

CYBERSECURITY INSURANCE



EXPLORE ▶

**USING A ROBUST PLATFORM FOR
CYBER THREAT ANALYSIS TRAINING**

**CUT THE FUD: WHY FEAR, UNCERTAINTY
AND DOUBT IS HARMING THE SECURITY
INDUSTRY**

**SOPHISTICATED THREATS? IT'S
USUALLY THE BASIC ONES THAT
GET YOU**



DON'T REACH FOR CYBER GREATNESS. REGISTER FOR IT.

Welcome to RSA Conference 2018, the world's largest cybersecurity event. Unbelievable innovations, expert-led sessions, invaluable networking opportunities—RSAC 2018 has everything to keep infosec professionals on the cutting edge of their field. So, can we count you in?

Visit rsaconference.com/helpnet-us18 to register for RSAC 2018 before January 5, 2018 and you'll **save \$1,000** on your Full Conference Pass. And while you're there, subscribe to our mailing list for the latest and greatest in cybersecurity podcasts, virtual sessions and more.

RSAConference2018

San Francisco | April 16–20 | Moscone Center

Follow us on: #RSAC    

TABLE OF CONTENTS

Page 05 - **Security world**

Page 10 - How consumers, enterprises and insurance providers
tackle cyber risk

Page 14 - Industrial cyber insurance comes of age

Page 17 - The modern challenges of cyber liability

Page 20 - **Malware world**

Page 24 - Rethinking corporate risk practices in the cyber age

Page 27 - Cyber insurance's inevitable evolution into risk
management services

Page 29 - As cyber risks enter the top three global business risks,
the insurance industry responds

Page 31 - **Events around the world**

Page 32 - Cut the FUD: Why Fear, Uncertainty and Doubt is harming
the security industry

Page 34 - Using a robust platform for cyber threat analysis training

Page 36 - Sophisticated threats? It's usually the basic ones that get you



(IN)SECURE Magazine 55 CONTRIBUTORS LIST

- **Sam Curry**, CSO at Cybereason
- **Lior Frenkel**, CEO at Waterfall Security Solutions
- **Joep Gommers**, CEO at EclecticIQ
- **Matthew Honea**, Cyber Director of Cyence
- **Rotem Iram**, CEO at At-Bay
- **Jason Krauss**, Cyber/E&O Thought & Product Leader at Willis Towers Watson
- **Zane Lackey**, CSO at Signal Sciences
- **Petra Uzorinac**, Head of Liability Underwriting at Allianz d.d.

Visit the magazine website at www.insecuremag.com

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

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

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

(IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without permission.



Android vulnerability allows attackers to modify apps without affecting their signatures

Among the many Android vulnerabilities patched by Google this December is one that allows attackers to modify apps without affecting their signatures.

“Although Android applications are self-signed, signature verification is important when updating Android applications. When the user downloads an update of an application, the Android runtime compares its signature with the signature of the original version. If the signatures match, the Android runtime proceeds to install the update,” Guard Square researchers explained.

“The updated application inherits the permissions of the original application. Attackers can, therefore, use the Janus vulnerability to mislead the update process and get unverified code with powerful permissions installed on the devices of unsuspecting users.”

The vulnerability (CVE-2017-13156) can be exploited to replace any kind of app, even a

system app, without the user noticing anything or Android preventing the installation.

The problem stems from the fact that a file can be a valid APK file (a zip archive that can contain arbitrary bytes at the start) and a valid DEX file (which can contain arbitrary bytes at the end) at the same time.

“[An attacker] can prepend a malicious DEX file to an APK file, without affecting its signature. The Android runtime then accepts the APK file as a valid update of a legitimate earlier version of the app. However, the Dalvik VM loads the code from the injected DEX file,” the researchers noted.

The vulnerability affects devices running Android 5.0 (“Lollipop”) and newer versions of the OS. It has been patched by Google, and the patch released to partners in November.

Users of Google smartphones (Pixel and Nexus) are protected right away, but those who depend on security updates being pushed out by other vendors and carriers are vulnerable until the patches are provided by the latter.

Five key trends to watch in 2018 as cybercriminals continue to innovate

The McAfee Labs 2018 Threats Predictions Report identifies five key trends to watch in 2018.

1. An adversarial machine learning “arms race” will develop between defenders and attackers - To win this arms race, organizations must effectively augment machine judgment and the speed of orchestrated responses with human strategic intellect.
2. Ransomware will pivot from traditional extortion to new targets, technologies, and objectives - The pivot from the traditional will see ransomware technologies applied beyond the objective of extortion of individuals, to cyber sabotage and disruption of organizations.
3. Serverless apps will save time and reduce costs, but they will also increase attack surfaces - Function development and deployment processes must include the necessary security processes, scalability capabilities must be made available, and traffic must be appropriately protected by VPNs or encryption.
4. Connected home device manufacturers and service providers will seek to over-

come thin profit margins - Because customers rarely read privacy agreements, corporations will be tempted to frequently change them after the devices and services are deployed to capture more information and revenue.

5. Corporations collecting children’s digital content will pose reputation risks - In their pursuit of user app “stickiness,” corporations will become more aggressive in enabling and gathering user-generated content from younger users.

In the corporate world, McAfee predicts that the May 2018 implementation of the European Union’s General Data Protection Regulation (GDPR) could play an important role in setting ground rules on the handling of both consumer data and user generated content in the years to come. The new regulatory regime impacts companies that either have a business presence in EU countries, or process the personal data of EU residents, meaning that companies from around the world will be compelled to adjust the way in which they process, store, and protect customers’ personal data. Forward-looking businesses can leverage this to set best practices that benefit customers using consumer appliances, content generating app platforms, and the online cloud-based services behind them.

Enterprise USB security is outdated and inadequate

While USB drives are ubiquitous for employees across all industries, security policies for these devices are often severely outdated or grossly inadequate for protecting critical enterprise data, according to Apricorn.

By failing to effectively monitor USB usage, organizations are leaving themselves vulnerable to data breaches, as well as putting their clients’ and employees’ personal information at risk.

While nine out of 10 employees rely on USB devices today, only 20 percent of them are utilizing encryption on those devices. Eight out of 10 employees use non-encrypted USBs, such as those received for free at conferences, trade events or business meetings.

The study also found that roughly 70 percent of employees surveyed maintained that USB drives improve the efficiency of their organizations’ IT operations and increase their productivity.

Other key findings:

- 69 percent of respondents agree that the use of USB drives increases productivity in the workplace
- Only 15 percent ask permission to use a USB drive
- 50 percent are required to seek permission to use external USB drives, while the other half are not
- 58 percent organizations have adequate governance and policies to manage the use of USB drives in the workplace.

DDoS attackers increasingly targeting cryptocurrency exchanges

The unregulated nature of the cryptocurrency ecosystem makes it possible for things like statements by widely esteemed financial executives to have a sizeable impact on the currency's price.

Another way to influence the price is through DDoS attacks against bitcoin exchange sites. According to a recently released report by Imperva, three out of four bitcoin exchanges and related sites that use their services were hit with DDoS attacks in Q3 2017.

"Overall, more than 73% of all bitcoin sites using our services were attacked this quarter, making it one of the most targeted industries, despite its relatively small size and web presence," the company noted. It's possible that the DDoS attacks against bitcoin exchange

sites are also made with the goal to extort money, but it's more likely that they are attempts to manipulate the price of bitcoin and other cryptocurrency – especially because similar attacks have been tried in the past.

A synchronised attack on several popular services, making them inaccessible while rumours are spread about the reason behind the outage, can allow criminals to "earn" considerable sums by simply buying cryptocurrency while the price is on a downturn, and waiting for the price to return to previous levels once the rumours are debunked and the sites are available again.

"This is a clear example of DDoS attackers following the money. As a rule, extortionists and other cybercriminals are commonly drawn to successful online industries, especially emerging ones that are less likely to be well-protected," Igal Zeifman, director at Imperva Incapsula noted.

Why phishers love HTTPS

As more and more sites switch to HTTPS, the number of phishing sites hosted on HTTPS domains is also increasing.

"In the third quarter of 2017, we observed nearly a quarter of all phishing sites hosted on HTTPS domains, nearly double the percentage we saw in the second quarter. A year ago, less than three percent of phish were hosted on websites using SSL certificates. Two years ago, this figure was less than one percent," PhishLabs' threat intelligence manager Crane Hassold shared.

The reasons behind this switch are several. For one, as phishers often compromise sites to host the phishing pages, it stands to reason that with the increase of legitimate HTTPS domains there will also be an increase of compromised HTTPS sites.

