Fintech: Rooted in the Past, Borrowed from the Future

Understanding Trends and the Cybersecurity Skills Gap

To CISOs With Love: Endpoints are Dead

Cyber Insurance and the Liability Paradox

Automation and Orchestration: The Big Picture
NO RULES
NO SIGNATURES
NO ASSUMPTIONS

Powered by machine learning and AI algorithms, Darktrace’s Enterprise Immune System detects emerging threats inside your network that no one else can find.

darktrace.com
“The clear leader in anomaly detection”

451 Research
INDEX

06 BUZZ
Cyber Insurance and the Liability Paradox

12 UNDER THE SPOTLIGHT
An Interview with Tim Fitzgerald

17 VIEW POINT
To CISOs with Love: Endpoints are Dead

22 COVER STORY
Fintech: Rooted in the Past, Borrowed from the Future

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

30 TABLETALK
Few Minutes with Foo Siang-Tse

35 EVENT FOCUS
A Curtain Raiser to Global CISO Forum

38 INDUSTRY SPEAKS
In Discussion with Tobias Gondrom

43 IN THE NEWS
Top Stories from the Cybersecurity World

49 TECHTALK
Automation and Orchestration: The Big Picture

56 KICKSTARTERS
Startups Making Waves in the Cybersecurity World

52 KNOWLEDGE HUB
Understanding Trends and the Cybersecurity Skills Gap

74 COLLABORATIONS
Famous Collaborations in the Cybersecurity World
It may not be wrong to say that fintech has changed the way financial services are offered to consumers. It is a perfect option for the consumers, businesses, and financial institutions who in today’s connected, on-demand world want to transact in a convenient, timely, secured, and efficient manner. The future may see financial transactions being made majorly through Bitcoins, Ethereums, and other future cryptocurrencies.

Traditional banks have realized that fintech is the future; they are either running for cover or trying to stay relevant by embracing new technology solutions. The countries are also aware of the evolving fintech landscape and understand how crucial it is for economic growth. However, for fintech, a number of challenges lie ahead. In the cover story, we throw light on some of these key challenges which include lack of unilateral polices and standardizations and several cyber attack vectors.

In the Buzz section, we discuss cyber insurance, a key mitigation tool for businesses in an age where deepening dependence on technology is exposing them to greater cyber threats. Move on the Viewpoint section where our executive contributor Chris Roberts pens a candid open letter to CISOs, stripping away the hype surrounding endpoint protection.

For this issue, we interviewed three cybersecurity stalwarts – Tim Fitzgerald, CSO, Symantec; Foo Siang-Tse, Senior Managing Director, Quann; and Tobias Gondrom, CTO, Huawei. They talk about their journeys, evolving cybersecurity landscape, and challenges ahead, among many other things.

The magazine comprises a host of other informative features that look cybersecurity from an all-encompassing perspective—regulations, workforce development, partnerships, 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
jay@eccouncil.org
CYBER INSURANCE AND THE LIABILITY PARADOX

Augustin Kurian
Addressing the gathering of CISOs at the 3rd Annual CISO Summit held in Mumbai, India, in July 2017, Sunil Varkey, CISO of Wipro Technologies, pointed out, “The role of CISOs is way more complex because they handle a domain called cybersecurity. CISOs pester the management to increase the cybersecurity spending. When asked by the management if higher spending would mean the organization would not be compromised, the CISOs often respond by saying, ‘I don’t know.’”

However, complexity often derives new solutions and one of them is cyber insurance. Cyber insurance is not a hot topic and has been around for over a decade and a half. It was designed to alleviate losses incurred from cyber attacks and is a key tool that plays crucial roles. According to the United States Department of Homeland Security, “A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured’s level of self-protection.”

Timetric, in its recent ‘Insight Report: Developments in Cyber insurance,’ concluded that the growing number of attacks have turned cyber insurance into a key mitigation tool. “Although cyber insurance does not replace the need for cybersecurity technology, it has the ability to complement cybersecurity standards through mitigating cyber risk.”

According to Allianz SE, organizations are paying roughly $3.25 billion each year in annual premiums for cyber insurance. But that number is small considering the cyber insurance market is expected to reach $20 billion by 2025.

WHO NEEDS CYBER INSURANCE?

Everyone! Cybercriminals are not Robin Hood, they do not differentiate between a large company and a small company, and they will do what they do best—steal. While big corporations fortify themselves with several layers of protection, small businesses often underestimate the potential impact of cyber attacks. Many small business owners believe that hackers only attack high-profile organizations when the reality is just the opposite. In fact, nearly 90 percent of breaches occur in small businesses. A bigger concern is that

“The role of CISOs is way more complex because they handle a domain called cybersecurity. CISOs pester the management to increase the cybersecurity spending. When asked by the management if higher spending would mean the organization would not be compromised, the CISOs often respond by saying, ‘I don’t know.’”
nearly 60 percent of small businesses who face cyber attacks shut down within six months of the attack. Because news coverage of attacks primarily focuses on big corporations, small businesses are unaware of the threat they face. “For small businesses, nothing is more important than protecting their livelihood. Cyber liability insurance is another tool they can use to prevent financial disaster in the event of a malicious attack,” stated Natalie Cooper, editor of BankingSense.com in a report from Cyber Insurance Guide.

THE MISMATCH
While cyber threats have drastically evolved from the time cyber insurance was first offered, the cyber insurance market hasn’t. One of the reasons is that the cyber insurance market is largely based on old-fashioned ideas about information security and what kind of coverage a breached company will actually need.

A study by Marsh and the UK Government in 2015 concluded that cyber insurance premiums are almost three times higher than commercial general liability policies.
But even here, there has been a huge gap between the damage incurred and the breadth of policy coverage. For example, in 2014, when PF Chang’s, a U.S.-based dining restaurant chain, was hacked and credit card information of nearly 60,000 customers were leaked, Chubb cyber-insurance, the insurer, only covered the cost incurred for investigation of the data breach, legal advice, and the expenses for notifying authorities and customers.

PF Chang’s policy with Chubb stated that it would “address the full breadth of risks associated with doing business in today’s technology-dependent world,” but, PF Chang’s argued, much of the cost of having been breached was not, in fact, covered. Due to this discrepancy, PF Chang’s sued Chubb to recover an additional $2 million the company was required to repay credit card companies whose details were stolen in the hack and subsequently used to make fraudulent transactions. The suit was rejected by the court upon hearing the argument from Chubb that the policy signed by PF Chang’s did not cover any external contract or agreement the company held.

Perhaps if more companies find themselves in situations like PF Chang’s did, cyber insurance policies will be forced to evolve in accordance to the needs of the market. As it stands now, high premiums keep

**TAKEAWAYS FOR CISOs**

- Work with your organization’s risk management stakeholders to understand prospective or existing insurance policies. Understand what is explicitly covered, what is not, and how the policy could be defended in court.
- Ensure that you are a part of the buying and renewal process.
- Be a part of the underwriting process.
- Communicate with insurers about prior breaches.
cyber insurance out of reach for most medium and small businesses, but as insurance companies strive to beat their competition with better, more comprehensive policies, prices will fall too.

**SOLUTION FOR THE PRESENT PERILS**

The PF Chang’s case is an example of a company not fully understanding its insurance policy, or at least, not fully understanding how that policy could be defended in court and leave them vulnerable. According to a report by JLT Re and JLT Specialty Limited, “Traditional P&C (property and casualty) products were not designed to protect against today’s fast-moving cyber risk landscape. And there are now growing fears that future losses may bring unanticipated accumulations due to potential ‘silent’ exposures.” Silent cyber risks are things like 

“(re)insurers’ potential exposure to cyber losses within P&C products where no explicit exclusions are included. And even where exclusions are included, gaps can emerge in the event of unforeseen causes of loss. As exposures evolve, the lack of understanding around silent cyber risks could pose a material threat to (re)insurers’ future solvency.”

While there is an increased number of takers for cyber insurance, the underwriters are concerned over the unquantified cyber coverage (like the incident of PF Chang’s). The report points out the need for, “greater certainty, expertise, capacity and stability from the (re)insurance market in a complex and growing risk area.” It also notes that the “standalone insurance market holds the promise of unlocking the potential for meaningful coverage for both insurers and buyers.” This means that traditional insurance companies’ longstanding history in the insurance business could actually be holding them back from offering the solutions that an industry as dynamic as information security really needs. The structures they have in place may not apply to cybersecurity because threats are often unforeseeable, the impacts of known threats aren’t easy to predict, and there is so much ongoing change that long-term policies can be out of date long before they expire.
As the Chief Security Officer (CSO) of Symantec, Tim Fitzgerald has been driving innovation on several security initiatives. He oversees the Global Security Office (GSO) and is also a member of the Symantec Security Council. Tim has a compelling view of industry trends and a unique perspective on how to best protect, monitor, analyze, and respond to security threats and issues. In a brief interaction with CISO MAG, Tim talks about his journey as a network security expert, current trends in cybersecurity, IoT hacking and cloud security, and the need to have a holistic approach to security.
Tell us about your journey from being a market analyst to a cybersecurity chief. What is Symantec’s Security Council? Tell us a bit about your role at the Council.

My early career was spent more on IT control, implementation, and evaluation. However, over the course, I became more concerned with having a job role that influences a company directly, rather than simply assessing and controlling what other people were creating. While working with one of the clients, I learned more about network security. Gradually, I started investing more in my education and research on network security, and that led to a job opportunity at Symantec as a manager. I was responsible for governance and compliance in the security department; it was a huge prospect for learning as in the early years of cybersecurity, we had a higher degree of turnover. Because of that, I had an opportunity to fill the gap, take on bigger roles, and try my hand at almost entire domain.

Coming to the Security Council, it serves the need for ground support for our security and our overall leadership in order to be successful in completing every mission. The Security Council is a governing body that we use to form our strategy and guide our security programs. The functioning of the Security Council is not my job singularly.

Symantec is known for a holistic approach toward security that merges cyber, physical, and employee security. Tell us a bit about it and how it helped the organization during the 2015 Paris attack. Do you think this sort of an approach can help other organizations combat incidents like these?

We are certainly taking advantage of forming personal relationship with the employees. I am responsible for ensuring cybersecurity of the company as well as employee safety—from our executive level to down to the lowest level employee in the company. I must admit, first when I had to take on that responsibility, I was hesitant as I didn’t know much about the space of personal and physical security. But, as we got into it, I came to realize that there is tremendous opportunity in improving the relationship with the employees, in such a way that we can demonstrate to our employees how much we care and how much we invest in their personal security.

Often many companies do the right thing in that space but do not take credit for that work. While the tragic Paris attacks happened, my physical security team reached out and contacted every single employee who was either working in the region or travelling to the region. They found out where they were, if they or their families were in any danger. We helped them get them to safety, get medical assistance, and even helped them know that somebody is looking out for them. You could imagine if you were in Paris that day, how frightened you would be and you would appreciate any level of resourcefulness even if were a reassuring voice on the other end of the phone. So, the next time we called them, or the next time we ask them that, we already have a friend, an ally, somebody who knows that you care about them personally.

In fact, we also noticed that that the employees whose lives we touched through these gestures also had a much lower rate of cyber security problems, the reason perhaps is because they take security more...
seriously and feel more responsible toward us. So, in a way, benefiting our employees was the most rewarding thing that could have happened. Many of my peers have said for a long time how employees are the biggest problem in an organization when it comes to insider threats, and in some aspects, it is true. But, we prefer to learn and treat them as an opportunity to turn our employees into advocates of security and another pair of eyes for us. It has been extremely powerful for us to leverage that human connection.

Tell us a bit about the evolution of cybersecurity over the years. How integral is it for organizations to have a cybersecurity expert among the top brass?

In many ways, I have grown up in the information security through my own learning. I have learned from my own mistakes, and from those of my peers. When I first started into cybersecurity, the CISOs were predominantly responsible for the implementation of technical controls. They were responsible for endpoint protection of some kind, or to make sure that the networks were secure, majorly focusing on technical controls. Gradually, the role evolved and CISOs moved into controlling the processes and technologies. However, over the last three to four years, they have evolved dramatically.

CISOs have become threat managers with a job to see how they implement controls that are known; this involves anticipating and analyzing a plausible problem from the start to the end. Additionally, CISOs are now involved with overall risk management. The role has shifted from the CISOs being the most technical security person in the room to being excellent risk managers. As a CISO, you are not just a manager, you are a negotiator, you become an influencer, a salesman, and a part of a much larger business discussion because you know you can speak the financial language, reputational terms, and brand terms. CISOs have now moved a little bit closer to a larger executive sweep. Driving conversations beyond just controlling the implementation, we also look at all the possible ways in which we might lose that information or data that we consider to be valuable to us. At Symantec, we have our threat evaluation methodology and ethics. As an interesting exercise, we look at not only what Symantec has used, but what others might be interested in gaining from us.

Tell us a bit about the evolution of Symantec from an antivirus company to a security solutions provider. Symantec has always been attributed as a legacy platform. What is your comment on that?

Symantec has always focused on endpoint protection, it was never just an antivirus company. Symantec has often been branded as a legacy antivirus provider, but Symantec has come far in the last 10 years in terms of providing endpoint protection against threats. Our capability in endpoint protection is so much greater and impressive that it has influenced the market in many ways. While most companies were confused with security space, Symantec went on to become a leader with market-leading products in every segment it played in.

