CISO MAG

beyond cybersecurity

Volume 2 | Issue 1 | February 2018

CYBERSECURITY THE PHOENIX SAGA

INDEX

EDITOR'S NOTE

The year of 2017 witnessed some of the most brutal cybersecurity meltdowns. The breaches were not always directed toward corporates; some were state-sponsored which did colossal damage to an inordinate number of Internet users. While Equifax and Yahoo stole the headlines with massive breaches, a number of cybersecurity facepalms–like Uber and Deloitte–didn't go unnoticed.

The year 2017 may have created mayhem for information security professionals, but it left them better prepared as well. Some organizations adopted a coordinated approach to cyber risk management and several nations spruced up their cyber divisions in the aftermath of the attacks. Our cover story "Cybersecurity: The Phoenix Saga" takes a look back at the brighter moments of 2017 and suggests that all is not lost.

Move to our Buzz section, where we discuss how cybercrime has jolted the pharma industry and become its biggest health hazard. The feature also suggests selective measures pharma companies can employ to safeguard themselves against intellectual property theft.

In our Under the Spotlight section, we have JA Chowdary, Special Chief Secretary & IT Advisor to Chief Minister of the Indian state of Andhra Pradesh. He discusses his vision for Fintech Valley in Vizag, Andhra Pradesh, and his efforts for continued development of the Fintech ecosystem in India.

We also interviewed Kelly Isikoff of RenaissanceRe, where she discusses cybersecurity practices in the insurance sector, women representation in the cyber world, and much more.

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 2 | Issue 1
February 2018

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

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

Feature Writer
Nishtha Pathak
nishtha.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
Pooja Saga
pooja.saga@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.

CYBERCRIME: A SERIOUS HEALTH HAZARD

Augustin Kurian

The pharma industry has always been in a tight spot. Keeping up with medical advancements and staying revolutionary in the space are just a couple of the many challenges they face. There is only one constant: the challenges and threats the industry has faced for decades. With technological innovations, cybercrime has joined this new legion of threats to the healthcare technology industry. In fact, a 2015 survey by Crown Records Management revealed that two-thirds of pharma firms had faced data breaches—with one-fourth of these firms reporting they wavictims of cyber attacks. In late October 2016, Northern Lincolnshire and Goole NHS Foundation Trust in the United Kingdom was targeted by a malware attack. Several operations scheduled on that day had to be cancelled, with some trauma patients forced to redirect to a different location. The United States fared no better, reporting an 18.5 percent increase in the pharma sector in 2016 compared to the previous year.

This culminated in May 2017 after the WannaCry attack crippled the UK's National Health Service along with several other companies and establishments. Hospitals and GP surgeries in England and Scotland were among the worst hit. Hospital staff were forced to resort to pen and paper, and their own cell phones because the attack affected key systems, including telephones. Operations, surgeries, and several appointments had to be cancelled after the malware scrambled data networks. The only wing functioning at affected hospitals was emergency medical care. The crypto-worm targeted Windows computers using the EternalBlue exploit, taking advantage of Windows' Server Message Block (SMB) protocol and installing a backdoor implant tool called Double Pulsar. Then, the crypto-worm transferred and ran the WannaCry ransomware package, which, in turn, encrypted data and demanded a ransom from victims in the form of Bitcoin. The attack is among the most infamous ransomware attacks ever, affecting more than 150 countries and 230,000 computers.

The WannaCry attack was a reality check to several pharmaceutical organizations. Following the incident, the industry saw cyber-attacks as a harbinger of several other major attacks the industry was poised to face. This was followed by the ECRI Institute announcing the "Top 10 Health Technology Hazards for 2018 list," which ranked cybersecurity as the number one threat to healthcare technology.

"This year's No. 1 hazard calls attention to the patient safety component of ransomware and other cybersecurity threats. In the healthcare environment, ransomware and other types of malware attacks are more than just an IT nightmare. They are potential patient safety crises that can disrupt healthcare delivery operations, placing patients at risk. Multiple ransomware and other malware variants have infected healthcare organizations, as well as other private and public organizations, throughout the world," ECRI stated. "Patient safety is on everyone's mind, but technology safety sometimes gets left behind," added David T. Jamison, Executive Director of the Health Devices Group, ECRI Institute.

WHY THE PHARMA INDUSTRY?

Simply put, healthcare records are valuable on the Dark Web, which is where black market drug sales occur most often. Pharmaceutical firms create and manage a large amount of intellectual property and data, which can include patient profiles and drugs that are currently in the development cycle (or are already developed). The research and development of these drugs is already cost-intensive for these companies, which makes holding them for ransom so easy to do.

Pharma firms are also targeted due to geopolitical reasons. Most of these companies are based outside of the U.S., making them a favorite of state-sponsored actors and extremist groups. According to a study by Deloitte titled "Cyber & Insider Risk at a Glance: The Pharmaceutical Industry":

"Evidence abounds that pharmaceutical companies are the target of sophisticated Internet criminals. The UK Government identified pharmaceutical companies as the primary target of cyber criminals bent on stealing IP. It estimated cyber-theft of IP cost the UK £9.2b, of which it attributed £1.8b to theft of pharmaceutical, biotechnology, and healthcare IP. Surveys of U.S. cyber attacks consistently find that pharmaceutical IP is a major target of sophisticated cyber gangs. Experts suggest China is using cyber-espionage to support its 5- year economic development plan.

That plan includes expanding China's chemical and pharmaceutical sector. Attacks against major U.S. pharmaceutical companies attributed to sophisticated Chinese hacking groups include Boston Scientific (a medical device-maker), Abbott Laboratories, and Wyeth, the drug maker acquired by Pfizer Inc. The same group successfully hacked the Food & Drug Administration's computer center in Maryland, exposing sensitive data (including formulas and trial data) for virtually all drugs sold in the U.S."

Sometimes, even hacktivists come into the picture, as many of the drugs are quite expensive. Hackers attempt to access proprietary information and disclose data that the firms usually keep confidential.

REGULATORY GLITCHES IN **PHARMA CYBERSECURITY**

Anne Petterd, Principal of Baker McKenzie Wong & Leow, in an interview with Health Care Innovation explained: "In terms of data sovereignty—where a jurisdiction places restrictions on taking data beyond its borders—healthcare data is an issue which comes up frequently when parties are trying to negotiate free trade agreements. There's a notion that if the data is within the country, it may be more accessible to those who need it, be it the patients or the healthcare providers. There's also the notion among regulators that if the data is within the country, it may be more secure. However, if you speak to the cloud providers, particularly those who spend a lot of time investing in security for their products, this may be one of the main issues that they want to discuss with regulators as to whether that is really true. Companies may want to deliver services from one central location for efficiencies across borders, and with that comes savings in terms of time and storage of data, especially when it comes to big data analytics. This is an issue that healthcare companies may feel is constraining them with what they want to do in the region."

She continued by saying: "It's a constant balancing that regulators need to do. Even if a law has been passed that strikes the perfect balance, something might change the next day which means the system is no longer in balance."

She also highlighted that following the WannaCry incident, "The UK government conducted several audits and reviews. One of the recommendations on striking the right balance suggests giving patients more control and choice over who their electronic records can be shared with."

WHAT CAN BE **DONE?**

The pharma industry has possibly the world's largest research and development sector. It is the duty of the CISOs/CIOs to make sure that customer data, intellectual property, and every other valuable asset are protected; more importantly, the companies must have a cybersecurity department at its disposal. Cybersecurity must originate from the foundation of the company—and it must be performed in tandem with the lifecycle of the firm.

It must never be an afterthought.

The attackers are evolving and keeping pace with them is of paramount importance. According to New Hampshire-based Elliot Health System's Chief Information Security Officer Andrew Seward, "You can set the conditions for success." Seward offered this advice in an interview with Healthcare IT News. "You can't know everything, but you can never go wrong with hiring the right people and building a condition of trust."

He continued, "It takes forward-thinking individuals who can see the risk and determine security is a business risk. When you're doing futureproofing, you have to determine how much is enough to manage security, and then how much security is enough."

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

http://bit.ly/2ivU4l9

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

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.

Volume 2 | Issue 1

Volume 2 | Issue 1

FEW MINUTES WITH KELLY ISIKOFF

Group Information Security Manager RenaissanceRe

Rahul Arora

An industry veteran with more than two decades of experience, **Kelly Isikoff** joined RenaissanceRe in 2016 with global responsibility for directing strategy, operations, and budget for the protection of information assets.

Before joining RenaissanceRe, Isikoff was an Executive Director for JP Morgan Asset Management, where she was responsible for setting security strategy and policies as well as managing operational security departments. Prior to her time with JP Morgan, she was a Senior Vice President for Citigroup and managed infrastructure, data management and security across departments. Previously, she has also worked at Warner Music Group, where she led security and new media initiatives to identify innovative revenue channels within technology.

In an exclusive interview with CISO MAG, she discusses cybersecurity practices in the insurance sector, women representation in the cyber world, and much more.

Please tell us about your role and responsibilities in RenaissanceRe.

I am the head of the information security for the global organization. I also manage all of the strategies, programs that will help us maintain our compounds across most of the regions. I also manage the additional groups that feed into security that have a role to support overall defenses. So that being said, a smaller organization unlike the larger organizations I worked with in the past were are using different types of managing security service providers for different capabilities to achieve the same level of security. So my role is to transform the organization and manage a lot of the overall security program and help it to maintain compliance and achieve compliance with pretty big regulations that are coming up and hitting a lot of other financial firms and worldwide global firms. It looks like a lot of the states within the U.S. have started to fall in line with the same cyber regulations that we have in New York. It seems like every country around the world is starting to uplift their cyber regulations, so making sure that we get things right and follow a standard process and framework is the key to making sure that we don't have to continue to go through our compliance checklist with each one of these different countries, states, and jurisdictions.

> Our strategy focuses on cybersecurity framework which is really flexible across the industries and really simple to follow.

Cyber attacks in the insurance sector are growing exponentially, as companies are migrating toward digital channels in an effort to create tighter customer relationships. What are the things RenaissanceRe is trying to keep the hackers away?

I mean there's not one practice that we follow. We have a lot of partners that we work with and a lot of vendors that we manage and that (Third party security management) is a big issue for a lot of companies, not just a company of our size. There are a lot of new companies that are entering the space and provide you assessment services. Unfortunately, some of them are not robust than others. So, third party security is a big issue and we are receiving more and more requests from clients for much more exhaustive security reviews of our control and a lot of my time is dedicated to calls with our investor group, different types of business clients to go over our security program with them and then go over their security program with us. So, there's a lot of vetting of partner security that's happening across the industry.

As you said, you are actually working with a lot of third parties and partners. What do you do to keep the data transfer absolutely secure?

Well we follow different frame works. Our strategy focuses on cybersecurity framework which is really flexible across the industries and really simple to follow, and we also follow top 20 critical security controls which were developed from a lot of industry practice within the community. So, that's our strategy and that's how we set our programs for the year.

How important is cybersecurity education or training for employees in keeping cyber threats at bay?

Security awareness training is very important to us. We have continuous programs as well as digital annual trainings and certifications. Also, there are company meetings on key security risks to the organization. Security is everyone's responsibility, not just one department's. As far as protecting ourselves against a cyber threat, we have a lot of controls on data access on an add need-to-know basis. We really have a strong program around building out our access control of critical data in critical systems.

What is your take on cyber insurance?

We're really seeing an evolution of cyber as a specific product to cyber as a peril which can influence multiple insurance products. Most insurance products today focus on credit marketing and notification cost, and these costs are often required by a regulation. So we see a potential growth for risk managers as they asses a cyber risk for their business and starting to work more with our insurers and re-ensure a way to access monitor and mitigate risks. This could include a broader cover for system failure, and interruptions for example.

Do you think cyber insurance is keeping pace with cyber-exposure?

Definitely, I know that a lot of large finance institutions are increasing their coverage through larger cyber offerings and a lot of other multiple insurance products are starting to develop cyber policies within it. So, we're saying more aesthetic cyber policies into multiple insurance clients.

The representation of women in cybersecurity has remained stagnant at 11 percent for the past four years, according to a report. This is despite growing awareness on cybersecurity, and expanding career options. Most of times, the reasons cited is the lack of women role model and the impression the industry carries. What can be done to break the

gender stereotype so that women, even in their teens, are inclined to join the cybersecurity space?

Well, you're right! There's definitely a skill gap and I do feel like a minority in my profession. I think some of the things we can do is promote cybersecurity across universities to encourage young women because it is really dynamic and interesting field that's constantly changing. It's not something for programmers or people who like technology. It is much more diverse than that. You need to have an investigative type of mindset, you need to look at a lot of different ways that your systems, your information, your business can be compromised and have the ability to work with business to understand your risk, so you can protect against them. It's really important for me to mentor young women who are interested and moving into security.

According to you, is there anything that the CISOs are doing wrong at a time when the threats are evolving with each passing day?

What we really need to learn from recent attacks is that CISOs need to understand the full scope of security. It's not just infrastructure parameter anymore. It's also about application, user behaviour, and other things. They need to know the overall threats that are targetting your organization. You need to follow the cybersecurity framework and employing it for your environment and understanding your risk level. For say, if you're managing a company that has a lot of Web exposure, you really have to up your application security program. Overall, understanding the risk level of your organization and speaking closely with the business leaders to comprehend the key risks and how do you mitigate those risks and build a depth of control around those risks. That's what I would recommend the CISOs or new CISOs entering into that space because that's where I've seen a lot of CISOs who failed.

What advice would you give to a budding information security professional?