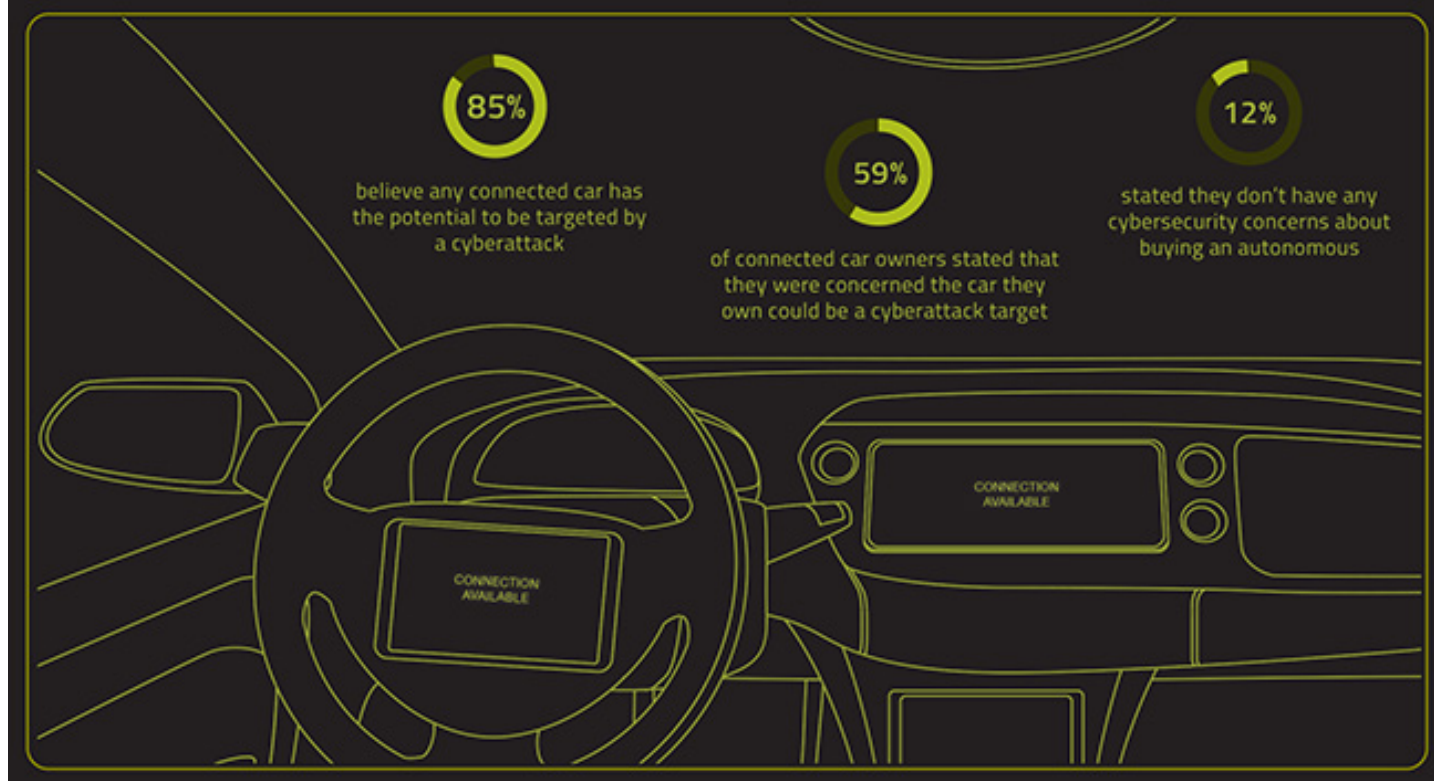
Secondly, as it got much easier, faster and cheaper to get SSL certificates, criminals are taking advantage of the situation to equip their phishing domains with HTTPS.

"Although a vast majority of SSL certificates used in HTTPS phishing attacks are obtained for free from services like Let's Encrypt or Comodo, their use is notable because, technically, they aren't necessary to create the phishing site. Without an SSL certificate, the phishing page would still function as intended," Hassold pointed out.

"So why would a threat actor take an extra step to create an HTTPS page when it is not actually needed? The answer is because phishers believe that the 'HTTPS' designation makes a phishing site seem more legitimate to potential victims and, thus, more likely to lead to a successful outcome. And unfortunately, they're right."

Too many users don't know that the presence of HTTPS only means that the communication between their browser and the website is encrypted. They believe that seeing a green padlock and HTTPS before a domain name means that the site itself is secure (i.e. safe for use = legitimate and not compromised).

The fact that browsers like Google Chrome label websites with SSL certificates as "Secure" in the URL bar doesn't help to dispel that assumption.



Cybersecurity concerns may stop consumers from purchasing a connected car

93% of consumers believe they do not own or do not know if they own a connected car and 49% do not own and do not plan on buying one in the future. However, the Irdeto Global Connected Car Survey of 8,354 consumers indicates that they are aware that a connected vehicle is susceptible to a cyberattack.

Of the consumers surveyed across six different countries, including Canada, China, Germany, Japan, UK and US, 85% stated they believe that any connected car has the potential to be targeted by a cyberattack. Both Canada and the UK responded the highest with 90% of consumers stating that a connected vehicle could be a target for hackers.

While the high percentage of consumers who say they do not own a connected car may be a result of not understanding the components that make up a connected vehicle, it is also possible that the awareness of safety risks and cyberattacks could be a major influencer in the reluctance of consumers to purchase a connected car.

The survey found that of the consumers who plan on purchasing a vehicle in the future, 53% are likely to research the car's ability to protect itself from a cyberattack. Consumers in China are most likely to conduct this research of all countries surveyed (71%), while consumers in Japan are the least likely to research a car's ability to protect itself against cyberattacks (37%).

The desire to consider cybersecurity when purchasing a car was most prevalent with younger generations aged 25-34, with 62% stating they would conduct this research.

On the opposite end of the spectrum, only 43% of consumers 55+ would look into the car's cybersecurity protection. The survey also found that 59% of current connected car owners are concerned that their vehicle could be targeted by a cyberattack.

Connected cars are also not the only type of next-generation automobile that consumers perceive as being a target. The survey results found that most consumers are aware that autonomous vehicles introduce new security risks. Only 12% of respondents stated that they don't have any cybersecurity concerns about buying an autonomous vehicle.



Enterprise security incident response trends to watch in 2018

Resolve Systems shared the top trends to watch in 2018 relating to incident response and automation.

1. Automation acceptance - Increasing volume of automated attacks will make it impossible for SOC's to keep up via manual processes alone.
2. Lower SOC entry level - Users will increasingly seek solutions that can lower the bar of entry to security teams. Due to security's significant skills gap, solutions that help less experienced professionals become quickly effective as Level 1 SOC analysts will be increasingly valued.
3. Continuous response - The market's focus on incident response will change from today's reactive position to a continuous one. Post-mortem analysis on security incidents will lead ongoing enhancements and testing for response playbooks.
4. Savvy MSSP shoppers - MSSPs will be affected, as clients begin to request MSSPs to demonstrate attack responses and share metrics on time to respond/remediate for specific incident types.
5. SOC as IR thought leader - The SOC team will become a driver for efficiency, automation, and best-practice procedures in IT, Network, and Service Desk, as the remediation activities that these teams perform in security incidents are critical for the success of the SOC.
6. SIR platform required - Having an incident response platform to orchestrate and automate cyberattack response will become a non-negotiable for security teams.
7. More money = more scrutiny - In the wake of recent catastrophic security incidents, CISOs and SOC's will see increasing investment and budget to purchase tools. However, with these added funds will come the onus to demonstrate measurable results and improvements, so teams will seek ways to demonstrate success with analytics, reporting, and attack simulations.
8. SOC developed automation - Leveraging their security expert's "tribal knowledge", many SOC's will find efficiency in building their own automations and look for tools that lower the programming barrier. They will seek solutions that enable those who know how to investigate and remediate incidents to create automations with no programming skills.
9. Possible CSIRT resurgence - As more and more organizations realize the necessity of enterprise-wide security response, the CSIRT will potentially become a way of attempting to solve cross-team collaboration challenges without having to completely rewire political and technical relationships between Security, IT, Network, and Service Desk.
10. More movement to MSSPs - Smart MSSPs – those that have the right personnel and tools available to build buyer confidence – that demonstrate the ability to meet core enterprise requirements and state-of-the-art responses to security breaches will attract the most interest.

How consumers, enterprises and insurance providers tackle cyber risk

By Zeljka Zorz



As the number of instances of hacks, data breaches, system compromises, ransomware, and cyber fraud keeps ballooning and shows no indication of stopping, the insurance industry is striving to keep pace by offering products that will meet the demand for cyber insurance.

The consumer perspective

In many ways, private individuals can have a much easier time deciding to get cybersecurity insurance than businesses.

For one, many have already personally experienced inconveniences, or have seen someone close to them having problems due to compromised personal data. According to the 2017 Identity Fraud Study from Javelin Strategy & Research, there were over 15 million incidents of identity theft in the US in 2016 - and that was before the Equifax breach, which resulted in the compromise of names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers of some 143 million US individuals, i.e. 44% of US consumers!

Martin Hartley, Chief Operating Officer, PURE Group of Insurance Companies, predicts that with the increase of fraud, cyber extortion and ransomware attacks, cybersecurity insurance will become a much more standard part of homeowners' policies in the coming years, as consumers find themselves liable for resulting costs.

"The risk of consumers' exposure will continue to increase and similarly, consumers can no longer solely rely on financial institutions, retailers and credit card companies to protect their customers' data," he says.

But the lack of consumer education in the category leads to confusion about exposure to and coverage for things like online and offline fraud (identity theft, forged checks, etc.), cyber

extortion (extortion payments, crisis management) and system attacks (data restoration, system cleanup).

"For private individuals, there is a lack of understanding of the loss that he or she might suffer as a result of a cybercrime, and therefore a misconception of what cyber insurance is needed for. While an individual may be embarrassed by having private photos or data made public, or lose photos and other records to cybercrime, the greatest financial risk is that cyber criminals steal money from the individual's bank, investment or retirement accounts – and that loss is not compensated by the institution," Hartley points out.

And, as cybercrime continues to evolve and become more complex, the nuances in policy coverage will continue to be incredibly important - both for consumers/businesses and insurance providers.

Hartley expects that, over time, cyber insurance offers will be tied more closely to risk management protocols.

"For example, today we will offer \$1 million of fraud and cybercrime coverage only to individuals who subscribe to an active cyber monitoring service, such as Rubica, on their personal networks and devices. Rubica's solution

actively monitors an individual's devices to block malicious items like malware and phishing attacks, investigate suspicious activity, and warn users of unsafe behaviors, like entering a password on an insecure website," he explained.

He also expects that, as consumers opt to add cybersecurity coverage to their overall insurance programs, insurance companies will begin to collect additional data to deliver more tailored products, from customized offerings to pricing that reflects the risk of each individual.

His advice to consumers thinking about whether or not to opt for cybersecurity coverage is to step back and do a holistic assessment of their lives in order to create a comprehensive risk profile.

"The number of connected devices your family has, use of public Wi-Fi, the number of bank accounts that could become comprised, the presence of children, how many third-parties (asset managers, assistants, attorneys, etc.) who help to manage your homes or financial accounts – these are all things that should be considered when assessing vulnerability. With that assessment, a person can make an informed choice about what offerings are appropriate for their particular risk profile."

Over time, cyber insurance offers will be tied more closely to risk management protocols

Cyber insurance is essential for modern businesses

Jerry Caponera, VP of Cyber Risk Strategy at Nehemiah Security, believes that all companies should have cyber insurance but not view it as a crutch or consider themselves "secure" just because they have it.

