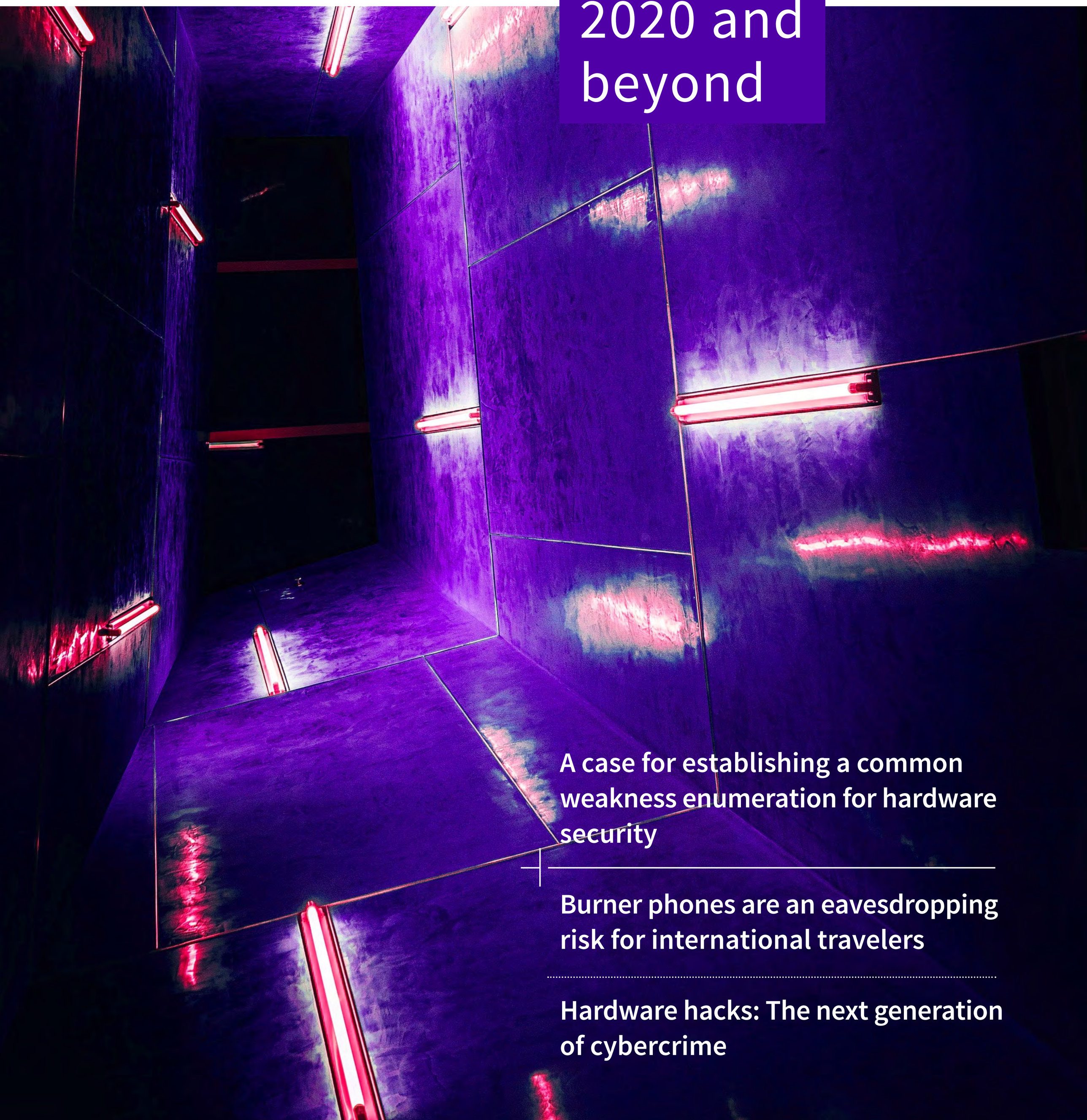
[+] (IN)SECUREMagazine

02 | 2020

ISSUE 65

2020 and beyond



A case for establishing a common weakness enumeration for hardware security

Burner phones are an eavesdropping risk for international travelers

Hardware hacks: The next generation of cybercrime

(ISC)²

Commit to **CERTIFICATION** in **2020**

Here's Everything You Need to Succeed – Without Excuses

Prepping for (ISC)² certification is a BIG commitment. We know you're dedicated, and this is the year to take it to the next level. We need talented, skilled people working to ensure a safe and secure cyber world for all. The movement has started. It's time for you to elevate yourself even higher! Leave excuses behind, set your goal and commit now.