Not many players in the security space can truly put their technology solutions together into a meaningful capability but Symantec, especially in the last few years, has found ways to do that. We not only continue to have market-leading products, but as a company, we always think about how our customers are going to use them. All these are backed with the inputs and suggestions from employees on future steps and connectivity between the solutions, that you don't find anywhere else in the market.

What are the major challenges for global enterprises against cyber attacks? What is the need of the hour? Also, what are the newer trends in cyber attacks?

Every organization is different and
the idea that we all face exact same threat universe is not helpful. If you go back five years, criminals or nations wanted to take something from you, but it was not very clear of what they were after. You had to review multiple companies to understand what were they looking for and what they got. That has changed. Majority of the cyber world has figured out how to monetize the information they steal, whether its credit card information, health information, or whatever it may be. Businesses need to evaluate their information and understand their threats, look at how their information might be monetized by the criminals, and then evaluate their threat support level. Secondly, recognizing nation/state actors and what countries might do in the information and protocol space is important. We were once concerned that nationwide actors worked either for property or profit. But now, as the U.S. elections, we are seeing governments sponsored actors are going after more than just profit. From my perspective, that is frightening. You look at some of the tactics that were used in many of these big attacks, they were not super sophisticated. We are also seeing the re-emergence of big hacking suites perhaps being associated with the NSA or other government organizations.

With IoT hacking and cloud security now hitting major headlines, can you shed some light on these subjects?

IoT in many ways is one of the next big frontiers in terms of cybersecurity. Firstly, the prevalence of IoT devices is continuously growing at an exponential pace and that has made it something to be concerned about. While talking about IoT as an attack vector, if you can take control of a whole bunch of IoT devices, it can do a lot of harm. Similarly, DDoS attacks, which is sort of an early foray, can create an army of IoT devices. What’s more concerning is that, there are many apps that claim to securing your devices, but most are far more worried about their market penetration and increasing the consumer base, with security as an afterthought. Companies must be concerned on managing the security of their devices in a way that they are less likely to be compromised. This provides a huge opportunity for every provider.

The shift toward cloud security in the last two or three years has been remarkable. But, many of the controls, the systems, the processes to make sure that the infrastructure is secured, doesn’t necessary apply in the cloud environment. The security professionals must understand and should think of ways to secure cloud environment. Symantec has made all the very moves in terms of being ready for the transition to cloud and is helping its customers get there.
Open letter, let’s see. I like the CISO opening, it’s truthful and it’s part of the spark for this. I’ve been vocal about endpoint being the mythical silver bullet for a while. Too many companies still rely upon it as the be-all/end-all for security and they typically can’t implement it all correctly, or monitor it. More and more organizations are selling the utopia of “secure endpoint and all will be forgiven.” This is a challenge to that thinking AND hopefully somewhat of a mindset change for people. We might as well start with the worst-case scenario and go from there, but I encourage you to read to the end as there IS hope! So, without further ado, here are my initial
feelings about endpoint protection in blunt bullet points:
• Nothing to gain?
• A waste of time and resources?
• Snake oil in a slick marketing campaign?
• All flash and no go?

It's arguable that the endpoint has already been compromised. Devices are still one of the core points of access into most organizations, therefore, don't bother with endpoint security, give up, go home and have a good cup of tea. That's what I really want to say BUT there must be some hope, some ray of light, otherwise why would we still have a vibrant and active commercial sector doing all they can to stave of what seems to be the inevitable onslaught of attacks launched at the very systems we strive to protect?

So, let's take a step back and look at what is working, what's not, and what we can do for the future. After all, there is little we can do to secure the actual user who still, after 25 years of InfoSec, wants to click on anything that comes into vision or is happy to jot down their passwords on post-it notes and leave them all over the office like confetti.

As an attacker, my goal is quite simple: get you or your computer to do something against your/its will, against (hopefully) company policy and against your best interest. To do this, I need to facilitate a behavior change or get lucky and hit the systems that are not patched or protected (too often this is the case, but for this exercise we'll take the utopian view that you have ALL your protection active).

Now, before we go on, let's take a quick look at what you and your endpoint have to have to be protected in today's world:
• Antivirus
• Antimalware or whatever that's called these days
• Heuristic detection capabilities
• HIDS (Host Intrusion Detection)
• Network behavior analytics
• UBA (User Behavior Analytics)
• OS patches
• Application patches
• Web browser patches
• We browser all protected too, meaning no flash, popups, redirects, Java, etc. Basically plain, vanilla text and nothing else!
• Web browser outbound analysis, DNS validation, and ensuring you
ARE going to the right cloud

- Application containerization
- Encryption
- Email filtering
- Email anti-malware, anti-anything-useful removal of all attachments enabled
- NOT admin on your local machine
- You, yes, you the squishy bag of flesh—you’d better have done your regular (monthly?) security training and know NOT to click sh*t, open attachments, give out your passwords or anything else.

So, a nice tidy list, easy to implement AND keep up-to-date daily (hourly would be preferable, but we don’t want to completely saturate the network with updates).

And we didn’t even get to the good stuff—the technology that is starting to make a difference, like the intelligent systems that are now being deployed within enterprises to facilitate the deceptive technologies, the preventative and proactive systems that monitor and watch traffic, logs, systems for behavioral anomalies and/or the logging systems surrounding them.

So, now we have all of this in place: we have the reactive, the proactive, and the preventative systems fired up, ready to protect us—and hopefully an army of staff behind the scenes watching, monitoring, managing, and generally causing a nuisance to the business by demanding security be considered at every corner. They’ll be standing by eagerly watching all the logs ALL the time for that one time the bad guy tries to get lucky.

Hopefully this sounds familiar to you all. Hopefully this situation is how you are operating, how you are protecting your users—you have not only their work systems wrapped up in an InfoSec condom but also all their portable devices, their phones, watches, wearables, home systems, kids’ systems, doorbells, Nests, and anything else that might somehow break into them to get to you. After all, you are the CISO and you have your hands firmly around all of this—right?

Ok, now reality has set in, you’ve grabbed yourself a good glass of something Scottish and peaty, and realized that this task is something more than slamming another product into the stack. It’s more than relying upon the latest vendor presentation and if you have your wits about you, it’s going to have a positive impact on that maturity model the last penetration test helped put together so you can finally track changes, risks, and report up to the board how you are being successful. You have looked at the statistics and realized that endpoint protection can be a useful tool in the defense-in-depth model as long as it’s implemented with other controls and procedures. Let’s take a look at some of those:

1. Users will still click sh*t even with protection in place. Protection does its best to mitigate, therefore, let’s train the users more effectively and combine some user grey matter with whatever brand of machine learning employed by the endpoint.

2. Users will be users—some won’t listen and will do their best to avoid the protections we put in place. Therefore, both evaluate what is necessary and required against a good risk model to ensure both the business and users can actually be productive and you can protect all the necessary assets. On top of this, add in a set of tasks to ensure exceptions are handled correctly and documented accordingly, and when the user doesn’t listen for the third
time, you have disciplinary processes in place to deal with them accordingly.

3. Not all endpoint users are to be treated equally. Therefore, remove everyone’s ability to administer their own systems and provide the required support structure and policies to deal with the special snowflakes that need and can justify the elevated privileges.

4. Endpoint can’t work effectively in a vacuum. Therefore, support it with a well-architected log management system that is also bolstered by more proactive, predictive, and preventative measures. Look beyond the traditional IDS/IPS stack towards the deceptive and other technologies that exist to complement the endpoints and other security systems. Chose wisely and don’t be fooled by the thousands of vendors that can solve all your problems.

5. Be aware that the attackers focused on your environment already have the upper hand; they have the time and resources to research not only you and your enterprise but also your people and technologies. The less you put out there about what is protecting you, the less you let your

vendors and partners talk about how they’ve protected you in a public forum, the better chance you have of slowing them down. You won’t stop them, but you will buy yourself valuable time. Combine this with an internal training focused on data, intelligence gathering, and other social engineering tactics that the users can use both in the work environment and at home, and you’ll have added another layer to what is traditionally the weakest link – us, the humans, the employees, the people at the keyboards.

Revisiting those opening statements, let’s add a little more context:

• Nothing to gain?

Relying on basic antivirus and some basic Web browsing heuristics is not going to protect you. If you are going to look at endpoint, then you need to focus on it, work through what you need for your enterprise, and approach it as carefully as you would a major overhaul of an ERP or other enterprise level system. It’s complex and requires both technical and human resources to be completely effective. Treat it with the necessary respect and you will have built yourself another effective layer of defense – treat it as a quick software purchase and you will find yourself living a lie, believing you are protected when you are not.

• A waste of time and resources?

No, but as with any product that is going to be integrated into an environment, careful planning and implementation will be key. Simply buying the software or solution and not also getting the professional services and training for your teams, or ensuring adequate coverage for the solution is going to end in failure and another product gathering dust on the shelf of useless ideas and wasted money.

• Snake oil in a well wrapped marketing campaign?

Yes, there are a number of vendors who wrap their solution in artificial intelligence, threat analytics, and other verbiage designed to entice and blind you to the simple fact that they’ve spent more on the marketing than the actual product. Some of these vendors are well known names, so do your due diligence, trust the team you employ to dissect the entire thing, and involve the end users in the selection process. Worst case call me – I’ll help!

• All flash and no go?

When they’ve spent more developing the GUI than the engine behind the tools, when the CLI has more horsepower than the flashy graphics, and the executive report has more colors to choose from than the latest car brochure, back away slowly and look for a vendor that allows you to talk with the geeks, where they are proud of what they have built, and they are willing to go geek-to-gEEK with your team at any point. Chose someone who actually is willing to work with you and not simply integrate you into this quarter’s sales numbers.

Hopefully, this has been helpful, insightful, and a little provocative. As a researcher and security architect, I’m in a unique position to be able to both assess what’s out there, break it, and implement it. In my experience, there ARE good tools out there the challenge sometimes is looking through the FUD to see the diamonds (sometimes still in the rough).

Good luck and thanks for reading to the end.

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.
Eliminating Network Blindspots

The Benefits and ROI of Ixia Visibility - Potential Areas of Impact/Savings

$500K
Speeds Troubleshooting
Even Saving Just 5 Minutes of Downtime Monthly

$205K
Aids in Compliance & Regulatory Requirements
For instance, saving an average FINRA fine

$3.8 M
Helps Protect Your Brand against Security Threats and Network Intruders
Average Cost of Data Breach

$150K - $1M+
Increases Resource Efficiency & Reduces both CAPEX and OPEX
Reduce Network Ops & Tools

Ixix Intelligent Network Visibility

Unmatched Ease-of-Use, Scalable & Flexible
Award-Winning Intelligent Visibility
Security & Performance Enabler with Powerful Metadata
Zero-Loss Visibility Platform
Application & Encrypted Data Insight

Call your Ixia Account Representative to learn how you can deploy end-to-end network visibility and experience these benefits

www.ixiacom.com

1 IDC, Feb 11, 2016, devops.com/2015/02/11/real-cost-out-smartly/
2 Forrester Institute, May, 2015 – 1500 interviews across 11 countries
3 FINRA Fine, June, 2015, FINRA (The US Financial Industry Regulatory Agency)
4 Ixia customer case studies
FINTECH: ROOTED IN THE PAST, BORROWED FROM THE FUTURE

Augustin Kurian
ew innovations in financial technology tend to be discussed as if the financial industry is only now being impacted by technological innovation. The fact is that banks and technology have always complemented each other. Technology making financial innovation possible can perhaps best be seen by looking at the 1950s when Diner’s Club introduced the first credit cards. By the 1960s, Chemical Bank of the United States installed ATMs aimed at replacing branches and tellers which dispensed cash when users inserted a specially coded card. The 1970s brought electronic stocks and by the 1980s, banks started using sophisticated computers to monitor financial data. The nineties and naughts brought internet and e-commerce to the fore and the Wall Street replaced telephone stock brokering with online stock brokerage websites.

Cut to the present and fintech, a new abbreviation simply meaning financial technology, found its way into the Oxford Dictionary as a term originated in the early 21st century. Fintech aims to leverage modern technology to craft innovative financial services that bring consumers and businesses closer. The fintech industry is one of the fastest growing segments to emerge out of cyber space – the global investment in Fintech sector skyrocketed from $928 million in 2008 to $12.7 billion by 2016. Fintech innovations like mobile wallets, payment apps, robo-advisors, etc all are largely enhancements to existing banking services, but with the direction the industry is going, the future could see fintech replacing banking services.
services or even competing with banks outright. This is the disruptive nature of startup technologies at work.

Haskell Garfinkel and Dean Nicolacakis, PwC’s US Fintech Practice co-leads, have this to say about the emerging industry: "We think about all the players in a larger fintech ecosystem, which we refer to as the As, Bs, Cs, and Ds. As are large, well-established financial institutions; Bs are big tech companies; Cs are companies that provide infrastructure or technology that facilitates financial service transactions; Ds are disruptors, fast-moving companies, often startups, focused on a particular innovative technology or process."

The evangelists of fintech have been predicting the demise of banks in the face of fintech’s explosive penetration. However, a bankless reality may be further away than some think, according to Garfinkel: “Fintech isn’t static. When we talk about the As, Bs, Cs, and Ds, we think of them as sectors in motion, all moving toward each other over time. For example, financial institutions are becoming more technology focused. At the same time, big tech companies are offering peer-to-peer payment solutions over social networks and email. Meanwhile, disruptors are providing financial services that, until recently, you could get only from banks or financial advisors,” adds Haskell Garfinkel.