"Cyber insurance can be a key part of your cyber risk strategy but it isn't the strategy. In-

surance can cover some of the company's financial loss but can't help with the damage the company, people's careers, and people's lives can incur," he says.

"The Equifax breach is a prime example of this. The CEO 'retired' the day after the attack and I don't expect to see him leading a company again. Equifax might not survive in its current form (or in its current market) depending on the size of the loss and what the public

perception / government regulators do to the company. Some of the people working at Equifax will lose their jobs and could struggle to find the next one. And, finally, what about the people whose identity was stolen? No amount of cyber insurance will remove the hassle or financial loss they could incur. So no, I don't think it's smart to lead with insurance as your strategy."

For businesses looking at investing in cyber insurance, the main challenge is knowing where to start.

According to Caponera, the enterprises' assessment and decision process should start with understanding all the business applications they have, the data (or digital assets) involved, and how an attack can get at those environments. To do this requires bringing together the business, IT and security teams to collaborate in a way that not all do today.

Next, they need to understand the details of the cyber policy they're reviewing: what's covered as well as what's excluded.

"There are a number of incidents currently in court where the insurance provider is either suing the enterprise to recover some money paid or refusing to pay. The basis for these suits range from the enterprise not having 'adequate' security measures in place to the insurance company claiming that a social engineering attack, in which an organization wired funds to a hacker unknowingly, isn't covered because the transfer wasn't faked," Caponera points out.

"Most cyber insurance policies cover the cost for forensic analysis of the attack. That's where issues like 'inadequate' security and social engineering attacks come to light. The key for enterprises is to understand the details

of the insurance contract they signed – preferably before they sign it – so that they can reduce the chance of not getting paid out."

And, lastly, they need to make sure they continually evaluate their policy every few months.

"Your risks will change as your business changes, and the policy you have should adapt accordingly. Bottom line – just because you have a cyber policy in place doesn't mean your insurance needs are covered for good," he adds.

Insurers: The challenge with cyber

According to the National Association of Insurance Commissioners (NAIC), cyber risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data.

"Insurance policies are typically priced (or quantified) by comparing the company's application to past related losses," Caponera explains. "The challenge with cyber is that while two cyber attacks might be the same on the surface – i.e. they both use ransomware – the environments could be very different, thus making the comparisons meaningless."

Insurers compensate the lack of that type of information by relying on qualitative assessments of an applicant's risk management procedures and risk culture. "As a result, policies for cyber risk are more customized than other risk insurers taken on, and, therefore, more costly," NAIC notes.

The customization also hinges on things like type, size and scope of the business operation, the number of customers, the business' presence on the Web, the type of data collected and stored, and many other factors.

For businesses looking at investing in cyber insurance, the main challenge is knowing where to start

Caponera, who a few years ago started a company (PivotPoint Risk Analytics) that was focused on quantifying cyber risk in dollars and cents, says that, in general, insurance folks are very smart about insurance but lack critical knowledge about cyber security.

As he's now back in the cyber risk quantification space, his goal is to work with insurance professionals and offer a "cyber perspective" so that they can truly understand the potential losses.

"There are no actuarial tables for cyber risk – it's a moving target. So if you're not looking at the asymmetrical nature of how a hacker behaves, you'll never understand the risk correctly to underwrite the correct risk. And, when attacks grow in size and scale (and when

claims aren't paid out because the lawyers write good contracts for the insurance industry), we're going to be facing a 'cyber insurance bubble'," he says.

"Given an explosive interest for cybersecurity insurance, fuelled greatly by expanding regulation and data protection laws such as the GDPR, brokers tend to get increasingly shorter timelines for presenting quotes, often within a single day," said Dubravko Stašek, Insurance Broker at InterOmnia d.o.o.

"Businesses need to understand that the intricacies of a tailored cybersecurity insurance policy require a deeper exploration of the organization's overall security posture, as well their expectations when it comes to coverage."

Traditional insurance companies will definitely have to innovate

Upcoming changes

Caponera hopes that breaches like Merck and Equifax, where the financial losses are high, are the beginning of the change needed in the insurance industry.

"The ideal situation would be an environment where an enterprise quantifies their cyber risk in dollars and creates a plan to buy down that risk. They get a policy that reflects their projected exposure but also takes into account the mitigations they are putting in place," he says, and notes that the insurance industry could provide a discount for implementing the mitigations, thus sharing the "risk reduction" they have for the reduced chance for a payout.

"I think over the next 12-24 months you'll start to see this shift as the market demands solutions that can quantify risk in an automated manner, using real world data to help mitigate risks," he opined.

Traditional insurance companies will definitely have to innovate in order to remain competitive as technological change keeps its dizzying pace.

According to a recent PwC report, that often means looking outside the industry – typically in the InsurTech space (e.g., drones, sensors, IoT) – for the best ways to improve their systems, processes, and products.

Global consulting outfit Accenture also recently noted that the insurance industry views AI and the IoT as critical to delivering increased levels of personalization and better real-world outcomes for customers.

"Artificial intelligence has the potential to transform the insurance industry from simply assessing risk based on past experience to monitoring risks in real-time and mitigating, or even preventing, losses for customers."

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

Industrial cyber insurance comes of age

By Lior Frenkel



In June 2017, a major global ransomware attack dubbed NotPetya swept through Microsoft Windows-based systems, targeting energy companies, power grids, bus stations, gas stations, airports, and banks. In October 2017, Carbon Black estimated that ransomware like NotPetya had cost businesses world-wide \$1B USD in just the first 9 months of the year.

Various types of ransomware have impaired operations on infected machines, disrupted normal operations at critical infrastructure sites, including ports, railways, telecommunications systems, a variety of manufacturers, and hospitals.

These ransomware attacks are just one sign that sabotage-oriented cyber attacks are becoming more frequent, and more capable. The WannaCry ransomware, for example, took advantage of vulnerabilities exploited by the nation-state-grade attack tool code-named "EternalBlue," believed to be the work of the NSA. Similarly, a sophisticated industrial control system attack tool named "BlackEnergy," which targets energy-sector infrastructure around the world, is believed to be the work of Russian intelligence agencies.

As a result of this continued increase in attack sophistication, many businesses are revisiting their cyber insurance coverage, and many insurers are revisiting their policies. Each is concerned about minimizing their potential losses.

Cyber insurance coverage and policies from different insurers are very inconsistent. For example, some general liability and business interruption policies cover cyber events, but other do not, and many insurers offer specific cyber insurance policies, but the policies differ widely in coverage. Some, for example, cover only the direct cost of flying experts to affected sites to identify and repair affected machines, while others cover those costs and a wide array of other costs, such as business interruption, intellectual property loss, and identity-theft liability lawsuits.

To make matters more confusing for industrial enterprises, most cyber policies are focused on data theft, privacy breaches and other consequences stemming from attacks on Internet-exposed, corporate IT networks, not attacks on industrial control system networks.

The consequences of IT versus industrial cyber attacks differ substantially. Attacks on IT networks can result in reputation damage, loss of intellectual property, and privacy lawsuits

from customers whose confidential data has been stolen. Industrial attacks can cause downtime for large, costly physical systems and can cause damage to costly and hard-to-replace physical infrastructure.

In the worst cases, an industrial cyber attack can cause significant loss of life (e.g. a passenger train collision due to a compromised railway switching system).

New actuarial research is driving change in both IT-centric and industrial cyber insurance coverage

Cyber catastrophes

New actuarial research is driving change in both IT-centric and industrial cyber insurance coverage, and an important new area for actuarial research is cyber catastrophes. A 2017 study titled "Counting the cost" by Lloyds and Cyence concluded that "cyber events have the potential to be as large as those caused by major hurricanes."

The 2015 "Business Blackout" study by Lloyds and the Centre for Risk Studies at the University of Cambridge concluded that a worst-case breach of the North American electric grid could yield widespread damage to generation infrastructure and long-term power system instability, costing businesses between \$243B and \$1T USD.

Because of research such as this, insurers are increasingly excluding cyber coverage from general insurance policies. While cyber insurance coverage is far from standard across the insurance industry, standard exclusions do ex-

ist, and are being applied increasingly widely. For example:

- CL 380, the "Institute Cyber Attack Exclusion Clause," excludes claims for damages caused by, or contributed to by, cyber attacks
- LMA3030 includes an exclusion for terrorism claims due to "computer hacking"
- NMA 2912 and 2928 together exclude any damage to computers or data, unless that damage is caused by conventional causes such as fires, lightning and explosions.

Businesses that need coverage for these excluded cyber events must generally pay extra to have the exclusions waived, or must purchase a specific cyber policy, or industrial cyber insurance policy. Cyber events are increasingly considered by insurance companies as potentially catastrophic events, the costs of which must be recouped through increased, or dedicated premiums.

Reducing cyber risks

With global IT and industrial cyber insurance premiums estimated to reach between \$7B and \$10B USD in 2020, the cyber insurance market is growing rapidly.

Insurers are responding to growth in both premiums and cyber claims in much the same way as insurers have responded historically in other markets: by taking steps to encourage clients to reduce risks.

Just as fire insurance policies for homeowners are routinely offered at a discount if the homes have working smoke detectors, cyber insurance providers are starting to build discounts into their policies to reflect reduced risks due to strong industrial cyber-security programs.

For example, THB, a member of the Lloyds syndicate, recently announced a new industrial cyber insurance policy. The policy is comprehensive, covering business interruption due to plant downtime, damages to physical and cyber infrastructure, cyber extortion and many other costs. The policy is available through CNA Hardy, and provides a discounted rate to businesses whose industrial cyber security programs include industry-leading Unidirectional Security Gateways from Waterfall Security Solutions.

This policy is a sign of considerable progress in the evolution of industrial cyber insurance, and reflects changing industry views as to cyber security best practices.

The level of security provided by Waterfall products is the reason for the premium discounts in this comprehensive policy. Waterfall's Unidirectional Security Gateways eliminate the risk of external network attacks to industrial control systems. Unidirectional Gateway hardware is physically able to move information from industrial networks to external IT networks and the Internet, and is physically

unable to communicate any attacks back into industrial networks.

Unidirectional Gateway software components replicate databases and other servers, so that industrial data is readily available to external users and applications, without risk.

