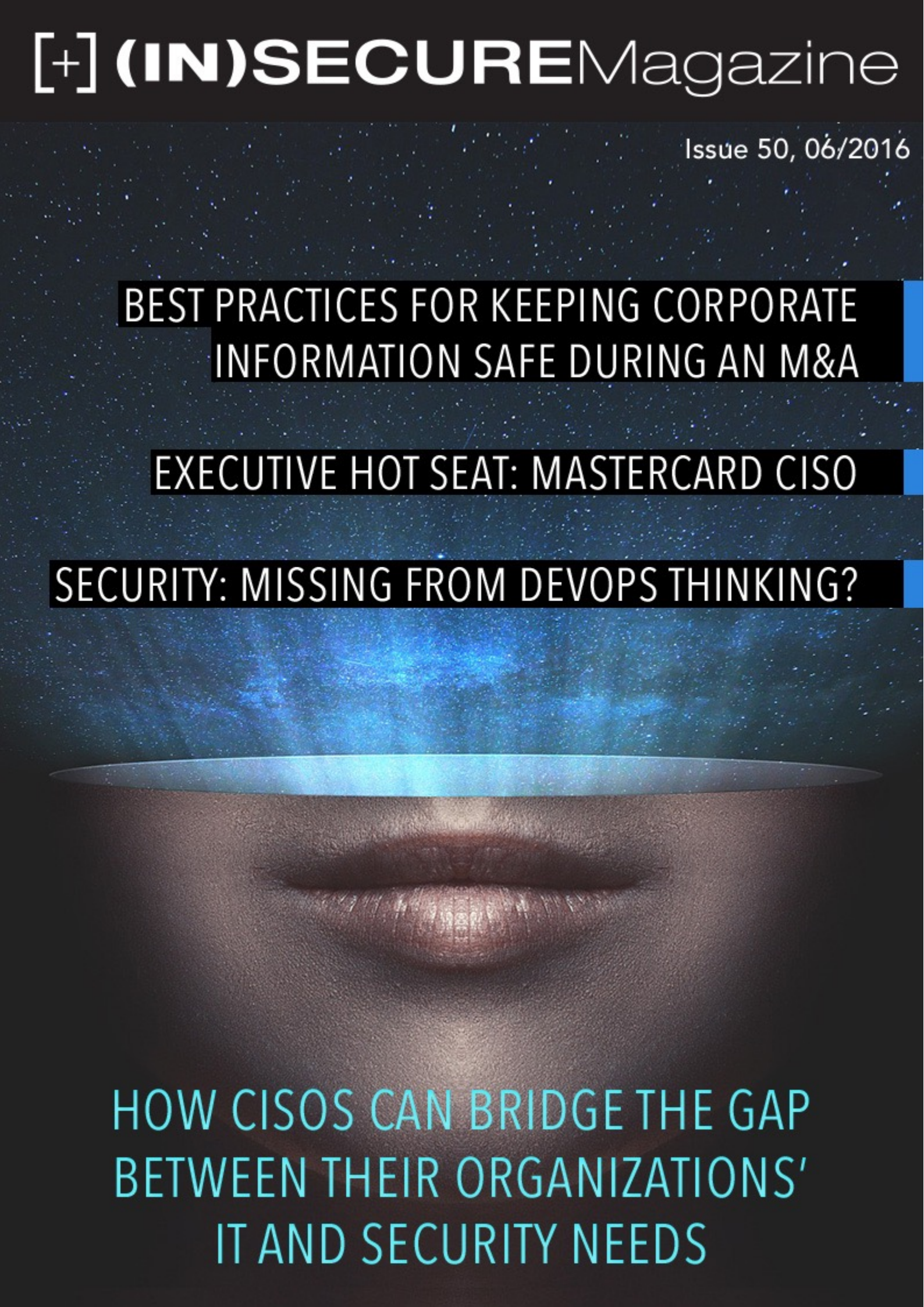
[+] (IN)SECUREMagazine

Issue 50, 06/2016

BEST PRACTICES FOR KEEPING CORPORATE INFORMATION SAFE DURING AN M&A

EXECUTIVE HOT SEAT: MASTERCARD CISO

SECURITY: MISSING FROM DEVOPS THINKING?



HOW CISOS CAN BRIDGE THE GAP BETWEEN THEIR ORGANIZATIONS' IT AND SECURITY NEEDS

No one wants to be half protected.

Full identity security for the enterprise.

Centrify®

Lily Hill House , Lily Hill Road , Bracknell , Berkshire RG12 2SJ , United Kingdom
+44 (0) 1344-317950

TABLE OF CONTENTS

- **Raimund Genes**, CTO at Trend Micro
- **Ron Green**, Executive VP, CISO at Mastercard
- **Jeremiah Grossman**, Chief of Security Strategy at SentinelOne
- **Alvaro Hoyos**, CISO at OneLogin
- **Zoran Lalic**, Senior Security Engineer at a large corporation
- **Saumil Shah**, CEO of Net-Square
- **Sumedh Thakar**, Chief Product Officer at Qualys
- **Joan Wrabetz**, CTO at Qualisystems.

Visit the magazine website at www.insecuremag.com

Contact

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

Distribution

Botnet-powered account takeover campaign hit unnamed bank

A single attacker has mounted two massive account takeover (ATO) campaigns against a financial institution and an entertainment company earlier this year, and used a gigantic botnet comprised of home routers and other networking products to do it.

“ATO attacks (also known as credential stuffing) use previously breached username and password pairs to automate login attempts. This data may have been previously released on public dumpsites such as Pastebin or directly obtained by attackers through web application attacks such as SQLi,” Akamai threat researcher Ryan Barnett explained.

The goal of the attacks is to identify valid login credential data, and either sell it on underground forums or use it to gain access to the accounts and, where possible, buy giftcards, cash out value from reward programs, etc.

The company identified the two campaigns by analyzing web login transactions across their customer base.

The attacker used an account-checking tool that had proxy capabilities, so that the login requests can be made to come from many different IP addresses.

In the campaign against the financial company, 993,547 distinct IPs were used. In that against the entertainment company, 817,390.

“When cross-referencing the attacking sources from both of these targeted campaigns, we identified that 778,786 IPs (more than 70% of the campaign participants) were attacking both customer sites,” Barnett noted. This made them conclude that the attacker is one and the same.

The login attempts came from proxy servers, but also from networking equipment. The researchers identified a big cluster of compromised Arris cable modems located in Mexico participating in the attacks, as well as compromised ZyXel routers/modems.

Tor Project tests new tool for foiling de-anonymization attacks

Upcoming hardened releases of the Tor Browser will use a new technique aimed at preventing de-anonymization efforts by anyone who might want to mount them.

Dubbed "selfrando," the technique allows for enhanced and practical load-time randomization. Selfrando is significantly more effective than standard address space layout randomization (ASLR) techniques currently used by Firefox and other mainstream browsers, the researchers say. The technique is meant to prevent code reuse attacks, i.e. attacks that use code that already exists in the app (browser, in this case). This type of attack can be executed only if the attacker can locate the needed functions, and selfrando randomizes their location (ASLR just randomizes the location of code libraries that contain the functions).

It makes it more difficult for attackers to exploit memory-corruption vulnerabilities to hijack control flow and achieve remote code execution.

"A linker wrapper intercepts calls to the linker and calls selfrando to gather information on the executable file. Then, it embeds TRaP (Translation and Protection) information and a load-time randomization library, RandoLib, into the binary file," the researchers explained.

"When the loader loads the application, it will invoke RandoLib instead of the entry point of the application. RandoLib will randomize the order of the functions in memory and then transfer control to the original program entry point."

The researchers found that selfrando can prevent most real-world exploits (e.g. those mounted by the FBI in the last few years).

"Attackers can only succeed in rare cases where they can disclose the complete heap and data section," they noted.

In the hardened version of the Tor Browser, selfrando works in conjunction with AddressSanitizer, a compiler feature that detects memory corruption bugs. According to the researchers, this defense technique is just one of several that the Tor project is trying out, and could ultimately end up being implemented in the non-hardened version of the browser.

Microsoft creates Checked C extension to prevent common coding errors

Fixing vulnerabilities in completed software and systems is all good and well, but with Checked C, an extension for the C programming language, Microsoft researchers want to prevent common programming errors that can lead to several types of frequently occurring vulnerabilities. The C and the C++ programming languages (the latter is derived from the former) are a popular choice for the development of system software. They allow programmers to use pointers – addresses of a location in memory – directly, and this allows programmers to write concise and efficient programs. But, there's a problem.

"Because pointers and array indices are not bounds checked in C, a programming error involving them may corrupt memory locations used by the program. The memory locations may hold data that is important to the computations being done by the program or data that is essential to the control-flow of the program, such as return address locations and function pointers. Memory corruption can lead to a program producing incorrect results or, in the hands of a malicious adversary, the complete malfunctioning of the program and the takeover of a running process by the adversary," Microsoft researcher David Tarditi explained in a technical report.

Checked C will provide new pointer types and array types that are bounds-checked, and thus should prevent occurrences like buffer overruns, out-of-bounds memory accesses, and incorrect type casts.

At the same time, Microsoft wants the extension to be backwards-compatible, and wants to preserve the efficiency and control of C.

AN AVERAGE

15 DDoS attacks

Companies suffer an average of 15 DDoS attacks per year

The average company suffers 15 DDoS attacks per year, with average attacks causing 17 hours of effective downtime, including slowdowns, denied customer access or crashes, according to A10 Networks.

As DDoS attacks become more popular, they are also growing harder to defend. While the average peak bandwidth of attacks was a staggering 30-40 gigabits per second (Gbps), 59 percent of organizations have experienced an attack over 40 Gbps. A majority of respondents (77%) also expect sophisticated multi-vector attacks to pose the most dangerous type of DDoS attack in the future.

Businesses are fighting back. More than half of the surveyed organizations said they planned to increase their DDoS prevention budgets in the next six months. IT security teams are the most likely to lead DDoS prevention efforts (36 percent), followed closely by the chief security officers (26 percent) and the CIO (26 percent).

“DDoS attacks are called ‘sudden death’ for good reason,” said Raj Jalan, CTO of A10 Networks. “If left unaddressed, the costs will include lost business, time-to-service restoration and a decline in customer satisfaction. The good news is our findings show that security teams are making DDoS prevention a top priority. With a better threat prevention system, they can turn an urgent business threat into an FYI-level notification.”

Key report findings

- The typical company was hit by an average of 15 DDoS attacks per year, with larger organizations experiencing more.
- One in five companies reported effective downtimes of over 36 hours, with the average attack resulting 17 hours.
- 33 percent of respondents reported DDoS attacks over 40 Gbps, with the most common attacks including UDP Flood (23%), Slow Post/Slowloris (16%) and SYN Flood (14%).
- 77 percent believe multi-vector attacks, which include volumetric and application layer attacks, will be the most dangerous in the future.
- Over half of the respondents plan to increase their DDoS budgets in the next six months (54%).
- 53% of respondents say that on-premise protection is required to be the most effective solution to address a multi-vector DDoS threat, either “hybrid” protection (34%), or an on premise appliance only solution (19%).

The average cost of a data breach is now $4 million

The average data breach cost has grown to $4 million, representing a 29 percent increase since 2013, according to the Ponemon Institute. Cybersecurity incidents continue to grow in both volume and sophistication, with 64 percent more security incidents reported in 2015 than in 2014. As these threats become more complex, the cost to companies continues to rise. In fact, the study found that companies lose $158 per compromised record. Breaches in highly regulated industries like healthcare were even more costly, reaching $355 per record – a full $100 more than in 2013.

"The amount of time, effort and costs that companies face in the wake of a data breach can be devastating, and unfortunately most companies still don't have a plan in place to deal with this process efficiently," said Caleb Barlow, Vice President, IBM Security. "While the risk is inevitable, having a coordinated and automated response plan, as well as access to the right resources and skills, will make or break how much a company is impacted by a security event."

According to the study, leveraging an incident response team was the single biggest factor associated with reducing the cost of a data breach – saving companies nearly $400,000 on average (or $16 per record). In fact, response activities like incident forensics, communications, legal expenditures and regulatory mandates account for 59 percent of the cost of a data breach. Part of these high costs may be linked to the fact that 70 percent of U.S. security executives report they don't have incident response plans in place.

The process of responding to a breach is extremely complex and time consuming if not properly planned for. Amongst the required activities, a company must:

- Work with IT or outside security experts to quickly identify the source of the breach and stop any more data leakage
- Disclose the breach to the appropriate government/regulatory officials, meeting specific deadlines to avoid potential fines
- Communicate the breach with customers, partners, and stakeholders
- Set up any necessary hotline support and credit monitoring services for affected customers.

Each one of these steps takes countless hours of commitment from staff members, taking time away from their normal responsibilities and wasting valuable human resources to the business.

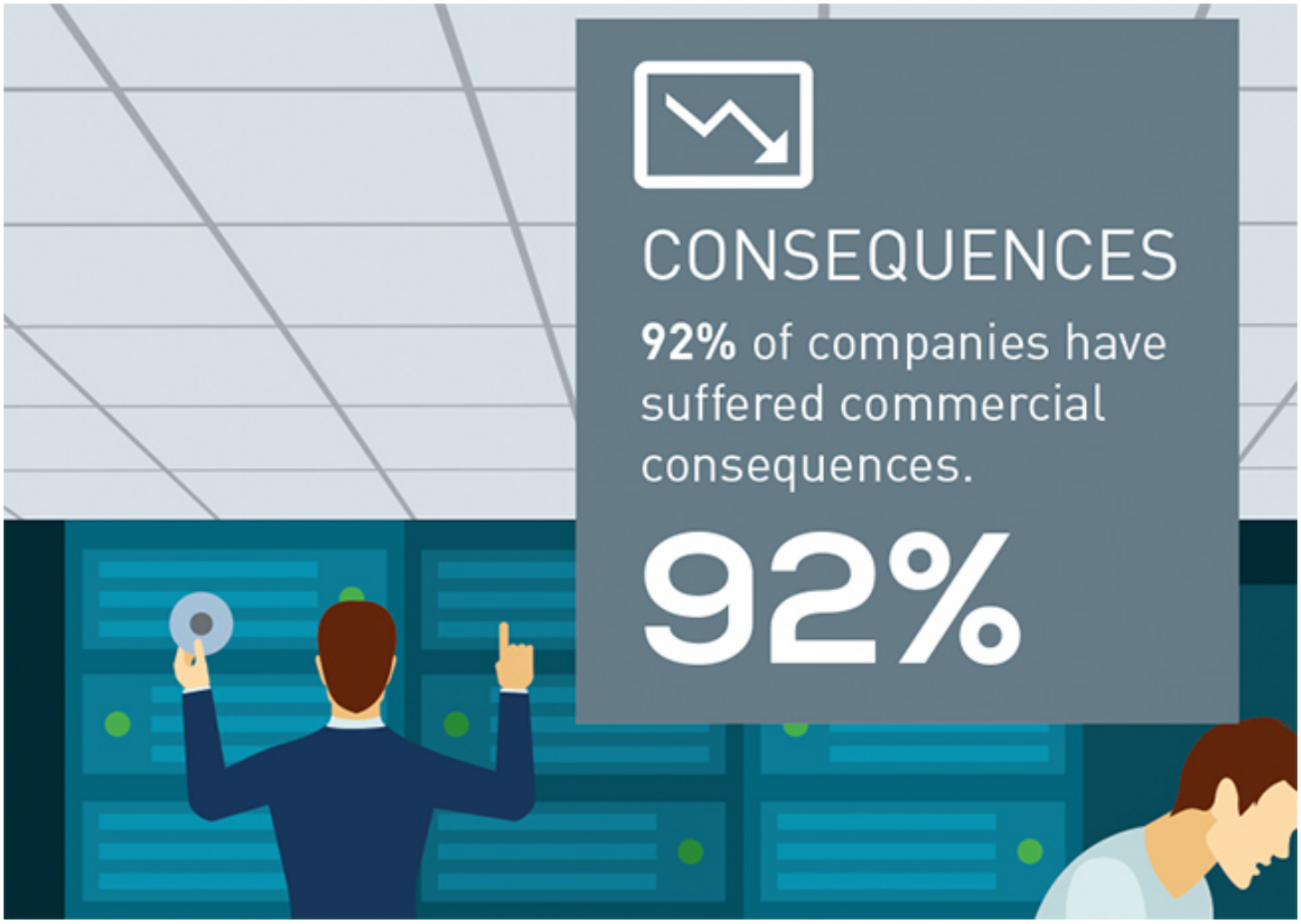
Incident response teams expedite and streamline the process of responding to a breach, as they're experts on what companies need to do once they realize they've been compromised. These teams address all aspects of the security operations and response lifecycle, from resolving the incident, to satisfying key industry concerns and regulatory mandates. Additionally, incident response technologies can automate this process to further speed efficiency and response time.