However, given the complexity of financial technology, one of the inevitable challenges is with regard to cybersecurity. It is highly likely
that there will be vulnerabilities, and those will be exploited.

**KEY CHALLENGES**

The first step towards securing any industry must begin with a fundamental acknowledgment of the importance of security. Instead of thinking of how to aggressively get to the market quickly (a scenario prevalent among startups), companies must first focus on securing their product. However, securing architecture cannot be a one-step process. There should be continuous testing and dedicated quality assurance teams to create less breakable and secure codes.

Blockchain is often seen as an added advantage and a natural fit for fintech. However, there has not been a mass exodus of the general population migrating from physical to digital currency. But, if such an exodus does occur, blockchain and cryptocurrency could lead to the demise of banks and other middlemen that fail to adapt to the new reality. Of course, even blockchain is not hack proof. For example, digital currencies like bitcoin are vulnerable to hackers stealing end-users’ wallets and bitcoin exchange private keys, mining DDoS bitcoins, or even exploiting code flaws. Added to this, bitcoin is famous among the hacker community and is the currency of ransomware. It is often impossible to trace or recover data and financial losses from attacks that have been triggered from blockchain-based systems.

Another key challenge is protecting the identity of end users, which often is the most complex part of the equation. Once a hacker reaches a user’s bitcoin wallet, the outcome can be as catastrophic as bankruptcy.

**COMPLIANCE AND REGULATIONS**

The security risks of fintech are now being recognized by organizations with special attention toward application vulnerabilities. Several standardization and regulatory measures have also been mandated while several others are in the pipeline. The existing measures include Basel II, Federal Financial Institutions Examination Council (FFIEC) Uniform Rating System for Information Technology (URSIT), Gramm-Leach-Bliley Act, Fair Credit Reporting Act (FCRA), Federal Trade Commission Act (FTC Act), among several others.

Basel II focused on, “The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.” Basel II helps organizations evaluate and mitigate operational risk losses. FFIEC established URSIT as a rating system. “The primary purpose of this rating system is to evaluate the examined institution’s overall risk exposure and risk management performance and determine the degree of supervisory attention necessary to ensure that weaknesses are addressed and risks are properly managed,” states FFIEC on its website.

FS-ISAC in its 2015 report pointed out the implementation of open source management policy to boost Fintech cybersecurity. It also recommended creation of open source Bill of Materials (BOM) to identify open source components.

The existing regulations also include open source vulnerability scanning and review, incorporating risk assessments into supply chains, audits on internal controls, cyber risk governance, cyber risk management, internal and external dependency management, examination of IT assets, among several other measures standard to other technology in the industry.

Upcoming regulations like the European Union (EU) General Data Protection Regulation (GDPR)
mandates all companies must protect personal data (including financial information) of citizens. The governing bodies will verify the protection measures adopted.

At present, fintech is one of the most regulated industries in the world. But the key challenge is the presence of too many governing bodies but no universal standards – a singular regulatory policy or framework for the industry is lacking.

Fortunately, fintech is on the right track, with enough attention on ensuring secured architecture. Cybersecurity is being incorporated into new layers in mergers and acquisition processes even in the fintech industry. Standardizations are also playing a crucial role. The National Economic Council in a statement of principals have provided “a framework for stakeholders in the Fintech ecosystem to assess their role in contributing to the policy objectives. These principles represent practical and actionable propositions to help the fintech ecosystem contribute to a well-functioning and inclusive financial system and to the economy as a whole.”

Fintech is revolutionizing the financial services industry and is contributing to its growth. All it needs is optimum utilization with enough attention to security.

**Key takeaways for CISOs**

- Identify blockchain attack vectors
- Safeguard user identity
- Limit access to consumer data
- Have role-specific security training
- Embed security testing and conduct penetration test after every major change
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 look at some new appointments in the information security domain.

CISO MAG staff

KEN GONZALEZ JOINS TRIDENT CAPITAL CYBERSECURITY AS MANAGING DIRECTOR

In July 2017, Ken Gonzalez joined Trident Capital Cybersecurity (TCC) as a Managing Director. Gonzalez, who previously worked as a Senior Vice President of Corporate Development and Global Alliances at FireEye, joins TCC with the primary focus of securing the Internet of Things (IoT), next generation identity platforms, behavioral data analytics, privacy, and secure payments and fraud prevention. Gonzalez joins fellow managing directors Alberto Yépez, Don Dixon, and Sean Cunningham.

Prior to FireEye, Gonzalez was with Avast Software as the Chief Strategy Officer, where he was responsible for corporate strategy, business development, inbound licensing, and M&A. Gonzalez has also had a tenure with at McAfee as Senior Vice President of Corporate Development. At McAfee, he oversaw licensing, acquisitions, and partnerships.

He graduated from Harvard Business School and the United States Military Academy at West Point, and served in the U.S. Army as infantry officer with the 82nd Airborne Division and the 75th Ranger Regiment.

Commenting on his appointment, he said, “I chose Trident Capital because of its stellar cyber investment record, its understanding of technology and because it is renowned for its connections in the cyber ecosystem. The firm also pays close attention to helping entrepreneurs build their companies and is active on their boards. That’s important to me.”

Cybersecurity
GHANA COMMUNICATIONS MINISTRY APPOINTS ANTWI-BOASIAKO AS CYBER SECURITY ADVISOR

The Communications Ministry of Ghana recently appointed Albert Antwi-Boasiako as the National Cyber Security Advisor. He is responsible for implementing the National Cyber Security Policy and Strategy (NCSPS), and building a secure information security management architecture that will bridge the gap between cybersecurity services and government functions.

He will also assist the government with implementing policies aimed at addressing the country’s cybersecurity challenges. “The technology environment of today requires the urgent implementation of important cybersecurity activities and programs to address Ghana’s cyber security challenges and Mr. AntwiBoasiko is expected to assist the ministry to implement the policy in this regard,” read a statement from the Communications Ministry.

Boasiako is the principal consultant of cybersecurity firm E-Crime Bureau as well as a cybersecurity expert with the Interpol Global Cybercrime Expert Group (IGCEG). He has worked on several cybersecurity incidents in Accra, Ghana. A PhD Research Fellow with the University of Pretoria, South Africa, Boasiako is also an expert with the Council of Europe’s Global Action on Cybercrime Extended (GLACY+) Project.

VERVE INDUSTRIAL PROTECTION APPOINTS BILL EASTON AS CTO

Prominent cybersecurity software architect Bill Easton recently joined Verve Industrial Protection, a provider of industrial controls engineering and managed asset protection services, as the Chief Technical Officer. Easton is known for innovatively integrating different types of endpoint protection to create a simple security process for the end users.

Easton, who was previously with RES software, is involved in expanding Verve Security Center (VSC), a threat management software used to evaluate the cybersecurity stance of the end user by consolidating antivirus, application whitelisting, change and configuration management, security information and event management (SIEM), patch management, vulnerability assessments, intrusion detection, backup management, compliance, workflow, and document management into a single console.

On his appointment, Easton said, “I am thrilled to join the Verve team. The complexity of cybersecurity, especially in the ICS environment, requires that providers find a way to simplify solutions. The Verve platform is one-of-a-kind. The ability to bring together the full view of threats into an orchestrated platform is key to ensuring protection. I am excited to help continue to expand Verve’s leadership.”
WILLIAM DIXON JOINS KROLL AS ASSOCIATE MANAGING DIRECTOR

William (Bill) Dixon has joined Kroll as an Associate Managing Director where he will oversee the company’s Cyber Security and Investigations practices. Dixon is a veteran in information security and his career spans over 16 years during which he’s worked with established organizations as well as startups.

Prior to Kroll, Dixon was the Vice President of Cyber Resilience with Stroz Friedberg. Besides handling the responsibilities of client executive leadership management for existing and new clients, he also managed four sub-service categories of the practice: risk assessment, penetration testing, security strategy, and incident response. Before joining Stroz, Dixon served with Accenture as Security Consultant Senior Manager and IBM as Security Services Sales Leader.

Dixon has entrepreneurship experience as well. He was associated with HALOCK Security Lab, where he oversaw solution design, business development, and marketing as Senior Client Security Advisor. He also co-founded Continuum Worldwide Corporation, where he worked as Consulting Director of Enterprise Security Solutions.

BOB THIBODEAUX HIRED AS CHIEF INFORMATION SECURITY OFFICER OF DEFENSESTORM

Cybersecurity firm DesertStorm appointed Bob Thibodeaux as the Chief Information Security Officer (CISO) in a bid to expand the company’s team of security experts, known as Guardian. Thibodeaux will oversee incident response processes, risk management, and penetration testing for community banks and credit unions across the U.S. He will also manage any security concerns of DefenseStorm and its customers, and facilitate action plans to counter them.

Thibodeaux has over 20 years of experience in the field and has previously worked with organizations like F5 Networks and The Seattle Times. While at F5 Networks, he worked as a senior security engineer, and handled tasks related to the development and management of the security network. At The Seattle Times, he worked as the senior network engineer for InterNAP Network Services.

Thibodeaux has completed his C-level IT executive business training at the MIT Sloan School of Management.
Foo Siang-Tse is an influencer in the cybersecurity industry in the Asia-Pacific region. He has been credited with establishing Quann as Asia’s leading cybersecurity services provider. Driving the growth and development of all aspects of Quann’s business, Siang-Tse has been instrumental in introducing new products and services, establishing partnerships, and opening new markets for Quann. In a brief interaction with CISO MAG, Siang-Tse discusses cybersecurity for organizations, the need for regulations, and major threat vectors.
What, according to you, are the key threat vectors? When coming towards handling threats, do you think organizations have their priorities misplaced?

The traditional approach to cybersecurity addressed external attacks. Nowadays, internal and external vectors have become more or less equivalent. We need to focus on cyber engineering as well as safeguarding our forts. We also need to recognize the weakest link in the cybersecurity, which most often is people in an organization. This is where the greatest vulnerabilities lie.

On whether the organizations have their priorities misplaced, I really don’t think that is much of an issue. The reality is cybersecurity is not just technology – it is a much more complex subject. Our decision-making should reflect our understanding of cybersecurity, which, unfortunately, is still lacking in many countries and organizations. Organizations must frame their cybersecurity policies while addressing business risks. They should also optimize their (cybersecurity policies’) feasibility from a governance and compliance perspective.

Should businesses have a holistic approach toward security by merging cyber and physical? How does Quann differentiate cybersecurity from physical security? What are the benefits of merging the two?

I think, fundamentally, the principles of security are more or less the same whether we talk about cybersecurity or physical security. We are addressing a perpetrator trying to penetrate an organization through whatever means. The key difference between cybersecurity and physical security is the means in which the attacks are perpetrated. So no matter how complex it may sound, there should always be attention to risk. Cybersecurity must have the same amount of attention as physical security, given that organizations are much more interconnected than ever before. There is also a need to prioritize cybersecurity, which is still lacking.

It is important that security is viewed holistically. We are witnessing a convergence of threats from various vectors. There must be better visibility across all domains whether it’s physical security, cybersecurity, or operational technology. This can enable enterprises to fend off attacks appropriately. If there is a more converged approach, you will be able to look at threats from a holistic perspective because threats, or rather perpetrators, do not differentiate between cybersecurity and physical security. They are basically looking for the most vulnerable part of the organization. You are only as strong as your weakest link. Organizations really need to raise the bar to ensure that they are safe from all kinds of threats.

In one of your interviews, you mentioned that the most vulnerable person in a company is the CEO. How should organizations handle insider threats?

It is not just the CEOs, but all employees. But here, the employees...
who are not involved directly in the IT part of an organization need special attention. Typically, non-IT professionals may underestimate the potential damage cyber threats can cause. Unfortunately, there really isn’t a solution to this; there really isn’t a magical technology or product that can solve this problem. All you can do is build awareness within the organization, have training programs so that the employees are familiar with threat vectors and hacking tactics, so that they are on guard all the time. If there is proper awareness, then the employees will not respond to emails from unidentified sources and can also spot strange inconsistencies in the network. The second most important thing is to have a proper governance policy within organizations. All employees must possess basic knowledge of cybersecurity. The roles of every employee must be segregated and differentiated from others, and access to critical data must be given only to a few.

Quann has the largest bank of malicious software that has been collected in over 15 years. Can you briefly tell us how malicious software has evolved over that period?

To correct your statement, we do not have the largest bank in the world, but we do have a large bank. In the beginning, there was something called the Brain virus in boot sector, which was among the first malware. If you recall, in those days hardware played a crucial role. By the time the internet became more prevalent, malware evolved. They needed to be downloaded and installed as programs and were in mostly in .exe formats. Malware gradually gained the ability to infect content through macros. Basically, even a flash document or pdf was sufficient to allow malware to propagate. What we have also witnessed in recent years is how worms are evolving. In the past, malware was containable but now malware can propagate on its own laterally, almost like a living organism. So when each affected computer becomes a launch pad to infect other computers, it is worrying. It is no longer static but highly dynamic. Malware is now stealing credit card information and critical personal information. We are also seeing the use of artificial intelligence (AI) in various sectors. We are not far from the time when AI-infused malware evades the measures the enterprises put to guard themselves.

How secure is Quann with a bank of malicious software? Don’t you think a leak or security breach would be catastrophic?

How we treat banks is nowhere different from how enterprises treat their critical data. Our access is not singular, we really have multiple approaches to ensure that the bank is kept separate and under wraps. We have several isolation measures installed to ensure that the bank is not even remotely connected to anything that could be compromised. And on top of that, we have all sorts of security measures which ensure only the right person can access the
bank. Unfortunately, I cannot tell you more about these, but we can assure you that the bank is safe and secure.

