holman, CIO & HIPAA Security Officer at St. David's Foundation.

The CCISO of the Year winner was Favour Femi-Oyewole, CISO of the Nigerian Stock Exchange, a self-driven, motivated, problem-solving CISO with a positive, can-do attitude. Oyewole strives to suggest ideas, innovations, and drive solutions. She worked tirelessly to deliver twenty policies within six months of joining the organization and this had grown to about 120 security policies at the time of the nomination.

SHADOW IT:
BLENDING INNOVATION WITH RISK

Tari Schreider
Chief Cybersecurity Strategist and Author, Prescriptive RiskSolutions, LLC

Shadow information technology (IT) is a term used to describe the use of applications, cloud services and computing equipment deployed outside of the authorization and control of IT. Shadow IT is nothing new; 20 years ago, unapproved Excel macros constituted unauthorized IT applications. Today, we have to contend with unauthorized micro-data centers, cloud applications, and mobile-based user applications.

CEB, a best practice insight and technology firm based in London, estimates that 40% of all IT spending occurs outside the IT department. That portends a whole lot of shadow IT. Shadow IT is the competition of IT enterprises as users seek ways to gain a business advantage by being faster and cheaper. Many users view their IT organizations as bureaucratic, unresponsive, and expensive.

What are the dangers of Shadow IT?

IT applications and services that hide in the shadows outside of the purview of IT represent a clear and present danger to your organization. When lines of business (LoB) operate outside the boundaries, it subjects your organization to increased threat of data breaches and inaccurate compliance reporting. Consider the risk of running systems that no longer comply with security policies, practice proper maintenance hygiene, disconnect from security monitoring, or opt out of threat countermeasures.

Not to mention unofficial and uncontrolled data flows make complying with security standards and regulations nearly impossible.

The following are key risks resulting from shadow IT:

- ▣ **Data Silos –** Data residing outside of data privacy protections violate legal and regulatory statutes.
- ▣ **Data Transfer –** Sensitive data transferred without data loss prevention monitoring creates a data breach monitoring blind spot.
- ▣ **Data Encryption –** Transferring and storing information without standardized encryption and key management elevates the potential for data loss and complicates data recovery.

Living with Shadow IT

Shadow IT is here to stay and no amount of security FUD is going to change the trajectory of this multibillion-dollar juggernaut. If you try to fight city hall, you will likely lose your management's support and possibly your job. As a CISO, you must be a thought leader in this area and be viewed as part of the solution and not the problem. Part of becoming the solution is to evolve your security organization toward service management. You must find ways to protect those who deploy shadow IT. In doing so, you may very well remove one of the reasons LoBs move to shadow IT.

Finding Shadow IT

There are three ways to locate shadow IT within your organization. The first is ground intelligence — speaking to users and departments to learn of unreported IT functions and operations.

One of the best places to start is accounts payable. Someone must be paying for the shadow IT services and an analysis of technology and service vendors may yield the source. Survey end users about their favorite applications or services to uncover names of applications and services that reside outside of the IT service catalog.

Next, you can use existing technology to identify shadow IT as it most always leaves a trail. The following are just some of the ways organizations have tracked down shadow IT using existing tools:

- **Bandwidth Analysis –** Baseline your bandwidth utilization and alarm on unexplained increases.
- **Cloud Billing Alerts –** Set billing alerts such as Amazon Web Services (AWS) CloudWatch to notify of cloud service overspending.
- **Flow Analysis –** Review network traffic to identify changes in flow or file sharing patterns or unexpected network protocols.
- **Network Discovery –** Use network auto-discovery to identify new devices attached to the network immediately.
- **Web Proxy Log –** Review logs to identify websites your organization connects, flag and investigate unauthorized sites.

The last option is to invest in an application designed to identify and control shadow IT. The biggest area of growth in shadow IT is the cloud. I am suggesting looking at acquiring a cloud access service broker (CASB). Not only can you manage your current cloud service providers and implement security policies, but you can also identify unauthorized IT sprawl.

Cloud Access Security Broker (CASB) Solutions

Cloud access security brokers (CASBs) have emerged as a way to not only monitor the instances of shadow IT, but also manage the approved cloud service providers.

CASBs can be provisioned either as an on premise or cloud-based solution. Placed between cloud service consumers and cloud service providers, CASBs enforce cybersecurity policies as consumers access cloud-based resources and services. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, and malware detection and prevention.

These products work especially well performing cloud discovery, providing data breach compliance monitoring, validating encryption strength, and searching for leaking sensitive information. Many of the CASB products bundle web application firewall (WAF) and data loss prevention (DLP) in a single solution. This may offer an opportunity to consolidate existing security technology.