There are so many different areas within the security to grow into. So, getting a broader in-depth knowledge of various kinds of security domains and understanding the different domains and skills you'd be doing in each area. Basically, understanding what might interest you! That's what I would recommend to anyone who's getting into the security because there are so many different specialties within security. It wasn't like that when I got into security. I worked between infrastructure and application groups, managing security process domain. There weren't many specializations then, whereas now there are so many specializations and with that there are many opportunities to learn and develop unique skills that make you even more valuable in the marketplace.

IT'S TIME TO GET BACK TO THE BASICS

Chris Roberts
Chief Security Architect, Acalvio Technologies

So, the CISO MAG staff and I were talking about an end-of-year article that might get people reflecting on 2017 AND concentrating on 2018. The prediction thing is too fuzzy and I have an aversion to crystal balls, the financial thing is pretty much sorted (everyone got their 2018 budgets locked and loaded? More blinky lights for everyone, right?), and if I hear again that AI or ML is going to solve everything, I will be whipping up another batch of Molotov cocktails to distribute. So, we decided to go back to basics.

The human, the poor sap we sit between the chair and the keyboard, is the one we expect to defend against people like me on a daily basis. We ask them to do this all the while juggling their regular jobs on systems that are either ancient or changing every 5 minutes with that annoying call of "where's my damn icon NOW?" ringing out across the office. We ask them to defend our companies after we take them for one hour each year and sit in a room with a geek who simply tells them to "Please don't click sh*t, please don't send sh*t, and please stop using P@ssw0rd1 as your Facebook, bank, AND company log in." That's one whole hour, once a year and you then expect them to remember that for the remaining 2,086 work hours in the year (I'm now waiting for someone to tell me it's 2,080 and I'll point out leap years and calendar fluctuations. Trust me, HR folks need advanced degrees in quantum math to work out holidays and work periods!)

> The human, the poor sap we sit between the chair and the keyboard, is the one we expect to defend against people like me on a daily basis.

Here's another thing you're probably not paying enough attention to: those servers. Yes, you know the ones, the ones sitting in the remote office, or the warehouse (yeah, you though I forgot about those didn't you). They're sitting on the same network segment as the rest of the organization, aren't they? The users, servers, printers, doors, AD, and probably even the IoT office-dogs bowl are all sitting on the same network. Just because it's easy, just because you don't know how DHCP or VLANS work, doesn't excuse you from putting some simple separation, segmentation, or other controls in place. Oh, also back to those Windows XP servers in the warehouse, just because the vendor or supplier is too lazy to upgrade them doesn't excuse you from taking adequate protection to reduce the risks accordingly.

And another thing. Recently, we were on an IR engagement and the attackers hit at 22:30 on a Friday night. They were done and out with "job done" left all over the screens 3 hours later (NOT the normal 12 hours AVERAGE it takes to get in and get out without being detected). It took them 3 hours and nobody watching the logs until 0800 MONDAY morning. Get some logging in place, get someone to watch them 24x7, and pony up the minimal money it costs to have some peace of mind!

Don't forget about the computers themselves. You've given each employee a new, shiny computer and you've entrusted them (you fool) with all your data. You're left praying that the sales guys don't trade their laptop for a round of drinks at the next client appreciation golf outing. Why? Because you didn't bloody encrypt them! Seriously, it's free, it's simple, easy, secure, and can be locally or centrally managed. Just do it! That way, the next time you lose the security plans for a major airport or government, you won't be on the 9 o'clock news!

You have lost the battle for the perimeter; accept that and you might be able to focus accordingly. Look at the simple fact that in essence "computer number 1" has been compromised and work accordingly. The concept of predictive, proactive, deceptive technologies should not be alien to you. Neither should you buy next year's purple blinky light F/W and expect it to do anything more than this year's did, EVEN if it has UBA or "Next Gen" or "AI/ML" on it. You have the basic tools; now it's time to elevate them with something OTHER thank the same sh*t that hasn't secured you for the last "x" years. Your presence on the Internets, all of the Internets, the open, dark, and deep – what do you know about yourself that might be out there, what do others know that is out there, and more importantly, what are your users, vendors, suppliers, partners, and trusted resources putting out there about you? Learn what's outside of your four walls and it might help you to focus better on how to protect what's inside them.

Oy vey, physical security still gets overlooked. The systems that are in place can still can be bypassed (in many cases) with a fake business card (Sprint/AT&T, Cable Company), an official looking folder, and a box that looks like an Internets upgrade. Failing that, we're going to go in via your shipping entrance, your vendor (HVAC, water, etc.), or some other way that gets us into your facility. When we get in, we'll find your surveillance is probably on the LAN and if it's working, nobody's watching it. It's still too easy, too simple to walk far enough into many facilities (not always the main office! Got to love satellite offices or warehouses on the LAN) and simply park yourself in their offices and let loose the dogs of war (or a scanner – both are equally effective). Fix the physical and you'll be amazed at the uptake in people caring about how they look after "their" company.

Ok, now on to communications. Let's NOT be another Uber. Sh*t happens – acknowledge it, learn from it, and move on. Humans can be forgiving if you ask for forgiveness, are contrite, accept the blame, and actually do better in the future. How do you avoid becoming another Uber? Communicate across the ranges – the basics of communication are fundamental to our understanding of our environments. Talk with people regularly, explain why decisions around security and integrity are being made, educate them as to the logic for protecting the organization, and help them implement the same protections at home and with their own family. Communication is free and it's a troublingly underutilized tool!

A good friend of mine (F1nux) has a somewhat amazing yet grounded-in-reality statistic. He talks about the number of accounts that are already breached in global organizations at any one point in time and it's ridiculous how many there are. It's more than you'd think, and it's right here, right now. If we can't keep control of our credentials what hope do we have of keeping control of our data?

Embrace the distributed workforce and their desire to connect into the mother ship and then make sure you throw the public facing RDP server off the bloody roof.

All your SQL, MySQL, Oracle, NoSQL and other types of databases that are sitting on the Internets belong to us. This has nothing to do with patching (you are already underwater on that and running round trying to patch things every day of the week isn't going to work). This is back to the fundamentals: certain things should NOT be on the Internets! There's no excuse, there's no way of lying your way out of this one, VPN's are free, easy to implement, and simple to integrate: get the low hanging fruit OFF the firing line!

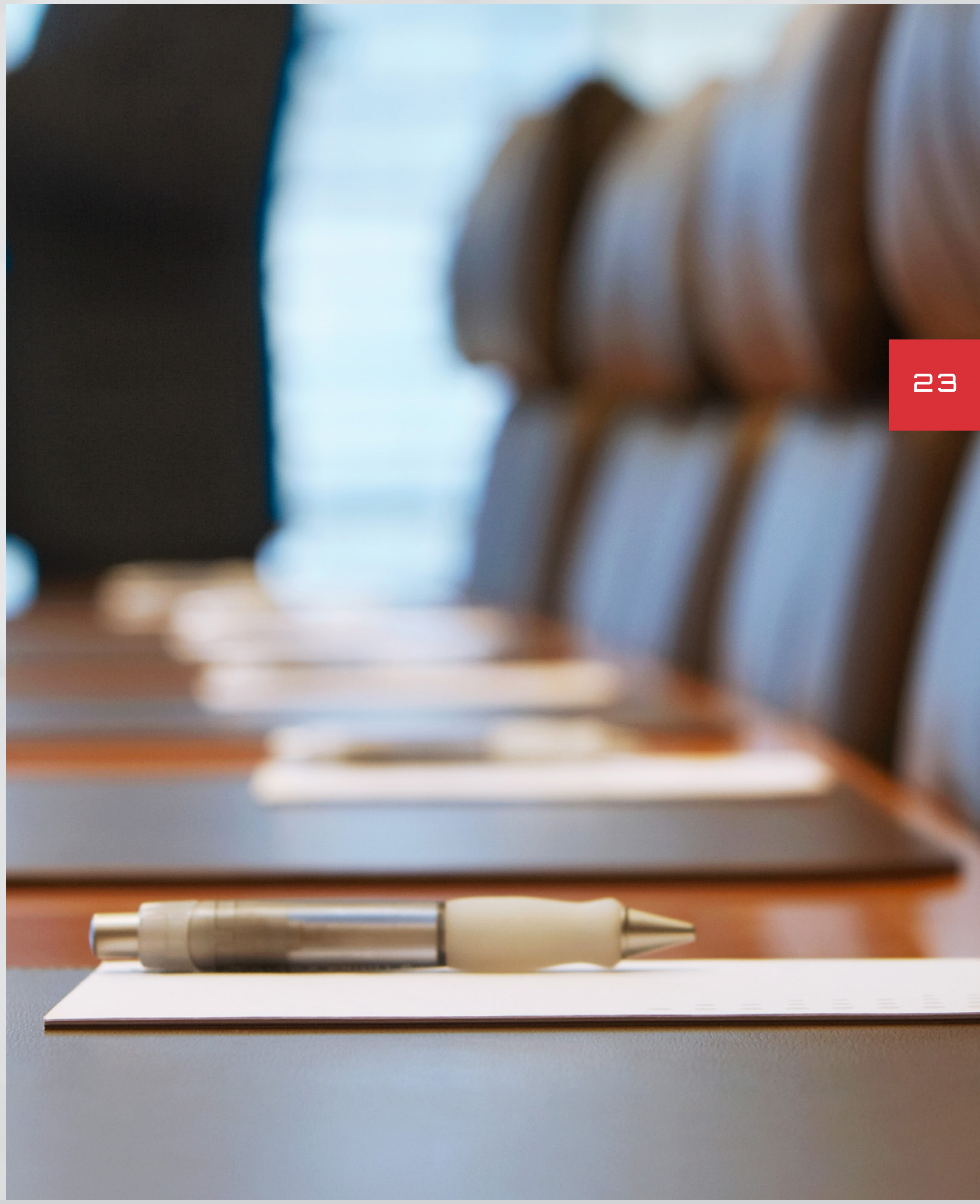
Lastly, the employees, those folks you continue to overlook: we started with them, so it's fitting we close with them. Let's look at a couple of things that you do wrong:

1. You trust them! Why on this great green planet do you do that? You are not nice to them yet you expect them to be loyal and look after your assets and then you are surprised when they turn against you and you have to call us in on the forensics to see what the heck happened and why they dropped all your dirty secrets out to WikiLeaks.
2. You don't train them and then wonder why they email all your PII/PHI/EHR all over the place?
3. You don't give them any incentives to help secure not only YOU (the company) but also their own families and friends, and you still trust them with everything and are surprised when they turn on you.

Good grief, look in a mirror and realize YOU, the capitalist corporation, are the problem. WE ARE NOT A NUMBER, OR A STATISTIC, we are HUMANS. Treat us as such, please.

So, in closing, when 2018 comes for us (or 5775 for those of you currently in a different set of though processes) and the vendors line you up in their sights for golfing, fishing, dinner, and other events to woo you into buying the next NGFW, UBA, purple-blinky light POS, please for all those of us out there fighting the good fight, take a step back, evaluate how that technology will fix the very basics that are crippling your organization (probably without you knowing it) put down the fork or golf club, say NO THANK YOU and spend the time, effort, and money on fixing some of the things I've covered above.

I promise you, if you miss your vendor steak, come to Colorado and I'll buy you one. I live on a golf course so you can go catch that one missed game and your enterprise will thank you a lot more for simply doing the basic things you need to do to protect them and their assets.



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 THE PHOENIX SAGA

Augustin Kurian

2017 may have been one of the worst years for the cybersecurity industry. Time after time, day after day, news of cyber incidents consistently made headlines in major publications across the world. Every kind of cyber incident—from breaches, to ransom campaigns, to DDos attacks, to hacktivism—seems to have taken place during the year. A Norton survey revealed that nearly 978 million people in 20 countries were affected by cybercrime in 2017; 44 percent of consumers were impacted by cybercrime in the last 12 months. All the incidents highlighted major vulnerabilities within systems and unpreparedness among organizations, leading to the damaged reputations of several companies. A study by Bitdefender found that ransomware payments hit $2 billion in 2017, which is twice as much as the year before. It was also the year when tools used by government hackers went public—and when hackers figured out that the best way to target companies was to resort to malware stashed by the government.

So, here is a quick rundown: Shadow Brokers breached the National Security Agency (NSA), leading to the release of a global ransomware campaign, WannaCry, which affected more than 150 countries and 230,000 computers globally. Equifax reported one of the biggest breaches in history, during which hackers infiltrated the website and stole the personal data of nearly 145 million people, including social security numbers. Around June, a virus called NotPetya hit Ukrainian businesses using compromised tax software. On October 24, 2017, Ukraine, Russia, Japan, and Bulgaria were hit by a wave of cyber attacks by a malware dubbed as "BadRabbit" and prompted the Ukrainian (state-run) Computer Emergency Response Team (CERT) to ask transport networks to be on alert. There were several others high-profile incidents, but these were the most notable ones.

There's more to come. However, there is some evidence that we are better prepared than ever before.

"In 2017, cyber attackers created havoc through a range of levers, from phishing attacks that influenced political campaigns to ransomware crypto worms that infiltrated operating systems on a global scale. With the growth of the Internet of Things (IoT), we have also witnessed a proliferation of distributed denial-of-service (DDoS) attacks on IoT devices, crippling the device's functionality," said Jason J. Hogg, CEO, Aon Cyber Solutions, in a statement. "In 2018, we anticipate heightened cyber exposure due to a convergence of three trends: first, companies' increasing reliance on technology; second, regulators' intensified focus on protecting consumer data; and third, the rising value of non-physical assets. Heightened exposure will require an integrated cybersecurity approach to both business culture and risk management frameworks. Leaders must adopt a coordinated, C-suite driven approach to cyber risk management, enabling them to better assess and mitigate risk across all enterprise functions."