The industry currently faces a massive skill gap when it comes to experts in cybersecurity. How should this skill gap be filled?
The demand for cybersecurity experts is at an all-time high. There is a huge mismatch between the demands of cybersecurity experts and the supply. The demand has been growing exponentially because the threats are growing exponentially, and that is the reason there is a shortage of workforce. Singapore has done something wonderful to increase the current workforce by promoting cybersecurity knowledge at various levels of education, and has been encouraging students to take up this industry. To me, that is one aspect—the second is recognizing that for enterprises, it is really challenging to recruit a new person from the market. One approach that can serve as a solution is to engage an external security service provider to help enterprises. This will help the companies manage their security without having to recruit employees to manage sophisticated software. This is one way to combat the urgent need.

Can you also comment on the relevance of certifications for network security experts and the importance of cybersecurity literacy among the current breed?
Certifications are important in that they provide external validation of the capabilities of individuals. And, it certainly is very important to know whether a person understands security and technology, as well as has the necessary skillset to take on the challenges in the industry. While saying that, I would add that there is much more to cybersecurity than certifications. I feel individuals gain the best experience in cybersecurity while working on difficult and complex problems. These help them hone their necessary skills to deal with cybersecurity risks. These are not the skills that one will learn from the books but is an art as it is extremely dynamic.

What are the future plans of Quann with regard to expanding its security operations center (SOC) footprint?
Like all businesses, we are looking to expand, we are looking to grow. And in this particular industry of managing cybersecurity, the most important aspect is coverage. The strength of a company is in its ability to cover a wide range of customer bases, verticals, and machines. Having broader coverage means better visibility and anticipating threats before they come. For us, the key area is the SOCs. We are looking for better market penetration and it is pretty exciting.

Quann has SOCs both in Singapore and India. While Singapore topped the Global Cybersecurity Index in 2017, India was ranked 23rd. What cybersecurity strategies can countries like India learn from Singapore? Also, do you think growing economies need stringent regulations to encourage better existing cybersecurity policies?
I think every country has different sorts of threats and different ways to approach threat vectors. I don’t think we need to analyze countries on that. The typical ingredients for ensuring that countries or enterprises are cyber secured are the support of the government, a robust regulatory framework, skilled professionals, and a free ecosystem of cybersecurity providers.

For enterprises, the focus must be on security, convenience, and cost. They must understand that cybersecurity is important for both individuals and enterprises. And, regulations be must be such that everyone is able to adopt them, be it organizations, enterprises, or individuals.
GLOBAL CISO FORUM

THE ART OF CYBERWAR:
THE CISO AS GENERAL

EC-Council Foundation’s Global CISO Forum (GCF) 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 seventh year, the 2017 Global CISO Forum promises to be the best yet with an exciting mix of industries, formats, and interactive presentations.

*Amber Pedroncelli*
The theme for GCF 2017 is "The Art of Cyberwar: The CISO as General." The conference will be an opportunity for the speakers and audience to explore the ways their leadership impacts their teams, organizations, and careers. Keynote presentations, panel discussions, and roundtable sessions will cover topics from IS frameworks, policy management, aligning a security program to the goals of the organization, among many others.

The 2017 GCF, EC-Council’s largest executive event of the year, promises to be the most relevant event for executives of the year. The event was constructed by the GCF speaker committee with an eye toward ensuring every executive who attends the event will come away better able to perform the duties of an information security leader.

The speaker committee chose from a formidable stack of speaker submissions to craft this year’s agenda. Starting with the realization that most CISOs are interested in the show and keynotes of the first half of the first day of Hacker Halted, the EC-Council event the GCF runs alongside, the two conferences will be joined to hear the opening keynote, debate, and second keynote. The first keynote will be, as tradition dictates, delivered by EC-Council CEO Jay Bavisi – historically one of the highest rated presenters of the conference year after year.

The debate following Bavisi’s address will address the topic “Hackers, The Media, Truth, Trust, and Alternative Facts” and will be moderated by industry veteran Winn Schwartau, Founder of The Security Awareness Company. Schwartau hand-picked his debate panel, inviting Dr. PH (c) Gregory Carpenter, Owner at GCE, LLC; Michael J. Masucci, Hollywood Producer; and Mark Rasch, CyberAttorney (former DoJ) to address some of the most pressing issues facing not just the industry, but the world at large.

Following the 90-minute debate, Chris Roberts, Chief Security Architect at Alcalvio, will present his keynote entitled, provocatively, “Leave your zero days at the door, leave your latest hacks behind, AND bring your playbook for the blue team.”

And with that, the CISOs will head to the GCF room for their closed-door, executive session. The first GCF keynote will be presented by Brian Phillips, CISO of Macy’s. Phillips, a seasoned executive and speaker, will highlight lessons he’s learned over his impressive career.

Following this day of high-level technical and executive content, the CISOs will be treated to a networking and cocktail reception at Atlanta’s Top Golf facility. The GCF speaker committee recognizes that one of the most important parts of any executive conference is the time allowed for networking and peer conversations. Therefore, a full afternoon will be set aside for this purpose. There are many CISOs who attend the Forum every year and look forward to the opportunity to catch up with friends they’ve made at past events.

The second day of the GCF is back to business with a keynote by Michael Santarcangelo, Founder of Security Catalyst, entitled “The three questions security leaders must answer to earn respect.” This topic was selected because of its relevance to the CISO role and the challenge CISOs face in breaking free from the idea that they are primarily technical managers. Following the keynote, Santarcangelo will lead a panel of security leaders in a discussion of their real-world problems and how effective leadership has helped through their careers. Santarcangelo will also be available for 15-minute coaching sessions for any GCF attendee interested in his mentorship.

Next on the agenda is a keynote entitled “From Banking to Energy to Healthcare to Criminal Justice Systems to Academia: A CISO’s Journey” by William Miaoulis, CISO at Auburn University.

A second panel discussion will follow, focusing on “Building an Information Security Program on a Budget” moderated by Sean Kelley, CISO of EPA, and featuring Favour FEMI-OYEWOLE, CISO of The Nigerian Stock Exchange; Eric Svetcov, CISO of MedeAnalytics; and Shane Durham, Security Threat Intelligence and Analytics Director at WorldPay. The topic of building a robust security program on a less than ideal budget drives many of the hard decisions security leaders are forced to make.

Following lunch, Kathy Fithen, Chief Privacy Officer at The Coca-Cola Company, will give a talk on “The Partnership Between Privacy, Information Security, and the Business,” touching on the CISO’s responsibility to bring different stakeholders of the business together to ensure the strength of the overall security posture.

Closing out the event will be industry authority Richard Seiersen, Chief Information Security Officer & VP of Trust at Twilio Inc. Seiersen will present “How to Measure Anything in Cybersecurity Risk” – a topic he knows very well. As the CISO role has increasingly included risk management as one of the most important facets, the closing keynote should leave the attendees motivated and ready to return to their offices to lead their programs to a more secure future.

EC-Council’s CISO events have been running annually since 2011 and have attracted increasingly large and loyal crowds of executives.
HACKER HALTED
ETHICAL HACKING TRAINING

CHOOSE FROM THESE COURSES

☑ Certified Ethical Hacker (CEH)
☑ Certified Security Analyst (ECSA)
☑ Certified Network Defender (CND)
☑ Certified Chief Information Security Officer (CCISO)

ALL COURSES INCLUDE 1 COMPLIMENTARY PASS FOR HACKER HALTED (OCTOBER 9 & 10)

ATLANTA, GA
OCTOBER 5-8 2017
www.hackerhalted.com
IN DISCUSSION WITH
TOBIAS GONDROM

Amber Pedroncelli
Tobias Gondrom is among the first generation of information security experts. He has been in the industry for over two decades and has witnessed its evolution very closely. Tobias is currently the CTO for security at Huawei and a global board member of OWASP. He is also a finalist for Certified CISO (CCISO) of the year. Gondrom was interviewed by Amber Pedroncelli, where they discussed the roles and qualities of CISOs, the need for certification among CISOs, and a bit of technology.

Let's start at the beginning! How did you get into security?
I got into security somewhat as a coincidence you could say, or maybe out of interest. I started as a developer, software development, software architect and back then security was not such a hot topic. Basically, not many people were excited about it. Not many people wanted to work in this area, and management didn’t really pay too much attention on this topic back then. So, responsible for system architecture for quite a large system and a number of people who developed this, one of the things that came up is ‘Hey, what about security? Who’s actually looking after that?’ And back then people would say oh, okay, maybe this is something for the global architect team to work on. So, that was my first encounter, and I would say I liked it, and I felt very excited about it. So, then I stuck with it and over the years you learn more and more. You see this as a growing community. People are very, very passionate about it and so did I feel very passionate about it and over the years you learn more people. You learn more. You see more best practices. You feel like you can engage in this global community very well. So, it’s an exciting job.

How did you get involved with OWASP?
I got involved with OWASP about 10 years ago. At that time, the CCISO program didn’t exist yet from EC council. So, one of the questions I had, how do you design the program? Who can you ask and there were not many people around that. So, I went to the OWASP community and there were at least a number of security like-minded people. So, it was great to engage with them, to discuss with them, hey what works for you? What are common security problems? Can we maybe share some training materials? That would be good, some documentation material across organizations, because at OWASP everything is open source and free. That was a brilliant way to do so. So, in fact, at that time I used quite a bit of that to ramp up my own programs.

How did your career develop from software development to the head of security for huge corporations?
I know there are very different angles how to become a CISO. Personally, I believe it’s good that you really know how software is being built, to make sure that you understand the basics when you design security around it because there is plenty of opportunities to make mistakes for the developers and so this was actually quite helpful for me to be able to write code. At some point, I was even teaching JAVA back then. So, it was very helpful to know how these things are really done with hands on, and then later, it always is good for me that I could open a book and read the source code if necessary and deep dive if it's important.

Do you find that a lot of CISOs don't know how to code?
I find that CISOs bring in different strengths. So, a number of CISOs bring in strength from an organizational perspective, from a governance perspective, risk management perspective, and some become more from the technology angle. And every flavor has its own advantages and disadvantages. So, yes, a number of CISOs may not know how to code. But, that's fine. They have other strengths. And actually from my side, one of the reasons why I recognize this is that in addition to the coding part, actually in 2008, I also did a senior MBA, the Sloan Master’s in leadership and strategy from London Business School, which basically helped me to...
get the second angle, the people angle, and the management angle, in addition to the technology angle. So, I believe that you need both of these strengths if you want to be a good CISO.

That is an interesting spot on your resume and it was before the trend of CISOs going to get their Master’s, or their MBA. You did that a while ago. So, I was going to ask how that helped your career.

Oh, yes, it was exceptionally valuable and quite exciting as well. It was a good opportunity to take one year, really a full break and basically deep dive into the whole management, leadership, and strategy education and I’m not sure whether you’re familiar with London Business School. They are ranked among the top 10 in the world for business schools. So, it was a good thing to learn these things and later when I actually moved back into the chief information security business, like doing advisory and so on, I incorporated quite a number of the learnings I had back then about organizational design management and leadership part of the CISO programs into my daily work. So, it was quite useful.

So, you’ve really gone out of your way to educate yourself on all the different facets of being a CISO. Have you had the opportunity to share some of your wisdom with other CISOs?

Yes. It’s actually not only part of my job, it’s part of my passion. So, I very much enjoy sharing and discussing with people and exploring what would be best practices. How can you advance global knowledge in this sphere? Because basically, we have been building this body of knowledge over the last 20 years and we are still building it. So, indeed I have been enjoying this tremendously and for example, like from 2009 to just before I started at Huawei a few years ago, I’ve been advising other CISOs and actually teaching CISOs. Probably so far, I have probably taught more than 100 of chief information security officers and senior security managers from other organizations and that was always an amazing experience, very challenging discussions, good questions, and of course, you felt very tired at the end of the day, but you also learned a lot and you could feel and see the benefit of how people learn and, yeah, when the people later said, “Hey, this was really great, and we took away a lot,” then that was the greatest reward for that day.

It seems that CISOs learn best by talking, debating, discussing every point and they seem to get a lot out of that. Have you noticed any trends that came out of discussions with CISOs where you saw one particular thing that they tend to struggle with that you were able to help them with?

Well, there were actually many points and I would say, no class was the same. CISOs are very senior people in general. They already have good basics, understanding and to learn things really means that you need to discuss and go as in-depth as you can until you finally see, ‘oh, okay, this is the problem, or maybe here's some knowledge limitations.’ And so, for these discussions are essential and we would touch on stuff like security development, life cycles, processes, governance. And depending on the group that would be in the class, the topics would be different because normally I would always ask at the beginning, okay, what do you care about?

And then we would deep dive into these specific elements, testing, training materials, how do you convince your boss that you should actually invest more in security or how do you balance how much you invest and different CISOs have very different needs and different problems depending on the organization, and the maturity of these organizations, or how do you execute your strategy and your roadmap for your next CISO program, or security program for the next one, two, three, four, five years depending on that?
So, I would say there were a couple of things. Maybe some of the things that were not covered so much by others is the trends that we are moving towards an application world and a number of CISOs, at least in the past, like when I started, were more about network security focus, which would be classic parameter firewall type of things. This is like 10 years plus ago, okay? And I did notice there is a strong trend towards application layer security needs. And that was quite an interesting shift I think for a number of CISOs to see that, hey, we are not only responsible, but there is no Malware. In fact, we’re also responsible for that all the application and systems that we are running are totally secure. And there’s a number of opportunities in that.