When the risk of network attacks is mitigated by Waterfall's products, overall cyber risk is markedly reduced, which enables both reduced premiums and increased policy coverage for industrial sites.

Lessons learned

Recent events continue to prove the truism that "cyber attacks only become more sophisticated over time." As attacks evolve, insurance coverage evolves as well. Standard exclusions for cyber events and attacks are being added to a wide variety of policies, including policies for general damages, business interruption and general liability.

Risk managers at industrial enterprises are advised to examine their current policies carefully, to understand whether cyber exclusions already appear in these policies.

Risk managers can also add value by setting expectations for industrial cyber-security programs at industrial sites throughout their enterprises.

Strong, best-practice-based industrial security programs, such as those requiring Unidirectional Gateways at interfaces between industrial networks and high-risk, Internet-exposed networks, have significant benefits. Such programs reduce industrial cyber risk directly, and enable industrial enterprises to access affordable and comprehensive industrial cyber insurance coverage to address residual risks.

For more information visit:
waterfall-security.com/cyber-insurance-partner

Lior Frenkel is the CEO and co-founder of Waterfall Security Solutions (waterfall-security.com). Privately-owned since 2007, Waterfall Security has focused on protecting critical infrastructure and industrial control systems from remote online cyberattacks, becoming the leading cybersecurity vendor for industrial control systems (ICS) perimeter security.



The modern challenges of cyber liability

By Jason Krauss

One of the largest obstacles that cyber insurance liability must overcome is a simple one: it is still a relatively new type of risk.

Underwriting a new risk is not easy. Compare it to typical property exposures: when a fire destroys a factory, the methods for determining the resulting loss to equipment and income are well established. The methods for assessing the risk of fire itself are equally well established, with decades of precedence to use as a reference looking at factors such as safety training, sprinklers, hoses, fire doors, flammability of materials, etc.

If, on the other hand, a hacker shuts down an online store, or irretrievably encrypts crucial customer data, how is such a loss measured? Should it be measured against the years it took to gather that data, or perhaps in the months or years it might take to win back those customers?

The cyber threat landscape is constantly evolving, and technology isn't necessarily helping the risk assessment process.

Companies across all sectors are looking to integrate the newest technologies into their business models, often without measuring the new risk that the shift exposes them to. For every new technology implemented to deliver customer satisfaction and gain competitive advantage, companies increase their exposure to a range of digital threats such as social engineering, theft of data and cyberterrorism.

Hackers and other malicious cyber actors, always ahead of the curve when it comes to technological understanding and capabilities, know how to take advantage of these situations, and use them as opportunities to introduce new types of cyberattacks. For example, social engineering attacks have developed from the original "advance-fee" scams targeting individuals to the more sophisticated "fake CEO" frauds that seek to gain access to an entire organization.

As these attacks evolve, so, too, must risk management strategies. For example, many organizations may find there are gaps in their protection when it comes to social engineering, as often neither cyber insurance policies nor traditional liability policies singularly cover the scope of losses associated with social engineering claims.

Given the acceleration in the number and complexity of attacks, it is imperative to fully understand the potential impact of a cyber event and ensure the right business continuity plans and insurance protection are in place.

As cyber insurance policies, which generally provide first- and third-party coverages, continue to evolve, there are several additional strategies that can and should be used both from an insurance perspective, and in addressing cyber culture within the organization.

Incorporating cyber protections into property insurance

The basic rule of property insurance is simple: if physical property suffers physical damage, the resulting losses are covered. But what if the property isn't physical?

Cyber data may not be physical, at least by the insurance industry's traditional definition, but there's no doubt it can be damaged, and losses can result from the damage. Every industry has seen files corrupted and data lost. And we've all seen news stories about cyber criminals threatening the data that is the lifeblood of business in the 21st century.

But the question remains: what steps to take to insure these losses?

While the cyber insurance marketplace has grown into a multi-billion-dollar business, the number of insureds with cyber exposures who do not have appropriate coverage is significant. But property insurance, which virtually every company purchases, can be leveraged to provide coverage for certain cyber risks. And that's beginning to happen - insurance companies are starting to take the initiative and including cyber protection in their property programs.

Until recently property insurers have not incorporated cyber risk, as there had simply been no demand for it, but there have recently been changes on this front. As insurance companies watch insurance buyers debate the expense of stand-alone cyber cover, some are offering another option: buying cyber protection along with their property protection, often at minimal or no extra cost.

Expertise is growing. The underwriters in the cyber insurance marketplace are developing the actuarial bases for estimating cyber losses. And property claim adjusters are already experts at analyzing a business and estimating the impact of unforeseen events.

However, there is still a long way to go before most markets embrace first-party losses from cyber events. So, to further protect themselves, companies need to look internally at how best to mitigate cyber risk.

Expertise is growing.

The underwriters in the cyber insurance marketplace are developing the actuarial bases for estimating cyber losses.

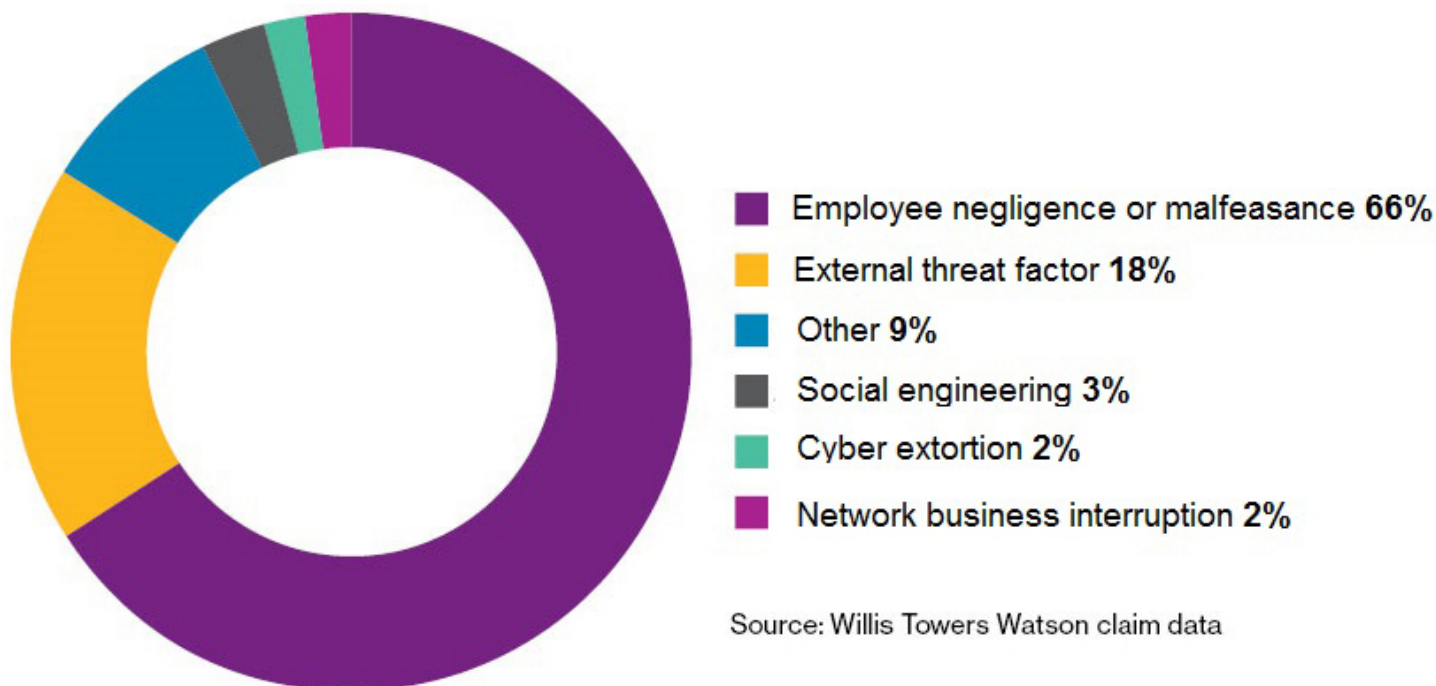
Analyze the people risk

Ultimately, the best way to minimize losses in the event of a cyberattack is to be proactive and develop a cyber-savvy workforce before an attack occurs.

In June 2017, Willis Towers Watson surveyed 163 US and UK employers and over 4,000 employees on their present and future cybersecurity strategies. This survey found that attention is now increasingly turning to the peo-

ple-related risks that, claims experience shows, leave companies exposed to cyber risk even with the use of state-of-the-art IT approaches.

While the concept of the malicious hacker breaking into a corporate network dominates the public image of a cyberattack, the survey found that two-thirds of cyber breaches can be attributed to employee negligence or malfeasance (see below).



Source: Willis Towers Watson claim data

Despite this major part of risk coming from employees, and most employers claiming to be aware of it, only 14 percent of respondents in the UK and 8 percent in the US claimed to have instituted and embedded cyber risk management into their company culture.

Companies cannot allow themselves to simply sit back. They must take action to educate their employees on cyber risk, and execute this on the executive and the employee level.

This also involves the breaking of some bad corporate habits, like over-reliance on IT functions to handle cyber issues, a lack of collaboration between corporate risk managers and HR, and a disconnect between executive cyber priorities and the viewpoint of the general

employee base. In addition, companies need to focus on developing comprehensive and ongoing training programs for their employees, not simply to check boxes, but to ingrain cyber awareness values into their entire organization.

Certainly, companies in every industry may have to adapt their operations to the constantly changing nature of cyber threats. Executives should also pay attention to the expanding risk mitigation options available through the insurance market. But employers should (and are) increasingly fostering a more cyber-savvy workforce, using innovative employee engagement, talent management and reward strategies so they may strengthen their cybersecurity position.

Jason Krauss is the Cyber/E&O Thought & Product Leader at Willis Towers Watson, a global advisory, broking and solutions company (www.willistowerswatson.com).

Malware world



Stealthy in-browser cryptomining continues even after you close window

As adblockers and some AV vendors are ramping up their efforts to block cryptojacking scripts from running, the crooks have to come up with new ways to keep them unnoticed. They are also testing new ways for keeping browsers open and mining even if the users leave the mining website.