The study also found the longer it takes to detect and contain a data breach, the more costly it becomes to resolve. While breaches that were identified in less than 100 days cost companies an average of $3.23 million, breaches that were found after the 100 day mark cost over $1 million more on average ($4.38 million).

The average time to identify a breach in the study was 201 days, and the average time to contain a breach was 70 days.

The study found that companies that had predefined business continuity management (BCM) processes in place found and contained breaches more quickly, discovering breaches 52 days earlier and containing them 36 days faster than companies without BCM.

"Over the many years studying the data breach experience of more than 2,000 organizations in every industry, we see that data breaches are now a consistent 'cost of doing business' in the cybercrime era," said Dr. Larry Ponemon. "The evidence shows that this is a permanent cost organizations need to be prepared to deal with and incorporate in their data protection strategies."



A third of organizations experienced a data breach in the past 12 months

Despite the increasing number of data breaches and more than 3.9 billion data records worldwide being lost or stolen since 2013, organizations continue to believe perimeter security technologies are effective against data breaches, according to Gemalto's Data Security Confidence Index.

Of the 1,100 IT decision makers surveyed worldwide, 61% said their perimeter security systems (firewall, IDPS, AV, content filtering, anomaly detection, etc.) were very effective at keeping unauthorized users out of their network. However, 69% said they are not confident their organization's data would be secure if their perimeter security was breached. This is up from 66% in 2015 and 59% in 2014.

"This research shows that there is indeed a big divide between perception and reality when it comes to the effectiveness of perimeter security," said Jason Hart, VP and CTO for Data Protection at Gemalto. "The days of breach prevention are over, yet many IT organizations continue to rely on perimeter security as the foundation of their security strategies.

The new reality is that IT professionals need to shift their mindset from breach prevention to breach acceptance and focus more on securing the breach by protecting the data itself and the users accessing the data."

According to the research findings, 78% of IT decision makers said they had adjusted their strategies as a result of high profile data breaches, up from 71% in 2015 and up 53% in 2014. 86% said they had increased spending on perimeter security and 85% believe that their current investments are going to the right security technologies.

Despite the increased focus on perimeter security, the findings show the reality many organizations face when it comes to preventing data breaches. 64% of those surveyed said their organizations experienced a breach at some time over the past five years.

Bug bounty report card: Industry diversification and growth

With a global rise in cyberattacks and a critical deficit of security talent to combat adversaries, bug bounty programs congruently grew in both volume and scope in the last 12 months, according to Bugcrowd.

Moving beyond technology companies, more than 25 percent of public and private programs are now run in more “traditional” industry sectors – with particular traction across retail & e-commerce, financial services & banking, and automotive – and deployed across larger organizations, with companies over 5,000 employees gaining particular traction in the last 12 months.

Number of bounty programs continuously increases: Bug bounty programs on the Bugcrowd platform have increased over 210 percent on average year over year since January 2013.

Larger enterprises are adopting bug bounties: Companies with 5,000+ employees accounted for 44 percent more of the total companies launching bug bounty programs over the last 12 months.

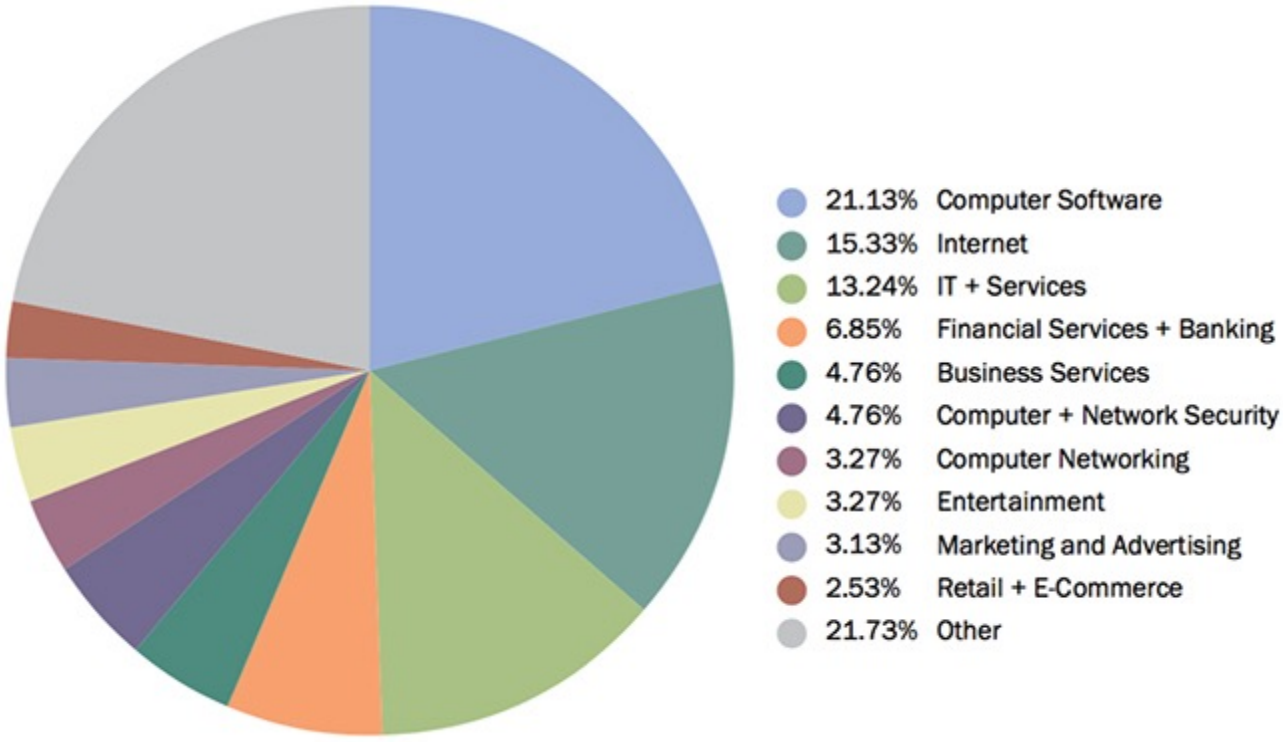
Average payouts are rising: The average bug reward to researchers rose 47 percent in the last 12 months. In Q1 2016, the average payout on Bugcrowd’s platform was $505.79.

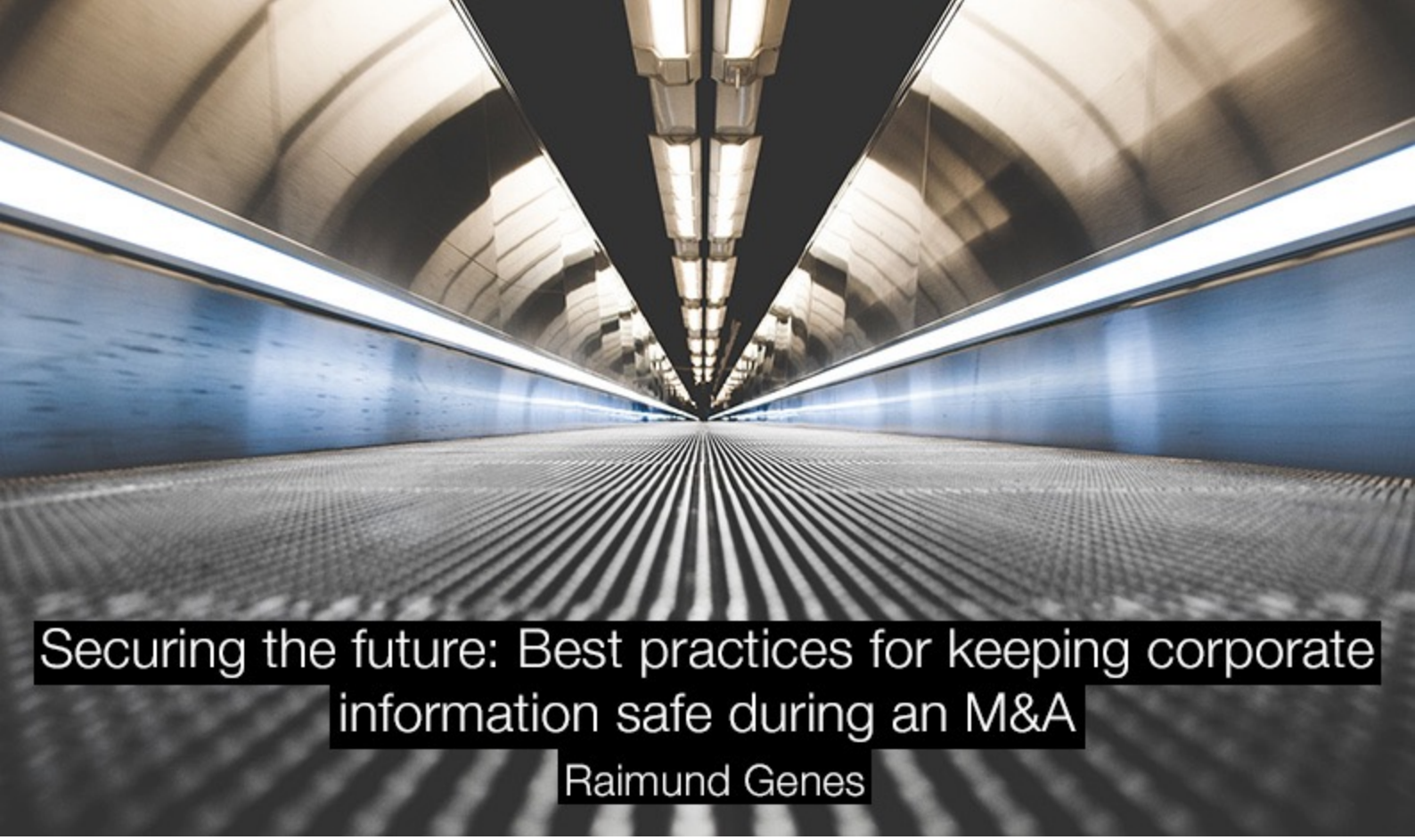
Vulnerability "super hunters" have emerged: "Super hunter" researchers earn thousands of dollars in payouts, and often participate in bug bounty programs as full-time positions. This contrasts with the majority of researchers (85 percent) participate in bug bounty programs as a hobby or part-time job, with 70 percent spending fewer than 10 hours a week working on bounties.

Bugcrowd researchers come from 112 countries, and activity varies by region: More than half (56 percent) of all submissions originate from two countries: India (43 percent) and the United States (13 percent). The top ten countries by volume of vulnerabilities submitted are India, the United States, Pakistan, the United Kingdom, the Philippines, Germany, Malaysia, the Netherlands, Australia and Tunisia.

Cross-site scripting (XSS) continues to dominate: XSS is still the single most discovered vulnerability type, at over 66 percent of all classified vulnerabilities disclosed.

Average priority of submissions are continuing to improve across all programs: Higher impact submissions (on a scale of 5 to 1 in rising priority) have increased from 3.88 to 3.75 on average over the last 12 months, reflecting the maturing skillset of the crowd.





Securing the future: Best practices for keeping corporate information safe during an M&A

Raimund Genes

Mergers and acquisitions (M&A) are constantly occurring and are complex transactions, often involving entities from around the globe: from bankers, lawyers and investors facilitating the deal, to the actual business owners and stakeholders who benefit. In the current era of cybercrime, however, the information security posture of both companies can have an impact on the financial terms, as well as the ultimate outcome of the arrangement.

Without proper security infrastructure and policies in place, financial and intellectual property, sensitive personnel and corporate information can be exposed. Therefore, the cybersecurity capabilities (or lack thereof) of the participating companies must be fully understood to ensure a seamless transaction without negative outcomes. This is also important for the ongoing stability of the reconstituted company.

There are countless moving parts to be addressed throughout an M&A within financial, HR and other business operations that drain time and resources throughout the process. Because technology is often out of sight/out of mind, IT and corresponding data security can potentially be an afterthought. A thorough assessment of current technology, and the potential risks, is paramount to bring these elements to the forefront.

In light of these challenges, it is of utmost importance that businesses consider the following components to ensure data is properly secured throughout the M&A process.

Advance preparation

Upon entering into discussion with a company they want to merge with or acquire, decision makers must analyze cybersecurity capabilities across the entire technology ecosystem of both organizations, including networks, servers, endpoints and third-party relationships. Both security gaps and overlaps should be considered during this process. Overlapping efforts can result in inefficient use of resources, and gaps expose both internal and external vulnerabilities.

This exercise should be viewed as an opportunity to start fresh, analyzing all assets to determine what does and doesn't complement

the new corporate structure. It's important to realize that the increased attack surface created during an M&A not only includes the companies involved, but third-party vendors as well. Once there is a level set of what security mechanisms are in place, and where potential pitfalls lie, expectations can be clearly communicated, monitored and evaluated to mitigate challenges or surprises.

A blended approach

After effecting initial due diligence regarding the security posture, and a deal is set in motion, an entire new array of attack surfaces can be exposed. Now both companies, whether they are merging or being acquired, must carefully assess the security environment of the new organization. What vulnerabilities exist once businesses are combined? Are there deficiencies that must be addressed immediately?

The best approach is to not force one company's solutions and requirements onto the other, but rather have a meaningful conversation between all parties regarding specific security needs. Ensuring sufficient software is in place to secure the entire organization is imperative for the overall wellbeing of the new company.

Not only are two companies and employee groups being combined, but third-party vendor and technology providers are also being conjoined. To maximize existing investments, be sure to evaluate what systems can remain in place, and perhaps integrated between the two companies to reduce expenses. Keep in mind, however, that it might not be possible to adequately verify all vendors prior to the merger or acquisition, adding an extensive risk.

Short- and long-term approach

Unifying an entire IT infrastructure takes time. During an M&A, standing contracts are typically kept through the remainder of their lifespan. As such, stopgap measures can be prudent from both an operational and financial standpoint.

For instance, combining existing solutions with an early breach detection system can buy the enterprise time to develop a broader, long-term strategy. Additionally, breach detection technology can provide warning in the event of a malfunction within the interim system, and is a more cost-effective approach than ripping and replacing existing systems and licenses.

To further safeguard corporate information during the execution of a deal, a data loss prevention solution is also advisable. These systems can prevent unauthorized access to sensitive files, block data exfiltration and otherwise protect information against misuse from untrained or disgruntled employees. Monitoring and restricting the flow of information before, during and immediately after an M&A provides peace-of-mind that access to corporate data isn't a free for all.

Additionally, an M&A provides an ideal opportunity to introduce penetration testing, by hiring third-party professional threat researchers to evaluate the new IT environment. It can also ascertain team members' awareness level about cybersecurity and potential threats. The feedback received from this assessment will provide a list of best practices and actions that employees should implement to keep corporate data safe. This is especially useful during a time of transition due to the new, vulnerable attack surfaces being introduced.

Every merger is different, however merging security policies is always best effected when the task is approached with an open mind and a holistic view of the new organization's needs. Blending security structures and processes is in the best interest of both parties, and provides an opportunity to reevaluate the overall IT environment. Proper risk assessment performed from the beginning, paired with proper testing and evaluation upon entering into a deal, will best position the new organization to defend against threats.

Raimund Genes is the CTO at Trend Micro (www.trendmicro.com). In his role, he is responsible for introducing new methods to detect and eradicate threats, and to predict movements in the digital underground with his team of threat researchers. Raimund has held several executive management positions within Trend Micro including General Manager for Trend Micro's Incubation Business, President of European Operations, European Vice President of Sales and Marketing, and Managing Director.

Executive hot seat: Ron Green
Executive VP, CISO at MasterCard
Interview by Mirko Zorz

How have your previous roles prepared you for your current role at MasterCard? What are some of the skills you've found to be essential and what did you learn in your first months on the job?