Get your no-excuses guide to success.

(ISC)² Exam Action Plan ▶

CISSP® SSCP® CCSP® CAP® CSSLP® HCISPP®

(ISC)² | Inspiring a Safe and Secure Cyber World

Table of contents

Featured experts

GALINA ANTOVA, Chief Business Development Officer, Claroty
MICHAEL CAMPBELL, Head of Government and Federal Business, Privoro
MARCUS CHUNG, CEO, BoldCloud
CHARLES EAGAN, CTO, BlackBerry
JASON M. FUNG, Offensive Security Research Manager, Intel
DYANN HEWARD-MILLS, CEO, HewardMills
ARUN KANUPARTHI, Offensive Security Researcher, Intel
HAREESH KHATTRI, Offensive Security Researcher, Intel
JASON LAWLOR, President, Lightship Security
NATHAN PALMER, Security Researcher, Raytheon's Cyber Offensive and Defensive group
MICHAEL SCHENCK, Director of Security Services, Kaytuso

Visit the magazine website and subscribe at www.insecuremag.com

Mirko Zorz
Editor in Chief
mzorz@helpnetsecurity.com

Zeljka Zorz
Managing Editor
zzorz@helpnetsecurity.com

Berislav Kucan
Director of Operations
bkucan@helpnetsecurity.com

A case for establishing a common weakness enumeration for hardware security

AUTHORS_

Jason M. Fung, Offensive Security
Research Manager, Intel
Arun Kanuparthi, Offensive Security
Researcher, Intel
Hareesh Khattri, Offensive Security
Researcher, Intel

As modern computer systems become more complex and interconnected, we are seeing more vulnerabilities than ever before. As attacks become more pervasive and sophisticated, they are often progressing past the software layer and compromising hardware. As a response, the industry has been working to deliver microarchitectural improvements and today, implementing hardware-based security is widely recognized as a best practice.

The industry needs a better and more in-depth understanding of the common hardware security vulnerabilities taxonomy, including information on how these vulnerabilities get introduced into products, how they can be exploited, their associated risks, as well as best practices to prevent and identify them early on in the product development lifecycle.

However, hardware-based security has its own set of challenges when not designed, implemented or verified properly. Combined with the fact that we are seeing increasingly sophisticated methods to exploit hardware by chaining them together with software vulnerabilities, it's evident that the industry needs a better and more in-depth understanding of the common hardware security vulnerabilities taxonomy, including information on how these vulnerabilities get introduced into products, how they can be exploited, their associated risks, as well as best practices to prevent and identify them early on in the product development lifecycle.

Today, a key resource for tracking software vulnerabilities exists in MITRE's Common Weakness Enumeration (CWE) system, which is also complemented by the Common Vulnerability and Exposures (CVE) system. A simple way to differentiate the two is that CWE includes a taxonomy of common security vulnerability types and provides different views for a user to traverse different categorical buckets, whereas the CVE maintains the list of specific vulnerability instances that have already been found and reported publicly. Multiple CVEs are usually mapped to specific CWEs.

With the growing awareness of hardware vulnerabilities, the CWE could be enhanced to include relevant entry points, common consequences, examples, countermeasures and detection methods from the specific hardware perspective.

Essentially, the two systems work hand-in-hand to provide the ultimate vulnerability reference guide. These resources aim to educate architects and developers to identify potential mistakes when designing and developing software products. At the same time, they enable security researchers and tool vendors to pinpoint current gaps, so they can offer better tools and methodologies to automate the detection of common software security issues.

With the growing awareness of hardware vulnerabilities, the CWE could be enhanced to include relevant entry points, common consequences, examples, countermeasures and detection methods from the specific hardware perspective. Furthermore, there are hardware-centric weaknesses that are related to the physical properties of hardware devices (e.g., temperature, voltage glitches, current, wear out, interference, and more) which the CWE does not yet categorize. Due to these missing reference materials for hardware vulnerabilities in the CWE, researchers do not have the same standard taxonomy that would enable them to share information and techniques with one another. If we expect hardware vendors and their partners to collectively deliver more secure solutions, we must have a common language for discussing hardware security vulnerabilities.