Malwarebytes' researchers detailed one of these efforts, which involves covert pup-under windows, throttled mining, and an ad network that works hard on bypassing adblockers.

The "attack" unfolds like this: the user visits a website that silently loads cryptomining code and starts mining, but throttles it so that user's CPU power is not used up completely. This prevents the machine from slowing down and heating up, and makes it more likely that the user won't notice the covert mining.

But, when the user leaves the site and closes the browser window, another browser window

remains open, made to hide under the taskbar, and continues mining.

"If your Windows theme allows for taskbar transparency, you can catch a glimpse of the rogue window. Otherwise, to expose it you can simply resize the taskbar and it will magically pop it back up," Malwarebytes researcher Jerome Segura explained.

The rogue pop-under window can then be closed, and the mining stopped. Unfortunately, too many users won't notice it or notice for a while that their computer has become somewhat sluggish.

"This type of pop-under is designed to bypass adblockers and is a lot harder to identify because of how cleverly it hides itself," Segura noted.

"The more technical users will want to run Task Manager to ensure there is no remnant running browser processes and terminate them. Alternatively, the taskbar will still show the browser's icon with slight highlighting, indicating that it is still running."

An analysis of 120 mobile app stores uncovers plethora of malicious apps

RiskIQ analyzed 120 mobile app stores and more than 2 billion daily scanned resources. In listing and analyzing the app stores hosting the most malicious mobile apps and the most prolific developers of malicious apps, their Q3 mobile threat landscape report documents an increase in blacklisted apps over Q2, as well as the continued issues of imitation and trojan apps in official app stores and the emergence of the massive WireX mobile botnet.

The analysis confirmed that feral apps – apps available for download outside of a store on the web – and the Google Play store were the most abundant sources of malicious apps each quarter. Plus, the top developer of blacklisted apps in Q3, Nyi Subang Larang, worked exclusively in the Play store. However, Google's percentage of malicious apps was overall decreased and fell to a low of 4 percent in Q3 after reaching a high of 8 percent in Q2.

In third place, secondary store AndroidAPKDescargar had comparable numbers to Google and feral apps. In Q3, it more than doubled its number of malicious apps to 20,907, making up about one-third of its total app count and outpacing all other stores by more than 10,000.

Rounding out the top four, ApkFiles rocketed to a huge number (25,545) in Q1 and then

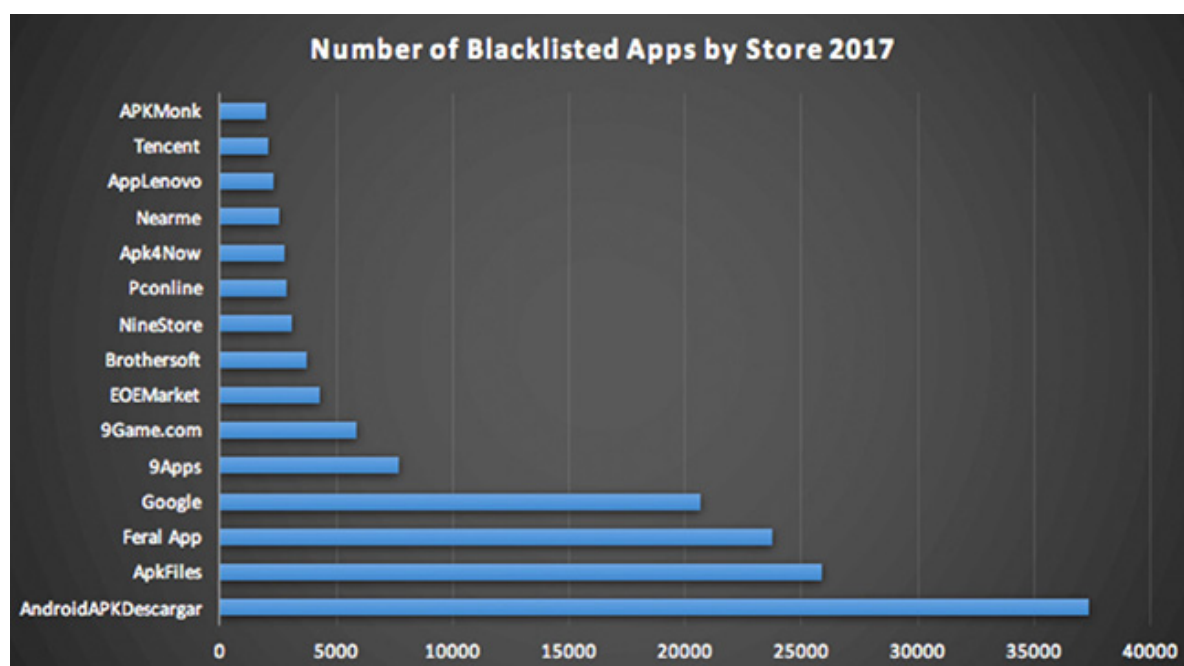
dropped off in Q2 before recovering slightly in Q3. Meanwhile, 97 percent of 9game.com's 6,052 apps (most of which purport to be games) were flagged as malicious.

Based on this data, RiskIQ concluded that some stores are being created and pumped up with huge numbers of malicious apps in short order. The firm's researchers speculate that this could be in concert with a particular campaign or to make detection of known bad stores more difficult.

One way malicious apps spread is through imitating others that are well known and popular. The Google Play store, in particular, is fertile ground for these attacks.

Coinciding with the increase in dangerous/imitation apps, Q3 also saw the emergence of a massive mobile botnet attack, known as WireX. In August, RiskIQ, Akamai, Cloudflare, Flashpoint, Google, Oracle Dyn, Team Cymru, and others collaborated to take down the new threat, affecting the devices of at least 70,000 Android users globally. After a short development stage, on Aug. 17, the botnet struck several content delivery networks (CDNs) – with between 130,000 and 160,000 unique IPs observed from 100+ countries.

Around 300 apps tied to WireX were identified in total, a subset of which was found in official app stores, such as the Play store. Google moved to block these apps and to remove them from all Android devices.



Return of Necurs botnet brings new ransomware threat

The Necurs botnet has returned to the top ten most prevalent malware during November 2017. Check Point researchers found that hackers were using Necurs, considered to be the largest spam botnet in the world, to distribute the relatively new Scarab ransomware that was first seen in June 2017.

The Necurs botnet started mass distribution of Scarab during the Thanksgiving holiday, sending over 12 million emails in a single morning. In October, RoughTed, a large scale malvertising campaign, remained the most prevalent

threat, ahead of the Rig ek exploit kit in second, and Cornficker, a worm that allows remote download of malware in third.

The most popular malware used to attack organizations' mobile estates remained unchanged from October, as Triada, a modular backdoor for Android, continued to increase in prevalence. It is followed by Lokibot, an Android banking Trojan and info-stealer, which can also turn into a ransomware that locks the phone in case its admin privileges are removed, and LeakerLocker, Android ransomware that reads personal user data and then presents it to the user and threatens to leak it online if ransom payments aren't met.



Keylogger found in Synaptics driver on HP laptops

For the second time this year, a security researcher unearthed a keylogger in a driver used on a number of HP laptops.

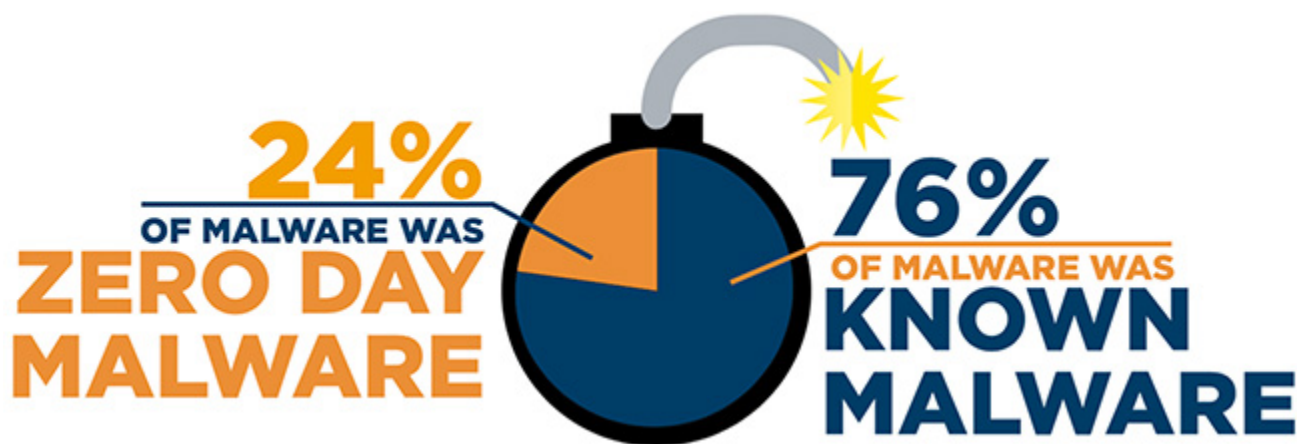
The first time was earlier this year, when Swiss security firm modzero AG discovered a keylogger in Conexant HP audio drivers that stored records of keystrokes in a file in the public folder, unencrypted. This time, the keylogger was spotted by security researcher Michael Myng (aka "ZwClose") while rifling through the Synaptics Touchpad SynTP.sys keyboard driver.

"The keylogger saved scan codes to a WPP trace. The logging was disabled by default but

could be enabled by setting a registry value (UAC required)," he noted.

Setting the required registry value can be easily performed by malware (e.g. remote access Trojans), which can then use the keylogger to harvest sensitive information entered by the user. Myng reported his finding to HP. "They replied terrifically fast, confirmed the presence of the keylogger (which actually was a debug trace) and released an update that removes the trace," he shared.

This was almost a month ago. HP made sure to note that "neither Synaptics nor HP has access to customer data as a result of this issue." Over 460 HP laptop models were affected by the flaw. But, according to HP, the issue affects all Synaptics OEM partners, so hopefully other laptop makers will push out an update soon – if they haven't already.



Script-based attacks and overall malware on the rise

Research revealed massive increases in scripting attacks and overall malware attempts against midsize companies throughout Q3 2017. In fact, WatchGuard Technologies found that scripting threats accounted for 68 percent of all malware during the period.