Do you find that sometimes security lags a bit behind technology? I believe now security’s actually driving technology. Yes, 10 years ago, 15 years ago, security was lagging behind, clearly. But, we have caught up. We did catch up with that and now if you look at where a lot of the innovation is, there is so much innovation in the security field, we start to use machine learning, artificial intelligence technologies, big data analysis, huge detection capabilities, refined analysis tools. If you look around this, I think security today is really close to state of the art what’s possible in technology, and really pushing the boundary quite a bit.

But yes, there is sometimes a challenge that people may want to roll out the feature first and think about security second. In fact, that’s how the internet was also built. I also have been working with the IETF, Internet Engineering Task Force, for 15 years as a working group chair in various working groups for security. And when we started defining some of the internet protocols, we didn’t really think about security like 25 years ago, 20 years ago, and so on. But, more and more this, so the internet technology itself, security has become a standard part in the considerations for every design we make. When it comes to the applications, I can see that a number of companies just a few years ago would still say, “Oh, okay. Let’s bolt security on afterwards. Let’s do security second.”

But, I think nowadays, like the last few years, after all these big security events in the news, more and more companies are quite aware that security can pose a huge risk for their bottom line at the end of the day. So, I would say many companies now have security by design which means they actually think about the security considerations right from the start, which is something that I also very strongly advocate and yeah, they also struggle with investments. It’s always a balance. You can build some more features, or you can make the features secure. And this is always a risk based decision you need to make. But, most companies I think, now got it that if they fail to make this decision the right away, then sooner or later it will come back and haunt them.

You’ve been a CISO for quite a while. How have you seen the role change? I would say it has moved from a technical person more to a recognized management and business person. Ten years ago, the role was for a technical person who wouldn’t talk with the board. But, the last few years, I think it has become quite apparent that a CISO actually has to give reports to the board and so that requires slightly different skills sets. It requires better communication ability, leadership abilities, the ability to influence stakeholders, etc. So, there have come a number of more management related tasks with it now that is shifting the scope, and for example, if you would be comfortable just with working with machines, I think the CISO role today would no longer be comfortable for you, because actually now you need to work a lot with people.

What’s your experience been like reporting to boards and working with boards? Interesting. I think this also, as I said, this changed over time. Years back, it was more an uphill battle. But, the last few years, actually, boards have been quite open to these risks and they were very curious about things. Of course, it took some interesting challenges how to explain the scope of security risks to them because you needed to explain it in a way that a less technical person, including a CFO, or a chief customer officer, or sales officer would understand, oh, this is a massive risk to our business. So, you need to translate these things. So, this was an interesting challenge. But once, you do that, actually I found many board members are very receptive to security because once you translate it into their language, once you speak their language, they fully comprehend, oh, this is a massive risk and we have to deal with it. And boards are quite professional when it comes to general risk management and looking at strategic topics. So, they can do that. You just need to speak in their language and then it’s actually a great opportunity.

Your business education helped you grasp that fairly quickly, right? Yeah, it definitely helped a lot and translating this, understanding ROI and all the other measures and metrics that you have, I think it’s still difficult to make a good case for
business investment for security because eventually you actually have to say you pay this amount for reducing a risk and if nothing happens, your boss may actually say, well, you know what? Nothing happens. Maybe we don’t have to pay so much. Maybe nothing happens next year too. And then you have to come and really show, hey, wait a moment. We are actually managing risks here and we are trying to control the risks for our organization that we don’t go completely out of business next year. And that’s something that’s not coming so natural for people. So, yes, business frameworks, decision making frameworks have been very helpful and to understand personal biases towards risk was a good tool in explaining how to make these decisions.

Personal biases. Tell me more about that.
If you look at security risks, in general if you look at risks, there’s actually a great talk by Bruce Snyder about this. People tend to overestimate certain risks. For example, if they are spectacular but rare, you may feel oh this is so dangerous. So, let’s say for example an airplane, if it may go down, yeah, this is a very spectacular, so everybody’s very scared of it. But, effectively, your risk of let’s say dying crossing the street is potentially higher than dying when you are sitting in an airplane. So, you have a bias towards misjudging which risk you actually should mitigate more, where you should invest, and there’s a number of learnings that you can take from that. So, if you recognize your own biases, that means you can compensate for them and adjust your investment decisions, and really investing in the stuff that really makes a difference, while maybe only moderately investing in the things that are spectacular in the news, but potentially not your main risk.

I’ve heard from a few CISOs that having big, spectacular breaches in the news has been helpful for them to drive their security budgets. But, I wonder if that leads to misallocation of budget?
If you don’t compensate for your biases, it will likely lead to that you ignore your most common risks and you may overinvest, well you may spend …The problem is your budget is limited and security budgets are still not as big as they should be, and for example, at OWASP, I did study, a CISO survey a few years back where we asked CISOs how is your budget? Are you increasing next year, and so on. This was really quite interesting and we could see the budget is not big enough to do everything that you need or that you think you need. So, if you overinvest in the spectacular things, that means you don’t have enough money for doing your homework, which is maybe not so sexy, and then effectively, you’re actually exposed on the low hanging food that you just didn’t cover.

Do you sometimes have trouble hiring for your many teams? I assume you have quite a lot of people under you.
Yes, of course. Of course. This is always a challenge hiring people and I think it’s not only me. Probably everyone I talk with in this sphere is like, ‘Oh, you want to hire security architect or a security analyst? Oh boy, okay.’ It’s really quite a challenge. But, I think this is a great opportunity for people who want to enter this market that there’s still a lot of room to grow.
Due to several data breaches in 2017, cybersecurity is a buzzing topic. It is imperative that information security executives are informed about the incidents around them as headline-making breaches can lead to boardroom discussions. Read on for the 10 most important cybersecurity stories of the last two months.

_CISO MAG staff_

**US–RUSSIA CYBERSECURITY UNIT: THE CONFUSION**

After a series of events, the idea of a U.S.–Russia cybersecurity unit is in doubt. The decision to build a joint cybersecurity unit was made on the sidelines of the G-20 Summit in Hamburg, Germany, where U.S. President Donald Trump and Russian President Vladimir Putin engaged in a lengthy conversation. The issue of cybersecurity was one of the key points discussed during their two-hour long meeting.

After the meeting ended, Trump tweeted, “Putin & I discussed forming an impenetrable Cyber Security unit so that election hacking, & many other negative things, will be guarded... and safe.” The comment drew widespread criticism from government officials in the U.S. who vehemently opposed the formation of any alliance with the Russian government. Following the uproar, Trump again tweeted, “The fact that President Putin and I discussed a Cyber Security unit...”
IN THE NEWS

doesn’t mean I think it can happen. It can’t—but a ceasefire can, & did!” within a few hours.

However, on July 20, 2017, a Russian government-run media organization quoted Russia’s special envoy on cybersecurity Andrey Krutskikh as saying the talks between the country and the U.S. on the joint cybersecurity unit are still on. He was quoted as saying, “there is no need to dramatize the working process, it is undoubtedly difficult, taking into account the current American realities, but this is a problem rather of the U.S. administration, not ours.”

Two days later, U.S. National Security Agency Director Mike Rogers dismissed the idea of the unit, saying “now is probably not the best time to be doing this.”

American television network HBO was in the news recently for wrong reasons, as hackers broke into its infrastructure and stole 3.4 terabyte of data, including forthcoming episodes and scripts of popular TV shows “Game of Thrones,” “Ballers,” and “Room 104,” along with personal data of employees.

The hackers sent an anonymous email to reporters saying, “greatest leak of cyber space era is happening. What’s its name? Oh I forget to tell. Its HBO and Game of Thrones!!!!! You are lucky to be the first pioneers to witness and download the leak. Enjoy it & spread the words. Whoever spreads well, we will have an interview with him. HBO is falling.”

The fourth episode of the highly-watched seventh season of “Game of Thrones” was released online two days after the hack, and a week later, the attackers leaked personal phone numbers, email addresses, and home addresses of cast members of the TV series. Asking for an undisclosed amount as a ransom to prevent further data leaks, the hackers released a video that said, “HBO spends 12 million for Market Research and 5 million for Game of Thrones advertisements. So consider us another budget for your advertisements!”

The latest security breach, which is supposedly several times bigger than the Sony hack in 2014, is reportedly under investigation by the FBI. The TV channel faced a similar situation back in 2016, when four episodes of “Game of Thrones” were leaked online. Amid the series of events, the fourth episode of “Game of Thrones” was leaked on August 4, 2017. HBO’s distribution partner Star India was held accountable for the leak. Amid the series of events, the fourth episode of “Game of Thrones” was leaked on August 4, 2017. HBO’s distribution partner Star India was held accountable for the leak. In connection to the incident, four men from Mumbai were apprehended by Indian cyber sleuths on August 15. The next day, HBO Spain mistakenly aired the sixth episode of the TV series before its official air date. The episode eventually landed on peer-to-peer sites and was downloaded globally.

The juggernaut of leaks didn’t stop there. On August 17, the social media handles of the cable giant as well as the Twitter account of “Game of Thrones,” was compromised by OurMine Security Group, a self-proclaimed white hat hacker group which hacks companies and approaches them with sales pitch. The group posted on the page stating, “Hi, OurMine are here. We are just testing your security. HBO team please contact us to upgrade the security - ourmine.org -> Contact.”

HBO AND THE SERIES OF UNFORTUNATE EVENTS
In a massive botched data transfer, Sweden’s Transport Agency sent information about every vehicle in the country to marketers. The agency believed it was moving the data to cloud storage via an outsourcing agreement with IBM, but apparently, the information was forwarded to third parties.

According to Pirate Party Founder Rik Falkvinge, who is also a key player at the Virtual Private Network (VPN) company Private Internet Access, a whole host of sensitive information was compromised. Several databases that may have had top-secret designation may have been included in the information security violation, including data on members of the military holding high-security positions, criminal suspects, and citizens in witness protection programs. The breach included names, photos, and addresses.

Falkvinge criticized the lack of punishment in the case. The department director found guilty in criminal court for being responsible for the incident was sentenced only to the loss of half of her monthly salary.

It also became clear that the response to the leak was lackadaisical, with the marketers who incorrectly received the information simply receiving a follow-up email requesting that they delete it with no follow-up. It has also been reported that IBM employees without security clearance outside of Sweden also had access to the information.

The Attorney General of the United States, Jeff Sessions, announced the shutdown of two “dark web” marketplaces, AlphaBay and Hansa. These sites were clearing houses for the illegal trade of products such as guns and drugs, including fentanyl and heroin. Both were Tor-based anonymous sites.

The investigation that led to the shutdowns included law enforcement agencies worldwide, led by the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), and the Dutch National Police.

AlphaBay servers were seized by law enforcement agencies in Thailand, Lithuania, Canada, Britain, and France. Alexandre Cazes, a Canadian citizen and founder of AlphaBay, was arrested in Thailand. He apparently committed suicide within a week of being taken into custody.

Europol estimates that AlphaBay had over 200,000 users and 40,000 vendors. Digital currencies, including Bitcoin, were used to process transactions. The largest online black market before being shut down, AlphaBay processed transactions worth hundreds of thousands of dollars and had taken over much of the market after Silk Road was shut down in 2013. According to FBI acting Director Andrew McCabe, AlphaBay was 10 times larger than Silk Road at its height.

Servers for Hansa were seized in Lithuania, the Netherlands, and Germany under the coordination of the Dutch National Police. Prior to shutting down the site, authorities took “covert control” of it in order to track migration from the shutdown AlphaBay site to Hansa.
**IN THE NEWS**

**MARCUS HUTCHINS, WANNACRY HERO, FACES 40 YEARS IN JAIL**

Marcus Hutchins, the man who discovered the WannaCry kill switch, is facing a jail term of at least 40 years. The FBI arrested him on August 4, 2017, on the charges of developing and selling banking malware as he was about to board a flight back to the United Kingdom from Las Vegas after attending the hacking conference DEFCON.

Hutchins stands accused of building and selling a banking trojan named Kronos. He and another unknown associate had allegedly sold the malware on the dark web between 2014 and 2015. During questioning by FBI, Hutchins admitted to writing some codes about a malware, but only for research purposes.

Hutchins has been in a jail in Nevada ever since. He appeared in court on August 14, 2017 in Milwaukee, WI, and pleaded not guilty to the charges. Currently, he is out on a $30,000 bail on several strict conditions such as no Internet access and an ankle monitor. He had to surrender his passport as well.

---

**LAWS OF ROBOTICS PUBLISHED BY UK FOR SELF-DRIVING CARS**

The United Kingdom Transport Minister Lord Callanan announced a set of privacy and security principles targeted toward automakers, distributors, and suppliers to safeguard the forthcoming automated vehicles from any potential cyber threats. The set of principles was jointly drafted by the UK’s Department for Transport with the assistance of the Centre for the Protection of National Infrastructure.