Several nations and organizations began sprucing up their cyber divisions in the aftermath of the attacks. For example, the United Kingdom government pledged £21 million to boost the cybersecurity of the National Health Service. The announcement was made in the wake of the WannaCry cyber-attack that crippled the sector. "Careful consideration of how to secure your legacy business systems, what, if any, network security appliances are needed, and which lower-cost solutions can be implemented will give management a better idea of what their needs are in terms of a cybersecurity budget," according to Crowe Horwath, one of the largest public accounting, consulting, and technology firms. "Once these needs are mapped into the organization's long-term plan, the available capital can be allocated for new development. When the budget for new projects is combined with the budget for ongoing maintenance and monitoring requirements, an organization will be able to determine its annual budget for both people and money."

China took major steps forward with the implementation of the China Cyber Law, which imposed strict requirements on data storage and scrutiny. The U.S. Senate imposed the IoT Cybersecurity Improvement Act, which states that smart devices need to meet basic standards if they are to be used by federal agencies. The Ukraine President Petro Poroshenko signed a law that "creates the foundations of a national system of cybersecurity as a combination of political, social, economic, and information relations, along with organizational, administrative, and technical and technological measures of the public and private sectors and civil society."

A proposed cybersecurity bill in the Malaysian parliament seeks to regulate not only current cybercrimes, but also lays the groundwork to deal with coming threats. Even the government of Ghana is mulling over establishing a national cybersecurity center to safeguard the nation against cybercrime. The government of India will introduce multiple checkpoints to ensure that equipment imported for the domestic power distribution sector is not vulnerable to cyber attacks.

Aon Cyber Solutions, a provider of risk advice and insurance solutions, announced its predictions for 2018 and pointed out that "increasing scale and impact of cyber attacks, coupled with companies having to accept more liability and accountability over cyber attacks,

will lead to significant changes in the corporate landscape."

According to Aon, adoption of standalone cyber insurance policies "will spread beyond traditional buyers of cyber insurance, such as retail, financial, and healthcare sectors, to others vulnerable to cyber-related business disruption, including manufacturing, transportation, utility, and oil and gas."

According to a *Forbes report*, "Half of all security budgets for IoT will go to fault remediation, recalls and safety failures rather than protection through 2022." For this very reason, the coming years would make cybersecurity a hot job opportunity, with tech companies indulging in a fastidious talent-hunting spree. The hiring in this space is only going to escalate. There would be a key focus on IoT security due to its explosive penetration. Newer curriculums are being introduced and cybersecurity education is being considered at an early age. Towson University and the Maryland National Guard recently signed an agreement to collaborate on several activities, which included cybersecurity training for students and guardsmen. The need for K-12 students to learn the basics of network security, cryptography, and cyber ethics was one of the key topics addressed in the National Initiative for Cybersecurity Education (NICE) conference in November. According to the speakers at the event, one of the best ways for young students to engage with cybersecurity is to solve real-world problems.

"In the coming years, we will see an expansion of cybersecurity content across the curriculum as all students represent entry points into the broadly defined cybersecurity workforce," said Diana Burley, a professor at George Washington University (2014 Cybersecurity Educator of the Year recipient) in an interview with Monster.com. "Continuous professional development is critical in the field of cybersecurity because the nature of the threat continuously evolves. Many options exist for current professionals to augment their skill set; including certificates from technical training companies, additional degrees through university study, or standalone, hands-on courses to develop specific skills. The right decision depends on specific knowledge or skill required. There are no one-size-fits-all."

> **"Increasing scale and impact of cyber attacks, coupled with companies having to accept more liability and accountability over cyber attacks, will lead to significant changes in the corporate landscape."**

Also, with the GDPR due for rollout this year, several nations will be imposing stricter laws and heavier fines for organizations not taking security seriously.

"In our experience, many organizations that are located outside Europe, but have a global employee and customer base, remain behind the curve in assessing the risks and opportunities of GDPR [...] With massive fines and requirements for notification that will push more breaches into the public eye, GDPR promises to make data privacy a potential public relations challenge. With proposed penalties for falling short of compliance—including fines of up to four percent of total worldwide annual turnover—these potentially staggering numbers have a purpose: to put privacy and data security on the boardroom agenda by bringing it in line with the highest sanctions for regulatory noncompliance—such as anti-bribery and anti-trust laws," said Raymond Teo, Senior Vice President, Business Development, APAC, NTT Security, in his column with *CISO MAG*.

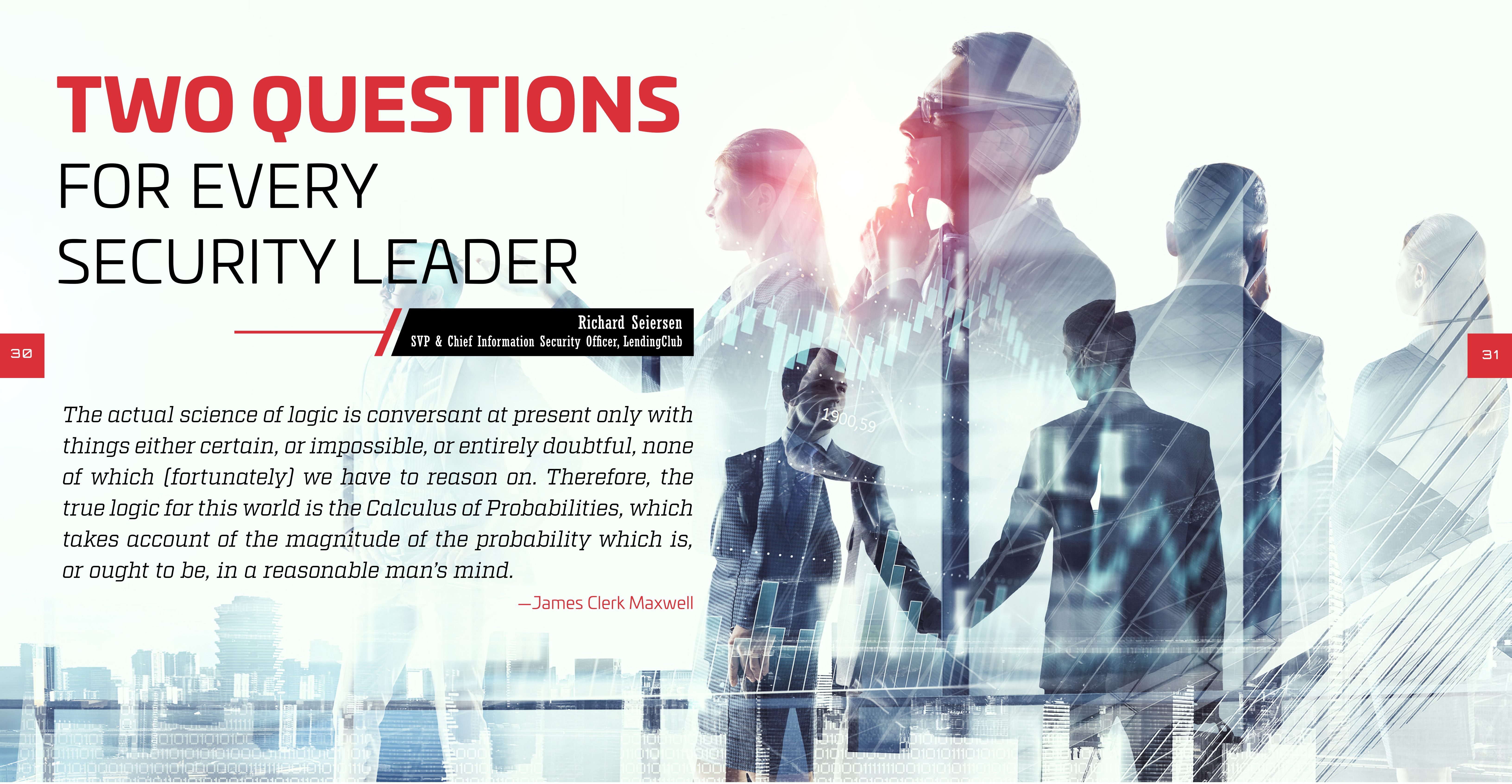
According to the Norton Trends Report, despite this year's cyber attacks, consumers continue to trust the institutions that manage their data and personal information; however, only 41 percent of consumers globally lost trust in their government to manage their data and personal information.

As the cyber world and the physical world are colliding, CISOs and CIOs are more important than ever because they serve as a bridge between the two. As for cybersecurity, it's possible the worst is behind us. However, in an industry as volatile as ours, it's very hard to predict. Much progress has been made, but there is still much to do. The work is not over. And for the ones that have suffered in the past, it is time they rise above the ashes and retell the Phoenix saga.

TWO QUESTIONS FOR EVERY SECURITY LEADER

Richard Seiersen
SVP & Chief Information Security Officer, LendingClub

> *The actual science of logic is conversant at present only with things either certain, or impossible, or entirely doubtful, none of which (fortunately) we have to reason on. Therefore, the true logic for this world is the Calculus of Probabilities, which takes account of the magnitude of the probability which is, or ought to be, in a reasonable man's mind.*
>
> —James Clerk Maxwell



There are two basic questions I ask myself, my teams, and security folks at large. First, "How do I know I have the right security capabilities?" and second, "What would I see occurring that would let me know my capabilities are improving?" I might add to that last one, "… while the business scales?"

DO I HAVE THE RIGHT SECURITY CAPABILITIES?

My co-author Doug Hubbard and I provide a detailed answer for the first question in our book, *How to Measure Anything in Cybersecurity Risk* (Wiley 2016)[1] . Measurement experts such as scientists, actuaries, mathematicians, statisticians, some engineers, and data scientists will find our approach familiar. Especially actuaries because the green book (as we affectionately call it) will become required reading for The Society of Actuaries exam prep from 2018 onward.

These experts would most certainly take a quantitative approach to my first question. Their tactics are grounded in the logic of uncertainty aka probability theory. Please don't be scared off by that "mathy" turn of phrase. You just need to know that probability theory simply counts up all the ways an event can happen and puts more weight on those possibilities that are most plausible. It's a centuries old shortcut born out of laziness, boredom, and the desire to beat the house.

TRUTH IS NOT THE GOAL, BETTER IS

Adopting a probabilistic approach means not looking for the "perfectly correct" answer to intangible questions like "do I have the right capabilities?" You want the most plausible answer(s) given your current state of uncertainty. This means being resourceful with what little empirical data you have. And if you lack empirical data you may be left with modeling your subject matter experts' beliefs. You likely paid a lot for their expertise, you might as well model it. Now that is being resourceful!

This is a key point for security folks. Security by its very nature is mired in uncertainty. We have uncertain sentient and artificially intelligent adversaries attacking a myriad of systems all in transient states. Our understanding, or model, of that world is by its very nature, woefully incomplete.

The statistician George Box made this point of view popular by saying, "all models are wrong, but some are useful." Which my co-author embellishes with, "… and some models are measurably more useful than others." Your goal is improvement over your current model at a reasonable cost. Don't let your uncertainty caused by a lack of perfect data stand in your way.

BETTER DECISION MAKING

Models, wrong or very wrong, exist to aid you in decision making as opposed to substituting for it. The model for answering my first question would help you figure out which capabilities best reduce risk (breach) given your risk tolerances . It should also take into consideration any reduction in opportunity loss (lost sales) as well as the cost of controls (cost of people and gear etc.). That's how we get the best return on investment (ROI) i.e. the best bang for our buck in reducing probable future loss.

ROI becomes a type of score for organizing our choices in order of importance. It's a huge improvement over risk registers, heat maps, and other qualitative scoring systems in the security marketplace. We and other experts in our book enjoy saying that those approaches are "worse than doing nothing."

BUT WAIT, WE'RE DIFFERENT!

Security folks may argue that the combination of systems complexity and chaotic actors make the possibilities of compromise uncountable (not that they have tried) and thus immune to probabilistic means. They say this as if fields that use probabilistic approaches must have easier problems to solve; fields like nuclear engineering, military logistics, epidemiology, seismology, and cytology (name your ology as long as it's not astrology … it doesn't work). The point is that measurement experts adopt probabilistic approaches because of uncertainty, not in spite of it.

[1] Doug Hubbard was my co-author: https://www.linkedin.com/in/dwhubbard/

[2] Risk tolerance could be your cyber insurance coverage or it could be multiple factors. Also consider that the NIST CSF, amongst others, expects risk management to consider tolerance.
[3] Opportunity loss is reduced when security meets customer, industry or regional requirements and allows for new and expanded sales.
[4] Security gear, people and etc.
[5] It's a mathematically unambiguous score. Unlike a "High" or a 10 on a 1-10 scale.

MAKING SECURITY RIGOROUS

If you haven't guessed it by now, I believe it's time for security to start measuring more like the sciences do, or like anyone with serious treasure at stake would do. And you don't have to be a scientist or a statistician to do this (I'm not). Statisticians, similar to cooks, do what they do for others to consume. Take plumbers for example: they don't need to know squat (pun intended) about the physics of fluid dynamics to fit the right pipes given the water pressure coming into a house. They just know which tools and materials to use for the particular problem at hand. Likewise, you don't necessarily need to understand the math as much as you need to understand the problem you are trying to solve. From there you are just fitting the appropriate quantitative materials together to make what will ultimately be a wrong (all models are wrong) but hopefully better model than you are currently using.

THINK MORE DO LESS

"A problem well defined is a problem half solved."