The findings reinforce expectations of continued growth of new malware and various attack techniques in the coming months, further emphasizing the importance of layered security and advanced threat prevention solutions.

“Threat actors are constantly adjusting their techniques, always looking for new ways of exploiting vulnerabilities to steal valuable data,” said Corey Nachreiner, CTO at WatchGuard Technologies. “This quarter, we found that script-based attacks – like the fake Python library packages discovered in September – appeared 20 times more than in Q2, while overall malware attacks shot through the roof. Staying vigilant regarding these developments is half the battle. Every business can better protect themselves and their stakeholders by employing multiple layers of protection, enabling advanced security services and monitoring network logs for traffic related to the top threats mentioned in this report.”

The ever-growing mob of constantly evolving security threats can seem overwhelming to the average small business with limited staff and resources.

Malware quantities have skyrocketed; a trend that will likely continue - Total malware instances spiked by 81 percent this quarter over

last. With more than 19 million variants blocked in Q3 and the holiday season approaching, malware attempts will likely increase dramatically in Q4 as well.

Cross-site Scripting (XSS) attacks plague web browsers, spreading internationally - XSS attacks, which allow cyber criminals to inject malicious script into victims’ sites, continue to grow at a measured pace. Previous reports detailed XSS attacks against Spain alone, but in Q3, XSS attacks broadly affected every country.

Legacy antivirus (AV) only missed 24 percent of new malware - Over the past three quarters, signature-based AV has missed malware at increasing rates, peaking at almost 47 percent in Q2. But this quarter was a marked improvement with only 23.77 percent of new or zero day malware able to circumvent AV. While this data is encouraging, behavioral detection solutions are still the most effective way to block advance persistent threats.

Suspicious HTML iframes surface everywhere - Attackers are continuing to evolve how they leverage the HTML iframe tag to force unsuspecting victims to suspicious, and often malicious sites. While potentially malicious iframes showed up everywhere, including the U.S. and Canada, their numbers jumped significantly in both Great Britain and Germany.

Authentication is still a big target - Though not as prevalent as in Q2, attacks targeting authentication and credentials (like Mimikatz) returned in a big way this quarter. Aside from Mimikatz, brute force web login attempts were also highly visible, proving that attackers are continuing to target the weakest link – credentials.

Rethinking corporate risk practices in the age of cyber

By Matthew Honea



Gartner estimates that by the end of 2017, organizations will spend \$86.4 billion on security technologies. Despite that, breaches and other cyber disasters are at an all-time high, causing massive losses for companies.

It's clear that the world doesn't have a technology problem, but rather a problem with managing risk around people, practices and perspectives.

And because no strategy or technology can offer complete protection, companies that want to improve risk mitigation will need to make a number of changes related to their processes and organizational structures. They will need to go beyond the "latest and greatest" technologies available and implement alternative ways to address unknowns and fill in gaps.

To help minimize the impact of breaches and other cyber disasters, many enterprises are turning to cyber insurance. According to PwC, demand is expected to grow the market from \$2.75 billion to \$7.5 billion by 2020.

To get the maximum benefit of cyber insurance, organizations need to adopt a new approach to managing risk. If you are among the

many who are struggling to understand how to move forward, here are a number of things to consider and pointers on where to start.

What best practice steps should CEOs, CFOs and CISOs put in place to model cyber risk?

The first step is recognizing that cyber should be part of a holistic risk approach.

Dependency on scalable infrastructure is rapidly increasing, and companies that don't include strategies to deal with related cyber risks will quickly fall behind. CFOs and CEOs should devote resources specifically designed to reduce risk in this area. Resources could include tools that provide security improvements, testing, detection and risk assessment. Historically, cybersecurity budgets have been lumped in with IT, but factoring them out individually will allow for greater protection and fewer damages when disasters strike.

CISOs don't need to reinvent a risk framework, but can instead adapt existing IT management and risk and compliance frameworks to include cyber.

Furthermore, executives should also start discussing cyber risk in the same terms they would discuss any other business risk – in dollars and probabilities. As cyber insurance becomes more prevalent, leaders are finding that money is the common language that adequately translates the impact of risk, whether they're discussing it with external vendors, security teams, or underwriters. People who move the conversation around cyber risk from arbitrary ratings and scores to quantified dollars and probabilities will be far more effective at driving meaningful change.

How can companies and insurers partner more strategically to understand exposure, close any gaps and ultimately lower risk?

From the insurance and underwriter perspective, personalization is key, as every company is structured differently. An underwriter should thoroughly research the company's cyber footprint beforehand, and then ask a core set of tailored questions to speed up the process and improve relationships. Additionally, as there are many variations of cyber insurance policies, cyber underwriters should provide clear definitions of inclusions, exclusions and retentions.

If you are seeking cyber insurance or looking to work better with underwriters – try to identify your organization's points of weakness early on. Companies will often avoid doing this altogether, as it can be difficult to do and can take time and resources. Instead, you should uncover potential faults early to help prioritize risk areas and put mitigation strategies in place that are specific to your business.

What tough questions should security and risk teams be asking their cyber insurance underwriters?

Communication between you and your underwriters is key and should be a two-way

street. This will help ensure that all areas of concern are covered and that effective policies are created.

Risk teams should do their homework on macro-economic cyber trends, as cyberattacks are very much driven by the market – i.e., the rise of ransomware and the availability of cryptocurrencies. Tracking which threats are evolving each year and how will equip you with the knowledge needed to have a productive cyber insurance experience.

In order to ensure proper coverage, you should inquire about policy language to understand exactly what will be covered, should an incident occur. When it comes time to renew contracts, companies shouldn't be afraid to let underwriters know what they have improved in their cyber postures. Discussing past, present and future plans will paint a clear picture for ongoing development.

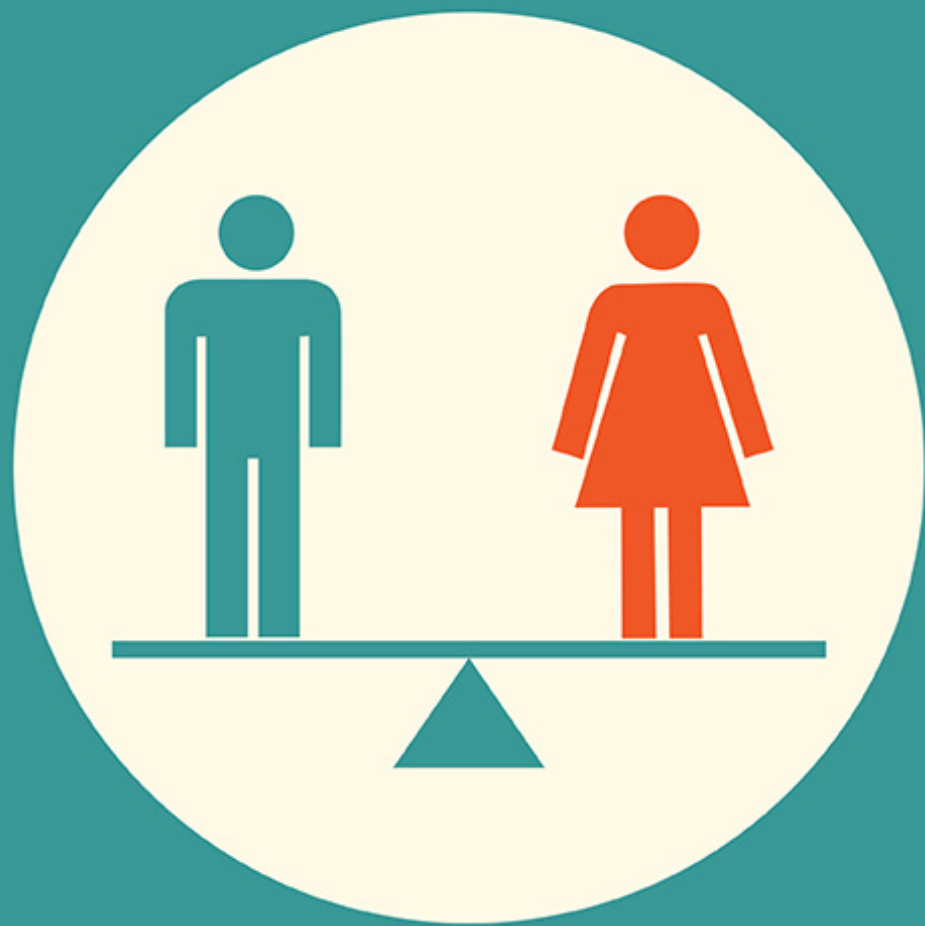
What role can a Chief Risk Officer play in addressing cyber issues?

A Chief Risk Officer has the power to convince other executives that cyber risks are now quantifiable and manageable – and should be treated as such. Chief Risk Officers should be communicating constantly with all areas of the business to ensure risk is considered from all internal and external angles. They should help evaluate the potential damage that could be caused by these factors and start the discussion around how to allocate resources accordingly. Beyond budget and executive buy-in, risk officers should also make sure that critical business systems are properly assessed on a regular basis. They should also put checks and balances in place to prevent any single person from controlling processes.

In this piece, I've touched on just a few aspects of how to approach cyber risk in the modern era. If followed, these high-level guidelines will provide you with an effective starting point for understanding how to drive necessary change to better protect your organization as it scales and expands its digital footprint.

Matthew Honea is the Cyber Director of Cyence (www.cyence.net). Cyence combines data science, cybersecurity, and economics into an analytics platform that quantifies the financial impact of cyber risk.

Gender influences risk.



Download the Security Culture Gender Report
<https://get.clt.re/gender>





Cyber insurance's inevitable evolution into risk management services

By Rotem Iram

Technology is evolving at a rapid pace, and recent events have demonstrated how effective and creative hackers can be in gaining access to important and sensitive data.

This threat increase has led more businesses to make cyber insurance an integral part of their risk management program. A recent survey of our customers found that the top reasons for a business to purchase cyber insurance was for access to risk mitigation and incident response services (67%) as well as risk transfer (65%).

Clients expect their cyber insurance carrier and broker to provide much more than insurance – risk managers need support in risk assessment, risk management planning and budget allocation, and incident response and recovery.