The eight principles come with several sub-principles that encourage all the participants in the supply chain to work together. The principles include:

- Organizational security is owned, governed, and promoted at the board level;
- Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain;
- Organizations need product aftercare and incident response to ensure systems are secure over their lifetime;
- All organizations, including subcontractors, suppliers and potential 3rd parties, work together to enhance the security of the system;
- Systems are designed using a defense-in-depth approach;
- The security of all software is managed throughout its lifetime;
- The storage and transmission of data is secure and can be controlled;
- The system is designed to be resilient to attacks and respond appropriately when its defenses or sensors fail.
A recent survey by United Nations International Telecommunication Union (ITU) revealed that Singapore has the best cybersecurity approach in the world. Singapore is ahead of U.S., Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France, and Canada. Equatorial Guinea was the lowest ranker with a score of zero.

The report lauded Singapore for a number of its cybersecurity initiatives, including the launch of their cybersecurity master plan in 2005 and the establishment of The Cyber Security Agency of Singapore in 2015 “to oversee cybersecurity and the country issued a comprehensive strategy in 2016.”

The survey featured 195 countries which were evaluated on the basis of their legal, technical, and organizational skills, educational and research capabilities, and cooperation in information-sharing networks.

It was observed that many wealthier nations did poorly in adhering to robust cybersecurity strategies, whereas some poor countries fared much better. The famously technically-advanced Estonia is ranked 98th in the world in GDP but 5th in the world on the ITU report – much higher than Germany, which ranks 4th in the world in GDP but 24th on this report. Small, rich countries such as Andorra, Liechtenstein, Monaco, and San Marino got low ranks as well.

WANNACRY ATTACKERS WITHDRAW RANSOM FROM ONLINE WALLETS

According to a BBC report, the online accounts involved in collecting ransoms from the WannaCry victims were emptied by late July or the first week of August. The attackers withdrew more than $140,000 worth of bitcoins and have been laying low ever since.

Bitcoins can be turned into real money but experts feel that a large amount of the ransomed bitcoins have most likely been put through a ‘mixer,’ allowing the digital money to be mixed with other larger payments that could be used inconspicuously and are harder to track.

The WannaCry malware that crippled businesses around the world was launched in May 2017. To unlock victims’ computers, attackers demanded ransoms between $300 and $600 in the form of bitcoins.

Despite instructions from cybersecurity experts and law enforcement agencies against payments, several victims gave in to the attackers’ demands.
CHINA ENFORCES FIRST ACTION UNDER NATIONAL CYBER LAW

Chinese authorities came down hard on a local Internet data center company for reportedly not adhering to the newly implemented National Cyber Law. The company reportedly failed to preserve a blog and was issued a warning from the Chongqing’s Public Security Bureau (PSB). The Bureau ordered the company to rectify the issue within 15 days.

This was the first instance of enforcing action against a company that did not adhere to the National Cyber Law that was implemented on June 1. The law requires companies to store data like information about Chinese citizens or data concerning national interests on domestic servers. It also requires every firm that exports bulk data to undergo an annual security assessment.

Four government departments have also jointly initiated "Action Plan for Personal Information Protection Improvement," under which an expert panel would examine the privacy policies of 10 notable domestic network product and service providers.

NORTH KOREA TARGETED BY HACKERS AFTER ICBM TEST

North Korea is facing a barrage of cyberattacks from an unknown hacker group. According to experts, the group is using Konni malware, a remote access trojan (RAT), to attack North Korean organizations. At least three campaigns have been detected so far in 2017, the most recent being in July after the intercontinental ballistic missile test.

Experts haven’t pinpointed a reason for the attacks but suggested it may be "geared towards espionage against targets who would be interested in North Korean affairs." According to researchers, the malware can "hide in the background" while victims are tricked into releasing the payload. Hackers can easily steal data using keylogger and screen grabbing features in the malware.

Researchers at Kaspersky Labs suggested that the malware could be created by people of Korean origin. Some researchers also suggested the attack could have originated from within South Korea.

Though presumably the victim in this case, North Korea has allegedly carried out a number of cyber attacks. Recently, South Korean government-backed Financial Security Institute suggested in a report that around 1,700 hackers are looking to break into a number of international banking systems to steal cash. If the report is to be believed, North Korean was behind the attacks on Bangladesh’s central bank as well some Polish banks.
AUTOMATION AND ORCHESTRATION: THE BIG PICTURE
Tari Schreider, Chief Cybersecurity Strategist and Author, Prescriptive RiskSolutions, LLC

CYBERSECURITY COUNTERMEASURES SPRAWL
Today, CISOs have a dizzying array of cybersecurity technologies offering the promise of a securer tomorrow. Each technology performs its appointed mission of protecting assets and information with aplomb. Layer by layer, one security technology is stacked upon another hoping to achieve defense in depth. However, the bad actors somehow still find a way around our defenses. No wonder CISOs have trouble asking for funding for the next galactic malware cure. CFOs may not say it, but they are thinking it, “if you cannot make what we have work together to reduce our risk, we’re just throwing good money after bad.”

If there were only way to leverage our growing complexity of desperate cybersecurity technologies and force multiply our limited SecOps
personnel with machine agility and speed. Well there is my fine CISO friend, there is. The age of automation and orchestration is dawning. Solutions now exist that allow you to automate your cybersecurity playbooks. With an extensible automation and orchestration platform, you can programmatically curate from your inventory of countermeasures your response to various threat scenarios.

**MARKET ADOPTION**

You may have already seen their booths at RSA or received marketing grams from various security automation and orchestration vendors and wondered does this thing have legs? To answer in a word, yes. Market and Markets Research published a report in 2016 forecasting the security orchestration market will grow from $826.1 Million in 2016 to $1.682.4 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 15.3%.

Some companies jumped on the security automation and orchestration train early by announcing integration partnerships.

An example of seemingly early adoption would be the Tufin Orchestration Suite integrating with Cisco Firewalls. These partnerships were generally a space holder to allow vendors to figure this market out and create products that actually live up to the promise of security automation and orchestration.

The field of players is becoming crowded and I expect an aggressive 2017 M&A season to follow on previous year’s activity. In 2016, we witnessed IBM acquiring Resilient Systems and FireEye acquiring Invotas as well Cisco Systems acquiring Tail-F in 2014.

**KEY PLAYERS**

At my last count, there were over thirty providers of products claiming placement within the security automation and orchestration market. If you attended RSA in February, you should have noticed these products were all the rage. Some claim they are a full automation and orchestration suite while others are carving out narrow niches in areas like policy orchestration or automated incident response.

Below are the ones creating the most chatter:

- Bradford Networks - Network Sentry
- Cisco Systems – Process Orchestrator
- Cyberbit SOC 3D
- CyberSponse Inc.
- Demisto
- DFLabs - IncMan
- Exabeam Security Intelligence Platform
- FireEye, Inc. – Security Orchestrator
- Gemini Atlas Platform
- Hexadite AIRS
- IBM Corporation - Resilient Incident Response Platform
- Intel – Open Security Controller
- Komand Security Orchestration & Automation Platform
- Phantom Cyber Corporation
- Resolve Systems
- Swimlane LLC
- ThreatNexus Orchestration Engine
- Tufin Orchestration Suite

### USE CASE

<table>
<thead>
<tr>
<th>USE CASE</th>
<th>RATIONAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Resolution</td>
<td>Reduce effort to aggregate, correlate, and resolve alerts from multiple sources.</td>
</tr>
<tr>
<td>Detect &amp; Patch</td>
<td>Automate risk scoring of patch advisories, scan for missing patches and remediate in one continuous motion.</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Execute incident response playbook in real-time.</td>
</tr>
<tr>
<td>Integrate Cybersecurity Countermeasures</td>
<td>Automate security technologies to work as a cohesive integrated workflow.</td>
</tr>
<tr>
<td>Metrics &amp; Report Consolidation</td>
<td>Reduce time required to chase down metrics, consolidate results and produce reports.</td>
</tr>
<tr>
<td>Threat Intel Fusion</td>
<td>Reduce time and effort to source, analyze and report on threat intelligence from multiple sources.</td>
</tr>
</tbody>
</table>
When looking at these products you will need to recognize that half of them will no longer either be in business or operate as an independent company within the next two years. You should also note that this is an arms race with feature advantage changing sides often.

I have not mentioned the girth of log management and security incident and event management (SIEM) products that have just created white papers to convince us they are a security automation and orchestration solution.

THE PROMISE OF AUTOMATION & ORCHESTRATION

The promise of automation and orchestration solutions lies in use cases. Depending on your solution, you can improve just about any SecOps function or process.

Below are some of the use cases best served by these solutions:

From what I can see from these products, your imagination is your only limitation on how deep you can automate SecOps.

ALL THAT GLITTERS IS NOT GOLD

If you are waiting for the other shoe to drop, well listen – thud there it is. Security automation and orchestration solutions are the next best thing to sliced bread, but they are not magic. You have to model your processes in advance before you can automate and orchestrate them. These solutions have no idea what you want to accomplish unless you tell them. Remember that old adage “garbage in, garbage out?”

Modeling a process is a 360-degree
exercise. You will need to consider People, policies, procedures, processes, products and proof (metrics). It is only through the union of these domains does automation and orchestration occur.

I know what you are thinking, “I can get rid of all my SecOps staff through automation and orchestration. I will have a lights out SecOps.” Wait what? Nice try but it does not work like that, you will still need people. Your goal is to root out the rote tasks of SecOps freeing your people up to focus on the strategic aspects of your cybersecurity program. Yes, you may be able to stave off hiring more staff addressing the growing skills gap, but don’t go into acquiring a security automation and orchestration solution thinking you’re going to cut staff.

SECRET SAUCE: PLAYBOOKS & PARTNERS

Sometimes the difference in being compromised or not is a matter of seconds. Security and automation software provides the ability to respond to attacks at machine speed. Designed to execute preset detection protocols, these solutions reduce the dependence on manual intervention. Some of the solutions already come with playbook templates.

Solutions that offer the broadest partner eco system and customizable library of playbooks should be at the top of your evaluation list. However, for them to acquire either, they will have had to log time in the seat. You will want a company; whose product has a reasonable size customer base (25+) and can provide evidence of automating and orchestrating dozens of security products within the same client.

ELIMINATING YOUR MSSP

Security automation and orchestration has been the secret of middle of the night. What if you could eliminate all the white noise of SecOps, automate your incident response and receive a call only in times of emergency? It can happen when you implement security automation and orchestration solutions.

DEVOPS

DevOps has produced one of the most profound changes in IT in the past five years. In many ways, it is a disruptive technology forever changing the landscape of application development and operations. Security automation and orchestration solutions are perfect for facilitating DevOps by supporting a playbook that integrates security-testing, validation and monitoring throughout the lifecycle of application development to deployment. Playbooks support the integration of security testing into the domain of application programmers rather than security personnel. Application development becomes their own gatekeeper and they no longer can blame deployment delays on the security department. Also, imagine the economies of scale of automating patching and hardening into release builds. In my mind, DevOps justifies moving toward a security and automation solution alone.

A WORD OF CAUTION

I am a huge believer in taking stock of the past to ensure I do not repeat an incident as a future failure. I searched my disaster archives and found an extreme example of an automation blunder that serves as a cautionary tale. In June 2012, Royal Bank of Scotland’s (RBS) NatWest and Ulster Bank subsidiaries descended into chaos following a glitch in their software workflow automation product.
The outage was so profound it got its own Wikipedia page. During the one-month outage, 1,200 branches had to remain open past normal hours, call center staff was doubled and millions of customers suffered. The CEO had to forego his bonus because of the fiasco’s impact on roughly 20 million customers, and RBS canceled its presence at Wimbledon that year. Game, set, match.

**CONCLUSION**

Orchestration and automation solutions are not new, but advances in technology have made their time finally come. As we try to maneuver around a critical shortage of IT personnel, manage an average of 60 security products, adapt to DevOps and strive to be more effective and efficient, few choices to accomplish all are left. As the CISO of your organization, you should be leading the charge toward SecOps automation.
NEW!

TAKE YOUR HACKING BY STORM

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

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

RETAIL $749 | DISCOUNT $699

Visit iclass.eccouncil.org and use code CISOMAG at checkout.
TOOL KIT CONTENTS

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

WIRELESS HACKING
WIRED HACKING
RF HACKING

* Customize at your own risk. You assume the responsibility for your device.
   No warranty is implied or given.
With cybersecurity gaining more importance than ever, cybersecurity startups have become a main 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

---

Argus Cyber Security is a privately held automotive cybersecurity company, working with the major private and commercial OEMs, Tier 1 suppliers, aftermarket connectivity providers, and fleet managers to address the growing security challenges posed by increasing vehicle connectivity. Argus was featured among the best cybersecurity startups in 2016 by Automobile LA in the LA Auto Show, in the annual Top Ten Automotive Startups Competition. Founded in 2013, Argus understands that the more connected vehicles become, the more vulnerable they are to cyber attacks. With hundreds of millions of connected cars expected on the roads by 2020, Argus enables the motorists to stay connected and protected.

Argus’ solutions are developed by a competent research team and automotive veterans and are based on the technology of over 29 pending and granted patents. These multi-layered, end-to-end solutions embed security into the vehicle from concept stage through production, protecting the vehicle and keeping passengers safe, preventing costly cyber recalls by automakers, and safeguarding customer data and property. Argus is headquartered in Tel Aviv, with offices in Detroit, Silicon Valley, Stuttgart, and Tokyo.
**B-SECUR**

B-Secur is a Belfast-based cybersecurity firm that has developed a biometric technology that authenticates identity through a unique heart pattern. The technology is a level ahead of the existing biometric technologies like fingerprint or iris scanners, which are known to be vulnerable to hackers. B-Secur’s solution is based on ECG technology that minimizes hacking or spoofing risks.