-Charles Kettering

> **If your problem is framed badly then no model, no math, no concoction of any kind can magically save you from yourself.**

If your problem is framed badly then no model, no math, no concoction of any kind can magically save you from yourself. In my experience, most security folks don't spend enough time thinking or framing their problems. The current trend is to knock out tasks (be a doer/builder) and deploy taken-for-granted technology in the hope things will improve. Task obsession is a sure-fire way to lose the forest for the trees in security. The bad guys would love nothing more than to have you whittling away the hours on low impact, uncoordinated busy work.

By way of example, I consulted with an organization not too long after the Equifax breach. I used what we knew of the breach as a tabletop exercise to determine the state of the current organization's end-to-end vulnerability management program. While they had historically knocked out numerous tasks related to the topic and made several key investments, they profoundly underperformed Equifax. Why? They couldn't rank-order what big outcomes were important in a systematic way. What they did have was "more security tasks … faster." That was their model. Now, after improving their vulnerability management program and focusing on ranking important outcomes, their results should beat their old model, which had near zero measurable outcomes, and Equifax to boot (at least I hope it will). The improvements were fundamentally about shifting their thinking from being task-oriented/busyness-obsessed to big picture strategizing for the organizations' assets.

As a security leader, don't be fooled by busyness and don't let your teams be fooled by it either. It's faux noble and will not be effective in light of increasing platform uncertainties and talented adversaries. Perhaps it's time to think more and do less? Specifically, thinking more about our capabilities and doing less busy work so you can focus on big impact, ROI-based, outcomes.

In my next article, I will address the second question. And who knows, I may throw in some code! 🔒

[6] Data analysis is an applied art. Analysts are API/tool users. Deeper math, statistics, probability theory and etc. is not required. But, it would certainly help in better understanding what is going on under the hood. Those people designed tools for you use to answer questions in your particular domain. Go for it!

[7] Use big breach announcements, new zero days, etc. as a form of table top. Collect the evidence from an article about the event and turn it on yourselves to see how well you would do. This is a much more productive way to read all the security blather that is out there. Ask "what if it were me?"

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

Volume 2 | Issue 1

Volume 2 | Issue 1

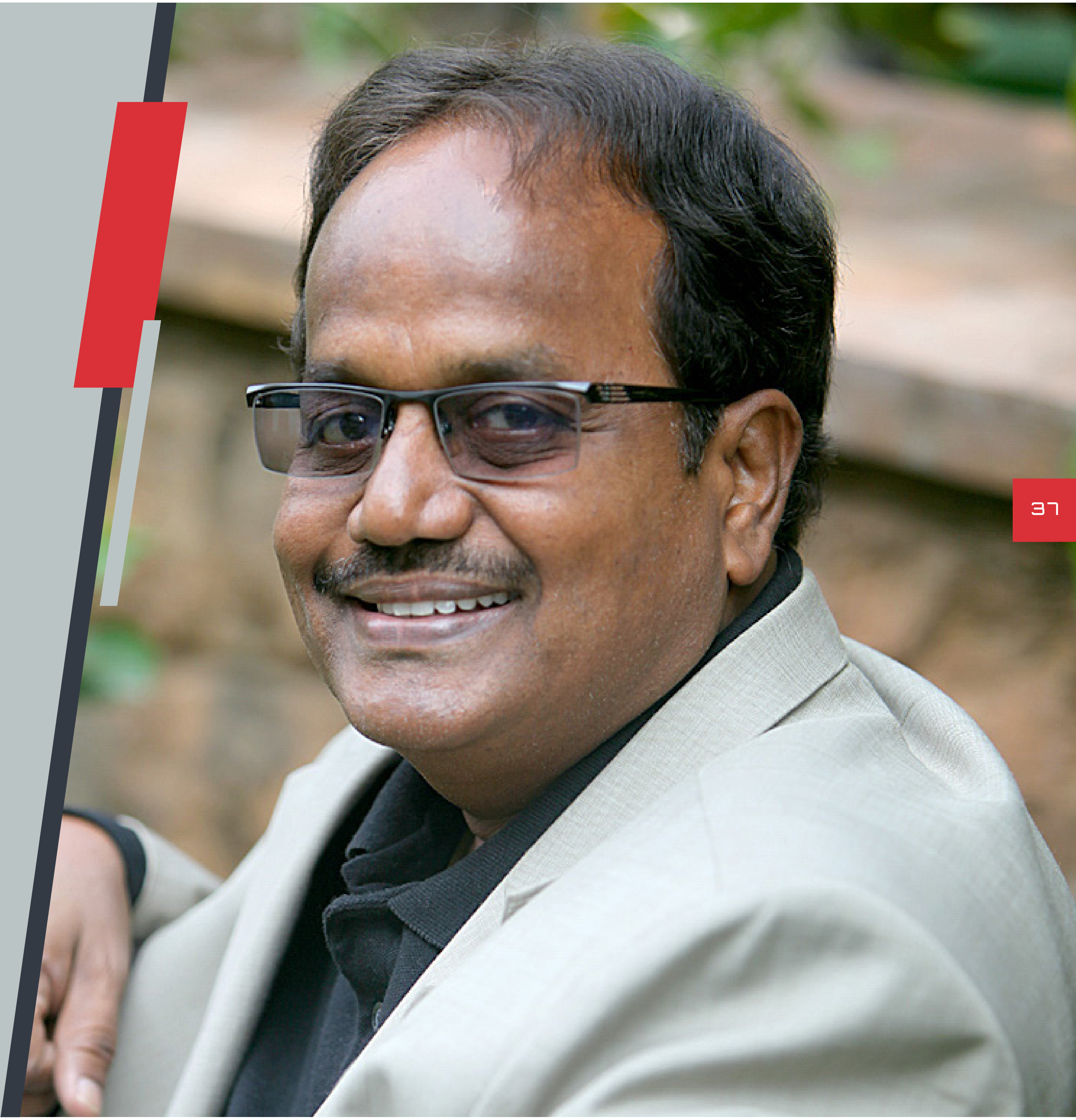
J A CHOWDARY

SPECIAL CHIEF SECRETARY & IT ADVISOR TO CHIEF MINISTER OF ANDHRA PRADESH

Rahul Arora

Under the able leadership of **J A Chowdary**, the Indian state of Andhra Pradesh has been able to create a culture of innovation for the Fintech sector as well as establish a vibrant ecosystem for startups to thrive.

In an exclusive interview with **Rahul Arora**, he talks about his vision for Fintech Valley in Vizag, Andhra Pradesh, and his efforts for continued development of the Fintech ecosystem in India.



What is the reason behind choosing Fintech as an area of focus?

Considering that resources are limited, there needs to be a sharp focus in a particular area, otherwise one will never be able to create real impact through just noise. We studied the areas and identified the major ones which may create a real impact. Ultimately, for any government, through economic activity, the key milestone is job creation. Especially with a population of 1.2 billion, it becomes even more fundamental for governments to focus on jobs. Now, with Indian IT 1.0 slowing down with automation and layoffs, we mapped sectors that are going to be crucial to creating the right jobs for our people. We narrowed down to three technologies: cybersecurity, blockchain—which is just emerging and key to preventing cyber hacks—and analytics, considering the digital footprint the country has been creating. We thought of focusing on one industry where all these technology changes are relevant. Fintech encapsulates all three and, as an industry, is growing globally at a CAGR of 26 percent.

As one of the cutting-edge technologies that break the traditional chain in financial sector, FinTech is the future of global economy and would play a pivotal role in developing the country through its innovative products and service. Fintech has enabled the unbanked to be brought under the formal system, so we have the potential to find robust and secure solutions by incubating potential startups. The FinTech Valley will act as a facilitator for information flow—a playground for innovators to disrupt traditional processes with new, more efficient, economically beneficial technologies that will change the way India does business. Fintech Valley Vizag forum will bring together regulators, banks, non-banking financial companies, educational institutions, and the government-to create the best practices for the sector.

Manpower, money, market access, mentoring and media—these five M(s) are the *Paanch Pandavas* (according to Hindu Mythology) that we have identified for the success of fintech startups. The role played by the media in stimulating a meaningful debate, and by educational institutions in providing skilled manpower, will be vital to our strategy.

We saw a massive conference focused on Blockchain in Vizag a couple of months ago. Which other areas of Fintech is the government looking to explore?

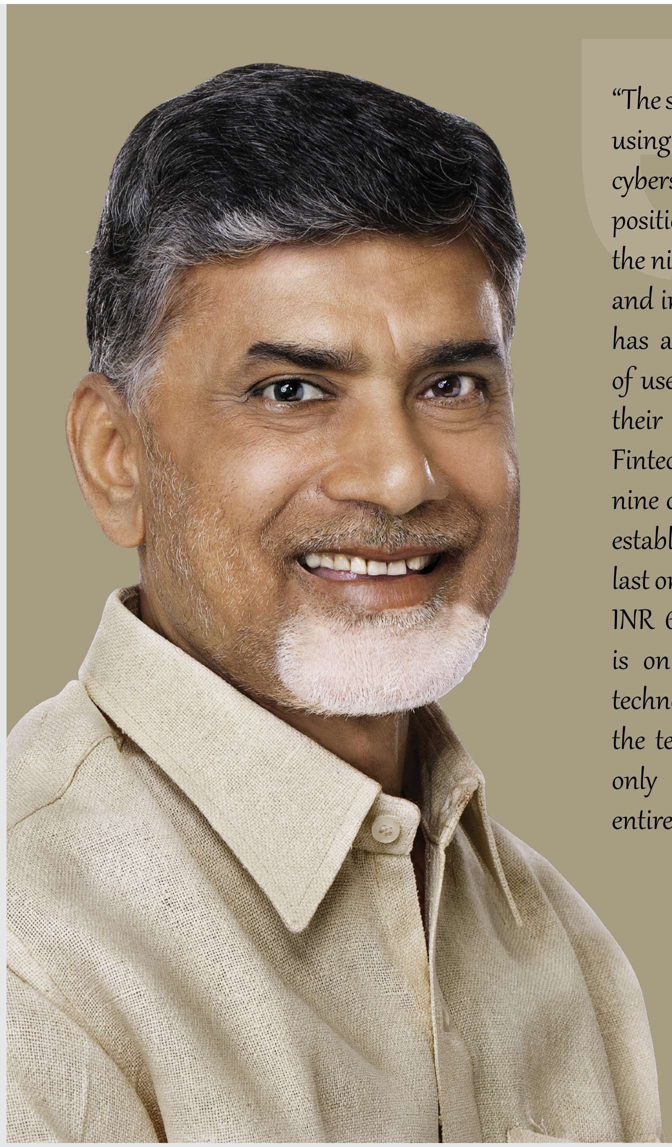
The AP government has taken the lead by incorporating Fintech and including Blockchain, Cybersecurity, Artificial Intelligence, Machine Learning and Analytics as its key strategy in FY17.

Apart from Blockchain, the government is looking at exploring new technologies such as big data analytics, Internet of Things (IoT), cybersecurity, and artificial intelligence.

> **The FinTech Valley would act as a facilitator for information flow—a playground for innovators to disrupt traditional processes with new, more efficient, economically beneficial technologies that will change the way India does business**

We saw several global companies and delegates at the Vishakapatnam event. What kind of efforts is the government putting to globalize the Fintech Valley?

As many as 26 countries participated in 'Blockchain Business Conference' to promote business opportunity and investment. The conference witnessed over 150 startups competing in four Fintech Challenges, of which 40 percent participants were from 15 countries. About 30 international delegations from Japan, Singapore, and Switzerland also participated in the event.



"The state is leading in e-governance; it is using Blockchain technology to address cybersecurity issues. Andhra Pradesh is positioning itself to take advantage of the niche technologies to create business and investment opportunities. The state has also created the largest repository of used cases for global startups to test their solutions. Today, as a part of the Fintech Valley Vizag initiative, there are nine companies set up and 16 are yet to establish their bases in Vizag. Within the last one year, we have been able to attract INR 600 crore in investment. Progress is only possible through adoption of technology. Our aim is for Vizag to be the technology and education hub not only in Andhra Pradesh but for the entire country.

"The government of AP has set aside INR 100 crore incentives to corporates who set up bases in Vizag. We are also speaking to several private equity firms to help raise more funds to promote Vizag as the Fintech hub. We are adopting Internet of Things (IoT) for real-time monitoring of all aspects of administration in the state. We have developed e-Pragathi, so that even soil testing will be done using technology with the help of drones and Microsoft.

"Our goal is very clear. In the IT sector, we have to create 100,000 jobs and secure $2 billion investment. In electronics, we have set a target of 200,000 jobs and an investment of $5 billion. To achieve these goals, we have made our own policies such as AP IT Policy 2014-2020, Electronic Policy 2014-20, Cyber Security Policy 17-20 and Global Inhouse Policy 2017-20."

- Nara Chandrababu Naidu

Chief Minister of Andhra Pradesh

Representatives from government bodies and industry working on Blockchain technologies gathered together to create business and investment opportunities for startups. The two-day conference included panel discussions related to scope in the field of financial technologies, as well as competition among the startups having best solutions for problems being faced in financial world.

The state government has decided to develop Visakhapatnam into a FinTech (financial technology) Valley by holding roadshows in the United States, the Middle East, and Europe to attract leading players in the field for partnerships and investments. After successful response to its attempt to involve Singapore in promoting the FinTech industry in the city, it has been decided to undertake overseas trips by Chief Minister N. Chandrababu Naidu and members of the Confederation of Indian Industry (CII) to showcase the huge potential for investment in Visakhapatnam—the largest city in Andhra Pradesh with an IT turnover of Rs. 2,000 crores and a

robust industrial base.