I consider myself really lucky to have held diverse and interesting positions across law enforcement and the private sector.

While with the Secret Service, I was a member of the first team of agents to receive formal training in computer forensics and electronic crimes investigations. We helped with the development of new forensics tools and systems which have become the eminent benchmarks for computer forensic utilities. We had access to the newest technologies to prepare for their potential misuse and help manufacturers address security concerns before they became real problems. We also developed hardware solutions, such as skimmer analyzers and field deployable forensic systems, to defeat technologies created by criminals.

Being in cyber security from the very early days has allowed me to witness the evolution of threats, attack tools and techniques. I've also had the chance to see which countermeasures are the most effective in addressing these attacks.

Prior to joining MasterCard, I worked in information security for financial services and technology companies. This experience allowed me to examine more deeply the challenges and threats around financial data and technology systems. It's been a great foundation for my role as CISO.

In my first months at MasterCard, I was impressed by the size and reach of the company and network. I'd previously worked for companies with up to 300,000 employees, but MasterCard, with just over 11,000, operates the world's only global payments network, and is a well-known consumer brand and enables commerce safely and securely.

What advice would you give to a newly appointed CISO with a voice in the boardroom? What should he or she keep in mind when talking security in the business context?

Speak plainly. The board and business partners do not live in our world. One of the greatest challenges that I see for CISOs is their ability to communicate the problems, how they intend to fix them, and their opinion of how concerned the board or business should be about the various issues. Companies (usually) want to do the right thing.

To do that, they need to understand what the issue is. You can lose them quickly by being overly technical and you can scare them to a point where you get much more help than you can handle.

Security is a fundamental priority in the business world today. It doesn't matter whether you're dealing with business clients, consumers, or government or employees, companies cannot succeed without the trust of their stakeholders.

Protecting that trust is critical. It takes a long time to earn it, but can be lost in just a few moments, through a single mistake.

For many companies, the biggest threat to business isn't from a competitor but from a security incident that causes their stakeholders to lose trust and seek out alternative options.

What's your take on large companies, such as Apple, still not having a CISO role? Hasn't it become essential?

Every organization is different. What may work for one may not work for another. It's more important to have security as a top priority, considered in every major decision, than it is to have a dedicated CISO role.

As long as an organization is committed to security, companies can structure themselves in whatever way works best for their business and allows them to achieve this goal. There is no one-size-fits-all answer.

MasterCard has been progressive in allowing for the integration of physical and cyber security in a combined security organization. This allows us to analyze logical and physical assets and to build a complete picture of our security profile. This is not unlike the Secret Service's planning of a presidential visit, as threats to the logical infrastructure can result in physical harm.

The CISO can lead the program, but it requires commitment on the part of the entire organization to support it.

We've seen a myriad of data breaches in the past few years, and these have moved the CISO role into the spotlight. How do you expect the role to keep changing in the next decade?

It really speaks to why security must be a fundamental part of any business plan in the world today. The CISO can lead the program, but it requires commitment on the part of the entire organization to support it.

At MasterCard, we tell our employees that security is everyone's responsibility, and let them know how they can support what we're doing as a team. You have to look it as a partnership, a true evolution of the function. We're in the midst of this shift already.

Today, security is viewed as a business enabler, counselor and advisor that helps support the trust companies seek to have from their customers. Years ago, it was thought of more as a service, one that placed restrictions on company networks, computers and software.

With the seemingly exponential growth in data, the financial and reputational risk that accompanies it and the need to protect proprietary information, the role of information security will only become more prominent and influential within companies, as they continue to look for ways to build trust with their customers.

It's a lot easier to get a good night's sleep when you're confident that you've put the best people, processes and technology in place.

When I joined MasterCard in early 2014, I was fortunate to walk into an organization that knew the value of security. With fifty years in payments, billions of transactions and expertise in data management, security has never been optional.

But, for many companies, this is unchartered territory. Information security becomes more complicated as an organization grows. From the basic understanding of the information to data protection requirements across international borders, information security will become increasingly important to businesses.

What keeps you awake at night?

I sleep fine. I lead a great team of security professionals, and they're working around the clock and across the globe to keep our systems secure. Even then, we plan and test our incident management plans very frequently to ensure we are prepared as we can be for an event, should one occur.

It's a lot easier to get a good night's sleep when you're confident that you've put the best people, processes and technology in place.

That's not to say I'm worry-free. I worry about what's going to be the next threat – whether it's something completely new, a takeoff on an old tactic, whether it will focus on people or technology. I consider that a good thing though. You'll never meet a CISO who has no concerns, worries or anxiety – it just doesn't happen in this business. But, being able to look at future threats in a strategic manner is a luxury afforded by confidence in your team and processes.

If all of your time is spent on what's happening today, it's impossible to stay ahead of tomorrow. You've got to do both these days.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.helpnetsecurity.com).

7 tips to get the absolute best price from security vendors

Jeremiah Grossman

Security budgets are always extremely tight, so it's smart to get the absolute best price possible from your security vendors. Never ever pay full price, or even take the first quote vendors give you. That price just sets the stage and it's best to think of it as the "dummy price," so don't pay it!

I've spent nearly two decades sitting at the price negotiation table in the security industry and seen all manner of techniques customers use to win discounts, and more people should use them. Customers, even small ones, can exercise a ton of leverage over their security vendors if they only knew how. And, more often than not, the vendors themselves don't really mind. It signals that a deal is likely to be made and to a vendor, that's what's most important.

While it's common for large companies to have negotiations handled by a separate department, typically called "Procurement," many leave the responsibility to whomever is actually making the purchase. In either case, security practitioners can personally say, do, and offer things the procurement department can't to help obtain the best possible price. Remember, security product margins can range anywhere from 40-60% or even higher. I've seen discounts well over 50% of the originally quoted price. Some vendors will even take a loss to win your business, depending on the size of your brand and the reference you'll provide.

I'm not a big fan of this as you risk not being treated well as a customer long-term. The vendor may decide to drop you later because you're unprofitable. So, allow vendors to make a profit, just not an obscene one.

Below you'll find my ranked list of the most powerful negotiating techniques I've come across in the purchasing process, many of which are applicable beyond security purchases.

1. Negotiate price at quarter end / year end

More than anything, businesses want financial predictability. They want to be able to plan out, with a high degree of accuracy, precisely how much business is expected to close at least two quarters into the future. Sales forecasting is largely a Sales department function.

So when the end of the quarter is just a few weeks away, and overall sales volume isn't where it needs to be, the sales rep (and their bosses) scramble and make concessions to bridge the gap and hit their forecast. The larger the sales forecast gap, and the closer to quarter end, the more desperate they become and more open they'll be to deep discounts or throwing in additional products / services to sweeten the pot.

Smart customers simply ask sales reps when their quarter or fiscal year ends, just after the vendor asks the customer what their budget range is. So, if you like the product, and you're likely to buy it, let them know you'll commit to the purchase in the current quarter, before the end, if they give you a good deal.

Vendors will routinely knock 10-30% (or more) off the price, just with the ability to accurately forecast a deal closing. If the vendor is unwilling to work with you and the purchase isn't urgent, let them know you're more likely to purchase next quarter, which adds uncertainty to their forecast and they'll have a decision to make. Rinse. Repeat.

2. Multi-year deals

As previously mentioned, businesses love predictability. For this reason, subscription-based businesses, like Software-as-a-Service, love predictable renewals rates. Security vendors know that just because you're a customer this year, it doesn't automatically mean you'll be a customer next year, as the market is highly competitive. They know they'll likely have to negotiate price with existing customers before the contract expires, which comes at a cost of time and sales forecast uncertainly.

To reduce this uncertainly, subscription-based businesses will often give attractive discounts to customers willing to sign up for multi-year deals. Two to three year deals are typical, likely fetching a 5-10% discount, possibly more if you're willing to pay up front, but we'll explore this more in a moment.

It's also best to refrain from committing to more than three years for security purchases as it's difficult to know what the business needs will be that far out, or how the product landscape may change in that time.

3. Paying in advance

For many security services, such as subscription SaaS products, you pay monthly or quarterly after services are rendered. For the security vendor's finance department, that means they're out some amount of money to service you before you pay them for those services. If you like a particular security service and plan to continue having it for a least another year, consider paying for a year or more in advance.

For the vendor, having getting cash up front is often attractive and it takes payment uncertainty out of the equation, giving their business additional flexibility. Obviously, the bigger the deal, the better in terms of discounting. This method can win another 5-10% or so in discounts on its own.

4. Customer reference, case study, Gartner reference

In infosec it's extremely difficult to get customers to speak publicly, or even privately, about their experience with a given security product. When a customer does consent to speak, it's incredibly powerful, and few things generate more business for security vendors than vocally happy customers. Customers should use this power to their advantage, especially if they really really like a security product and want to see the company do well.

To do this, customers can serve as a reference in a few different ways:

- Private Reference – speaks to other customers
- Public Reference, Individual – willing to do case studies, press, events, quotes, but as an individual versus the company
- Public Reference, Company – the company is endorsing the product and brand, including a logo on the vendors website, slides, etc.

All of this is good and even a non-contractual promise to be a reference can lead to great discounts. As a small warning, many organizations have policies regarding speaking on behalf of the company, so make sure to follow those. If you can find out if the security vendor is in the process of working with Gartner on the magic quadrant of their space, customers who are willing to be a positive reference in

this time period are like gold. I've personally seen seriously deep discounts here, even free offers!

5. Ask for more stuff, not always price discounts

Let's say you're asking for a discount, but for whatever reason the security vendor isn't agreeable. This could be because they need to keep their average sales price (ASP) above a particular threshold so their business looks good to their board and investors. In these circumstances, you can instead ask for them to throw in things that are more easy for them to give away or commit to.

a. Extra subscription time, especially if full deployment will take a while.
b. Additional services or software licenses
c. A better customer support package.
d. Free training.
d. Payment flexibility. How and how often payment has to be made.
e. Product roadmap enhancements that'll better serve you.

In many circumstances, security vendors will find the items on this list easier to give you than discounting the overall deal. You get more, but pay the same.

6. Find out what others paid

When entering pricing discussions, it's always helpful to know what other customers paid as a point of reference. You may or may not be able to get the same deal as they did, but you want something in at least the general vicinity. There are a couple of ways to obtain this information.

- Ask a colleague you personally know, who has already purchased a product you're considering. What kind of deal did they get?
- Ask the vendors for customer references during the evaluation process, which is something all customers should do as a matter of course. Not only ask the reference what they liked and didn't like about the product, but what they paid.
- Ask the vendor for their competitor's pricing, and how they compare with it.

In some cases, pricing information is considered confidential, but it doesn't hurt to ask. Having this pricing research on hand greatly helps get you the best deal possible.

Additionally, you're probably considering between two or more comparable products to solve a particular security problem. If the products themselves are a toss up, meaning you'd be happy with either option, consider sharing the bids with the competing security vendors. No security vendors want to lose a competitive deal in the last stage simply because the competition slightly edged them on price. You'd be surprised how quickly vendors will knock off 5—10% as a take away from the competition.

7. Go direct

Many customers have a preferred reseller, typically called Value Added Reseller (VAR), through which they make their security purchases. Among other things, VARs make vendor management much easier for customers. They'll help identify security program gaps, document purchase requirements, product selection, answer questions, and more. For the value they add, VARs usually take a roughly 30% margin on each product sale. Then, of course, they can tack on additional dollars for consulting and implementation if there is a need. The remaining 70% of the sale price goes to the security vendor.

Here's the thing, the business of the VAR is in the first two letters — V.A… VALUE. ADDED. If a VAR is not adding enough value, which is often the case, they're justifiably not entitled to their 30%. And in these circumstances, the VAR can and should be bypassed to go direct to the security vendor where the customer can get a [30%] discount without costing the vendor anything. And, unless there is a good reason not to, get bids from 3 VARs so they'll have to fight to get you the best deal – fight to win your business. Often VARs will cut into their own profit margin to land the deal.

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

Ransomware targets Android smart TVs

If you own a Sharp and Philips smart TV running the Android TV OS, you should know that it could be hit by FLocker, a device-locking ransomware that targets both Android-powered mobile devices and smart TVs.

"The latest variant of FLocker is a police Trojan that pretends to be US Cyber Police or another law enforcement agency, and it accuses potential victims of crimes they didn't commit. It then demands 200 USD worth of iTunes gift cards," the researchers shared. "Based on our analysis, there is also no major difference between a FLocker variant that can infect a mobile device and one that affects smart TVs."

The malware is good at hiding itself, is able to fool static code analysis, and to bypass dynamic sandbox protection.

After infecting a device, it waits 30 minutes before running, then contacts its C&C. The C&C delivers a new APK file and the ransom note – a HTML file with a JavaScript (JS) interface enabled – which initiates the APK installation, takes photos of the affected user, and displays the photos taken in the ransom page.

FLocker avoids targeting users located in Kazakhstan, Azerbaijan, Bulgaria, Georgia, Hungary, Ukraine, Russia, Armenia and Belarus, but goes after all others. Those who are hit receive a localized ransom message that sports their IP address and photo, and this could be more than enough for the victims to start panicking and pay the fine.

"If an Android TV gets infected, we suggest user to contact the device vendor for solution at first," the researchers advised.

"Another way of removing the malware is possible if the user can enable ADB debugging. Users can connect their device with a PC and launch the ADB shell and execute the command 'PM clear %pkg%'. This kills the ransomware process and unlocks the screen. Users can then deactivate the device admin privilege granted to the application and uninstall the app."

Malware exploits BITS to retain foothold on Windows systems

If you're sure that you have cleaned your system of malware, but you keep seeing malware-related network alerts, it's possible that at some point you've been hit with malware that uses Windows' BITS to schedule malicious downloads. BITS – Background Intelligent Transfer Service – is a native Windows tool that facilitates file transfers and it's used by the OS and some third-party software to retrieve updates. But it's also sometimes exploited by attackers and malware authors.

SecureWorks researchers explained why: "Attractive features for threat actors include the abilities to retrieve or upload files using an application trusted by host firewalls, to reliably resume interrupted transfers, to create tasks that can endure for months, and to launch arbitrary programs when a task completes."

They have recently encountered one instance when the malware misused the service to download and launch malicious files.

The malware itself was not present on the computer anymore, having been removed months before, but they believe it to be the DNSChanger Trojan (aka Trojan.Zlob.Q), because the scheduled BITS tasks were meant to download malicious files from two domains that have been previously associated with it.

"The poisoned BITS tasks, which created installation and clean-up scripts after their payloads were downloaded, were self-contained in the BITS job database, with no files or registry modifications to detect on the host," the researchers pointed out.

Russian ransomware boss earns $90,000 per year

A recent report by Deep & Dark Web intelligence outfit Flashpoint details one organized Russian ransomware campaign, and the guy at the top is pulling in an average monthly "salary" of $7,500 (that's $90,000 per year).

This boss, whom the researchers believe to be Russian, and active since at least 2012, is not the only one getting paid for the effort.

His is a Ransomware-as-a-Service (RaaS) setup, and he's been recruiting less technically savvy criminals to spread his ransomware for him. These affiliates might operate botnets, or known how to compromise servers and websites in order to spread malware, or know how to spread it via file-sharing sites, but are not knowledgeable enough to create ransomware on their own.

So, they become affiliates of this boss, and get 40 percent of the ransoms paid by the victims, i.e. an average of $600 per month. This particular operation functions with the help of 10-15 affiliates.

The boss keeps 60 percent of the total for his efforts, which includes communicating with the victims via email, collecting and validating Bitcoin payments, issuing decryptors, sending (part of the) ransom payments to the affiliates, and laundering the money via Bitcoin exchangers.

"On at least one occasion, the crime boss demanded additional payments even when a ransom payment had already been received, before providing a decryptor to the compromised victim," the researchers found. I expect this additional haul was not shared with affiliates.

All things considered, ransomware revenue amounts are not as fruitful as often reported or imagined, the researchers noted. But if the amount that the boss pulls in does not seem large to you, try looking at it from the perspective of an average Russian person, who earns 13 times less.

Granted, the affiliate revenues are not that big, but consider the fact that their efforts are not time-intensive and that there is a very small chance they will ever be held accountable for what they do, and you can see why many choose to become affiliates.