It's no secret that quality incident response services can dramatically reduce costs. IBM Resilient found in their 2017 Cost of a Data Breach study that having a good incident response plan and executing it quickly can reduce costs by over 25 percent. However, for

insurance carriers, providing risk management services throughout the lifetime of the policy is even more important. When risk changes so quickly, no snapshot of the company's security can accurately assess risk; therefore, to help companies maintain a predictable and low risk level, carriers need to provide active support.

Simply put, if the carrier can help the customer to avoid a breach, it also avoids paying for damages.

Providing risk management services requires the insurance company to bridge the gap between security expertise and financial risk management expertise; gain deep understanding of their customer's technology stack; what business processes and assets rely on each technology; and how evolving threats create probability and exposure for compromise of those assets.

It is a complex undertaking that requires a re-design of the insurance underwriting and service model, moving away from analysis of historical data sets and embedding cyber security DNA at the core of the organization.

More importantly, carriers need to collaborate with multiple parties such as insurance brokers, incident response and forensic firms, lawyers, credit monitoring service providers and PR firms (to name a few). Providing active risk management throughout the lifetime of the policy can be achieved by pulling together IT security monitoring and management solutions, threat intelligence providers, insurance underwriters and claim managers.

The last piece of the insurance risk management model is the client. Insurance buyers are typically not experts on IT security.

The relationship between IT security and risk managers has always been sensitive given the gap between domains of expertise, lack of common language and budget allocation politics.

A technical risk management program has the potential to bridge this gap in the organization and create a synchronized and collaborative program that fits the complex needs of this risk.

TO HELP COMPANIES MAINTAIN A PREDICTABLE AND LOW RISK LEVEL, CARRIERS NEED TO PROVIDE ACTIVE SUPPORT

Cyber risks are becoming more pervasive and have detrimental impact on businesses both large and small. Regardless of the complexity of an organization, even a simple ransomware attack can cause significant damages to a company, as experienced by Maersk and FedEx earlier this year.

More than 50% of businesses consider ransomware a significant threat to their organization, and half lack confidence that their com-

pany can prevent a significant ransomware attack.

As technology becomes more pervasive to how we live and work, there is an increasing need for CISOs and CFOs to work together to develop a comprehensive cyber risk management program that includes a mix of investments in security technology, security operations and cyber insurance; redesigned, to meet the needs of tomorrow.

Rotem Iram is the founder and CEO of cyber insurance start-up At-Bay (www.at-bay.com). Rotem previously served as a managing director and COO in the Cyber Security practice of K2 Intelligence, a global risk management firm focusing on cyber intelligence, cyber defense strategy and incident response. Rotem holds a bachelor's degree in computer engineering from the Hebrew University and an MBA from Harvard Business School.

As cyber risks enter the top three global business risks, the insurance industry responds

By Petra Uzorinac



Cyber risks require a sophisticated approach, and the old-school relationship between insurer and client does not fit the purpose any longer.

Being a prudent insurer when covering emerging cyber risks involves both insurance cover and risk management services. Providing clients with access to experts in the field of IT forensics and crisis management is essential in order to deliver an adequate insurance package.

Pre- and post-loss risk management services may be included in the annual premium providing clients with special access rights and priority in case of a loss.

Top concerns for businesses

The Allianz Risk Barometer from 2013 and 2017 shows how the awareness about cyber threats has changed. If we look at data from 2013, cyber risks were not even in the top 10 global business risks. Back then the biggest concerns were business interruption/supply chain, natural catastrophes, and fire/explosion.

This year launched cyber risk into the top three, while risks that can lead to physical damage lost relevance. Companies are mostly concerned about risks affecting intangible rather than tangible assets. Business interruption is still considered as the top risk, but a cyber incident could be a potential root cause of, or trigger, half of the top 10 risks.

2017 has also brought more increased regulatory pressure. According to the EU General Data Protection Regulation, as of May 2018 companies can be fined up to 4% of the annual worldwide turnover, or up to 20 million EUR (whichever amount is greater) in case of data privacy breaches.

Targeted attacks

As the world becomes more interconnected, organizations are increasingly more susceptible to cyber risk. Cybercriminals increasingly focus on targeted attacks which yield the most

money. Their targets? Everybody: from public and fiscal authorities, to banks and insurers, logistics and suppliers, service providers, manufacturers, and so on.

The weakest link are the employees. According to the Allianz Risk Barometer 2017, employee errors account for more than 30% of cyber incidents. In order to protect themselves efficiently, organizations need to improve security awareness and create a culture of security.

Cyber insurance and IT resilience

A mature IT infrastructure/department decreases the probability of claims but not their financial impact. It is important to have the client's IT department at the table during a sales discussion, and it's extremely important to stress that cyber insurance is only an additional risk management instrument to IT resilience.

Traditional lines of business (e.g. property and liability) cover only small portions of cyber risks. Business interruption and restoration costs are the most severe financial exposure at first glance, but there are so many other which can easily surpass them.

Do not forget about other first party claims such as consultant services, cost of IT forensics, crisis communication, cyber extortion, data recovery, or bring even third party exposure to privacy and data breach in the picture.

Future prospects

Exclusions in traditional policies will become more commonplace and standalone cyber products will eventually become the main source of liability.

The main driver for Europe is expected to be the EU General Data Protection Regulation. Within the next 20 years, KPMG (one of the Big Four auditors) expects a strong shift in demand towards SMEs and private persons.

What's on underwriters' desk today? A very complex reality:

1. Take a look into the annual/financial report and try to develop three potential scenarios and their outcome for the following risks:

- Loss of data
- Reputational damage
- Business interruption through non-physical damage.

2. Take a look into the annual/financial report and try to calculate potential business interruption losses. Combine it with the scenario analysis.

The importance of cyber exposure

Global insurers recognize the importance of cyber exposure and are continuously developing expertise and products. Insurance companies that are present all over the world can offer unique service to their clients by bringing global benefits to local solutions.

Local cyber products are very valuable as they are based on local sales support, local law, local underwriting team and claims management in the local language, but at the same time, they benefit from a global overview. This should change the "hard to get" paradigm about cyber insurance. This type of insurance is starting to become more available to small and medium entrepreneurs, who are regularly facing obstacles in finding approachable and easy-to-buy insurance solutions.

Making cyber insurance widely affordable is a precondition for insurers to have balanced books. Once this is achieved, it will be possible for the insurance industry to provide security to all segments of economy and society.

An evolving risk landscape leads to a higher exposure of cyber incidents. The "ostrich strategy" will not help. Be aware of the reality by keeping abreast of emerging risk information regarding cyber, make self-assessment and talk to professionals. The homework you do today will preserve you from future errors.

Events around the world



RSA Conference 2018


rsaconference.com/helpnet-us18 - San Francisco, USA / 16 - 20 April 2018

RSA Conference 2018 takes place April 16 to 20 in San Francisco! Take this opportunity to learn about new approaches to info security, discover the latest technology and interact with top security leaders and pioneers. Hands-on sessions, keynotes and informal gatherings allow you to tap into a smart, forward-thinking global community that will inspire and empower you.

Real World Crypto 2018

rwc.iacr.org/2018/ - Zurich, Switzerland / 10 - 12 January 2018

Real World Crypto Symposium aims to bring together cryptography researchers with developers implementing cryptography in real-world systems. The conference goal is to strengthen the dialogue between these two communities. Topics covered focus on uses of cryptography in real-world environments such as the Internet, the cloud, and embedded devices.



Cut the FUD: Why Fear, Uncertainty and Doubt is harming the security industry

By Sam Curry

Although the acronym is close to a century old, FUD (Fear, Uncertainty and Doubt) has come to be closely associated with the technology industry since the 1970s.

FUD is a simple but effective strategy that relies on supplying the audience with negative information to influence their decisions and, with the ever-present threat of another major attack, it's easy to see why it's become so prevalent in the world of cyber security.

Security vendors obviously have a vested interest in having potential buyers worried about the risks of imminent cyberattacks, as this fear will sway their decision to invest in more security solutions.

Likewise, media coverage of cyber incidents usually reinforces these doom-laden warnings, with a particular focus on the cost of attacks and the likelihood of further incidents. Again, this is unsurprising, as negative headlines have always been known to shift more copies or, more recently, earn more clicks.

Thanks to the increasing number of incidents impacting well-known brands or public infrastructure, we have seen this approach increasingly played out in the mainstream media.

Even non-commercial efforts by governmental bodies and not-for-profit organizations around security tend to lean towards FUD as a way of getting individuals and enterprises to take the issue seriously. Much of the discussion on the upcoming EU GDPR, for example, has focused on the risk of huge new fines, rather than more positive messages.

What harm does FUD do?

In small doses, FUD can be quite useful in gaining attention and spurring action. However, I encounter a lot of hyperbole around cyber, with terms like “hurricane force” and “weapons of mass (cyber) destruction” being thrown around, along with a focus on unlikely doomsday scenarios.

This does not help people take action, but rather pushes them in one of two counterproductive directions. It's possible all the doom-saying will shake some cash loose from the organization, but it is unlikely to go to the right places, and will instead be wasted on whatever the new technology of the moment is.

Alternatively, the hyperbole can simply inure people to the real risk, resulting in no action at all. Those who cry “FUD” are like the boy who cried “Wolf!” Doing it winds up hurting the CISO as a voice of reason regarding IT risk, by making them seem unbalanced and fearful of disaster to the point that they can’t have an adult conversation.

It is, of course, very true that serious cyberattacks will continue to happen, and there are many threat actors out there who can employ advanced tools to devastating effect.

It’s also true that many organizations are not paying enough attention to key security issues such as single points of failure and resiliency. However, the right way to mobilize decision makers is not through exaggeration and prophecies of doom.

What should the industry be focusing on?

We need to stop fetishizing FUD and instead start a meaningful dialogue regarding the most likely risks and how we can address them in practice. Whether we’re talking about a major attack on national infrastructure or an attack on a specific enterprise, the focus needs to be on ensuring confidentiality, integrity and availability of our systems and data.

Central to this is addressing the single points of failure (SPOF) – the elements of a system that will cause the entire system to stop working if anything happens to them.