Fintech Valley Vizag invited experts from the Fintech ecosystem, government officials, and CXOs of enterprises for closed-door meetings to discuss and share ideas on blockchain applications in key areas including cybersecurity, regulatory, trade finance, and logistics. The Blockchain Business Conference had closed-door discussions, investor connect where startups pitched to investors, customer connect where startups met large corporates to provide opportunities to investors and startups globally.

We signed an MoU with the Monetary Authority of Singapore (MAS) to explore projects of mutual interest on innovative technologies such as digital payments and Blockchain (database) technology, and collaborate on the development of education programs/curricula on FinTech. The MAS and the State government would also work together on emerging FinTech trends and addressing regulatory issues related to innovations in financial services. Delegations were already sent to Boston and Silicon Valley to impress upon investors and FinTech experts to explore opportunities in the proposed FinTech Valley.

Several startups are making breakthroughs in Fintech and taking the banking industry head-on. What is the AP government doing to assist or promote them?

The potential to create successful startups lies in how we build our

"We are the first state to use blockchain pilots. The Fintech Valley Spring Conference is our step in joining the Fourth Industrial Revolution which is a spectacular combination of technology and Internet of Things (IoT). In recent times, technology has started influencing our lives in a comprehensive manner. The demand for Fintech is growing each day. To meet this demand, we would need the support from Fintech and cybersecurity companies. We also need the academic institutions to adapt curriculum that trains individuals to contribute to fintech sector.

"We are very proud of the fact that currently we have created over 22,000 job opportunities in IT sector and 40,000 in electronic sector in the state. By 2019, we aim to create job opportunities to the scale of 100,000 jobs in IT sector and 200,000 in the electronics sector. Govt. is not only making tremendous efforts in inviting Fintech companies to Vizag, it is also trying to create socio-economic development in the city by focusing on infrastructure. Congenial policies, burgeoning pool of talent, and strategic investments are attracting investors to set up operations in Vizag. The Govt. of Andhra Pradesh is making all the efforts to embark on its vision to make Vizag the Fintech hub of India.

"The technology was required to prevent tampering of land records, which had already been digitized and placed online. Similarly, the technology is used in Transport Department to streamline titles of the vehicles. The government has brought advisory major KPMG and card network majors Visa as partners in this initiative. It has also partnered with six educational institutions for imparting special courses on financial technology for necessary skill-building. A New Jersey-based company, Conduent, is setting up a 5,000-seater facility here and another major company has agreed to set up center here, generating 5,000 more jobs."

- Nara Lokesh

IT Minister, Andhra Pradesh.

infrastructure. Under our chief minister, we have developed the Fintech Valley Vizag as an ecosystem of success that helps identify and nurture financial technology institutions and startups. We intend to bring together the fintech community and catalyze the sector's growth by hosting global business competitions and awarding innovation.

We have partnered with Wipro, Microsoft, Lattice80 (a Singapore-based fintech hub), UIDAI (Unique Identification Authority of India), and the NPCI (National Payments Corporation of India), among others to boost our research and development capacity, and provide the startups with the best intelligence.

To encourage financial technology sector, Andhra Pradesh government announced an INR 100 crore fund of funds to invest in the startups in this area.

The AP government is providing free infrastructure for six months, free fiber (high speed internet) connectivity, and preferential market access to facilitate POCs of the start-ups. Additionally, fund of funds strategy and alternate payment options are being discussed and expected to be on the books soon. An advisory council consisting of global thought leaders from the FinTech space headed by the chief minister is also being planned to handle funds and map out intricacies.

The AP government is supporting the startups by providing the following incentives:

- **Regulatory support and incentives**
- **Access to local and global investors**
- **Leverage learnings from mentors**
- **Access to professional services providers (e.g. tax, recruitment)**
- **Access to talent pool**
- **Access to corporate partners**
- **Access to free physical infrastructure**
- **Access to high speed connectivity**

The identifying information of an individual and its verification is often considered an important tool for Fintech companies to mitigate fraud losses and create better assess credit worthiness. What efforts did the AP government put in to form a robust identity regime?

Aadhar is a standalone platform, which has robust mechanism in protecting individual identity. The AP government would like to take Aadhar as a source of identification for all its initiatives. In addition to that, the government is proposing to have AP CODE, which is a secured platform, which will arrest any misuse of data and would like to bring this initiative through an enactment by state legislation. The government has setup new state-of-the art State Data Centre (SDC), central repository of the state, online delivery of services, citizen information portal, state intranet portal, remote management and service integration, and disaster recovery. ePragati is the nodal agency to implement blockchain initiatives across departments in association with blockchain technology companies in AP and agency is taking every step in protecting the interests of common man through securing various digital assets.

According to you, what is the role of regulations in Fintech? When is a regulation good and when is it bad?

A democratic country like India where more than 1.3 billion population exists, it is necessary to have a regulation in all fronts including Financial technologies. Due to proper measurements by government of India, India is able to provide a stable and trusted economy while many other international economies disrupted like such as subprime crisis.

Financial Technologies have opened many doors for the financial inclusion. At the same time, Fintech is very much vulnerable to data security and ever increasing digital attacks. Indian Citizen cannot be exposed with highly speculative currencies like Bitcoin (digital currency). Due to this reason, Reserve Bank of India, the central bank of the country, has decided not to promote speculative currency like Bitcoin.

THE MISSING LINK TO FINDING **INSIDER THREATS:** HR

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

According to the Ponemon Institute's 2017 Cost of Data Breach study, 47 percent of the organizations represented stated that the root cause of the security breaches they suffered was a malicious insider or criminal attack. Respondents reported that breaches caused by insider criminal attacks were costlier than system glitches and human error. Some of the largest and most infamous breaches have been classified as insider threats. There are numerous technologies in the marketplace that do their part to help organizations protect themselves against insider threats, but having the right technology isn't enough to stop these kinds of threats. A thoughtful insider threat program that addresses technologies, policies, and procedures is needed to combat insider threats. There is a human element in every single breach. Sometimes, it's a malicious actor with the intent to harm the company and ensure that they benefit; other times, it's an employee who accidentally clicks on a phishing email, for example, and unexpectedly exposes the organization to malware. In an Insider Threat Task Force white paper, a recent observation was made that of the organizations with a formal insider threat program, there is little evidence that insider threat programs use detection strategies focusing on non-technical behaviors—such as alarming psychosocial events in the workplace. So, the question remains:What can we do to prevent this from continuing to happen at this scale and how quickly can the incident response team find the breach when it inevitably does occur?

One area of the organization that seems to be overlooked or underutilized for using detection strategies and combating the insider threat is Human Resources. It's typically not the first area that security leaders think of when focusing on insider threats, but it should be. HR professionals bring a diversity of thought that is inherently focused on human psychology and is typically different from the technologist's point of view. Similar to how the enterprise risk management groups in larger organizations are viewing and assessing all types of risk across the company, HR sees the patterns of various employee issues that are happening across the organization and may be able to spot trends in certain departments or employees before they do harm to the company.

HR should play an integral role in an insider threat program with multiple touch-points throughout an employee's career (beginning at the hiring stage) according to the CERT Insider Threat Center. CERT also provides a list of best practices that organizations can adopt to shore up their insider threat programs.The ones that are easier to implement and provide the biggest impact include:

MATURE YOUR **INSIDER THREAT PROGRAM**

Implement or mature your current insider threat program to include the broader organization—IT, HR, legal, enterprise risk management, and other areas of the company. Due to the sensitivity and confidentiality of this work (potentially probing into an employee's private life), it is important to utilize HR as a starting point for policies and for ensuring that HR employment laws align with the program.

TRACK **TERMINATED EMPLOYEES**

Since 70 percent of insider threat intellectual property incidents are completed 60 days prior to an employee leaving the organization, you should have HR provide an automated list of voluntary and involuntary terminated employees to track their activity.

IMPROVE **EMPLOYEE ENGAGEMENT**

Preliminary studies show that engaged employees who are fulfilled in their jobs are less likely to pose an insider threat. Partner with HR to understand best practices for maturing employee engagement programs.

DEVELOP A WATCHLIST OF EMPLOYEES WITH **BEHAVIORAL INDICATORS**

HR will be essential in creating a list of employees who are exhibiting behaviors that could be an indicator for insider threats. Some examples are frequent policy violations, disruptive behavior, financial hardship, and job performance problems. Disgruntled employees are a consistent factor when it comes to insider threats.

ADD INSIDER THREAT AWARENESS TRAINING TO **OVERALL SECURITY AWARENESS TRAINING**

At this point, a majority of organizations have security awareness training for their employees. Partner with HR to add insider threat awareness to the security awareness training. Like other training that is mandatory, ensure all users have completed the training and provide refreshers throughout the year, so employees stay abreast of red flags and can spot malicious or accidental threats when they see them.

Companies have been successful by making updates to:

Pre-hiring practices

Larger organizations have pretty robust background check processes when hiring employees; however, some of the smaller companies must continue to mature their hiring practices by updating policies to include Google searches and social media searches. Since past performance is an indicator of future performance, this additional data check can help with hiring decisions and determining if the candidate could pose future employee issues.

New hire on-boarding

During on-boarding, the new employee is provided with mandatory training. Insider-threat awareness training should be added to the training deck an employee must complete. It can also be administered during the times of the year that there may be higher cases of security breaches or insider threats.

Mandatory vacation policies

Many organizations have roles—typically in finance, payroll, or trading—where the employee is subject to mandatory vacation. These policies should be expanded to some high-risk IT roles where employees have access to admin rights that could be a threat to the company if used maliciously.

In conclusion, there is no question that policies, procedures, and technologies are necessary in trying to prevent and detect insider threats; however, in order to minimize the damage of breaches in the future, there should be a multifaceted approach with an emphasis on a partnership with HR to provide the best barrier of protection against your own employees.

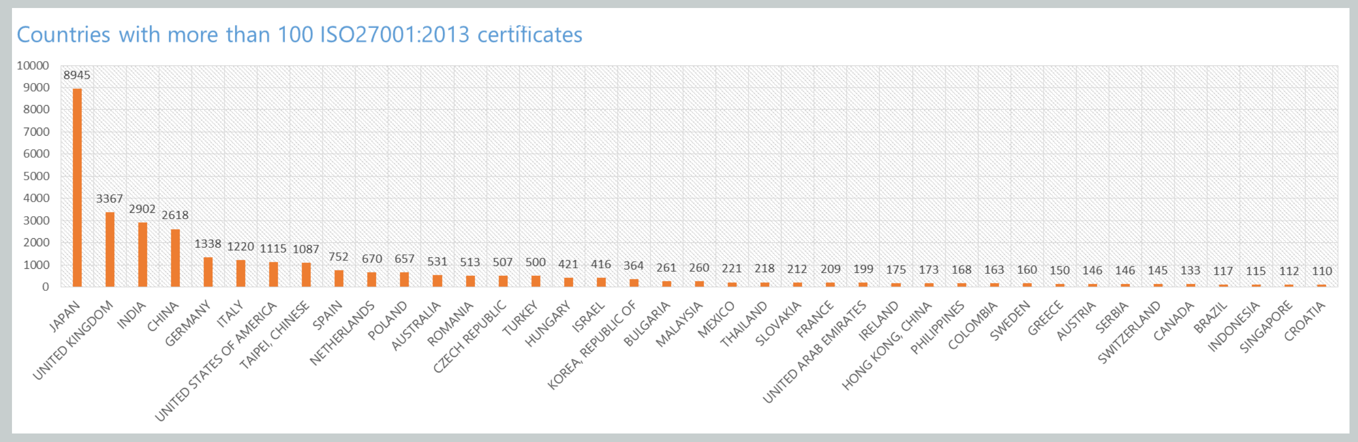
The opinions expressed within this article are the personal opinions of the author. The facts and opinions appearing in the article do not refl ect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

GET YOUR **RETALIATION** IN FIRST

Agnidipta Sarkar
Global Information Risk & Continuity Officer, DXC Technology

In 2016, ISO contacted accredited certification bodies and requested information about the number of valid certificates they had as of December 31st, 2016. The results revealed that 33,290 organizations had been certified for ISO 27001, which is a steady growth rate of 21 percent year over year. That is the good news. The bad news: only 39 countries have more than 100 certificates.

In sharp contrast is another number: the breaches. More data records were leaked or stolen during the first half of 2017 (1.9 billion) than all of 2016 (1.37 billion). Compared to the losses, the ISO 27001 story looks like a bleak effort at standardization; it is not clear if ISO 27001 is helping or not. Currently, no data is available about how many of these certified organizations had breaches and how successful or unsuccessful the ISO 27001 journey has been in regards to reducing the breaches or their impact. And the perpetrators are having fun: educated global criminals, unethical corporate competition and greed, advanced persistent threats, blatant insider abuse, radicalization of script kiddies, and many other cybersecurity violators are breaching our security.



> **Many have relegated ISO 27001:2013 to a mere certificate on the wall, and are not leveraging it as an inherent enabler to a robust and lean governance of an information security management culture.**

There is still hope. In June 2016, PECB, a leading certification body, published a whitepaper claiming, "No ISO 27001 Certified Companies among Largest Data Breaches 2014-2015." Released in 2013, the revamped ISO 27001:2013 heralded a sea change in security attitudes, from security being thought of as asset-based instead of being related to the context of protection. Unfortunately, not many organizations have embraced that logic, primarily because change is disruptive. Many have relegated ISO 27001:2013 to a mere certificate on the wall and not leveraging it as an enabler to a robust and lean information-security management and governance culture. Cybersecurity speaker John Sileo had this to say: "Corporations continue their delusional belief that data security and cyber privacy are a byproduct of purchasing better technology. It helps, but it's the human beings using the technology correctly (or not, in the case of most breaches) that actually delivers results." Information security management and governance will only succeed when the technology is used effectively.