ICS-focused IRONGATE malware has some interesting tricks up its sleeve

FireEye researchers discovered a malware family that's obviously meant to target ICS systems, but found no evidence that it was ever used in the wild. They were unable to associate it with any campaigns or threat actors, and posit that it simply could be "a test case, proof of concept, or research activity for ICS attack techniques."

The researchers unearthed the samples in late 2015. They were uploaded to VirusTotal, but were not detected as malicious by the AV engines used by the service – despite some of its strings including the word "dropper" and containing a module named scada.exe.

While IRONGATE malware does not compare to Stuxnet in terms of complexity, ability to propagate, or geopolitical implications, both pieces of malware look for a single, highly specific process, and both replace DLLs to achieve process manipulation, they found.

"IRONGATE's key feature is a man-in-the-middle (MitM) attack against process input-output (IO) and process operator software within industrial process simulation," the researchers explained.

"The malware replaces a Dynamic Link Library (DLL) with a malicious DLL, which then acts as a broker between a PLC and the legitimate monitoring software. This malicious DLL records five seconds of 'normal' traffic from a PLC to the user interface and replays it, while sending different data back to the PLC. This could allow an attacker to alter a controlled process unbeknownst to process operators."

The malware is also able to detect the use of VMware or Cuckoo Sandbox environments, and won't run if it does.

There are many things that indicate the malware could be just a PoC that was not used in the wild. Also, the Siemens ProductCERT has confirmed that the code would not work against a standard Siemens control system environment.

The gravest dangers for CMS-based websites

Based on the reports by Sucuri's Incident Response Team and Malware Research Team, in the first quarter of this year 78 percent of the successful compromises were of websites built on WordPress. Joomla!-based sites came in at 14 percent, Magento at 5 percent, and Drupal at 2.

Magento-powered e-commerce sites are usually hit with exploits for the critical remote code execution bug patched in February 2015, and the XSS hole that can lead to e-store hijacking, plugged in January 2016. Obviously, not all admins update their installations regularly.

In fact, admins of Magento sites are the worst at this: 97 percent of the Magento installations Sucuri's experts encountered during cleanup were out of date. WordPress admins are much better – "only" 56 percent of the installations were out of date.

For WordPress sites, outdated plugins are a greater danger.

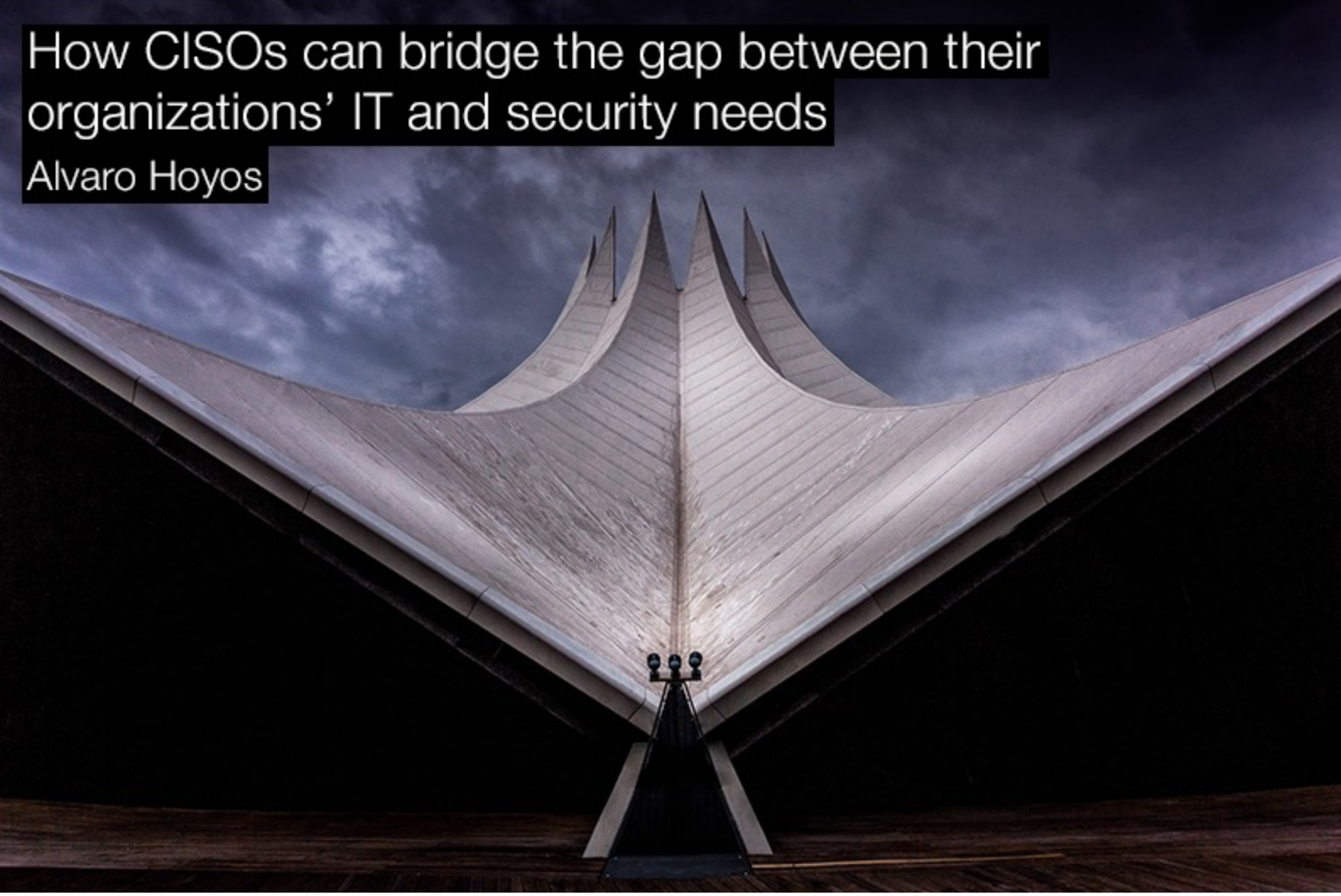
"The three leading software vulnerabilities affecting the most websites in the first quarter were the RevSlider and GravityForms plugins, followed by the TimThumb script," researchers noted.

"All three plugins had a fix available over a year, with TimThumb going back multiple years (four to be exact, circa 2011). This goes to show and reiterate the challenges the community faces in making website owners aware of the issues, enabling the website owners to patch the issues, and facilitating the everyday maintenance and administration of websites by their webmasters."

The problem with RevSlider, in particular, is that its embedded within WP themes and frameworks, and many users don't even know they use it. It's up to the authors of these offerings to keep the plugins updated, but too many can't be bothered.

How CISOs can bridge the gap between their organizations' IT and security needs

Alvaro Hoyos



Over the last few years, a perfect storm of trends has blown cloud computing into the enterprise mainstream. Between advancements in cloud solutions (which subsequently lowered cost barriers to adoption), mounting pressure to innovate faster, and the workplace demands of an increasingly tech savvy workforce, organizations have had little choice but to embrace this new paradigm.

The prevalence of cloud today cannot be understated: research indicates that the average organization uses more than 1,100 cloud services. However, unlike previous technologies, the cloud presents a unique challenge to IT and security teams; employees have preconceived notions about what the cloud experience in the workplace should be, based on their experience with the cloud in their own personal lives.

Workers of all generations already rely on apps from Evernote, Dropbox, Google Apps, and even Microsoft in their everyday lives. In an age when constant connectivity makes the term "work-life balance" somewhat archaic, personal habits invariably bleed into their professional lives.

Ubiquitous cloud solutions empower the workforce to be more efficient, but at the same time, personnel expectations have shifted and as a result, there's unprecedented pressure on IT teams to introduce new apps and cloud-enabled solutions as quickly as possible. Inevitably, lack of budget and bandwidth come into play, and IT and security departments struggle to keep pace with end user requests.

This has given rise to rampant shadow IT, the widely stigmatized notion of non-technical employees procuring apps and other technologies on their own, without the IT or security department's consent or knowledge.

According to a 2015 analysis from the Cloud Security Alliance, only eight percent of organizations understand the scope of shadow IT within their ranks. This startling figure may compel many IT security leaders to opt for more end user restrictions, tighter corporate policies, and closer internal surveillance. Not only would such an authoritarian approach turn employees off, it could easily undermine the efficiency and innovation everyone's striving for.

Going forward, CIOs, CISOs, and their teams need an alternative approach to cloud procurement that protects the benefit of empowered, tech savvy end users, while mitigating the inherent risks of the cloud.

Shadow IT's silver lining

The reality for most organizations today is that IT shoulders a tremendous burden. On average, IT professionals may field up to 11 lines of business requests for new cloud services each month. Compounding the administrative workload, security teams often need almost three weeks in order to evaluate a new solution.

Because of this strain on technical resources, organizations are starting to move away from fighting shadow IT and proactively explore ways to channel this rogue behavior for the overall benefit of the organization. With shadow IT already embedded so deeply into organizations' day-to-day operations, it makes sense for IT leaders to harness the legwork business employees are already performing to focus their efforts on key areas that they most care about, like expediting the "last mile" of app deployment.

All of this is not to say that IT leaders' desire to oversee all aspects of the cloud application lifecycle will dissipate anytime soon. However, this stipulation should not be an obstruction to gaining efficiencies by leveraging the ability to rapidly deploy cloud solutions.

No CISO or CIO can alter the fact that a marketing employee can sign up for a free app trial, and have their entire department using the solution in minutes. And no CISO or CIO should ignore the reality that, in many instances, doing so ultimately translates to notable time and cost-savings for the noncompliant department, albeit with the exception of a solution that lacks adequate security controls and ends up being ripped out by a furious IT team. For organizations to promote and sustain productivity, speed and quality service, shadow IT must be able to coexist within their IT environments.

How to stop worrying and learn to live with shadow IT

Shadow IT has become ingrained in many IT professionals' and business executives' minds as a systemic problem and a source of boundless risk. Helping these stakeholders to see the positive potential in shadow IT requires a not insignificant amount of effort.

Managing shadow IT's reputation starts at the top. Here are a few steps CISOs can take to help their colleagues see the upside of shadow IT:

Codify informal shadow IT habits into formal processes: By definition, shadow IT is an unstructured, chaotic office phenomenon. IT and line of business leaders must start by shedding light on the rogue processes their teams follow in order to yield the benefits of them.

This exercise gives IT and security staff insight into the minimum requirements line of business departments can accomplish on their own when procuring apps, in regards to due diligence, training and ongoing support. With these factors documented, IT departments can identify any gaps – i.e. around security or identity management – that require their intervention. IT must be also be comfortable with the business departments' due diligence processes to make sure there are no gaps in the risk management process itself.

This might take some upfront investment in helping business lines understand minimum security requirements to go along with their self-defined feature requirements. In effect, IT is recruiting business lines to weed out any solutions that will just not meet the organization's security needs, saving them time and effort.

Give end users some benefit of the doubt: A degree of end user "shaming" has become common practice among IT leaders and the media alike, obscuring the fact that consumers are more aware of cyber risk than ever before.

Vulnerabilities like Heartbleed, along with major breaches at Target, Sony, and the US Office of Personnel Management, have raised end users' awareness of (and concern about) data and device security. Take phishing attacks as an example: two years ago, most end users wouldn't think twice before blindly clicking on links or attachments from unknown email senders.

Today, constant media coverage of these types of attacks has led consumers to be more discerning, if not more paranoid, when using technology. That's not to say there is plenty of work left to do in the area of security awareness, but at least we are in a much better place than in pre-Heartbleed days. Adjusting how IT and security teams perceive end users' behavior and intentions goes hand in hand with shifting internal perception of shadow IT.

Security leaders have to foster a culture in which the lines of business aren't afraid to collaborate with IT, or made to feel that looping in IT means having to sacrifice agility.

Everyone's in this together: Within traditional definitions of shadow IT, it's easy to throw blame around; whether it's faulting IT teams for insufficiently monitoring end user behavior, or condemning line of business managers for implementing solutions that put sensitive information at risk.

It's in no one's interest to waste time playing the blame game; corporate security leaders have to send the message that every employee is accountable for protecting the organization's IT environment. No marketing team lead or business line VP wants to be the scapegoat for a rogue app gone wrong.

Security leaders have to foster a culture in which the lines of business aren't afraid to collaborate with IT, or made to feel that looping in IT means having to sacrifice agility. To achieve this, IT and security staff must work together to identify risks early and often and enact smarter process changes. Better alignment between these groups helps mitigate the impact of strained resources, and positions IT as a true enabler, rather than a bottleneck, for line of business innovation.

Cloud computing isn't going away any time soon, and – despite IT departments' best attempts – neither is shadow IT. Rather than tax their already limited resources trying to fight this trend, organizations can unlock a new world of value by embracing a new world that is highly cloud enabled and a workforce that is increasingly tech savvy.

Alvaro Hoyos, CISO at OneLogin (www.onelogin.com), architects and leads the company's risk management and compliance efforts. He also works with prospects, customers and vendors to help them understand OneLogin's Security, Confidentiality, Availability, and Privacy posture and how it works alongside, or in support of, customers' own risk management model. Alvaro has over 15 years in the IT sector and prior to joining OneLogin, helped startups, SMBs and Fortune 500 companies with their compliance and data privacy efforts.

Risk management: Risks are lurking everywhere

Zoran Lalic

In today's digital age, every organization, regardless of its size, must have a plan to adequately manage and minimize data risk. Whether you create your own approach or adopt a risk management framework, it must be designed in a way to recognize and reduce the risk to a level that the organization is willing to accept.

It's no secret that in most data breaches, hackers discover and exploit hidden risks that organizations do not know about or have chosen to ignore.

Organizations must assess the entire environment for potential risks, as they are hidden and lurking from the most unexpected corners. Consider the following examples:

1. You created a "secure island" where you host extremely sensitive data.
You have implemented dual firewalls between the "secure island" and the rest of your network. The only path to this isolated segment is through these firewalls. All necessary security controls have been implemented, including detective and preventive controls. You conducted a vulnerability scan and penetration test against this environment and it came back clean - no vulnerabilities and/or exploits have been discovered. Your SOC team monitors your environment 24/7/365 for any suspicious activities. Plus, your "secure island" is compliant with multiple regulatory standards. One morning you come to the office and you learn that a file with highly sensitive information from your "secure island" has been discovered to be up for sale on the dark web. After an analysis, you discovered what happened:

- Your internal data processing user received a phishing email with an attachment, on a PC that's not part of the "secure island".
- The user opened the attachment, and his or her computer has been fully compromised.
- The user has STFP software on the PC in order to upload files to the "secure island" SFTP server.
- The created "SFTP Site" on the infected PC had the username and password saved, so that the user does not have to re-type the password in order to connect.
- The hacker who compromised the PC connected to the SFTP site located in the "secure island" without having to know and enter the needed credentials.
- At that point, the hacker could download files from the SFTP server and upload malicious files to it.

2. You purchased an expensive multi-function printer. The most useful feature is the scan-to-email. Your desktop support team installed and configured the printer. Several weeks later you find yourself executing the incident response plan because your domain controller has been compromised.

You have a comprehensive security program in place protecting you both internally and externally from treats and attacks - how is it possible that your internal domain controller is now compromised?

The incident response determined the following:

- The internal customer service PC has been compromised via phishing attack. The compromised user had no privileged access on the network.
- The new multi-function printer was mapped on this PC.
- The hacker was able to access the web interface of the printer.
- The default admin username and password for this printer were never changed. The hacker found default credentials online and gained admin access to the printer.
- The LDAP server configured on the printer was the actual domain controller.
- The hacker changed the LDAP IP address to his own rogue listener.
- When this printer connected to the rogue LDAP server, it passed the real LDAP credentials in plain text and the hacker was able to capture them.
- The hacker used the captured credentials to gain access to the domain controller.

There is a general perception that "it's just an end-user with an unprivileged account," or "the subnet that PC belongs to is segmented and isolated from the highly protected environment," and "it is just a printer."

Typically organizations choose to exclude these scenarios from their risk assessment, thus the security controls do not get implemented. The above examples clearly demonstrate that there is a good possibility for that logic to be fatal.