The following table lists the top CASB products in the market:

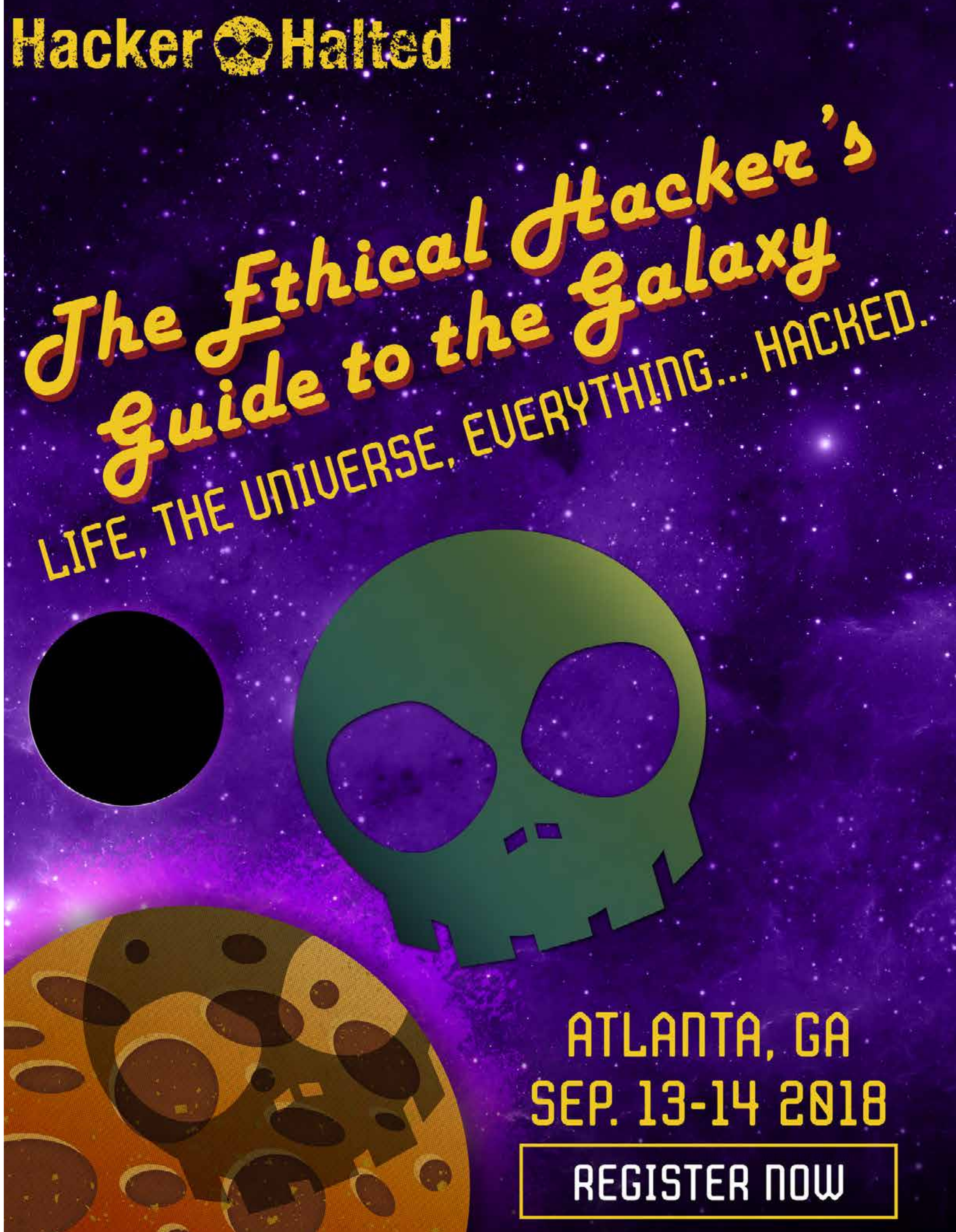
Company	Product
Bitglass, Inc.	Cloud Access Security Broker
CipherCloud	Cloud Security Broker (CSB)
Cisco	CloudLock
Forcepoint by Ratheon	Skyfence Cloud Gateway
Managed Methods	Cloud Access Monitor
Microsoft	Adallom
Netskope	Netskope Shadow IT
Oracle	Palerra LORIC
Palo Alto Networks	CirroSecure
Skyhigh Networks	Skyhigh for Shadow IT
Symantec + Bluecoat	Elastica
Zscaler	Cloud Application Visibility & Control

According to market research firm MarketandMarkets, the CASB market is estimated to grow from $3.34 Billion in 2015 to $7.51 Billion by 2020, at an estimated compound annual growth rate (CAGR) of 17.6%.

One of the most famous examples of shadow IT is Hillary Clinton's use of a private email server deployed at her home office. She essentially became the poster child of shadow IT, bringing to light what can happen when an employee goes IT rouge.

If we cede to the research that insiders are the cause of the majority of attacks, would it not be a safe assumption to say that shadow IT could only contribute to that fact?

As the CISO for your organization, you have to be the thought leader in the area of shadow IT security.


Hacker Halted
The Ethical Hacker's Guide to the Galaxy
LIFE, THE UNIVERSE, EVERYTHING... HACKED.
ATLANTA, GA
SEP. 13-14 2018
REGISTER NOW

CHECK POINT vSEC

Check Point vSEC protects assets in the cloud from the most sophisticated threats with dynamic scalability, intelligent provisioning and consistent control across physical and virtual networks, ensuring you can embrace the cloud with confidence.

For more information visit:
checkpoint.com/products-solutions/vsec-cloud-security

Check Point
SOFTWARE TECHNOLOGIES LTD

CLOUD • MOBILE • THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

Wherever you are. Wherever you go. Whatever the future brings. Check Point keeps you one step ahead.

WELCOME TO THE FUTURE OF CYBER SECURITY

CLOUD • MOBILE • THREAT PREVENTION

Check Point
SOFTWARE TECHNOLOGIES LTD

Learn More: checkpoint.com