The priority for all organizations should be to identify any SPOF within their operations and eliminate them by building in redundancies and other measures. On a national scale, this means ensuring that critical services cannot easily be knocked out by a single attack.

We saw a classic case of this when the WannaCry attack disrupted work at a large number of NHS hospitals, because they had no back-

up plan to get around the problem of systems being locked by ransomware.

Likewise, private enterprises need to ensure a high level of resistance, which will enable critical business processes to continue in the event of attack. Resilience – the ability to bounce back quickly with as little interruption to availability as possible - is also critical.

Linked to this is the principle of least privilege, which holds that every element of a system – from applications to users – should only be able to access information and resources necessary for their role.

When a compromise occurs, least privilege means the attacker will find it much more difficult to escalate their attack and spread to other systems.

The growing number of threat actors and proliferation of new tools means it is inevitable that system infrastructure will be breached at some point. But, the breach of information itself can and should be avoided with more attention and focus. It’s gotten so bad that tools are chosen simply on the basis of their ability to find things without regard to the negative impact on business.

People looking for the best mouse trap for their houses (enterprises) are deploying tools so coarse that they often maim and kill the children (users, systems and business processes) in our IT environments.

While the continued reliance on FUD may seem to be a useful sales tactic for the solution of the day in the short term, in the long term it is damaging the credibility of the security industry and causing decision makers to throw cash in the wrong direction, or simply ignore the threat entirely.

Instead of scaremongering, we need to help steer organizations towards essential security processes that will ensure confidentiality, integrity and availability even if a doomsday scenario does occur.

Sam Curry is the CSO at Cybereason (www.cybereason.com).



Using a robust platform for cyber threat analysis training

By Joep Gommers

We have recognized threats coming more regularly from sources such as nation-states, hacktivist and cybercriminal actors. Coupled with many new public policies aimed at mitigating the negative effects of data breaches, cyber espionage and intellectual property theft, it's clear a new ecosystem of cyber threat intelligence sharing is emerging.

The need for trained threat analysts is also increasing, but there are few that can represent their findings in a manner helpful to decision-makers. To correct this, organizations need to train cyber threat analysts using a technique that builds on the use on a threat intelligence platform (TIP) as a key tool in conveying the tradecraft of cybersecurity threat intelligence.

Developments in the threat intelligence sharing ecosystem

Through the development of this ecosystem, a global standards body known as the Organisation for the Advancement of Structured Information Systems (OASIS) has sponsored the further development of a standardised language, syntax and logic for a set of protocols for threat intelligence sharing. These are:

- Structured Threat Information Expression (STIX)
- Trusted Automated Exchange for Indicator Information (TAXII)

Parallel to this, several key corporate giants and innovative start-ups have developed their own tools for enabling the sharing of indicators of compromise (IOCs) and context around intrusions, breaches, information theft and other kinds of attacks that affect the confidentiality and integrity of data resources.

Despite this, policy analysts have pointed out that there is a severe lack of trained analysts for applying the STIX and TAXII protocols, which are the standards of this ecosystem.

In light of this, many public and private universities have begun developing training

programmes to fill this critical skills shortage and gap in the education system. But, it's also in the organizations' interest to train their existing threat intelligence analysts as well as new analysts in this universal "language."

Building training on a threat intelligence platform

A threat intelligence platform (TIP) has multiple functions, including:

- The aggregation of threat intelligence "feeds" from various open and proprietary sources while serving as a platform for enriching IOCs with supplemental data and information.
- Aiding the threat analyst in understanding the TTPs of the threat actors, as conveyed through the interpretation of enriched IOCs.
- Being able to distinguish between human readable threat intelligence (HRTI) and machine readable threat intelligence (MRTI).

Training cyber threat analysts via a TIP is key to making them capable of conveying the tradecraft of threat intelligence. Giving an analyst a robust TIP that is designed to give them a high level of configurability will expose them to the internal logic of the system, thereby empowering them to carefully design the threat detection, response, and prevention parameters. This will help reduce false positives and increase the value of the data collected for use in defensive or remedial actions.

Whether for workforce training or academic education, applied, hands-on lab work is critical to learning objectives and arming students with practical knowledge to build upon. It is important that the training analyst is given theoretical frameworks – such as Kill Chain and the Diamond model – that guide hypothesis formation and testing as well as knowledge of the craft for effective integration into ongoing threat intel teams.

To effectively apply a TIP-based learning system for students, lessons should be drawn directly from the workflows of operational units such as red teams, incident response teams

and SOC teams. Specific case studies can give students a sense of how TIPs function within an organization where different teams collaborate on threat intelligence sharing. Having a robust and highly configurable TIP ensures that the analyst understands these basic workflows, use cases and various features needed for ingesting feeds, performing analysis and presenting findings.

The growing need for skilled threat analysts

There is a growing realization of the benefits of threat intelligence sharing for fortifying networks, and reducing liabilities and risks associated with data breaches. This has increased the need for individuals to understand exactly how to interpret the IOCs, enrich the data and how to characterize the activity of threat actors that may be engaging in attacks on member networks.

There are currently very few threat analysts that understand how to use TIPs and STIX-formatted data, how to refine IOCs and how to analyze the patterns in order to test hypotheses on threat actor intent and motivations.

The poaching of cyber security talent is becoming a growing concern for organizations, as highlighted by the lawsuit brought against Nike by Mastercard in 2015. Not only is cyber security talent being poached from other firms, they are also being recruited from roles such as network engineers, database managers, ethical hackers as well as other disciplines that have a bearing on the information and cyber security fields.

Even for these specialized workers, it's a steep learning curve to develop an understanding of the tools and techniques used to analyze attacks and developing application interfaces (APIs) between TIPs and existing in-house tools for monitoring networks and generating metrics.

Workforce development will continue to be a concern for companies and public-sector organizations and employers would do well to support their employees that seek development in the ecosystem of threat intelligence.



Sophisticated threats? It's usually the basic ones that get you

By Zane Lackey, CSO at Signal Sciences

If you listen to the headlines, the threats we face today are so sophisticated and intense, they can only be evaded with the help of artificial intelligence and machine learning. Losing sleep over zero-day cyber APTs launched by nation states? You shouldn't be. It's much more likely to be a common password or an off-the-shelf web app attack that puts you at the mercy of hackers.

If you want to protect your business, you're better off focusing on addressing the basics—because chances are, you're still at risk from the same boring attack techniques that have been around for the past decade or more.

Over the last dozen years, I've had opportunities to see security programs from a variety of different angles—as a security consultant, seeing the security program at a different F500 company every few weeks; as the in-the-trenches CISO for Etsy, building its security team during the company's explosive growth; and now as the co-founder and CSO of a security vendor helping defend companies in their shift to DevOps and the cloud. Time and again, the breaches come down to off-the-shelf attack techniques around phishing, social engineering, credential re-use, and web app attacks.

Why are so many companies still facing the same security challenges? For one thing, it's

hard—or at least, people assumed that it had to be, that security had to come at the expense of usability. That led to cumbersome products and processes that deterred adoption, undermining their effectiveness. It was a false narrative all along, but only recently are we seeing security solutions designed around a good user experience.

There's also been the misconception that compliance equals security, so addressing the first meant you were covered for the second. While in some cases compliance can help with security, it is often tangential (at best) to it. Finally, there's the perennial headcount problems that every CISO faces. There are open reqs on virtually every security team on the planet, making it difficult or impossible to make effective use of tools historically designed for security experts.

That's the why. Now, the how: here's what you need to do to get your core defenses in place.

DEVICES WILL ALWAYS BE LOST OR STOLEN, BUT YOU CAN KEEP IT FROM TURNING INTO A MASSIVE DATA THEFT PROBLEM

Limit the damage of a compromised endpoint

The most important shift to make when it comes to defending your endpoints is to stop thinking that all attacks can be prevented, and to begin with the assumption that your endpoints will be successfully compromised. The priority now is to obtain visibility and limit the scope of that compromise.

There are a number of next generation endpoint security companies like Carbon Black and Red Canary that provide a great starting point, along with strong two-factor authentication from a service like Duo can severely limit the ability of attackers to laterally move around inside your network, raising the bar dramatically in the typical environment.

You can also use tools like Thinkst Canaries to set traps for attackers and gain visibility into when they're laterally moving across your network. Just as importantly, because of the strong focus on a good user experience, these sort of effective security controls don't introduce friction for your users.

As for the endpoints themselves, make sure you're using the full-disk encryption available on the laptops and mobile devices in your environment (e.g. BitLocker for Windows, FileVault for MacOS, and the built-in encryption on iOS and Android). Devices will always be lost or stolen, but you can keep it from turning into a massive data theft problem.

Keep your head in the cloud

While there is often a wariness of cloud services, in many cases they can actually make an organization more secure, not less. Take email, for example. Not that long ago, even small organizations had to host their own mail

servers to provide email access for their employees. This meant that the highly technical burdens of securing and maintaining this often-complex bit of infrastructure fell on those who typically didn't have the resources to do it well.

Fast-forward to today, however, and you have service providers, like Google and Microsoft, providing email services while handling the vast majority of the associated complex administrative tasks. Additionally, by using Platform-as-a-Service providers like Pivotal, a company no longer has to deal with datacenter or even infrastructure-level security and system administration issues.

Get smart about your web apps

Over the past two decades, the attack surface at the web layer has dramatically expanded. Initially, organizations' websites were typically marketing channels that, if compromised, could be defaced, but wouldn't expose any legitimate customer data.

Compare that to today, where web applications (and the APIs that power them) are in fact the main customer-facing products for many companies. From an attacker's perspective, targeting a company's web applications is often the most direct route to compromising sensitive data.

Just as attackers have shifted, defenders, too, must shift to a greater emphasis on defending the web applications, which are the conduits to sensitive customer data.

My advice? Don't stay up at night worrying about the 1 percent nation-state zero-day scenario when it's the 99 percent of common attack techniques that end up leading to the vast majority of breaches.

Zane Lackey is CSO and co-founder of Signal Sciences (www.signalsciences.com), a protection platform for the modern web. Previously, Zane built and led the Etsy Security Team, where he pioneered and published new approaches to practical defense based on his background in offensive security. Follow him @zanelackey @signalsciences.