Each organization has its own risks. Some organizations must comply with certain regulations. However, the main goal of risk management is to assess the level of risk the organization is facing and ensure to lower it to an acceptable level. In order to accomplish this goal, organizations typically follow these steps:

Asset inventory

The first step of risk management is to identify and document assets. Consider the following types of assets:

- Hardware
- Software
- Documentation
- People
- Company secrets.

Without a proper inventory, it would be nearly impossible to know what to protect within the organization. If you are not aware of the asset's existence, you cannot assess it for risk and properly protect it. It is extremely important to keep the inventory list up to date. If you are a small organization and do not have inventory software, you can always create a simple spreadsheet template to record your assets.

For example:

		Asset Inventory			
Asset Name	**Asset Category**	**Asset Details**	**Asset Criticality**	**Asset Owner**	**Additional Information**
XYZ Printer	Hardware	Multi-function printer in HR	Medium	XYZ Desktop Support	Printer IP: 10.1.1.1

Tip: For your hardware and software inventory, consider leveraging an asset discovery tool/software.

Consider an example where a zero-day vulnerability has been made public. Your customers require an immediate confirmation whether their environment is affected. If you don't maintain the inventory, how can you provide them with a quick update?

Depending on the environment, sometimes you would have to spend days to trace it down. When you document your assets, ensure to document the respective version (where applicable).

Risk assessment

The organization needs to understand what risks exist in the environment before formulating proper security controls to address them.

The organization needs to conduct a risk assessment to identify both external and internal threats and vulnerabilities their environment poses that may be a danger to the organization. The bottom line is that an organization needs to assess the risks they face in order to determine the impact and probability of that particular risk occurring.

Armed with the risk details and probability of occurrence, the organization then has all required components to decide what to do with the risk. There are two primary methodologies that you will encounter when conducting risk assessment and risk analysis: quantitative and qualitative.

Quantitative - In this approach you associate the loss with a financial impact. This methodology will help you identify your greatest risk based on financial value. If your plan is to conduct a cost-benefit analysis, it would be near impossible not to choose the quantitative approach to conduct your risk assessment. The security controls are implemented based on the financial value and impact. Quantitative approach is very time-consuming and costly, but at the same time a better way to communicate the risk to executive management.

Qualitative - The qualitative approach is more common, as the assessment is quicker and less costly to conduct. This methodology does not require the dollar value of an asset. Instead, it prioritizes the risk using the likelihood of particular risk occurring and the corresponding impact. The mitigation is based on the organization's risk appetite.

Tip: Conduct network/web app penetration testing and vulnerability scanning and map the risks/vulnerabilities of your assets.

Let's walk through the qualitative risk assessment example of XYZ organization using a simple spreadsheet template:

Risk Assessment

1	2	3	4	5	6	7	8	9	10	11	12	13
Identified Asset	Confidentiality	Integrity	Availability	Asset Criticality	Vulnerability Type	Vulnerability Severity	Associated Threat	Threat Severity	Threat Action	Likelihood	Impact Severity	Risk Severity
Demo/Reporting Server	Extremely High	Extremely High	Medium	High	Remote Desktop directly exposed on Internet	Extremely High	External malicious hacker	Extremely High	Brute-Force Attack	Extremely High	Extremely High	Extremely High

Tip: Consider adding the asset description and vulnerability description to the above template.

1. Asset Name: Demo/Reporting server is identified as an asset.

Tip: An asset is anything of value to your organization. This includes people, processes and technology. Even if an asset has very low value, consider that it could be a bridge to your highly valuable assets.

2. Confidentiality: This server contains customer data; therefore, confidentiality is categorized as extremely high.
3. Integrity: This server contains customer data; therefore, integrity is categorized as extremely high.
2. Availability: This server does not have to be accessible at all time; therefore, the availability is categorized as medium.

Tip: Map a(n) confidentiality, integrity, availability level to each asset. You can assign different categories (I typically use Extremely High, High, Medium and Low).

5. Asset criticality: Asset criticality is categorized as high. The customer data does not contain PII.

   Tip: Determine the criticality of identified assets based on confidentiality, integrity and availability. How important is this asset to your business? What would be the result if this asset were to be compromised?

6. Vulnerability type: "Remote desktop is directly exposed on the Internet" is identified as vulnerability type.

   Tip: Ensure to assess the entire spectrum. Design and implementation vulnerabilities can be as fatal as an unpatched server.

7. Vulnerability severity: The vulnerability type is now assigned a vulnerability severity. In our example it is categorized as extremely high.

   Tip: Base the severity on confidentiality, integrity and availability values previously identified. You might consider the following as vulnerability severity rating:

Extremely high – Remote exploitation without user interaction that could result in compromise of confidentiality, integrity, and availability of customer data.

High – Internal exploitation without user interaction that could result in compromise of confidentiality, integrity, and availability of customer data.

Medium – Internal exploitation with user interaction and no customer data at risk.

Low – Exploitation is very difficult and no data is at risk.

8. Associated threat: We associate a threat to the identified vulnerability. In our example it could be any hacker on the Internet.

   Tip: Make sure to include all different types of threats such as environmental/natural, hackers, malicious insiders and malicious activities.

9. Threat severity: Next we assign a severity level to the identified threat. In our example it is categorized as extremely high.
10. Threat action: We identify a possible way for an associated threat to exploit the identified vulnerability.
11. Likelihood: We determine the likelihood of the identified threat taking advantage of the identified vulnerability.
12. Impact severity: The details above help us to determine impact severity, which should be based on the asset criticality, vulnerability severity, and threat severity

Tip: Impact severity can be based on disruption of service. You might categorize it as follows:

Extremely high – Compromise of the confidentiality, integrity and availability of production data.

High – Server compromise with no customer data.

Medium – Minor web performance disruption / minor denial of service attack.

Low – No impact to the environment.

13. Risk severity: Now we are ready to determine risk severity. Risk severity is the result of the harm likelihood and harm impact categories. Once we determine risk severity, we need to make an educated decision on what to do about the risk.

Tip 1: Risk severity is always based on your organization's risk appetite and acceptance.
Tip 2: Your risk action plan might be based on the following risk severity matrix and definitions:

Extremely high – Immediate attention.

High – Plan needs to be in place ASAP.

Medium – Team to determine if corrective action is necessary.

Low – Accept the risk.

Risk Severity Matrix	Likelihood			
Impact Severity	Extremely High (Very Likely)	High (Likely)	Medium (Moderate)	Low (Unlikely)
Extremely High (Severe)				
High (Major)				
Medium (Minor)				
Low (Minimal)				

Extremely High Risk
High Risk
Medium Risk
Low Risk

Risk Treatment Plan

1	2	3	4	5	6	7	8	9	10
Asset Name	Identified Risk	Risk Score Severity	Current Control	Risk Action	Recommended Control	Risk Exception	Risk Owner	Expected Completion Date	Likelihood of occurence after treatment
Demo/Reporting Server	Server with customer data in danger of being compromised via brute-force attack	Extremely High	Complex username and password & located in DMZ	Reduce	Server not to be directly exposed to Internet. To be accessable only once the user authenticated via the VPN.	No	Director of Information Security	4/10/2016	Low

Risk treatment

After you have successfully completed the risk assessment, you need to identify the security controls to eliminate the risk or to bring it down to an acceptable level. The best approach to accomplish this is by conducting a security control analysis.

The goal of this analysis is to determine the efficiency of the security controls that are currently protecting identified assets.

If the current control is not sufficient to protect an asset, you must identify and implement a new control that will eliminate or minimize the probability of a threat exploiting the vulnerability.

1. Asset name – Asset identified during the risk assessment.

2. Identified risk – Risk identified during the risk assessment.

3. Risk score severity – The risk severity assigned during the risk assessment.

4. Current control – This is the current security control protecting an asset from being exploited.

5. Risk action – At this point you must make a decision about the identified risk – the risk can be managed using the following criteria:

I. Avoid
II. Mitigate
III. Reduce
IV. Transfer
V. Accept.

6. Recommended control – This is the control that is recommended for implementation in order to reduce the risk to a level acceptable to the organization.

7. Risk exception – This is a very important and critical piece of risk management. There will be situations where you are not in position to reduce, avoid or mitigate the risk immediately. For this reason, you must have an exception process in place that is approved by the executive management.

8. Risk owner – It is essential to assign the risk owner. This is the individual/team responsible for ensuring that the risk is remediated in the planned time frame.

9. Excepted completion date – Targeted date to “close” the risk.

10. Likelihood of occurrence after treatment – You must make sure that the risk severity upon implementing the recommended security controls is acceptable to your organization.

Risk management lifecycle

The risk management lifecycle is not an option, but a requirement to eliminate and minimize the risk to a level that would be acceptable to your organization.

Consider the organization's risk appetite - what is acceptable for one organization, might not be acceptable to you, or another organization.

Risk management is a living thing and the lifecycle should be a continuous improvement of an organization's security posture.

The risk evolves daily and what was in a secure state yesterday might be very well in a vulnerable state today. The hackers search for vulnerabilities to compromise our networks, and we must be a step ahead of them in order to protect our assets.

The best way to accomplish this is to constantly monitor our network for indicators of attack and to keep reassessing the assets to identify new risks. When you make major changes to your infrastructure, make sure to conduct the risk assessment to identify the new risks introduced with the changes.

Risk management is a requirement for complying with a number of standards and regulations such as HIPAA and ISO 27001/02.

Even if you have not made major changes, make sure to reassess your environment at least once annually. Your information security program should dictate when and how frequently you should conduct the risk assessment.

Risk management is a requirement for complying with a number of standards and regulations such as HIPAA and ISO 27001/02. Additionally, if you are implementing a comprehensive security program at your organization, the risk management is the heart of your information security program.

There is no silver bullet to make an organization risk-free - there will always be some risk. A risk-based approach to security will establish a unified set of security priorities based on critical assets and impact to the business if these assets are compromised. It also ensures that all business units within the organization (including the executive management) are in agreement about the risk your organization is willing to accept.

My years of experience with risk assessments and analysis allow me to offer you the following 12 tips:

1. When you conduct risk assessments be sure to identify and interview the key staff.

2. Define the scope of the assessment. If you use a cloud provider, make sure they are included in the scope.

3. When you identify threats and vulnerabilities make sure they are realistic.

4. Assess for risk even in areas that do not seem to be a threat, as they can become a way in for attackers. Consider printers (as previously mentioned), modems, cameras, fax machines, old PBX systems, and any other legacy devices that you would never expect to be exploited.

5. Privacy impact assessment (PIA) can be very beneficial during your risk assessment as it is designed to discover if sensitive/PII information is collected, stored and/or transmitted and if it is properly secured. During your risk assessment PII data will typically take priority.

Some of the questions to ask during the PIA:

   I. What PII information is being collected?
   II. Is it necessary to collect it?
   III. How is it collected?
   IV. Who has access to it?
   V. What security controls have been implemented to protect it?
   VI. For how long is it retained?
   VII. How is it decommissioned?

6. Business risk assessment is sometimes a good approach to risk from a high-level perspective. Executive management typically prefers this type of risk assessment. In order to conduct this analysis, you must understand the business-critical functions. Once these functions have been identified, you can formulate proper safeguards. Business risk assessment concentrates on the business side of an organization and excludes the technology side of equation.

7. Your risk treatment plan becomes your risk register. Put plans in place to monitor it and keep it updated. Having an updated risk register gives you the ability to provide accurate risk updates to your auditors, customers, and executive management.

8. When you mitigate the risk, review the residual risk and update the risk register.

9. Make sure risk is controlled. For example, if you have an exception in place that is approved for high severity risk and then you learn about a new zero-day vulnerability that raises the risk from a high to an extremely high level, ensure this new risk is known to and re-approved by your executive management.

10. Assess your supply chain vendors. In many data breaches they were the link hackers needed to compromise the target.

11. With some risks/vulnerabilities you will feel that you are chasing a ghost.

12. Develop a risk management report and present it to your executive management.

And remember: some lurking risks are hiding in broad daylight. Do not assume that you can be protected today and tomorrow by leveraging yesterday's protections.

Zoran Lalic is a Senior Security Engineer with extensive industry experience in information security program development, penetration testing, forensics analysis, vulnerability management, security architecture design and incident response. His experience spans environments of all sizes – small offices to global networks. Zoran has been an active researcher of new techniques used to compromise networks.

Report: Infosecurity Europe 2016

Infosecurity Europe is Europe's largest information security event. The 2016 edition featured some of the industry's most senior experts, thought-leaders, policy-makers and commentators sharing their expertise across a broad spectrum of information security issues.

Infosecurity Europe's Conference Program hosted 160 hours of sessions with over 260 renowned thought-leading speakers presenting in eight conference theatres.

The event attracted over 15,000 information security industry professionals attending from every segment of the industry from over 70 countries. Infosecurity Europe saw more companies exhibit than ever before, including three times more new exhibitors than in 2015.

The event featured:

- UK's most innovative small cyber security company of the year
- Technology showcase - exhibitors demonstrated new solutions and technologies
- Intelligent defense - two-day technical conference focused on latest research into vulnerabilities and exploits, and how to defend against them
- Tech talks and strategy talks - bite-sized presentations addressed the latest business challenges
- Information security exchange theatre - end-user and vendor communities came together to debate current challenges in information security
- Security workshops - security experts hosted sessions on a business topics.

Recognising his long term contribution to the information security sector, Brian Honan, Founder and CEO of BH Consulting, was inducted into the Infosecurity Europe Hall of Fame for 2016. Established in 2008, the Infosecurity Europe Hall of Fame celebrates the achievements of internationally recognized information security visionaries, luminaries, practitioners and advocates.


CipherCloud
Trust in the Cloud™
Multi-Cloud Security
Encryption & Tokenization
Data Loss Prevention
GDPR Policy Controls
WWW.CIPHERCLOUD.COM
A Perfect Storm of Converging Data Privacy Forces


ENJOY SAFER TECHNOLOGY
rapid7.com


CRONUS
ONE STEP AHEAD
Soliton


Infosecurity Europe Hall of Fame 2016
Inductee: Brian Honan
KEYNOTE STAGE
infosecurity
EUROPE


Centrify
eset
Bitdefender
No one wants to be half protected.


FORTINET
Security Without Compromise
NETWORKING BAR
#infosec16
SOPHOS

CipherCloud unveils first GDPR-ready cloud security solution

CipherCloud announced the availability of a cloud security solution designed to help companies comply with the European General Data Protection Requirement (GDPR).

Their Cloud Access Security Control (CASB) platform now has built-in GDPR-readiness capabilities, including the ability to detect sensitive personal data across multiple cloud applications, proactively remediate problems, encrypt or tokenize sensitive data to prevent unintended leaks, monitor user activity and detect geographic anomalies.

GDPR is a set of regulations put in place by the European Commission designed to strengthen data protection for EU citizens.

The legislation was approved last month and companies must comply by May 2018 or face substantial risk and steep fines. Given the complexity of GDPR requirements, this is a very short timeframe for companies to become fully compliant with the new data privacy regulations.

CipherCloud's CASB platform enables global enterprises to leverage the cloud while avoiding risk and legal entanglements by assuring data privacy, residency, and sovereignty. For organizations that need to comply with GDPR regulations, the platform offers:

- GDPR-specific policies to detect and protect personally-identifiable information
- Policy controls based on source, location, content, and destination of files and database content in the cloud
- Proactive remediation of policy violations with blocking, quarantining, notification, and end-to-end file encryption
- Activity monitoring and geographic anomaly detection to spot suspicious activity from non-EU locations
- Strong encryption and tokenization with local key management to effectively maintain EU data residency and sovereignty, regardless of cloud provider location.

"The benefits of cloud computing for businesses can be substantial, but companies will always be held responsible for protecting private and sensitive customer information, regardless of where it resides," said Willy Leichter, vice president of cloud security for CipherCloud.

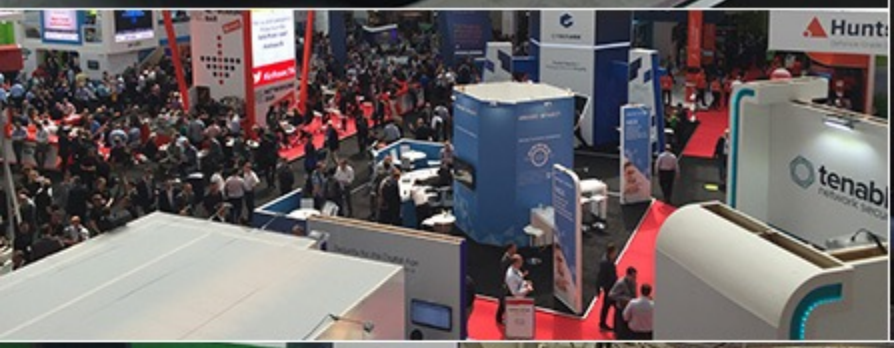
"Our solutions enable organizations to adopt the cloud, while maintaining visibility and control over sensitive data—key requirements for complying with the new GDPR regulations."