B-Secur has several approved patents that include B-Secur Tracker, B-Secur Smartcard, and B-Secur Mobile. The company claims that all these solutions make the experience of authentication more secure, convenient, and cost effective for the end user.

The company was included in the Top 30 fintech startups of 2015 by Silicon Republic. It was also one of the finalists at the Accenture’s 2015 Fintech Innovation Lab Dublin and Google’s Adopt-A-Startup program.

**BIOWATCH**

Founded in 2015, BioWatch is a Swiss startup that claims to have created world’s first miniaturized wrist vein scanner that can be integrated into a module and added to any watch or wearable, turning the user’s wrist vein into an avenue for authentication.

The BioWatch solution can be used as replacement for badges, keys, cards, passwords, and PIN numbers. It can be used to unlock a car, access an office, log in to systems, purchase goods and services, and sign contracts and digital documents. The device leverages always-on authentication for the user for the entire period of wearing it.

BioWatch has offices in Martigny, Lausanne and Neuchâtel. Matthias Vanoni, a former EPFL/IDIAP PhD student, and Joe Rice, a former engineer at Kodak are the co-founders. The company recently got recognized at the Swiss Fintech Convention in 2017, held in Geneva. It has also participated in multiple accelerated programs and was recognized at various events, including Kickstart Zurich in 2016 where it secured third position in the Future and Emerging Technologies category.
Corelight is an American cybersecurity solution provider headquartered in San Francisco, California. It is the creator of Corelight Sensors, an open-source framework that provides network visibility by transforming high-volume network traffic into high-fidelity data for incident response, intrusion detection, forensics, and more. Corelight claims that Corelight Sensor features a comprehensive API, enterprise integrations for Splunk, Amazon S3 and Kafka, and performance optimizations yielding 3-4x higher data processing throughput compared to standard servers. The sensor helps in the investigation and prevention of ransomware, denial of service, unauthorized access, misconfiguration, abuse, exfiltration of data, malware infection, insider threat, port scanning, and advanced persistent threat (APT). It can also be helpful to track phishing or other mail-based attacks or incidents.

According to consumers, the solution is used as a “flight data recorder” for their network because users can easily go back in time to quickly understand sophisticated cyber attacks more effectively than ever before.

Capsule8 has developed a threat prevention and response platform to protect legacy and next-generation Linux infrastructure. The company claims that its solution spans the entire Linux infrastructure in data centers, in the cloud, and as across virtual machines, bare metal, and containers.

Capsule8 Protect aims to provide simplified and automated security solutions for organizations that are adopting containerized and microservice architectures. The platform provides visibility, ensures real-time threat prevention, and performs “intelligent investigation” that allow the user to review old data stored in the distributed “flight recorder” to search for signs of an attack.

Founded in 2016 by experienced hackers and seasoned security entrepreneurs, the company is headquartered in Brooklyn, New York. Earlier this year, the company raised seed funding of $2.5 million from Bessemer Venture Partners as well as individual investors Shardul Shah of Index Ventures and Jay Leek of ClearSky.
unCaptcha claims to be the world’s only managed CAPTCHA service. It uses a patent-pending 3D model approach to create gamified puzzles that leverage gaps in machine vision. Working with researchers such as Mathworks (MatLab), the company ensures that all its security images are outside the gaps of off-the-shelf machine vision software, forcing would-be attackers to write PhD-level software to attack FunCaptcha.

This approach turns one 3D model into millions of unique images by automatically introducing variations such as random noise, changing the camera angle, and shifting the image position. Every security image is unique to the user, which makes it heavily resistant to all forms of automated abuse, machine learning, client decryption, brute forcing, and sweatshop techniques. This approach also makes it easy to undo machine vision and training attacks.

Additionally, dedicated data scientists monitor FunCaptcha traffic patterns 24/7 and respond to threats within a guaranteed SLA rendering automated abuse inoperative and disarming attackers before they can recoup their costs.

FunCaptcha was founded by Kevin Gosschalk in 2013, and is headquartered in Brisbane, Australia.
Sentryo is the creator of Sentryo ICS CyberVision, a network monitoring and threat intelligence platform that protects Industrial Control Systems (ICS) and SCADA networks. The solution, which is made up of various sensors, central data visualization, and analytics software, provides analysis on industrial network communications, meaningful information about network assets, advanced anomaly detection, and real-time alerts.

Sentryo was founded in 2014 by two former tenants of Arkoon Network Security, Thierry Rouquet (CEO) and Laurent Hausermann (COO). The company collaborated with ET Digital, a digital innovation and entrepreneurial education organization, in 2014. In 2016, Sentryo raised two million Euros ($2.36 million) from ACE Management and Rhône-Alpes Création in France.
THINK SECURITY. THINK AHEAD

You might consider a cyber-attack against your business to be a remote possibility. But attack methods become more sophisticated everyday and organisations are more reliant than ever on technology to drive every aspect of their business. This means any organisation is vulnerable to a cyber-attack. Many regulatory bodies, such as General Data Protection Regulation (GDPR), MAS, SEC, etc. require organizations to demonstrate effective controls to protect data. Apvera Insight360™ supports compliance reporting and audits, making it easy to provide comprehensive insights to internal and external auditors. Apvera Insight360™ provides profiling and anomaly detection to detect and neutralize user-based threats. And it all happens in real time. New kind of threat visibility, helping clear the air.
UNDERSTANDING TRENDS AND THE CYBERSECURITY SKILLS GAP

By Amber Pedroncelli
First, the survey collected basic geographic and industry demographic data, which is important to keep in mind when interpreting the results from other categories. Represented in the survey were the following regions:

<table>
<thead>
<tr>
<th>Region</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>South America</td>
<td>5.6%</td>
</tr>
<tr>
<td>Europe</td>
<td>16.7%</td>
</tr>
<tr>
<td>Asia</td>
<td>16.7%</td>
</tr>
<tr>
<td>Middle East</td>
<td>16.8%</td>
</tr>
<tr>
<td>USA</td>
<td>38.9%</td>
</tr>
<tr>
<td>Africa</td>
<td>5.6%</td>
</tr>
</tbody>
</table>

As for industries represented in the survey, there was quite a diverse range:

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking, finance, insurance</td>
<td>33.3%</td>
</tr>
<tr>
<td>Consultancy or business services</td>
<td>11.1%</td>
</tr>
<tr>
<td>Government, public service, military</td>
<td>22.2%</td>
</tr>
<tr>
<td>IT</td>
<td>11.1%</td>
</tr>
<tr>
<td>Manufacturing or construction</td>
<td>11.1%</td>
</tr>
<tr>
<td>Transportation, utility, telecommunication</td>
<td>11.1%</td>
</tr>
</tbody>
</table>
The last area of demographics collected was on the CCISOs current level within their companies:

What level is your current position?

<table>
<thead>
<tr>
<th>Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-Level, VP, SVP, etc.</td>
<td>23.5%</td>
</tr>
<tr>
<td>Consultant</td>
<td>29.4%</td>
</tr>
<tr>
<td>Director</td>
<td>35.3%</td>
</tr>
<tr>
<td>Manager</td>
<td>11.8%</td>
</tr>
</tbody>
</table>

The first section of questions dealt with how CCISOs hire new employees for their teams. This section was important because it highlights challenges that managers, directors, and C-Level executives have when it comes to filling their teams. EC-Council was interested in determining where these leaders are feeling the known information security skills gap the most. The results point to some interesting conclusions.

First, the leaders were asked how many job openings on their teams they are currently looking to fill. Over 57% of them reported they had between 1-5 job openings currently available. Another 31% have over 5 job opportunities with one survey respondent reporting 300 jobs needing SOC analysts!

How many information security positions are you currently looking to fill with new hires?

<table>
<thead>
<tr>
<th>Number of Jobs</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>5.3%</td>
</tr>
<tr>
<td>1 to 3</td>
<td>47.4%</td>
</tr>
<tr>
<td>3 to 5</td>
<td>10.5%</td>
</tr>
<tr>
<td>I don't make hiring decisions</td>
<td>5.3%</td>
</tr>
<tr>
<td>Over 5</td>
<td>31.6%</td>
</tr>
</tbody>
</table>

The next question asked how many jobs had already been filled in the current year, finding that most leaders had only filled between 1 and 3 jobs.

How many information security positions have you filled in the last year?

<table>
<thead>
<tr>
<th>Number of Jobs</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>6.3%</td>
</tr>
<tr>
<td>1 to 3</td>
<td>50.0%</td>
</tr>
<tr>
<td>3 to 5</td>
<td>6.3%</td>
</tr>
<tr>
<td>Over 5</td>
<td>37.5%</td>
</tr>
</tbody>
</table>
When asked which jobs are the hardest to fill with qualified candidates, the CCISO reported a range of problem areas, which the most popular job being Security Analyst with 31.3% of respondents pegging it as the most difficult to fill.

<table>
<thead>
<tr>
<th>What position is the most difficult to hire due to a lack of skilled candidates?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISO, Director of Information Security, CSO</td>
</tr>
<tr>
<td>Computer Forensics Investigator or Forensic Analyst</td>
</tr>
<tr>
<td>Consultant</td>
</tr>
<tr>
<td>Information Security Manager</td>
</tr>
<tr>
<td>Penetration Tester</td>
</tr>
<tr>
<td>Security Analyst</td>
</tr>
<tr>
<td>Security Architect</td>
</tr>
</tbody>
</table>

The next subsection of the survey dealt with what is most important to infosec leaders when deciding whom to hire. The results point to many different facets of a resume all being crucial to landing an information security job. The most important, however, is finding a good personality fit for the culture or the team, which 81.3% of CCISOs rating that quality as either extremely or very important. Limiting hires to people with specific personality traits can be troubling, as studies have shown managers tend to hire people with their own personality traits, leading to teams without diversity in point of view or other areas. Conversely, it’s easy to understand why looking for a good fit for a team can lead to better cohesion. As long as hiring practices are fair and open-minded, hiring based on cultural fit can be a good option.

The next highest rated characteristic for a job-hopeful to have is experience that exactly matches the job, with 62.5% reporting this as either extremely or very important. Requiring experience that exactly matches the job has been flagged as problematic by industry experts over the years for the simple reason that it is difficult to gain experience in a particular role when all the jobs available for that role require previous experience exactly matching what the employee will be doing. This means that companies are trying to lure employees to make lateral moves with better salaries and benefits. No security leader has an endless budget, so it might make better fiscal sense to find new hires that show potential or whose previous roles and certifications make them good candidates to grow into new roles, for potentially smaller salaries.

However, it is easy to understand why leaders might want turnkey solutions to their problems. It takes time to train new employees, even those who have the exact experience needed for a new role. When an employee both has to learn new skills as well as a new company, independence in their work will take significantly longer. This may point to an opportunity in the industry for education providers to offer customized solutions to help teams overcome this obstacle and hire for potential rather than on specific experience.

Other top finishers for candidate qualifications were relevant certifications and years of experience, each with 56.3% of respondents finding those qualities extremely or very important.

<table>
<thead>
<tr>
<th>How important is experience that exactly matches the job in hiring decisions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely important</td>
</tr>
</tbody>
</table>
### How important is personality fit with culture/team when making hiring decisions?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely important</td>
<td>50.0%</td>
</tr>
<tr>
<td>Important</td>
<td>12.5%</td>
</tr>
<tr>
<td>Very important</td>
<td>31.3%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>6.3%</td>
</tr>
</tbody>
</table>

### How important are Relevant industry certifications when making hiring decisions?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely important</td>
<td>12.5%</td>
</tr>
<tr>
<td>Important</td>
<td>31.3%</td>
</tr>
<tr>
<td>Very important</td>
<td>43.8%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>12.5%</td>
</tr>
</tbody>
</table>

### How important is years of experience when making hiring decisions?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely important</td>
<td>12.5%</td>
</tr>
<tr>
<td>Important</td>
<td>18.8%</td>
</tr>
<tr>
<td>Very important</td>
<td>43.8%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>25.0%</td>
</tr>
</tbody>
</table>

The second main section of the survey dealt with the current and past employment and salaries of the leaders themselves. When asked how long they had been in their current role, most respondents reported only 1-5 years of tenure at their current organization. This fits the common wisdom in the industry that CISOs tend to change jobs every 18 months. It was interesting, however, to see that over 23% of CCISOs have actually been in their jobs for over 10 years, showing the maturity of the information security market.
The next question dealt with salaries. All salaries have been converted to US dollars for the sake of comparison. Very few CCISOs earn less than $75,000 per year, with most making between $150,001 - $200,000. EC-Council expects salaries to grow for security leaders every year that they continue this survey.