ABOUT
ISO 27001:2013

Unlike the 2005 standard, the ISO 27001:2013 creates a framework that follows a very simple logical breakdown of how information security (and all its other names, like IT security and cybersecurity can be managed. The standard requires organizations to determine stakeholder requirements and then remediate gaps if any exist. It then expects that the organization will establish information security objectives and establish plans to implement them. These may require the establishment of operational processes for information security management, and then identification, assessment, and evaluation of information security risks in order to treat them. Evaluate the performance of the information security operations through the already established objectives, and then improve the established ISMS (information-

[1] To read more about the ISO survey, go to: http://bit.ly/2p0O3yN.
[2] To read more on the data breaches, visit the "The Register" website at: http://bit.ly/2ByyHYh.
[3] To read more about the PECB whitepaper, go to: http://bit.ly/2yLZxGV.

[4] To learn more about the breaches, go to: http://bit.ly/2efGM5I.
[5] To learn more about Annex SL, go to: http://bit.ly/2kDlHGt.
[6] To learn more about ISO 27009:2016, go to: http://bit.ly/2BoSHKI.
[7] To learn more about AWS ISO27018, go to: http://bit.ly/2yN9qUV.
[8] The learn more about AWS ISO27017, go to: http://bit.ly/2j9rvXP.
[9] To learn more about Microsoft ISO 27017, go to: http://bit.ly/2BnJFNW

security management system) by addressing non-conformances identified through audits. At all times, the ISMS program should be visible to top management personnel through appropriate management reviews.

Nothing could be simpler in the context of the complicated cybersecurity challenges we face today. Does this mean we do not need high-tech equipment to protect our cyber infrastructure? No, it does not. But an ISO 27001 ISMS program puts the appropriate focus and rigor into determining the requirements for the best possible network security. Does that prevent breaches? Yes, to a large extent. Today, data breaches and information security incidents are part of our daily life. And your ISO 27001 certification can be more than just a "best practice."

The first step to leverage you ISO 27001 certification is to ensure that the ISMS is fulfilling the requirements of the stakeholders; its performance is measured based on the information security objectives. In order to do that, organizations are increasingly making sure that the all information security reviews are guided by the ISO 27001. Organizations that are successfully using ISO 27001 to improve their security posture are continuously denying perpetrators the chance to breach their security, which satisfies their stakeholders. By example, Japan, which has the highest number of certified organizations, has consistently reduced its exposure—from 21 in 2015, 16 in 2014, and 1 in 2017 (www.breachlevelindex.com).

> **Organizations that are successfully using ISO 27001 to improve their security posture are continuously denying perpetrators the chance to breach their security, which satisfies their stakeholders.**

However, this is not an adequate indicator of the benefits of ISO 27001:2013. We need to understand how the ISO technical committee focuses on developing the ISO 27001 family of standards.

Determine Context	Address Risks	Operate the ISMS
Organizational Intent (policies) Contractual expectations Legal & Regulatory Expectations ➡ Stakeholder Requirements Information Security Management Programs ➡ Issues Operational Environment for cybersecurity operations ➡ Dependencies	Identify Information Security Risks Assess impact and likelihood of their occurrence Evaluate these risks vis-a-vis the risk criteria set by the organization. Take appropriate risk decisions to implement controls, to reduce risks within acceptable limits. Build a Statement of Applicability by comparing the controls with those in Annex A, while documenting the reasons for implementation & exclusion.	From the requirements documents information security objectives to operate an ISMS Establish information security procedures to ensure that the information security objectives are met and the risks are maintained within acceptable limits Conduct audits & management reviews to assess performance Correct non-conformances and continually improve the information security management system.

[10] To learn more about BS 10012:2017, go to: http://bit.ly/2AIletx.

LEVERAGING STANDARDS

In order to create consistency in structure and terminology across ISO management systems standards, ISO released Annex SL, which was previously known as ISO Guide 83. Annex SL describes the 10 clauses that define the ISO 27001:2013 (and also ISO 9001:2015, ISO 22301:2012, and many more). One of the biggest benefits of Annex SL is providing a universal, high-level structure, identical core text, and common terms and definitions for all management system standards. It was designed to make it easier for organizations that have to comply with more than one management system standard.

If your organization subscribes to more than one management system standard, adopt the Annex SL method to integrate management systems. In doing so, you reduce resource wastage, reduce expenses, and improve performance by focusing the right amount of leadership to ensure a high level of security.

In 2016, ISO released ISO 27009. ISO 27009 explains how to include requirements additional to those in ISO 27001, how to refine any of the ISO 27001 requirements, and how to include controls or control sets in addition to ISO 27001, Annex A. ISO 27009 is a big step toward enabling organizations to face cyber-threats. It has heralded a new world in regards to implementing controls to reduce both the likelihood and impact of security and privacy threats by introducing the concept of sector-specific application of ISO 27001. And these sectors may be a specific field, application area, or even a market sector.

The most popular of these sector-specific implementations are the two cloud certifications for ISO

27017, for information security in cloud operations, and ISO 27018, for protection of personal data in the cloud. Both AWS & Azure have obtained these certificates and assure their customers that their data is protected. Both standards are called "code of practices" and contain a list of controls that extend the ISO 27001 program. These extensions include two types: controls that modify existing ISO 27001 Annex A controls (to make them relevant to the sector) and controls that are additional to ISO 27001 in order to enhance the capability of the operational ISMS. Needless to say, the ISMS needs to be optimally resourced to continuously improve the management system.

GDPR: THE NEXT FRONTIER

The regulatory environment will change the equations soon. GDPR looms (April 25, 2018), and many countries (including Great Britain, Singapore, India, Philippines, etc.) are introducing new legislation (or modifying existing practices and regulations) to make the computing world more secure. May 25, 2018 isn't just about the GDPR; the ePrivacy Directive and the Law Enforcement Directive (LED) also comes into effect on that day.

It is no secret that most organizations are unprepared to meet the requirement of this regulation. There are clear gaps in how we are organized. While most privacy experts assume that security will protect privacy, many security experts are waiting for privacy teams to tell them what needs to be protected.

The only sure-fire way to address the GDPR is to implement a management system. BS 10012:2017 is the only privacy management system standard in the world. However, it does not address requirements to protect privacy information.

BSI revised BS 10012 in 2017 to align with Annex SL in order to ensure there was good governance around data protection and that it was anchored at the board level—with a very specific focus on aligning with ISO standard structure and the existing GDPR standard. The new standard has a section for updated terms and definitions, as well as separate sections concerning "planning" and "implementing/operating" the management system; it also contains a comparison between UK DPA and the GDPR. ISO, for its part, has released the base privacy framework though a free standard called ISO 29100; and has already released ISO 29134, which is a necessary implementation for a privacy impact assessment program. Financial services organizations may also use ISO 22307, which is helpful during privacy compliance audits. Additionally, there is ISO 29190, which provides organizations with high-level guidance about how to assess their capability to manage privacy-related processes.

However, a full implementation of GDPR requires not only a privacy information management system, but also an accompanying information security management system. In order to enhance the coverage of ISO 27001 (ISMS), ISO has also released ISO 29151, which, like all other sector-specific standards, is a code of practice and contains privacy-specific information-security controls—both as an extension of Annex A and as modifications of existing controls that can be used to extend the scope and coverage of the ISO 27001 program.

With so much going on around us, standardization in security and privacy provides the discipline to ensure we cover all our bases. As Willie John McBride, captain of the famous 1974 rugby team dubbed "The Invincibles," told his teammates: "Get your retaliation in first."

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

INFOSEC PARTNERSHIPS

In 2017, cybersecurity took center stage with other crucial topics like climate change, decolonization, big data, and atomic energy. Significant mergers and acquisitions took place as the year came to an end, the effects of which will be observable in the near future. Following the trend of collaboration, many startups and innovators joined hands with established cybersecurity brands to pursue aggressive courses of action. Also, the governments and defense departments around the world, along with other industries, began taking cybersecurity more seriously. Below are a few stories from 2017 that made front-page with their substantial acquisition amounts and futuristic outlook.

CISO MAG Staff

McAfee acquires Skyhigh Networks to Provide Cloud Services

The acquisition of Skyhigh Networks, a prominent name in the Cloud Access Security Broker (CASB) category, by McAfee on November 27th is an example of a large company purchasing a smaller, niche company to add to their security repertoire. Skyhigh CEO Rajiv Gupta, who will be heading McAfee's cloud business unit, wrote in his blog on the company's website, "As part of McAfee, we will have access to even greater resources to accelerate delivery of Skyhigh's product roadmap, further advancing our vision of making cloud the most secure environment for business."

Although the financial terms of the deal remain undisclosed, according to an online database, Skyhigh Networks raised $106 million in funding last year from its investors, including Sequoia, Greylock, and Salesforce.

McAfee was valued at $4.2 million when it announced its separation from Intel in April 2017, marking itself as a standalone in the cybersecurity domain. The addition of a CASB to its offerings will certainly increase its value. McAfee, the world's largest technology security company, will now be able to increase its expertise in the cloud security realm. "Skyhigh's leadership in cloud security, combined with McAfee's security portfolio strength, will set the company apart in helping organizations operate freely and securely to reach their full potential." said Chris Young, CEO of McAfee.

Nominum's Acquisition by Akamai Expected to Expand their Carrier Customer Base

Akamai, a company involved in offering in content delivery network (CDN) services, announced the acquisition of Nominum on October 11th 2017. Nominum is a leader in the domain name services (DNS) industry for carriers and this merger will expand Akamai's array of cybersecurity services. The amount of the transaction wasn't disclosed. The merger was in the last week of November 2017. In an official Press Release on Akamai's website, Robert Blumofe, Executive Vice President, Platform & General Manager for the Enterprise and Carrier Division, said, "We believe this acquisition is a key investment in our security capabilities because Nominum will bring complementary technology, engineering, technical support, and sales talent to better reach and serve our carrier partners and their enterprise customers."

Considering the rising number of cases of cyber attacks on both carriers and enterprises, CDNs like Akamai need robust cybersecurity solutions that can identify and thwart breach attempts. CEO & Co-founder of Akamai Technologies, Dr. Tom Leighton, stated "Nominum provides Akamai important technology and DNS expertise to help protect carriers and enterprises increasingly targeted by attackers attempting to exploit weaknesses and gaps in their cybersecurity defenses. With our acquisition now complete, we're looking forward to deepening our relationships with our carrier partners as we work together to make the Internet faster and more secure."

US Democrats, Republicans Join Hands with Harvard to Prevent Hacking in Elections

In order to safeguard the 2018 midterm elections from hacking and related propaganda, a bipartisan Harvard panel recently launched a "Cybersecurity Campaign Playbook." This initiative is being led by the Belfer Center for Science and International Affairs, in conjunction with top security executives from tech and cybersecurity giants such as Google, Facebook, and CrowdStrike.

According to a report by *Reuters*, it is a 27-page guide recommending leaders to prioritize security while campaigning, emphasizing practices like two-factor authentication when accessing emails and using complete encryption from service-providers such as Signal and Wickr. The security handbook is the first effort of its kind and covers topics like The Vulnerable Campaign Environment, the threats campaigns face, managing cyber risks, and steps to securing your campaign are covered in this playbook.

Eric Rosenbach, Belfer co-director, has already announced the release of a second guidebook for state election officials, scheduled for release in spring. "Deterring information operations is inherently a government responsibility, and the technology firms will decide how to act on their platforms, but state organizations are the victims," said Rosenbach.

The Belfer Center is also sending their students to various states to analyze different voting technologies and procedures.

Air Force Awards $50 million Contract for Cybersecurity Research

Ball Aerospace and Technologies Corp., a leading spacecraft, components, and instruments manufacturer, has been awarded a new contract by the U.S. Air Force for the security of its weapons from cyber threats. "Ball Aerospace & Technologies Corp., Boulder,

Colorado, has been awarded a $47,900,000 modification (P00003) to a previously awarded contract (FA8650-16-D-1878) for research and development to provide investigation and development of methodologies, tools, techniques, and innovative solutions to identify susceptibilities and mitigate vulnerabilities in Air Force weapon systems, and protect those systems against cyber attack," the Air Force stated in a statement. "Work will be performed at Wright-Patterson Air Force Base, Ohio, with an expected completion date of March 29, 2023. Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio, is the contracting activity."

The drive is expected to lead the operationalization of numerous important components identified by the Air Force in its extensive cybersecurity strategy. Air Force leaders also created a new unit tasked with handling cyber threats called the Cyber Resilience Office for Weapons Systems, or CROW.

Automotive Giant Continental AG Acquires Israel's Argus Cyber Security

In a PR released on its website on November 3rd, 2017, Israel-based startup Argus Cyber Security announced it had been acquired by Germany's Continental AG. A prominent automotive manufacturer, Continental acquired Argus for its expertise in protecting connected cars from hacking. Helmut Matschi, Executive member of the Board at Continental, said, "Only secure mobility is intelligent mobility. With the acquisition of Argus Cyber Security, we are enhancing our abilities to directly develop and offer solutions and services with some of the world's leading automotive cybersecurity experts to our customers around the globe in order to truly make mobility more intelligent and secure."

Argus will become a part of Elektrobit, Continental's stand-alone software company. The automotive cybersecurity provider has previously partnered with EB in October 2017 to introduce technology for delivering over-the-air vehicle software updates. Recently, the automotive industry has faced strong criticism for its negligence in securing connected vehicles. Alexander Kocher, President and Managing Director of Elektrobit said, "Adding Argus to our portfolio will allow us to further advance the development of our software. We are now offering to the automotive industry – carmakers and suppliers alike – a complete secure solution for the development of highly automated and connected driving. This will enable them to develop safer, smarter and more efficient vehicles."