TRANSFORM SECURITY
ORGANISERS OFFICE
QUALYS
tripwire
TREND MICRO
splunk>
splunk>
UNSIDER


logically
Co-ord. Communicate
#becrypt
Centrify
Centrify
Centrify
Centrify


Live Car Hacking
PEN TEST PARTNERS
Live Car Hacking


Privilege vulnerability
INFINIGATE


Hunt
tenab


FORCEPOINT
PLANNING FOR SUCCESS
Site Resilience
Connectivity Resilience
Management Resilience
Resilience before beats Risk Mitigation after
FORCEPOINT
THREAT DETECTION
We Deliver:
FORCEPOINT

Do companies take customers' security seriously?

75 percent of adults in the UK would stop doing business with, or would cancel membership to, an organisation if it was hacked. This suggests, however, that a quarter would carry on using that company despite the security risk to both personal and financial information.

The Centrify study of 2,400 people across the UK, Germany and the US, looks at consumer attitudes towards hacking and how likely consumers are to continue transacting with businesses, including retailers, banks, government, travel, health and hospitality organisations, after a cyber attack.

To some degree, most consumers expect to be hacked today, with 73 percent in the UK admitting that it has become normal or expected for businesses to be hacked. Despite this, only half feel that they are taking enough responsibility for the security of their customers' or members' personal information.

Most people believe that the burden of responsibility for security falls to the business. About two-thirds in each country rated organisations as a 9 or 10 on a 10-point scale in terms of how responsible they should be for preventing hacks and securing the personal information of their customers.

Individuals most likely to take their business elsewhere following a data breach include those who have had their personal information compromised in a hack previously, people who are tech savvy and who shop regularly online.

"If three-quarters of customers are prepared to walk away from a business if it has been compromised, then what kind of message is this sending to those organisations?" says Bill Mann, Chief Product Officer at Centrify. "We would say that it is a very clear call to action to those businesses to sort out their processes and do everything they can to protect confidential customer information.

According to the survey, financial institutions have the best reputation when it comes to dealing with security breaches compared to other sectors. They top the list of seven different industries in terms of how well they handle security issues for their customers, although government/local government and HMRC come in a respectable second.

Worryingly, retailers rank fourth and travel sites fifth in each country, while membership and hospitality businesses are the lowest ranked.

The study also shows that organisations are increasingly going public with news of security attacks and data breaches, often notifying their customers directly. Around one third in the UK have been notified of a hack. Of those notified of a hack, less than half (45 percent) of those in the UK found out that their personal information, such as an address or credit card information, had been compromised.

Monitoring bank transactions and changing passwords – both with the hacked organisation and on other sites – are the most common steps suggested by organisations after advising customers of a hack. It is less common for a business to recommend that customers request any kind of alerts, such as a fraud alert, or to consider a security freeze, or implement multi-factor authentication.

Top tips for businesses

- Educate customers about good "password hygiene" – make it core to your security policy.
- Make sure you offer alternatives to just passwords, such as multi-factor authentication or biometrics, and let your customers know about them.
- Educate your own staff and have clear security policies internally. Also, control who has access to what data, giving privilege access only to those who need it as part of their job.
- Encrypt sensitive data, including customers' credit/debit card details.
- If your site has been hacked, inform customers as soon as possible. Under the new EU GDPR, a business will be required to notify the ICO (Information Commissioner's Office) of a data breach no later than 72 hours afterwards, unless it is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals.

YOUR VOTE DECIDES THE TALKS AND SPEAKERS

KEYNOTE SPEAKERS

ERIN JACOBS

Founding Partner
Urbane Security

KATIE MOUSSOURIS

Founder & CEO
Luta Security

FABIENNE SERRIERE

Founder
KnitYak

3-Day Technical Trainings

August 22nd, 23rd & 24th

TECH TRAINING 1 – Subverting Access Control Systems
TECH TRAINING 2 – Linux Kernel Exploitation Techniques
TECH TRAINING 3 – Mastering Burp Suite Pro: 100% Hands-On

2-Day Technical Trainings

August 23rd & 24th

2-DAY TECH TRAINING 1 – Offensive Social Engineering
2-DAY TECH TRAINING 2 – Cryptography & Cryptology
2-DAY TECH TRAINING 3 – Advanced Web Hacking

Register online at **http://gsec.hitb.org/sg2016/** to vote at **http://gsec.hitb.org/vote/**

Should you sync your family's calendar to your refrigerator or have it display photos? Samsung believes you should. They also think you need cameras that display the food inside, to help during shopping. Sure, these features can make life easier, but how would you feel about someone accessing this information? What could a stranger do if he knew you're out of the house tomorrow night? I'm not saying the Samsung refrigerator is insecure, but do you have any assurances it's secure? How do you know the data it uses is safe from prying eyes?

During the past few years we've seen examples of all sorts of IoT devices exhibiting glitches, getting hacked, manipulated, and the information they hold exfiltrated:

- At Black Hat USA 2015, security researchers Runa Sandvik and Michael Auger demonstrated how they hacked a Linux-powered rifle made by Texas-based company TrackingPoint. They found vulnerabilities that can be exploited to make users hit targets they didn't intend to.
- Earlier this year, SF Globe reported on a deeply disturbing hack: someone accessed a Washington's family Foscam baby monitor and talked to their child at night.
- In January, Alphabet-owned smart homeware company Nest has asked users to reset their connected thermostats after a software bug drained its battery and sent homes into a chill in the middle of the night.
- A vulnerability in the mobile app used to interact with the Nissan LEAF electric can be exploited by remote, unauthenticated attackers to switch the car's AC and heating system on and off, but also to extract details about the owner's journeys, security researcher Troy Hunt has demonstrated. This is not a one-off, there have been many issues with vehicles, and even the FBI says that car hacking is a real risk.
- In early May, researchers have managed to exploit design flaws in the Samsung SmartThings smart home programming platform and successfully mount a series of attacks that could result in smart homes being entered, burglarized, and generally made insecure by attackers via malicious apps.

And, are you ready for the really bad news? The examples outlined above are just the tip of the iceberg. Thousands of devices are being connected to the Internet, and there is no set of rules or regulations that would force manufacturers to make them secure. I believe we still haven't seen all the real dangers that the Internet of Things will bring.

The privacy paradox

The Snowden revelations have propelled privacy concerns into the mainstream. People are blocking their computer webcams by putting things over the lens, but at the same time they're wearing smart watches that track their movements, they're using Smart TVs that monitor their viewing habits, and they're buying all sorts of appliances that connect to the Internet insecurely.

"There are two reasons people are selective about privacy. They are unaware of the big picture or they have no alternative. Many don't realize that they bought a TV that tracks them, all they want is the latest TV. In many cases buyers would probably prefer a more privacy-friendly option, but that option is often hard to find, if available at all," according to Jaap-Henk Hoepman, Scientific Director, Privacy & Identity Lab, Radboud University Nijmegen.

"As with most consumer electronics devices, cyber security is an afterthought that will be integrated into the product in version 5 if we are lucky. When faced with a looming deadline like the holiday shopping season, given a choice between shipping a product or securing it, manufacturers will choose to ship every time," Bob Baxley, Chief Engineer at Bastille, told (IN)SECURE Magazine.

"The big risk is not that a criminal will be able to break into your house through your smart lock, but that the smart lock will provide the attacker access to your network and online credentials. Why would a sophisticated criminal steal a $500 TV, when he could instead raid your bank account through your Internet connection?" he added.

There are two reasons people are selective about privacy. They are unaware of the big picture or they have no alternative.

You could argue that a random user is not important enough to be the focus of someone interested in exploiting careless IT security hygiene. "It is a huge inconvenience to forego the latest and greatest technology innovation only to prevent a low-probability (but high consequence) cyber attack," Baxley explains the manufacturers' point of view.

That being said, if you knew that there was a probability, no matter how small, that because your baby monitor was not secure enough, someone could see and talk to your child at night, would you buy it anyway? And if you would, what is the thing that would make you go back on that decision – where do you draw the line when it comes to convenience vs security?

IoT expansion

Without a doubt, IoT is now mainstream. In fact, IoT use is growing rapidly across almost every industry. One of the things that makes IoT so disruptive is that its impact isn't restricted to a single sector or function. From consumer devices to jet engines, logistics to product development, healthcare to municipal planning, enterprise IoT is having a huge impact, according to the "State of the Market: Internet of Things 2016" report by Verizon Enterprise.

Enterprises are susceptible to attack through the IoT infrastructure they have in their environments. According to Baxley, this is scary for two reasons:

1. Enterprises don't even know what IoT devices are in their environment because these devices tend to communicate using off-network wireless protocols.
2. Enterprises usually keep more sensitive information than an individual does.

"Enterprise threats look very similar to the home IoT threats but are much more frightening given their scale," he notes. "For example, a facilities group installs an industrial control system that, unbeknownst to the IT security department, has an open Zigbee network enabled and accepting connections. Or, they install wireless keyboards using an insecure non-standardized 2.4GHz protocol to send key presses to all the computers in a corporate environment."

Enterprise threats look very similar to the home IoT threats but are much more frightening given their scale.

All of these attacks are predicated on the idea that you can't see the wireless IoT networks. "Unlike the one or two pipes to the Internet through which all corporate wired traffic flows, there is no perimeter around the RF space. While an enterprise's wired network looks like a thick-walled house with a single well-guarded door, your RF space is more like a screen porch with millions of holes," he explains.

There is some potential good news. According to Gartner, worldwide IoT security spending will reach $348 million in 2016, a 23.7 percent increase from 2015. Furthermore, spending on IoT security is expected to reach $547 million in 2018.

We can only hope that this leads to more security-conscious product development, and voice our preference for products that have been proven to be secure.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.helpnetsecurity.com).

Executive hot seat: Sumedh Thakar Chief Product Officer at Qualys

Interview by Mirko Zorz

As Chief Product Officer at Qualys, Sumedh oversees worldwide engineering, development and product management for the Qualys SaaS platform and integrated suite of security and compliance applications. Sumedh is active in the PCI and security community working closely with the PCI Council on the development and enhancement of PCI DSS.

What are the most significant challenges when it comes to building complex products and managing user wishes at the same time?

The main challenge continues to be understanding our customers' needs and translating it to deliverables in a way that appeals to all users. The SaaS model with agile development has a significant advantage because in releasing quick updates to the platform, users can get new functionality every 6 to 8 weeks.

More often than not a unique feature request coming from a user turns out to be a great opportunity to bring new functionality to other users who didn't even know they needed it.

How will cloud domination in the enterprise ultimately shape the future of information security? Will CISOs ever be able to successfully tackle security basics?

Today's enterprises are faced with the challenge of having to rebuild their entire infrastructure as they confront the issues of securing information in the public and private cloud, on mobile devices, and in the data gathered by all of the sensors associated with the Internet of Things. Businesses still need to secure everything, but they are architected for the old client/server world.

We can use the analogy of home security systems to see how cloud security services for the enterprise need to work: sensors in the enterprise environment gather security and compliance information, asset information and other data about the state of the systems, and all of that data is then sent to a cloud service for analysis. This provides security teams the information they need to protect their environments.

For example, Qualys recently released a new agent-based cloud technology that allows customers to continuously track and secure all their IT assets, whether on premise, in the cloud, or mobile. This technology will help CISOs get a comprehensive inventory of their

assets, find and search assets across millions of devices in a matter of seconds, and perform continuous security and compliance assessments on them. Such technological innovations will certainly help CISOs ease the move in the cloud while keeping security matters under control.

How do Qualys Web Application Scanning (WAS) and Qualys Web Application Firewall (WAF) integrate? What are the essential features that make these products stand out in the marketplace?

Both of these products are built to scale. Qualys WAS provides customers the ability to continuously discover, catalog and scan web applications on a global scale with a high degree of accuracy. Qualys WAS crawls and tests web applications for OWASP top 10 risks and web site misconfigurations. When Qualys WAS identifies a threat or a risk, it can automatically deploy the relevant virtual patch to the Qualys WAF to mitigate it. Additionally, Qualys WAF monitors all web pages visited by users and automatically shares this information with the web application scanner, ensuring these pages are not missed during the next scan. This approach helps block attacks on web applications, prevent disclosure of sensitive information, and control where and when applications are accessed.

By integrating security rules and policies from our WAF solution with Qualys WAS data, our differentiator is that we give organizations flexibility and automation and help them move toward a complete automation of web application security.

Qualys was born in the cloud and we continue to grow in the cloud.

What are your long-term goals for the Qualys SaaS platform and Qualys PCI?

Qualys was born in the cloud and we continue to grow in the cloud. Our goal is to keep adapting our solutions so that we're giving our customers a continuous view of their security and compliance landscape — we're letting them see the network the way hackers do.

The introduction of our new cloud agents opens the doors for Qualys to have a footprint at the endpoint, which in turn allows us to do more for our customers. Our cloud platform essentially capitalizes on the speed and flexibility of the Internet to provide faster and more thorough security checks and responses than services that are not in the cloud.

Unlike traditional in-house enterprise software security, we can help our customers get security intelligence on demand. And as their IP-connected devices and web applications continue to explode, we are able to scale and grow with them.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.helpnetsecurity.com).

HITB GSEC 2016 Singapore

bit.ly/hitbgsec2016 - Singapore / 22 - 26 August 2016.

The 2nd annual HITB GSEC security conference takes place at the end of August in Singapore and features an all-women keynote line up in a 2-day single track conference format. It puts the power of paper selection in your hands – you vote on the talks that are of interest and get to meet speakers.

Borderless Cyber Europe 2016

bit.ly/bc_2016 - Brussels, Belgium / 8 - 9 September 2016.

Join CIOs, CISOs and cyber threat intelligence experts from industry, government and CSIRTs worldwide to share experiences, strategies, tactics and practices that will improve your state of preparedness and more effectively protect your business against cyber threats.

IP EXPO Europe 2016

ipexpoeurope.com - London, UK / 5 - 6 October 2016.

With six top IT events under one roof, 300+ exhibitors and 300+ free to attend seminar sessions, IP EXPO Europe is a must-attend IT event for CIOs, heads of IT, security specialists, heads of insight and tech experts.

Security: Missing from DevOps thinking?

Joan Wrabetz

DevOps is a practice of continuously deploying applications into production clouds. In order to automate the deployment of applications into production, it would seem essential for security testing to be a part of that automated process. But when talking with one financial services firm, I discovered that they don't deploy continuously into production because they are concerned that by doing so they would break the law.

They are required by law to make sure that applications comply with regulatory and privacy requirements before they are deployed into production. The only way to do that is to perform security testing. Thus, in order to achieve continuous deployment, they would have to integrate security testing into their DevOps flow.

So, why isn't security testing a core part of DevOps already? The reasons are both technical and organizational. Organizationally, security testing is usually handled separately from development or product release oriented testing, often by a completely separate group. As a result, it is not necessarily associated with the application release process.

The technical reasons are related. Historically, security testing has involved reproducing the production infrastructure and network configuration as accurately as possible so that security vulnerabilities can be identified. Often development and test teams working on DevOps do not invest in creating accurate reproductions of production infrastructure for their normal development and testing. So, they are not prepared to perform security testing as part of their normal DevOps flow.

Security testing at many financial services firms exemplifies both of these issues. These firms typically outsource their security testing to one of a number of service firms who perform that testing on their own networks or in the cloud. The outsourcing of the security testing process is a big inhibitor to incorporating security testing into a continuous and automated DevOps process. In addition to that, when we asked these financial services firms how well their outsourced security testing represents their real production IT infrastructure,

they really had no idea. Clearly, any testing that does not match the production environment is not helping to reduce the security risk that the organization faces.