<table>
<thead>
<tr>
<th>In what range is your current salary in USD?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $75,000</td>
<td>6.3%</td>
</tr>
<tr>
<td>$75,001 - $100,000</td>
<td>6.3%</td>
</tr>
<tr>
<td>$100,001 - $150,000</td>
<td>31.3%</td>
</tr>
<tr>
<td>$150,001 - $200,000</td>
<td>37.5%</td>
</tr>
<tr>
<td>Over $200,000</td>
<td>18.8%</td>
</tr>
</tbody>
</table>
The third section of the survey dealt with how CCISOs go about finding new jobs. Asking about a number of aspects of a new job, the survey found the CCISOs value the culture of an organization and the compensation package on offer, with 82.4% of respondents rating these things as extremely or very important. In second place was having an alignment in the vision for the security program with the organization, with 76.5% of CCISOs finding this extremely or very important. Coming in just behind alignment of security vision was the work to life balance offered by the organization with 75% of the survey participants rating it as extremely or very important. The rest of the results can be found below:

<table>
<thead>
<tr>
<th>When looking for a new job, how important is an adequate budget for security program?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important</td>
</tr>
<tr>
<td>Very important</td>
</tr>
<tr>
<td>Extremely important</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When looking for a new job, how important is alignment in vision for security?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important</td>
</tr>
<tr>
<td>Very important</td>
</tr>
<tr>
<td>Extremely important</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When looking for a new job, how important is Culture of organization?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important</td>
</tr>
<tr>
<td>Very important</td>
</tr>
<tr>
<td>Extremely important</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When looking for a new job, how important is the number of direct reports you will have?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
</tr>
<tr>
<td>Somewhat important</td>
</tr>
<tr>
<td>Important</td>
</tr>
<tr>
<td>Very important</td>
</tr>
<tr>
<td>Extremely important</td>
</tr>
</tbody>
</table>
### When looking for a new job, how important is the prestige of company/organization?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
<td>6.3%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>18.8%</td>
</tr>
<tr>
<td>Important</td>
<td>25.0%</td>
</tr>
<tr>
<td>Very important</td>
<td>18.8%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>31.3%</td>
</tr>
</tbody>
</table>

### When looking for a new job, how important is compensation including salary, signing bonus, stock options, etc.?  

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important</td>
<td>17.6%</td>
</tr>
<tr>
<td>Very important</td>
<td>17.6%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>64.7%</td>
</tr>
</tbody>
</table>

### When looking for a new job, how important is the title?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Somewhat important</td>
<td>20.0%</td>
</tr>
<tr>
<td>Important</td>
<td>20.0%</td>
</tr>
<tr>
<td>Very important</td>
<td>46.7%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>13.3%</td>
</tr>
</tbody>
</table>

### When looking for a new job, how important is to whom you will report (CIO, CEO, CFO, etc.)?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Somewhat important</td>
<td>5.9%</td>
</tr>
<tr>
<td>Important</td>
<td>23.5%</td>
</tr>
<tr>
<td>Very important</td>
<td>35.3%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>35.3%</td>
</tr>
</tbody>
</table>
### When looking for a new job, how important is work/life balance?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Somewhat important</td>
<td>6.3%</td>
</tr>
<tr>
<td>Important</td>
<td>18.8%</td>
</tr>
<tr>
<td>Very important</td>
<td>43.8%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>31.3%</td>
</tr>
</tbody>
</table>

### When looking for a new job, how important is the opportunity for advancement?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
<td>10.5%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>5.3%</td>
</tr>
<tr>
<td>Important</td>
<td>26.3%</td>
</tr>
<tr>
<td>Very important</td>
<td>31.6%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>26.3%</td>
</tr>
</tbody>
</table>

The final section of the survey asked CCISOs about the factors that contributed the most to their success. The overwhelming winner for this category was networking. 83.3% of respondents said that networking was very or extremely important to the success of their careers. It's easy to understand why there are so many information security conferences around the world with results like these. Cultivating relationships, sharing information, and increasing their spheres of influence are all things that can be done at conferences. The second key to CCISOs’ success is education, with 58.8% of respondents saying their college or university educations have been extremely or very important to their success. The rest of the categories can be found below:

### How important has earning industry certifications been to the success of your career?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
<td>27.8%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>5.6%</td>
</tr>
<tr>
<td>Important</td>
<td>27.8%</td>
</tr>
<tr>
<td>Very important</td>
<td>27.8%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>11.1%</td>
</tr>
</tbody>
</table>
### How important has college/university education been to the success of your career?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
<td>17.6%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>5.9%</td>
</tr>
<tr>
<td>Important</td>
<td>17.6%</td>
</tr>
<tr>
<td>Very important</td>
<td>35.3%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>23.5%</td>
</tr>
</tbody>
</table>

### How important has effective networking been to the success of your career?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
<td>5.6%</td>
</tr>
<tr>
<td>Important</td>
<td>11.1%</td>
</tr>
<tr>
<td>Very important</td>
<td>50.0%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>33.3%</td>
</tr>
</tbody>
</table>

### How important have executive recruiting services been to the success of your career?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
<td>23.5%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>35.3%</td>
</tr>
<tr>
<td>Important</td>
<td>23.5%</td>
</tr>
<tr>
<td>Very important</td>
<td>11.8%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>5.9%</td>
</tr>
</tbody>
</table>

### How important have executive recruiting services been to the success of your career?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
<td>23.5%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>17.6%</td>
</tr>
<tr>
<td>Important</td>
<td>64.7%</td>
</tr>
</tbody>
</table>
CONCLUSION

The skill gap in the cybersecurity industry spans all levels, from CISOs to security analysts. It appears that the shortage of skilled professionals is not a problem that will be solved in the conceivable future. Most CISOs have several job openings yet to be filled and CISOs and the others involved in the recruiting process are looking for prospects with relevant certifications and experience. A major hurdle in the recruitment process is finding the right fit both with culture, personality, and experience that matches the job.

Another key finding was that most infosec professionals were holding onto their seats for years, with several CCISOs serving the same position for almost a decade. The reasons cited for this were work culture, pay scale, the organization’s approach towards security, and work-life balance. For most infosec experts, networking is one of the key components of their success. Several respondents also felt mentorship and earning industry certifications were crucial for success.

How important has mentorship been to the success of your career?

<table>
<thead>
<tr>
<th>Importance Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all important</td>
<td>5.6%</td>
</tr>
<tr>
<td>Somewhat important</td>
<td>22.2%</td>
</tr>
<tr>
<td>Important</td>
<td>22.2%</td>
</tr>
<tr>
<td>Very important</td>
<td>33.3%</td>
</tr>
<tr>
<td>Extremely important</td>
<td>16.7%</td>
</tr>
</tbody>
</table>
Fight cyber crime from the corner office

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

**CISO MAG staff**

**SNAP ACQUIRES STRONG. CODES**

Snap, the company behind Snapchat, has acquired Strong.Codes, a Swiss startup that specializes in creating software protection codes to make the process of replicating an app or program difficult. Snap’s hiring of Laurent Balmelli, the co-founder and software engineer of Strong. Codes, triggered the acquisition. Most of the staff members at Strong. Codes followed Balmelli and joined Snap, leaving only a few employees in the company that led to its closure. The remaining employees in Strong. Codes former headquarters in Switzerland now work for Snap.

Snap had spent months in Europe looking for cryptography and
cybersecurity experts, and the move to acquire Strong. Codes is seen as part of the company’s strategy to expand into Europe. Snap’s growth potential is currently limited by the dominant position of Facebook in the social media sector and the ability of Facebook to incorporate some of Snapchat’s most popular features into its stable of features. It is believed the acquisition of the Strong. Codes portfolio is an attempt to limit Facebook’s ability to adapt popular Snapchat features, though it is not clear that Facebook is basing new features on Snapchat code.

BLACKSTONE GROUP TO BUY 40% STAKE IN ISRAELI FIRM NSO GROUP

According to reports, Blackstone Group is in the advanced stages of negotiations with Israeli cybersecurity firm NSO Group to acquire 40% of the company at an estimated value of $400 million. As a second buyer, Clearsky is expected to collaborate with Blackstone for 10% of the stocks, as reported by Israeli business newspaper Calcalist. None of the firms made any comment regarding the deal.

The Blackstone Group is a multinational company based in New York that specializes in private equity, credit, and hedge fund investment strategies.

The NSO Group, a maker of spyware for mobile devices, was founded in 2009 by Omri Lavie and Shalev Hulio, and is headquartered in Herzliya, Tel Aviv. The firm is known for the development of Pegasus software that targets mobile phones to gather information and provides “authorized governments with technology that helps them combat terror and crime.”

Prior to the deal with Blackstone Group, private equity firm Francisco Partners owned a majority of the NSO Group stake. The new deal will see the holdings of Francisco Partners reduced to 40%, with Blackstone and Clearsky jointly also holding 40%. The owners will account for 6% each while the 500 employees of the company will hold another 8%.

Recently, NSO Group caught the attention of the international community due to the alleged use of the Pegasus software by the Mexican government on the devices of opposition lawmakers and private citizens, including human rights lawyers and journalists. The Mexican government denied any such involvement by terming the allegations as false rumors calling for an investigation.

OPENTEXT TO ACQUIRE GUIDANCE SOFTWARE

In a recent announcement, Ontario-based content management company OpenText said it is all set to acquire Guidance Software as a fully owned subsidiary for an overall price of $240 million in a deal that is expected to close by the third quarter of this year. The shareholders of Guidance will be paid $7.10 a share which translates to a total value of $18 million, making the final price just around $222 million.

Guidance Software is a forensic security and eDiscovery vendor that
has a customer base of 78 of the Fortune 100 companies. The acquisition will give OpenText complete access to the forensic and eDiscovery tools along with the rich customer base of Guidance Software, though some overlapping functionality is included in the package. OpenText had already closed another high-profile deal with overlapping functionality last year when it acquired enterprise content management firm Documentum from EMC for $1.62 billion.

Several other analysts from the content management industry research firms expect to see more such acquisitions from OpenText in the coming months.

HPE PARTNERS WITH CYBERINC

Cyberinc has signed an original equipment manufacturer (OEM) partnership with Hewlett-Packard Enterprise in a move to promote and market its advanced web malware isolation system Isla. The partnership will allow Cyberinc to leverage HPE’s go-to-market infrastructure and supply chain to roll out Isla on a major scale.

Isla was developed to counter cybersecurity threats in a unique way. Unlike the commonly followed ‘detect and respond approach,’ it uses unique technology to isolate all the content in a website outside the network perimeter, thus improving protection from malware-based threats.

Phillip Cutrone, vice president and general manager, Worldwide OEM, Data Center Infrastructure Group of HPE acknowledged the importance of Isla technology to counter malware-based attacks. He said, “Partnerships like this enable both HPE and Cyberinc to utilize our strengths to deliver unique solutions that bring unique technology to isolate all the content in a website outside the network perimeter, thus improving protection from malware-based threats.

**SIMPLILEARN AND EC-COUNCIL PARTNER TO TRAIN TOMORROW’S CYBERSECURITY EXPERTS**

Digital economy training company Simplilearn and cybersecurity leader EC-Council announced their partnership to bridge the growing skill gap in cybersecurity. Simplilearn will now offer the same EC-Council Certified Ethical Hacking course used by many of the U.S. Government’s military and security agencies.

A report by Frost & Sullivan predicts that there will be a global shortage of 1.5 million cybersecurity professionals by 2020. In the U.S. alone, over 40,000 information security analyst jobs go unfilled every year and employers are challenged to fill 200,000 other cybersecurity related roles, according to cybersecurity data tool Cyber Seek. To bridge this shortage in skills, employers must not only increase their hiring of certified and skilled professionals for these lucrative and high-demand security jobs, but also train existing employees from within to meet these strategic goals.

The course is available through online self-learning as well as live virtual classrooms where individuals can learn from global instructors. This partnership further provides flexible training access to attend multiple live classes for all learners who enroll by August 31. EC-Council’s in-depth training in cyber security is augmented by Simplilearn’s learning model that allows learners to access community forums, projects, teaching assistance, study plans, and reminders. Upon completing the courses, learners will be better prepared for IT security job roles across the industry.

**FIREEYE INC. AND WATERFALL SECURITY SOLUTIONS PARTNER TO BOOST INDUSTRIAL CONTROL SYSTEMS**

Israeli industrial cybersecurity firm Waterfall Security Solutions has announced a global partnership with California-based cybersecurity firm FireEye Inc. that will enable Waterfall to protect their Industrial Control Systems (ICS) that will enable Waterfall to integrate its Unidirectional CloudConnect with FireEye’s cloud-based Helix service. The move will allow Waterfall to integrate its Unidirectional CloudConnect with FireEye’s Threat Analytics Platform (TAP), drastically reducing any potential threat of remote cyberattacks to the ICS environment.

Waterfall caters to customers from different industrial sectors, including power plants, nuclear plants, manufacturing plants, utilities, and the oil and gas sector across the Middle-East, North America, Asia, and Europe. Waterfall is already accredited with global standards like NERC CIP, ANSSI, NEI, NRC, and IEC.

The integration of the FireEye’s TAP with the Unidirectional facility by Waterfall will allow security teams and plant managers to monitor industrial networks on a real-time basis, without interrupting the daily processes of the organization. Through the partnership, Waterfall also looks forward to bringing new customers who had stayed away from using any cloud or IoT services due to their concern over external cyber risks. 🌍
DESIGN, DEVELOP, AND DEPLOY

ENTERPRISE SECURITY AND GRC SOLUTIONS

GRC Solutions
Assessments, Advisory, Consulting, Technology, Implementation, Integrations

SecOps
Virtual CISO, Assessments, Advisory, Consulting, Technology, Implementation, Integrations

Vendor Management
Advisory, Consulting, Technology, VMaaS Service, Vendor Threat Monitoring

DEFEND, FORTIFY, AND SECURE YOUR DIGITAL KINGDOM
LEARN MORE AT TEMPLARSHIELD.COM

TEmplar SHIELD
CYBERCONNECT360

12 SEPT 2017
SINGAPORE
WWW.CYBERCONNECT360.COM
THE HAGUE, NETHERLANDS
09.26.2017
CISO SUMMIT

The highest level executives from across all industries and countries join to discuss the most pressing issues in information security.

www.ciso.eccouncil.org