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 three months.

CISO MAG staff

UBER PAID $100,000 TO COVER UP BREACH THAT AFFECTED 57 MILLION USERS

On November 21, 2017, it was reported that Uber paid hackers $100,000 to keep a data breach a secret. The personal information of about 57 million accounts was reportedly compromised in a hack that took place in October 2016. The incident was first reported by *Bloomberg*. The company reportedly fired its Chief Security Officer, Joe Sullivan, and a deputy, Craig Clark, the following week for concealing the hacking incident.

Dara Khosrowshahi, who replaced co-founder Travis Kalanick as CEO in August, wrote in a blog post, "None of this should have happened, and I will not make excuses for it." He also revealed that he only learned of the breach recently.

Kalanick learned of the breach in November 2016, but he reportedly chose not to share the incident with fellow board members. He still continues to be on Uber's board and Khosrowshahi said that he regularly consults the former CEO.

While announcing that the exposé led to the sacking of two employees, Khosrowshahi said, "The stolen information included names, email addresses and mobile phone numbers of Uber users around the world, and the names and license numbers of 600,000 U.S. drivers."

Khosrowshahi was quoted saying as "While I can't erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes. We are changing the way we do business, putting integrity at the core of every decision we make and working hard to earn the trust of our customers."

To investigate the breach, Khosrowshahi said that his company has hired Mandiant, a cybersecurity firm owned by FireEye. Uber has also hired Matt Olsen, former general counsel of the U.S. National Security Agency, to restructure the company's security teams and processes.

In a statement, Uber said "Uber passengers need not worry as there was no evidence of fraud, while drivers whose license numbers had been stolen would be offered free identity theft protection and credit monitoring."

The company alleged that two hackers gained unauthorized access to information on Github and stole Uber's credentials for a separate cloud-services provider where they were able to download driver and rider data.

Meanwhile, Uber spokeswoman said the hack was not the result of a failure of GitHub's security while adding that the New York attorney general has opened an investigation.

In 2014, Uber acknowledged that its employees used a software tool called "God View" to track passengers. 🔒

UK proposes ban on Kaspersky Labs products

After the clamor at the United States Senate and the following ban in

the nation, Britain's cybersecurity agency has warned government departments to refrain from using antivirus software from Kaspersky Labs citing concerns over the company's ties to the Kremlin and Russian spy operations. In a letter addressed to the head honchos of several civil service departments, Ciaran Martin, head of the National Cyber Security Centre, stated that, "The specific country we are highlighting in this package of guidance is Russia. As the Prime Minister's Guildhall speech set out, Russia is acting against the UK's national interest in cyberspace. The NCSC advises that Russia is a highly capable cyber threat actor which uses cyber as a tool of statecraft. This includes espionage, disruption and influence operations. Russia has the intent to target UK central Government and the UK's critical national infrastructure."

According to him, the overwhelming majority of UK individuals and organizations, "are far more likely to be targeted by cyber criminals" than by the Russian state but still advises "that where it is assessed that access to the information by the Russian state would be a risk to national security, a Russia-based AV (anti-virus) company should not be chosen." 🔒

Russia meddled with UK's telecom systems, confirms NCSC chief

The United Kingdom's National Cyber Security Center (NCSC) Chief Ciaran Martin confirmed that Russian hackers targeted the country's telecommunications systems, media, and energy networks over the past year.

Martin's remarks came amid heightened scrutiny of Russia's influence in last year's Brexit referendum. Addressing the Times Tech Summit in London on November 15, 2017, Martin said, “I can't get into precise details of intelligence matters, but I can confirm that Russian interference, seen by the National Cyber Security Centre over the past one year, has included attacks on the UK media, telecommunication and energy sectors.”

Part of Martin's speech summary was released on November 14, 2017. Martin said, “the Prime Minister sent Russia a clear message in her speech to the Lord Mayor's Banquet on Monday night. Russia is seeking to undermine the international system. That much is clear. The PM made the point on Monday night — international order as we know it is in danger of being eroded.”

On November 13, 2017, Britain's Prime Minister Theresa May had said that Russia was “weaponizing information” and meddling in elections to undermine the international order.

Sending a stark warning to Russia, May said, “We know what you are doing. And you will not succeed. Because you underestimate the resilience of our democracies, the enduring attraction of free and open societies, and the commitment of Western nations to the alliances that bind us.”

1.7M emails and passwords compromised in 2014 Imgur hack

Image hosting site Imgur, which later metamorphosed into a meme haven for social media users, has apparently been subjected to a massive data breach. The hack occurred in 2014 and involves the stolen data of 1.7 million users. Imgur discovered the incident on November 23, 2017.

The incident came to fore after Have I been Pwned founder Troy Hunt notified the company. “He (Troy Hunt) believed he was sent data that included information of Imgur users. Our Chief Operating Officer received the email late night on November 23rd and immediately corresponded with the researcher to learn more about the potential breach. He simultaneously notified Imgur's Founder/CEO and Vice President of Engineering. Our Vice President of Engineering then arranged to securely receive the data from the researcher and began working to validate that the data belonged to Imgur users,” Imgur stated in a blog spot.

The data is believed to be a fraction of Imgur's user base which usually sees the traffic of 150 million monthly users. The affected data may only include email addresses and passwords of the users as the site never gathered personally-identifying information (PII) like real names, addresses, or phone numbers. According to Have I Been Pwned's database, 60 percent of the hacked email addresses were already on the deep web.

DHS hacks Boeing 757

Robert Hickey, the aviation program manager within the Cyber Security Division of the DHS Science and Technology (S&T) Directorate, revealed on November 08, 2017, that DHS once successfully took control of Boeing 757 airplane while the passenger jet sat on the runway at Atlantic City airport, New Jersey.

He revealed the details of hack that was conducted in 2016 while giving his keynote address at a summit. “We got the airplane on Sept. 19, 2016. Two days later, I was successful in accomplishing a remote, non-cooperative, penetration,” said Robert Hickey, aviation program manager within the Cyber Security Division of the DHS Science and Technology (S&T) Directorate. “[Which] means I didn't have anybody touching the airplane, I didn't have an insider threat. I stood off using typical stuff that could get through security and we were able to establish a presence on the systems of the aircraft.”

While the details of the hack are still under wraps, Hickey revealed his team of DHS cyber sleuths achieved the feat by accessing the radio frequency communications of the plane. The initial response from experts was, “'We've known that for years,'” and, “It's not a big deal,” Hickey said.

Ukrainian President signs law on cybersecurity

On November 07, 2017, Ukraine President Petro Poroshenko signed a law which “creates the foundations of a national system of cybersecurity as a combination of political, social, economic and information relations, along with organizational, administrative and technical and technological measures of the public and private sectors and civil society,” the press service of the head of state reported. The president will coordinate activities in the field through National Security and Defense Council of Ukraine.

According to a report on Ukinform.net, “The law defines the legal and organizational foundations for ensuring the protection of vital interests of citizens, society and the state, the national interests of Ukraine in cyberspace, the powers and responsibilities of state bodies, enterprises, institutions, organizations, individuals and citizens, the basic principles of coordination of their activities, and also basic terms in cybersecurity.”

As per reports, the bill also summaries that several cyber threats mitigation efforts will focus on protecting critical infrastructure. The law also explores the possibilities of partnering with private agencies and civil societies as well as takes into account several proposals from the European Union and NATO.

Paradise Papers rocks the world

The "Paradise Papers" findings released by the US-based International Consortium of Investigative Journalists (ICIJ) have opened a can of worms. ICIJ is the same organization that was behind the Panama Papers' sensational exposures. The major cyber breach has been reported from Appleby, a multi-national offshore law firm known for its tax planning services. The Panama Papers leak exposed millions of documents from the Mossack Fonseca law firm.

The leaked documents, dubbed the Paradise Papers, were released on November 6, 2017 and consisted 13.4 million records including emails, loan agreements, and bank statements that contain sensitive financial information pertaining to highly prominent figures. Out of 13.4 million records, 6.8 million documents came from a cyber attack on Appleby files. The Appleby files were obtained by the German newspaper *Süddeutsche Zeitung* who shared them with the ICIJ along with 95 media firms to maximize the exposure of the leaked information.

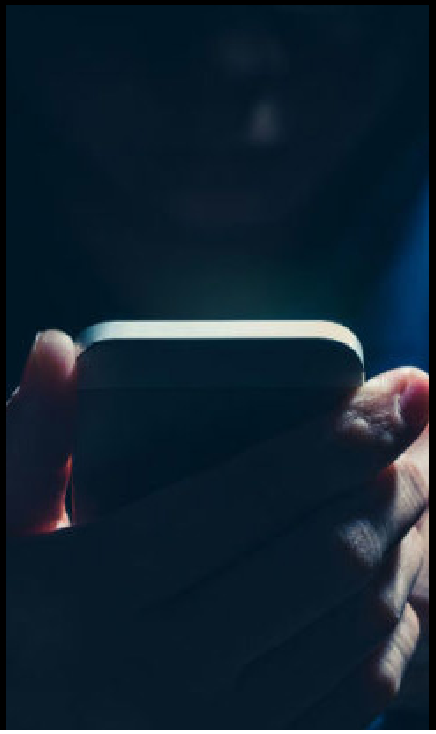
The long list of international leaders and celebrities on the list includes Britain's Queen Elizabeth II, Colombian President Juan Manuel Santos, Canadian Prime Minister Justin Trudeau's chief fundraiser Stephen Bronfman, individuals linked to the U.S. President Donald Trump, singers Bono and Madonna, and U.S. Commerce Secretary Wilbur Ross among several others.

John McAfee's Twitter Account Breached

John McAfee recently declared that his Twitter account was hacked and used to endorse some minor-league cryptocurrencies. Although he claimed to have enabled the two-factor authentication, his mobile phone was jeopardized leading to the cyber attack on his social media account.

The former presidential candidate said that he got the first indication of his phone being hacked when he turned it on to see a dubious error message on the screen. In an interview with the *BBC*, John mentioned, "I knew at that point that my phone had been compromised. I was on a boat at the time and could not go to my carrier (AT&T) to have the issue corrected. All that the hacker did was compromise my Twitter account. It could have been worse." The claim that the Twitter account of the former owner of one of the world's first anti-virus companies was successfully hacked led to some ribbing by the security community.

While cybersecurity experts are assessing the perils of AI-empowered cyber breaches, it is indeed worrisome that the frequency of break-ins have increased. Although veracity of John McAfee's account hacking is debatable, the rapid surge in cyber-attacks has led to reconsidering the present cybersecurity guidelines and methodologies.

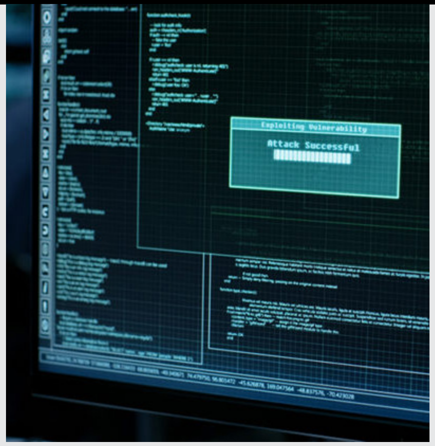


Chinese nationals indicted for hacking into Moody's, Siemens, and Trimble

Three Chinese nationals have been charged by U.S. prosecutors for hacking into Siemens AG, Trimble Inc, and Moody's Analytics. The trio tried to steal business secrets of the three companies through "coordinated and unauthorized" cyber attacks between 2011 and 2017. The three accused have been identified as Wu Yingzhuo, Dong Hao, and Xia Lei.

An indictment that was unsealed on November 27, 2017, said all three of them were associated with Guangzhou Bo Yu Information Technology Company Ltd, a cybersecurity company located in Guangzhou in southern China. Two U.S. government officials told *Reuters* that Guangzhou Bo Yu is affiliated with the China's People's Liberation Army Unit 61398.

During a hearing in federal court in Pittsburgh, Pennsylvania, on November 27, 2017, the acting U.S. attorney for Western Pennsylvania Soo C. Song said arrest warrants had been issued for the three men. The indictment, which was filed in September 2017 at a federal court in Pittsburgh, Pennsylvania, claims, "the hackers monitored email correspondence of an unidentified Moody's economist; stole data from transportation, technology and energy units at Siemens; and targeted Trimble as it developed a new and more precise global navigation satellite system."



Japanese cryptocurrency exchange suffers massive breach

On January 26, 2018, Japanese cryptocurrency exchange Coincheck lost 58 billion yen ($530 million) in what has dubbed as biggest cryptocurrency heist ever recorded. Coincheck had to immediately halt sale and withdrawals of the currency NEM, and later extended restrictions to other cryptocurrencies except Bitcoin.

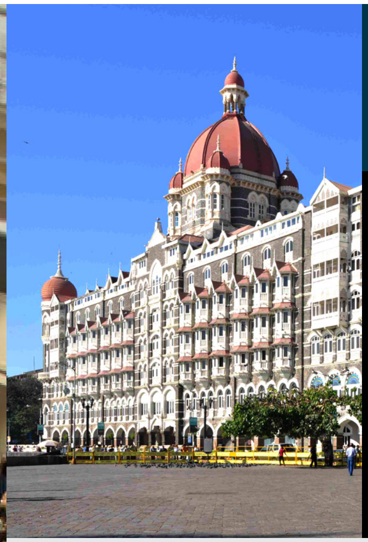
During the course, Japan's finance regulator Financial Services Agency instructed the company to improve its operations and to submit an incident report, where the company would highlight the preventive measures adopted by it to avert any further incidents.