The type of security testing that is most relevant to the DevOps flow is application compliance testing. For this type of testing, new applications are inserted into a network that emulates the IT production network as accurately as possible. Testing with load, traffic and disruptive events is performed to determine whether the new application or upgrade might open up a vulnerability in the production environment.

This testing is performed prior to pushing any new upgrade or application into production to ensure that compliance requirements will be maintained. That includes compliance with privacy and data protection regulations, security requirements, and any other business compliance standards that the organization is subject to.

The type of security testing that is most relevant to the DevOps flow is application compliance testing.

Common problems with security testing as part of DevOps

There are some common problems that make this type of testing uniquely difficult as part of a DevOps process, and in many cases, much harder to perform than other hardware and software testing. For example:

The tests must run in a configuration that matches the current production configurations exactly. One of the common characteristics of security testing is the need to create an environment that mimics the production environment as accurately as possible (i.e. with high fidelity). This includes creating a clone of the network configuration as well as simulating the traffic and load on that network.

Security tests are system-wide tests, not tests of a single piece of hardware or software. For example, if an organization is testing whether their network will protect them from cyber attacks, they need to incorporate all of the software and devices that work together to provide protection, including switches, firewalls, routers and load balancers. Simple tests that run against a single network device will not test the cumulative effectiveness of the entire network security solution.

The tests must run with realistic traffic that simulates typical production traffic. Many of the newer security devices operate by identifying abnormal traffic patterns and user or application behavior. Testing any new or changed application is dependent on accurately simulating realistic traffic patterns and loads.

Security testing must allow automation of set up, configuration and testing processes in order for it to be incorporated into a DevOps flow. To efficiently support a DevOps workflow, it is critical to automate the setup and teardown of the network infrastructure, traffic generation, security device configuration, the applications being tested, as well as the testing processes that are to be performed.

Networks are large scale and difficult to reproduce in a test. In order to be successful, security testing must emulate the true size and scale of the production network and all of its components. It is usually cost prohibitive to create a redundant full-production network. Good security testing solutions replace some of the physical infrastructure with virtual infrastructure and then mix these to provide a realistic replica of production but at a much lower cost.

When financial services firms were asked how well security testing represents their real production IT infrastructure, they really had no idea.

Security testing solution requirements

Based on the testing problems mentioned above, any application security testing solution must respond to the following requirements:

- The ability to create an isolated environment for testing that mimics the production environment as accurately as possible (i.e. with high fidelity).
- The ability to create a clone of the network configuration as well as to simulate realistic traffic patterns and load on that network
- Support for system-wide testing of a mix of physical and virtual network infrastructure as well as applications.
- Be able to automate the setup and teardown of the network infrastructure, traffic generation, security device configuration, and testing processes.
- Provide API driven access to the automation so DevOps tools can easily initiate and automatically set up security tests.
- Support for many testing environments to be run simultaneously.

Sandboxes for DevOps-integrated security testing

A critical enabler for integrating security testing into a continuous integration or deployment process is the “sandbox” software. A sandbox is a personal replica of a real complex production environment that is isolated from other sandboxes. Sandboxes include four key capabilities:

- They model all of the physical and virtual infrastructure and applications so that a configuration that exactly mimics a production configuration can be created on the fly.
- They provide workflow orchestration that is used for automated setup and teardown of the sandbox, as well as orchestration of traffic generators and all other aspects of security testing.
- They are initiated through an API with access controls, allowing them to be easily integrated with DevOps tools.
- They allow many users or groups to simultaneously run security testing in a shared lab while providing full isolation.

Summary

Security testing to ensure that applications do not create vulnerabilities to cyber attacks is the only way to stem the tide of red ink around the failure of enterprises to protect their constituents, employees and customers.

While security testing is difficult, existing technologies for public and private cloud sandboxing can be readily applied to the problem.

Sandboxing ensures that testing is isolated from production, accurately replicates the real production network environment, traffic and load, and allows for system-wide testing of applications. More importantly, sandboxes enable security testing to be included in automated DevOps processes, making continuous deployment a possibility for many regulated enterprises.

Joan Wrabetz is the CTO at Qualisystems (www.qualisystems.com). Most recently, she was the VP and CTO for the Emerging Product Division of EMC. Joan holds a BSEE from Yale, MSEE from Stanford University and a MBA from UC Berkeley, and has been awarded patents in load balancing, distributed systems, machine learning classification and analytics. She has also held adjunct teaching positions at multiple universities.

The life of a social engineer: Hacking the human

Mirko Zorz

A clean-cut guy with rimmed glasses and a warm smile, Jayson E. Street looks nothing like the stereotypical hacker regularly portrayed in movies (i.e. pale, grim and antisocial). But he is one – he just "hacks" humans.

Street is a master of deception: a social engineer, specializing in security awareness and physical compromise engagements. He's outspoken, friendly, always wearing a smile, and besides working in the field, he's also the InfoSec Ranger at Pwnie Express, and is well-known for his books and conference talks around the world.

Social engineering skills

Information security professionals generally agree that humans are the weakest security link. Employees need access in order to do their job, and so attackers increasingly target them instead of the network, in order to infiltrate the system.

A successful social engineer has to have a wide set of skills, ranging from psychology to IT. Most importantly, he has to understand the depth of human emotion. Reading people's faces, interpreting gestures, especially in a foreign country with a noticeably different culture, is a complex undertaking that takes plenty of practice and skill.

Essentially, a seasoned social engineer is the closest thing we have to a mind reader. He has to instantly size up the person and the situation he finds himself in, and create a scenario that gives him an advantage.

As Ernest Hemingway said: "When people talk, listen completely. Most people never listen." Well, successful social engineers do.

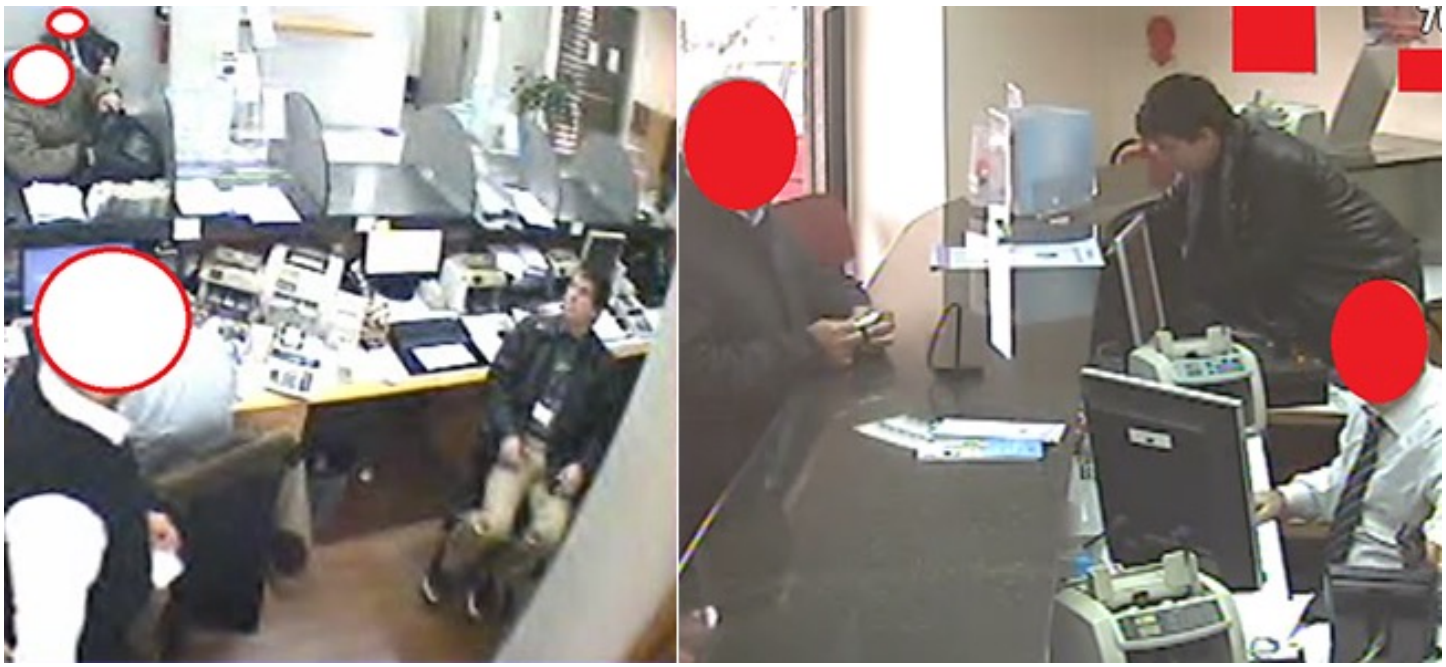
The world through the eyes of a social engineer

Information is the most valuable commodity in today's world, and Street knows how to get it. During our talks I learned that he broke into seemingly highly secure places all over the world, including the US, Malaysia, Jordan, Germany, Jamaica, France and Lebanon.

Some of the gear used in the field

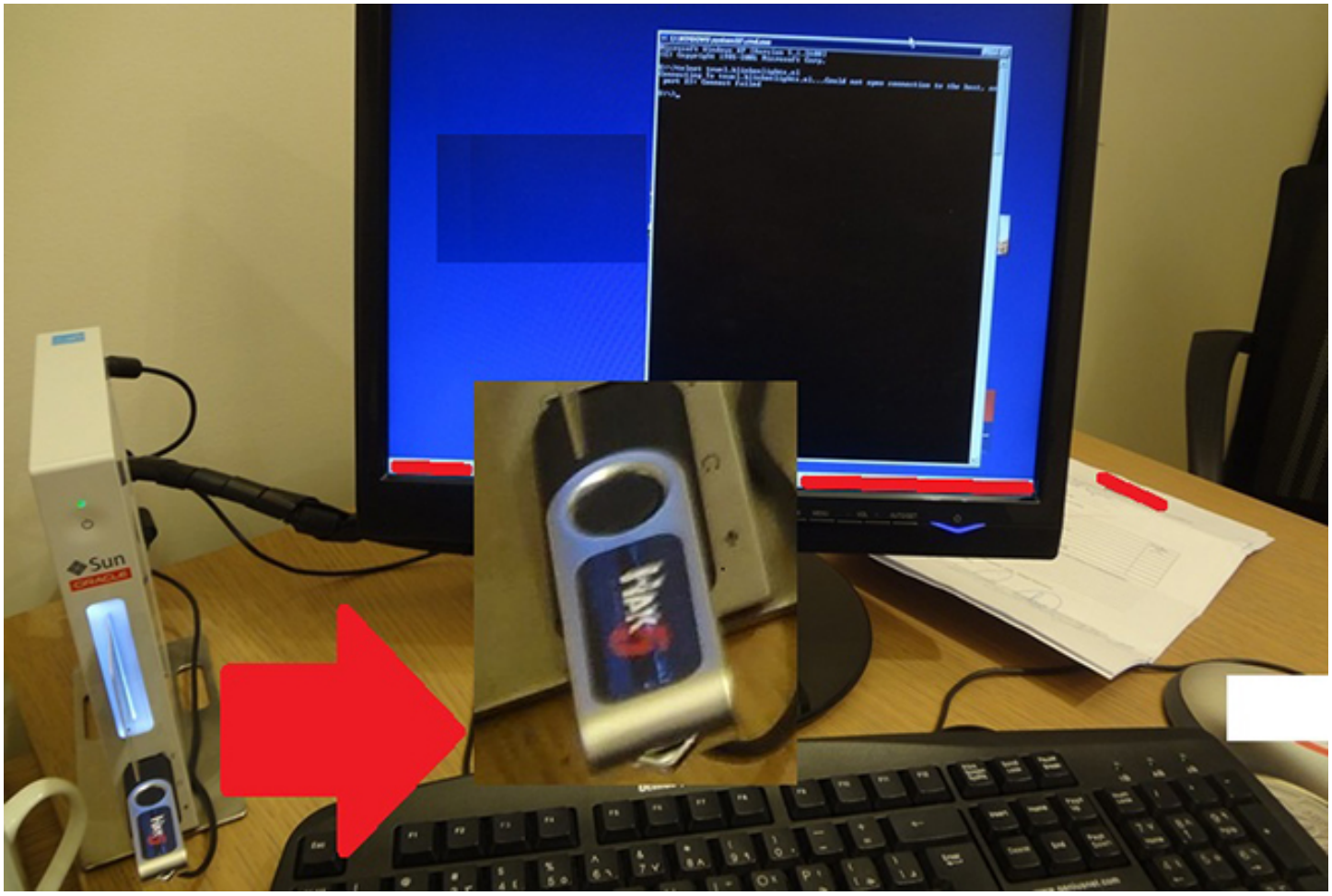
"I'm breaking into banks in Beirut, Lebanon, and I'm wearing a DEF CON leather jacket. I don't speak Arabic or French, and frankly, I don't blend well in this city," he recalls one such engagement.

As you can imagine, that didn't stop him. He ended up twirling in an office chair after talking a teller into allowing him to plug in his Hak5 Rubber Ducky USB into their computer system. In addition to that, at the end of that particular incursion, he had the bank manager assistant's user ID, password, and smart card.



Street in action behind the teller line

“Armed with this information I go to another branch during business hours. I talk my way behind the teller line, disconnect a computer, and take it with me,” he recounts. “And what do I do next? I go to a third branch and find my way into their internal LAN.”



The Hak5 USB is in

The owners were shocked at the lax security. They knew that someone with this kind of access could have committed all sorts of fraud. The point Street is trying to make is simple – if you want strong information security, you need proper physical security. In order to protect your data, you need to safeguard the hard drive on which the data resides.

“I’m not the best coder or exploit writer. I’m never going to be that guy. But I don’t have to be if I have a screwdriver and I can take a hard drive from your server. I don’t have to bypass the firewall if I can bypass the receptionist,” he says.

The importance of physical security

Street says he’s never failed to get access to target assets. But he loves to challenge himself, and sometimes his approaches seem outwardly ridiculous. For example, last year he managed to penetrate the entire infrastructure of a high-class hotel on the French Riviera while wearing Teenage Mutant Ninja Turtles pajama bottoms and walking around barefoot.

Self-assurance is key, and he knows how to deliver. During this job he stumbled upon an unprotected entrance to the employee area, and within 30 minutes he was in the corporate office. They never expected anyone to have access to these premises after office hours and security was nonexistent: keys on desks, unlocked computers – game over.

“I’ve never had a problem with guards anywhere, even at government or financial institutions. Actually, a night guard once helped me carry the server out of the computer room to my car,” he remembers merrily.

You may have guessed it, he's not supposed to be there

How to prevent social engineering attacks

"Never mistake what I'm doing for red teaming. I'm not trying to destroy an organization. I do social awareness engagements – my job is to educate and make people understand," he explains.

As a matter of fact, Street genuinely likes getting caught. In the last stage of an engagement he does obviously suspicious things deliberately in order to be unmasked.

"I always come with warning labels. I broke into a highly secure building in New York across from Ground Zero, wearing a shirt that says 'Your company's computer guy'," he remembers.

After the compromise he goes back to the building and explains to the people involved what just happened and why. The point of his job is to increase security awareness through effective teachable moments.

"Despite the outcome of my engagements, I've never met a stupid user," he notes. "I see uneducated users that haven't been properly trained. And explaining the importance of security should be an essential part of employee training."

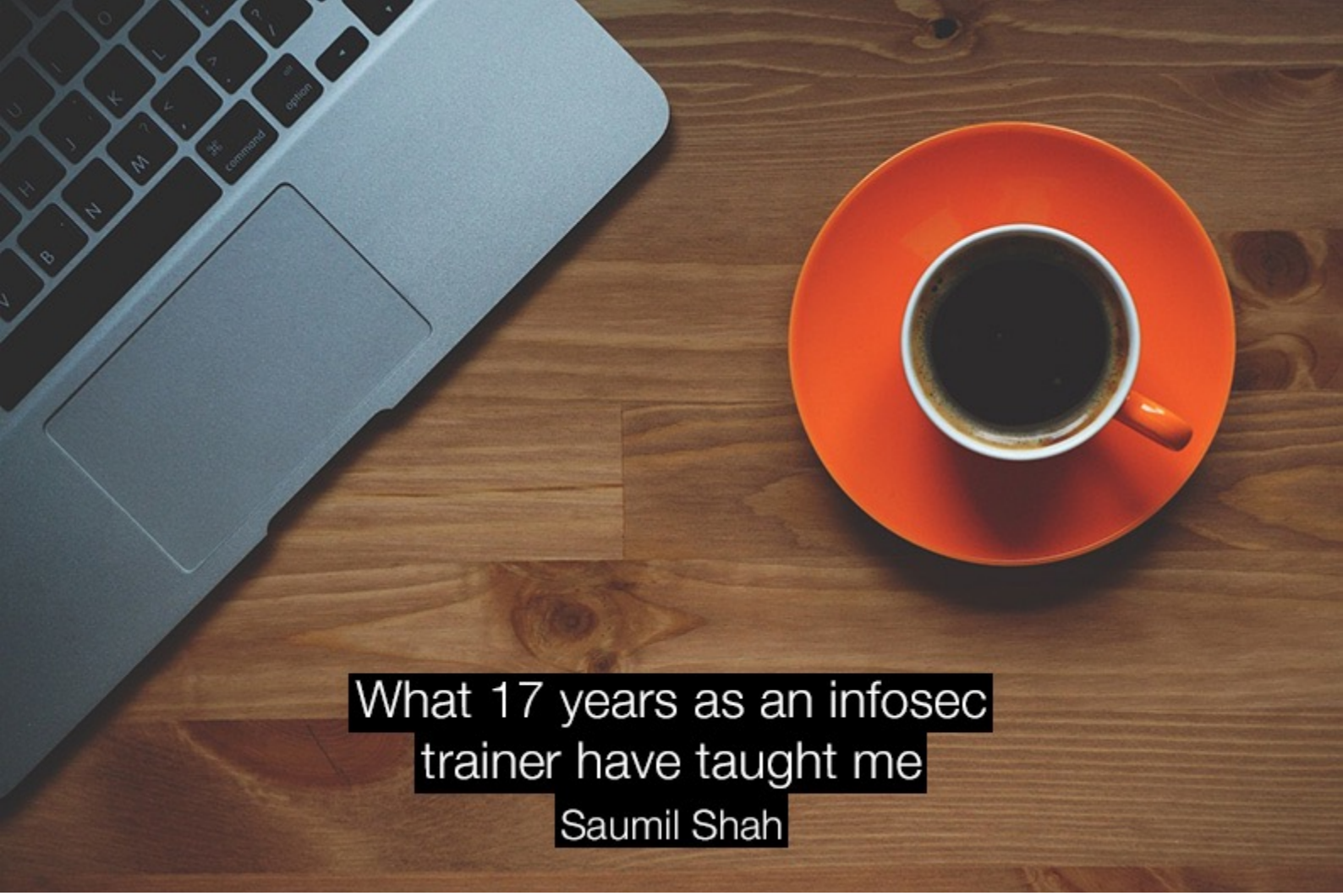
He's of the opinion that most social engineering attacks can be prevented, and offers the following tips:

1. If you get a feeling that something isn't right, listen to the voice in the back of your head telling you this and react.

2. Organizations should have a number for people to call when in doubt, an email address through which they can reach out for help. Every employee should know that if they see a suspicious person walking around, or they get a sketchy email, they can alert someone, and that someone will investigate. "Don't approach the person, don't open the attachment, inform security," he advises.

This advice might sound deceptively simple, but Street's adventures around the world prove that even the world's biggest organizations still haven't implemented basic security measures or trained their employees. Until we introduce the proper measures, humans will remain the weakest security link.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.helpnetsecurity.com).



July 2016 shall see me complete 17 years in the infosec training circuit. It has been an amazing journey, with humble beginnings.

I had a strong academic background in Computer Science – Operating Systems, TCP/IP and Cryptography. I was fortunate to work on my master's degree under Eugene Spafford in the COAST lab (now CERIAS) at Purdue.

The late 90s witnessed a meteoric rise of what became known as Silicon Valley Bubble 1.0 – job offers everywhere. I ended up picking the most oddball job description (and the lowest paying of them all): "Member of the Attack and Penetration team."

My first introduction to the larger world of information security outside academia was Black Hat and DEF CON 1999. Those were my early years as a professional penetration tester, pulling off exploits from Technotronic and Packetstorm, reading Phrack and Textfiles and popping rootshells on Solaris and Irix boxes. But the fun was not destined to last. Firewalls killed all opportunities to own Solaris boxes over RPC buffer overflows, and I needed a new way of getting into my target networks. Rather than bypass what is blocked, focus on what is available – this was my approach when I started finding and exploiting weaknesses in web applications. I had to walk up to the front door called "HTTP" and jiggle the doorknob until it opened.

Infosec conference talks those days were full of buffer overflows and DLL injection and memory corruption attacks. There was no research on "web hacking" – even the term was yet to be coined. In 2000, I was working on techniques to achieve total compromise of a target network simply by packaging attack vectors in HTTP. I wrote a research paper called One Way Web Hacking which formed the basis of web exploitation as we know it today – webshells, SQL shells over HTTP, web uploaders, and even tunneling arbitrary protocols such as RDP over HTTP proxies. I presented many talks on web hacking, starting with Black Hat 2000 and continuing on several other conferences around the world.

How I began security trainings

The company I was working for wanted to offer private trainings on web hacking. I wrote up the course syllabus and taught the first training in our offices in California in 2000.

I continued my independent research on web application security, developing the first HTTP fingerprinting tools, the first webshells, filter evasion and also came up with the first software WAF prototype. It was then that I decided to continue offering web hacking training at Black Hat, followed by Hack In The Box, and several other conferences around the world.

Training kept me challenged, as it brought a lot of curious minds together in a room for two full days. As I taught my students, I learned, too. The best ideas come to me when I am staring at the whiteboard trying to explain a concept to my students for the eleventy-first time. This is where new inspiration strikes, new opportunities unfold, new avenues open as I rethink age old infosec problems again and again.

In 2010, when I was teaching browser exploits, a student asked me: "How can you make browser attacks bypass malware inspection engines?" This question got me thinking very hard, and five years later, Stegosploit was born out of my passion for browser exploits and photography. Steganographically encoding a browser exploit in an image polyglot, i.e. a file that is a representation of two different data types, makes for some incredibly stealthy exploit delivery, and can be a visual treat as well, depending upon the chosen photograph.

In 2001, I was invited to keynote the Malaysian government's IT security conference in Kuala Lumpur. I was to speak on my findings from the Honeynet Project (a very different topic than web hacking). It was then that I met up with SK Chong.

SK was a hacker specialising in Windows shellcode and binary level attacks. He had followed my research on one way web hacking, and we met up to discuss how one way techniques can be applied directly to shellcode. SK eventually went on to publish his technique in Phrack and we kept in touch regularly.

Binary exploitation, working directly with memory layouts, pointers, registers and assembly code, had always been my first love. I used to reverse engineer DOS viruses back in the 90s. I had come a long way teaching web hacking and it was time to go back to my binary hacking roots.

In 2006, SK and I decided to team up and conceptualised The Exploit Laboratory over drinks at the Telawi Street Bistro in Kuala Lumpur. To me and SK, this was a historic moment that we look back upon every year. TSB has long shuttered its doors, but The Exploit Laboratory continues into its 10th year in 2016!

The Exploit Laboratory has been a fantastic journey. Teaching along with SK helped us keep a fantastic pace and overhaul topics and introduce new examples rapidly. We had a very simple philosophy: we wanted to teach the latest and greatest, in a very simple manner. Our challenge was to bring rocket science down to earth, and so we did.

It was through The Exploit Lab that I learned one of the most fascinating concepts in offensive techniques – Return Oriented Programming. Over the years, we taught several advanced concepts in exploit development. We created three more classes as a continuation to the basic Exploit Lab class – a Red Team class, a Master class and a class on fuzzing and vulnerability discovery. And to keep up with the times, the 10th year of the Exploit Laboratory will see a brand new class on ARM exploit development.

With the weight of the Internet shifting from desktops to mobile and IoT platforms, ARM exploit development is going to be an essential offensive skill to be acquired. I already taught two iterations of the ARM Exploit Laboratory at CanSecWest and SyScan this year, and am looking forward to advancing ARM exploit development even more.

The ARM Exploit Lab reminds me of the early days when we just started the Exploit Lab classes. There were little or no tools for assisting with exploit development.

Today the x86 exploit development world is full of mature tools and processes. ARM exploit development is still a new area with lots of opportunities to build tools and discover new techniques.

The challenges of infosec training

Infosec training demands a lot of background work: soaking up new research, improvising existing techniques, identifying new topics to be added to the course.

I pride myself on providing cutting edge topics with every class. The rate at which I add topics and rework the content ends up overhauling my entire course once every 6 months (on an average). I have been teaching for 17 years with more than 200 classes in my track record, and I have enough data points to back up my statistics.

My classes have followed a learn-by-doing pedagogy from the start. Today, hands-on training is the norm at infosec conferences. Students are expected to bring their laptops and work with a portable lab environment. In my early days, we used to rent laptops for our students to provide a consistent training environment, and I used to spend an entire day ghosting disk images onto laptop drives.

One of the constant challenges of training is time. Two days started becoming an increasingly short time duration to start from the basics and progress up to the cutting edge of offensive techniques.

In 2003, I switched over to using virtual machines as hypervisor technology matured and became mainstream. But even with virtual machines, I spend more than half of my preparation time fine-tuning the images and ironing out the hands-on exercises.

One of the constant challenges of training is time. Two days started becoming an increasingly short time duration to start from the basics and progress up to the cutting edge of offensive techniques. New topics needed to be added very rapidly, yet the basics cannot be compromised.

After every class, I make it a point to revisit my notes and identify topics that could have been explained more efficiently. I have been extremely fortunate to have had a fantastic training coach – Mr. Udayan Shah – who also happens to be my father.

My father went back to college in 1982, taught himself programming, and eventually started teaching programming professionally in 1986. I used to observe how he prepared diligently for each class. His flowcharts, hand written notes, talking points, everything. It stayed with me.

My father and I were also members of a computer hobby club during 1990-93. It was there that I conducted several meetings and public workshops on various emerging topics in computing such as Windows 3.1, Slackware Linux 1.0 and how to recover from DOS viruses such as Dark Avenger.

I got to learn the finer points of delivering a high energy workshop from my father. Most importantly, he taught me how to “sing to the audience”. Everything mattered: the size of fonts used on the projection screen, high contrast text and background, legibility of on-screen demos from the very last row of students, the art of handling questions and answers and fostering discussions, the importance of demo rehearsal. And even after 17 years, if I fail to “pray to the demo gods”, I still fall flat on my face.

I have the good fortune to still be able to pick my father’s brain on teaching style every now and then, and he never fails to teach me a new trick or two!

My day job, and how it helps me to teach

Many people have asked if I teach for a living. I don't. My day job involves running my company Net-Square, doing what we do best for the past 15 years – penetration testing and reverse engineering. Starting up and running a pen-test shop has enriched me with several real world scenarios which end up being modeled in hands-on exercises in my classes. I never use textbook or artificial examples.

Teaching for a living is a very different profession. It wouldn't have allowed me to make frequent changes to my classes and keep them up to date at the pace at which I do.

My day job provides the inputs, innovation and fresh new perspectives needed for my classes. For me, training is an intense workout. It is very taxing, yet very gratifying.

Mass manufactured certification is not even worth the paper it is printed on.

Infosec training and certification

Every discussion on training eventually brings up the unavoidable topic of certification. The entire IT industry is obsessed with certification. Here I shall quote the Saumil Shah theorem on IT certifications – "The value of a certification program is inversely proportional to the number of students certified annually," and its corollary – "Mass manufactured certification is not even worth the paper it is printed on."

We need to step back and understand the purpose of certification. Most certificates are given for participation in the training programme – they provide no insight into the capabilities of the student at the end of the training. A few certifications do conduct tests at the end of the training. These provide a statement of capabilities, but keep in mind that the statement is like a baseline – a lowest common denominator.

The problem is exacerbated when certification becomes the criteria for recruitment, business development and compliance. It then becomes a means to an end, and not a vehicle for gaining knowledge.

I personally fell for the CISSP certification hype back when it was really new. I passed my CISSP in 1999. The only thing I got out of it was a rectangle with my name printed on it along with the letters CISSP and a few signatures.

That having been said, I am increasingly leaning towards the concept of limited numbered certificates. This would provide a means of recognizing exceptional efforts and identify students who bring sincerity and a high level of proficiency to the table.

Infosec training DOs and DONTs

Although 2016 will be my seventeenth year teaching at Black Hat USA, in the past five years I have preferred teaching at smaller conferences. I like a focused conference crowd, and a sharp and active mix of students in my class.

Hack In The Box, SyScan, REcon, Cansecwest, 44CON – these have been some of my favourite conferences to teach at. These conferences are places I call "home" – familiar turf, warm and friendly crew members, compact class size and extended 3 and 4 day training sessions make for high energy training.

Black Hat is on its way to become a training factory, with many classes now having over 100 students each.

Black Hat is on its way to become a training factory, with many classes now having over 100 students each. Our Black Hat training features a larger crew, with two teaching assistants to ensure that even a larger class runs smoothly. A class size beyond 50 just doesn't work. The diversity in capabilities becomes too wide and I risk the class being held up for a few insistent stragglers. I'd rather stick with quality and depth over quantity at this point in my journey.

We have seen student groups undergo a transformation over the past decade and a half. These days, students seem more shy and reserved, but the greatest value of instructor-led training is derived from discussions and Q&A sessions in class. Sometimes we instructors have to work on uncorking the questions bottle.

Every now and then, we get a fantastic group with a critical mass of proactive students and the pace and energy picks up instantly! We love teaching a vocal crowd, and there are times when I will risk breaking out unrehearsed material and go way above and beyond the planned syllabus. At the end of the class, I have only my students to thank for bringing out an extended performance.

The other challenge we face is in managing expectations. It took a couple of years for us to figure out the gaps. We took great pains to ensure that our syllabus and learning objectives are very clearly communicated in the course description. For private infosec training, I like to have a conference call with the stakeholders to discuss the topics they want, and then work out the final syllabus after a couple of iterations.

Matching expectations is very critical, as it can make or break the class. We also started writing tutorials and exercises to help students prepare in advance for the classes. I have seen several proactive students take advantage of my free tutorials and exercises and come to the class loaded with questions and ready for action. As an instructor, I am delighted to see students armed and ready to go.

There are exceptions though. I'll never forget when a student at the Black Hat Abu Dhabi infosec training rocked up with an iPad when I had clearly asked for a laptop running VMware as a prerequisite. He was pretty insistent that the iPad would suffice. At that point, I told him to install VMware for the iPad and when he was ready, I'd be glad to transfer the VMs over. He needed about 20GB free space for it. He vanished after the first coffee break.

My plans for the future

I intend to continue teaching. With a firm base in x86 exploit development, I am excited to dive deeper into the world of ARM Exploitation and continue maturing The ARM Exploit Laboratory over the next few years.

I have been writing tutorials to help students prepare core concepts for my classes. I continue to seek feedback from students for areas to improve upon. Last year, I published two hands-on challenges – Tinysploit and Tinysploit2. These act as a litmus test of preparation for students wishing to take the ultra-advanced Exploit Laboratory classes.

Many people have encouraged me to make my training available online. I still feel that there is no substitute for an in-class instructor led training. After all, I am the son of a teacher-man!

Saumil Shah is the CEO of Net-Square (www.net-square.com), an information security consulting company.

Learn How Cyber Threat Intelligence Sharing Can Better Protect Your Organisation

Borderless Cyber Conference provides an interactive learning experience that produces valuable, actionable outcomes, by building communities of best practice through cyber threat intelligence information sharing.

CTI experts will also reveal the latest on the STIX, TAXII, CybOX standards initiatives through live use case studies and implementation demonstrations.

Conference delegates will learn:

- **Emerging security technologies**
- **Mitigation methodologies**
- **Threat management strategies**
- **How to better protect your organisation**

Date: 8-9 September, 2016

Venue: European Commission HQ

Location: Brussels, Belgium

For more information visit: http://borderlesscyber.oasis-open.org/eu16

Organised by

OASIS

BORDERLESS CYBER CONFERENCE

Official Partners

CERT-EU

FINANCIAL SERVICES Information Sharing and Analysis Center

WORLD BANK GROUP

ETSI

enisa European Network and Information Security Agency