Coincheck assured its users that it would return about 90 percent of the stolen money through with internal funds. According to a *Reuters* report, "The NEM coins were stored in a "hot wallet" instead of the more secure "cold wallet", outside the internet (...) It also does not use an extra layer of security known as a multi-signature system."

"It's been long said that cryptocurrencies are a solid system but cryptocurrency exchanges are not," Makoto Sakuma, research fellow at NLI Research Institute, told *Reuters*. "This incident showed that the problem has not been solved at all. If Coincheck screws up its crisis management, that could deal a blow to the current cryptocurrency fever." Following the incident, the price of NEM fell from $1.01 to $0.78 within a day.

The significant technology shift to mobile and connected devices has left vulnerabilities to cyber breaches that need to be addressed aggressively. EC-Council's annual calendar of events all over the world is an attempt to bring together leaders and dignitaries of various industries and advocates of information security. Through our live events, we have been able to create awareness and bring together the best in the industry. Here's a sneak peek into our upcoming events:

CISO MAG staff



Pharma CIO Leadership Series

20th February, 2018

Mumbai, India

Takeaways:
The event features deliberations on innovations, emerging opportunities and instrumental strategies, with an elite panel of keynote speakers sharing their knowledge on the adoption of critical cybersecurity prospects.

MALAYSIAN CYBER SECURITY SUMMIT

20th March, 2018

Kuala Lumpur, Malaysia

Takeaways:
A joint effort with CyberSecurity Malaysia, the wing of Malaysia's Ministry of Science, Technology and Innovation (MOSTI), this is one of EC Council's premier events. The event deep dives into the most pressing information security issues and advocates the adoption of systematic cybersecurity methodologies. Malaysia was number three on the UN's Global CyberSecurity Index (GCI) last year and the country's progress in information security makes it an ideal host for a security event of this stature. The event is an invite-only executive session for leaders from across the ASEAN region to work together towards solving some of the world's most pressing cybersecurity problems.

MENA CISO SUMMIT

18th - 19th April, 2018

Dubai, UAE

Takeaways:
The MENA CISO Summit is the regional counterpart to our annual Global CISO Forum in Atlanta, GA USA. This cross-industry event invites leaders, specialist, chiefs, and innovators in information security and other industries to discuss current trends, threats, and solutions. The Sapient panel discussion includes experts from information security and beyond to ensure that the message of information security isn't siloed in one industry.

4th EDITION CISO SUMMIT

08th June, 2018

Mumbai, India

Takeaways:
The 3rd CISO Summit India focused on national cybersecurity architecture, investments in cybersecurity, ensuring safer use of cloud, securing IoT infrastructure, and skill set scarcity in the information security ecosystem. Our 2018 event will tackle issues just as critical to the information security industry with a larger audience than ever.

ASEAN CISO FORUM

16th - 17th August, 2018

Singapore

Takeaways:
With the world gearing-up to turn into a glocal (globally local) village, the urgency to adopt effective measures against cybersecurity threats in the connected world has become intense. Another regional subsidiary of the Global CISO Forum, the ASEAN CISO Forum invites CISOs, CTOs, and other security leaders from different industries to share their knowledge and to improve information security in the ASEAN region and beyond.

3rd EDITION FINTECH SECURITY SUMMIT

10th October, 2018

Manama, Bahrain

Takeaways:
The 3rd edition of the Fintech Security Summit is motivated by the successful recognition of the first two Summits in Singapore and Abu Dhabi. Bahrain is set to launch its Fintech Bay in February 2018 for better banking and finance innovation standards in a secure environment. EC-Council's Fintech Forums bring Fintech forerunners and information security evangelists together to exchange views and discuss cybersecurity threats looming over the sector, the problems with standard IT practices, and the best measures to overcome and prevent this promising industry from being hampered by poor security.

GLOBAL CISO FORUM 2018

13th - 14th September, 2018

Atlanta, Georgia

Takeaways:
EC-Council's Global CISO Forum is an invite-only, closed-door event gathering the highest-level executives from across industries and countries to discuss the most pressing issues in information security. Now in its eighth year, the 2018 Global CISO Forum promises to be the best yet with an exciting mix of industries, formats, and interactive presentations.

HACKER HALTED 2018

13th - 14th September, 2018

Atlanta, Georgia

Takeaways:
The brainchild of EC Council, Hacker Halted 2018's theme is "The Ethical Hacker's Guide to the Galaxy: Life, the universe, everything...Hacked." 2017's Hacker Halted was the largest in history, drawing incredible speakers and huge audiences. The event is open to all those passionate about the latest information security vulnerabilities, hacks, and defenses. 🔒

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

Trapp Technology hires **Jim Mapes** as CISO

Phoenix-based Managed Service Provider (MSP) Trapp Technology announced the appointment of its new CISO, Jim Mapes, last month. Mapes has 25 years of experience in IT, including 19 years dedicated to information security. Mapes plans to further enhance Trapp Technology's array of security services, with more attention towards cybersecurity assessments and security managed services for mid-market to enterprise-level businesses.

About his new role, Mapes said,

"I've been impressed with Trapp Technology's success in the managed services market, and I firmly believe that the company is well-poised to lead the cybersecurity services mid-market with smart, business-driven solutions. Throughout my career, I have always approached cybersecurity as a business problem, unlike competitors who have traditionally viewed it as a technology concern. Company owners are very concerned about the impact a cyber breach can have on their bottom line, and this keen interest is driving a new conversation around how much security is really enough to eliminate as much risk as possible. Trapp will help these companies determine the answer to that question, and then get them to where they need to be."

Mapes has held the title of CISO in eight previous jobs and has a strong background in designing information security programs and operations. He also has technical expertise in intrusion testing and forensic investigations.

FBI's Former IT Assistant Director Joins Deloitte

James Turgal, former FBI executive assistant director of the Information and Technology branch, has joined Deloitte Risk and Financial Advisory's Cyber Risk Services practice as managing director. This is the second former FBI employee to join Deloitte for the same position, after Linda Walsh in April 2017. Turgal, who served in the FBI for 21 years, was a member of the C-suite supervising FBI's worldwide IT needs including digital forensics and investigations, identity management, data privacy, and cyber resiliency.

In his new role with Deloitte, Turgal is responsible for advising clients on cyber incident response, cyber resilience, and cyber war-gaming. About his new job, Turgal said, "Deloitte recognizes that a comprehensive understanding of the cybersecurity landscape is critical to helping organizations stay ahead of emerging threats. Finding the right balance between technology and talent, and knowing when and how to best utilize each, can significantly strengthen cyber incident response programs."

Turgal is a well-known name in the intelligence community and frequently consulted for his expertise in cyber counterterrorism, criminal, and security issues.

Renitalynette Anderson is the New President of Quality Technology Inc.

Quality Technology Inc., popularly known as QuTech, has chosen Renitalynette K. Anderson as its new president. Anderson brings 30 years of experience, which include 19 years at the National Institute of Health (NIH) as well as her recent tenure at the Federal Deposit Insurance Corporation (FDIC) as Deputy Director. During her tenure with NIH, Anderson was appointed as the Deputy Director for Information Technology where she renovated the data center, telecommunication services, and call centers improving the computing environment through better security and increased capacity.

QuTech is an IT company specializing in cybersecurity, data management, and cloud services among others. Renee Parker, CEO of QuTech, stated, "We are excited to have such an accomplished professional with proven leadership, executive-level experience, and business acumen to lead our company."

Volume 2 | Issue 1

MetTel appoints **Dr. Curtis Levinson** as CISO

Communications solutions provider MetTel has appointed Dr. Curtis Levinson as the new Chief Information Security Officer (CISO) for the firm as well as its Federal team. Levinson will oversee all IT security for MetTel and the EIS solutions it provides to Federal agencies.

Levinson has worked as a strategic consultant providing cybersecurity guidance to a range of clients for more than 30 years. Levinson continues to serve as US Cyber Defense Advisor to the North Atlantic Treaty Organization (NATO).

"2018 is projected by leading analysts as a tipping point for digital transformation with up to $13 trillion in IT spending across businesses and government," said Marshall Aronow, CEO of MetTel. "Running our government more efficiently, effectively and securely through upgrades spurred by the GSA's Enterprise Infrastructure Solutions program and the Modernizing Government Technology Act will help restore US competitiveness."

Levinson is a proven technologist with his expertise ranging from cybersecurity/defense, continuity/recovery of operations, and information governance. He has served with distinction, two sitting Presidents of the United States, two Chairmen of the Joint Chiefs of Staff and the Chief Justice of the United States. In June 2017, Levison joined the advisory board of CISO MAG.

Major General Djoko Setiadi sworn in as the chief of the new BSSN

Major General Djoko Setiadi was sworn in as the chief of the National Cyber Encryption Agency of Indonesia, also known as BSSN, at the State Palace in Jakarta on 3rd January 2018. The regulation for the establishment of BSSN was signed in June of last year by President Jokowi. The agency will be under the direct control of the President of Indonesia.

Djoko Setiadi earlier served as the chief of the National Cyber Security Agency, Lemsaneg, which has been dissolved. The newly appointed chief of BSSN is aggressively hiring for the agency as the date for local elections to be held across the country is fast approaching.

The country of Indonesia has been notable for social media hoaxes and online religious zealotry leading to adoption of such vigorous arrangements by the president. "Our responsibility is to provide protection in the cyber world to government institutions, even private companies, but most importantly to the public," said Djoko during a press conference in Jakarta.

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

Shape Security

Founded in 2011, Shape Security, a cybersecurity startup based out of California, is led by Derek Smith, Sumit Agarwal, and Justin Call.

What sets Shape Security apart: The company helps apps and websites change their source code constantly to prevent automated attacks by deploying polymorphism.

Market adoption: Its tool makes the website's source code appear different every time it is viewed, thus, preventing botnets and malware from running scripts. The process happens all under the hood without the user noticing any changes.

The company claims to have thwarted more $1 billion in losses for its customers, including several Fortune 500 and government companies. The company's last series of funding was spent on expanding in the Asia-Pacific region. The company is also a participant in the Hewlett Packard (HP) Pathfinder program; HP is reportedly offering Shape Security's products to its own customers globally.

Versive

Founded by Chris Metcalfe and Stephen Purpura in 2012, the Seattle-based firm sells on-premises software, cloud services, and professional service solutions that help businesses in automation.

What sets Versive apart: Versive uses artificial intelligence to automatically and dynamically contextualize behaviors within the adversary campaign mission stages, which enables companies to separate campaigns that warrant investigation from network noise.

Market adoption: Versive focuses on adversary detection. The company recently announced it has raised an additional $12.7 million in funding, reaching a total funding of $54.7 million. The company has also earned recognition from prominent industry stakeholders, including CB Insights' prestigious Artificial Intelligence 100 list ("AI 100"), Best of Interop for Emerging Vendor in Security. Apart from these, John Johnson, a member of Versive's CISO Advisory board, was a delegate at the Hacker Halted conference in Atlanta, GA. In addition, Bryan Hurd, Versive's Senior Director of Security Strategy, spoke at the EC-Council's Global CISO Forum, also in Atlanta.

Bugcrowd

Founded in 2012 in Australia by Casey Ellis, Bugcrowd is now based in San Francisco and specializes in application security, mobile application security, penetration testing, secure development, bug bounty programs, bug bounty, and bug hunting.

What sets Bugcrowd apart: Bugcrowd connects companies and their applications to a crowd of tens of thousands of security researchers to identify critical software vulnerabilities.

Market adoption: Bugcrowd is currently one of the world's top bug bounty startups. To date, the company has enrolled 60,000 security researchers on its platform. The startup serves as a bridge between white-hat hackers and companies, where the hackers assist the latter in finding bugs and vulnerabilities. It has a revered clientele like MasterCard, Pinterest, and Fiat Chrysler of America. The firm is backed by Blackbird Ventures, Costanoa Ventures, Industry Ventures, Paladin Capital Group, Rally Ventures, and Salesforce Ventures.

Sqrrl

Sqrrl was founded in 2012 by a team of several network engineers who left their jobs at the National Security Agency to start their own firm. The team included Ely Kahn, the former Director of U.S. Cybersecurity Policy,

What sets Sqrrl apart: Sqrrl specializes in threat-hunting, which enables organizations to target, hunt, and disrupt advanced cyber-threats.

Market adoption: Originally headquartered in Washington D.C., Sqrrl moved to Cambridge after receiving $2 million in venture capital funds from Kendall Square's Atlas Venture. Sqrrl relied on Apache Accumulo and used the open-source technology for cybersecurity. It is believed to be an industry-leading threat detection and response platform that unites several threat detections and prevention techniques in an integrated solution. Since its inception, Sqrrl has bagged several top innovator awards from numerous publications. In early January 2018, Sqrrl was acquired by Amazon Web Services.

Confirm.io

Founded in 2015 by Bob Geiman, Ralph Rodriguez, and Walt Doyle, this Boston-based startup specializes in mobile ID verification, ID authentication technologies, online identity vetting, identity verification, and remote identity proofing.

What sets Confirm.io apart: Confirm.io offers an API that allows companies to verify whether a user's government-issued identification card (like a driver's license) is authentic.

Market adoption: Over the last three years, Confirm.io raised at least $4 million from several investors, including Cava Capital, Zelkova Ventures, Rho Ventures, and Meyer Keith. The company invested its seed funds on advanced forensics to gather details from an ID card, as well as mobile biometrics and facial recognition. The USP of Confirm.io is its API, which instantly confirms a person's identity for any transaction that requires or benefits from proof of identity. In January 2018, Facebook acquired the company in order to potentially use Confirm.io's technology to have people confirm their identities if they're locked out of their devices for any reason.

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