Over the past few years, Intel researchers have been active in raising public awareness on common hardware security vulnerabilities (through academia, at conferences, and even with the industry's first hardware capture-the-flag competition). But more can always be done. Here are six ways the industry would benefit from a standardized Hardware CWE:

1_Product architects and designers could gain a deeper understanding of the common hardware security pitfalls, allowing them to potentially avoid repeat mistakes when creating solutions.

2_Verification engineers could be more fluent in the commonly made security mistakes and how they can be effectively detected at various stages of the product development lifecycle. This would enable them to devise proper verification plan and test strategies for improving the security robustness of products.

3_Security architects and researchers could better focus their energy on systemic issues and work to identify effective mitigations that help eliminate risks and/or make exploitation much more difficult for attackers.

4_Electronic Design Automation (EDA) vendors could prioritize and expand their verification tool features and offerings. This could improve the effectiveness of their tools in guiding users to avoid the introduction of common vulnerabilities. It could also provide a common platform for **EDA tool users** to compare and benchmark the capabilities of different tool options, enabling them to identify the right ones that meet their specific needs.

5_Educators could develop training materials and best practices that focus on the most relevant areas of concern, so university curriculum and corporate trainings could help audiences gain the necessary skills they need.

6_Security researchers could leverage a common taxonomy to communicate without ambiguities, facilitating learning exchange, systematic study and collaboration. And a public database would also make the research field more accessible for aspiring researchers.

As our industry moves forward to combat the latest threats, it is vital that we invest in research, tooling and the proper resources to catalog and evaluate both software and hardware vulnerabilities.

Today, categorizing hardware vulnerabilities, root causes, and mitigation strategies often feels like an uphill battle. As hardware vulnerabilities continue to get more complex and challenging for the industry, creating a common taxonomy for discussing, documenting and sharing hardware-based threats becomes paramount.

Let's work together as an industry to ensure that we are speaking the same language when it comes to researching and mitigating the hardware vulnerabilities of the future.

Long-term business success is rarely (if ever) a result of stumbling into opportunities and making makeshift decisions.

In cybersecurity, as in any other industry, one might start with a good idea and an adequate first realization of it, but if there is no plan for the future, there will be no desired future.

Things to keep in mind when raising capital for your cybersecurity venture

AUTHOR_ Mirko Zorz, Editor in Chief, (IN)SECURE Magazine

The cybersecurity industry

The advent of modern computer and digital information systems, their widespread use in all aspects of our private and business lives and endeavors and the fact that they have weaknesses that are exploited by malicious actors have spurred the creation and exponential growth of the cybersecurity industry. The latest bout of globalization, which coincided with the rise of IT, also played an important part.

Because of the steady introduction of new IT technologies, the cybersecurity industry continues to be open to newcomers with a good-enough product and plan. For most, that plan involves outside capital/strategic investment or an acquisition/merger at some point in the future.

In order to come to that point, a cybersecurity company must become an attractive target.

A good target for acquisition

Investors and acquirers generally look for companies that meet the following criteria: great team, great technology, great product market fit, strong customer traction, strong unit economics, and so on.

"Acquirers keep in mind additional considerations such as strategic fit with their product portfolio/roadmap, customer profile (both current and future targets), go to market/sales motions, potential cross-sell/up-sell opportunities, and more," noted Dino Boukouris, Founding Director at Momentum Cyber, which specializes in offering strategic advice for companies in the cybersecurity industry.

> *Getting an incredibly high valuation does not mean they have to (or should) take it.*

"These aspects also factor into the consideration of how feasible it will be to integrate the acquired company into the larger company's operations post-acquisition."

Though it might seem counter-intuitive, a cybersecurity company suffering a breach will not always be a deal-breaker for potential acquirers.

"For the most part it is assumed that a cybersecurity company selling cybersecurity products/services has a robust internal security program and any potential breaches would be a concerning signal for a potential acquirer (i.e., if a company cannot protect itself from a breach, why should a customer trust them to be a vendor in their security stack?)," he shared.

"That being said, valuation exercises aren't yet directly influenced by breaches in a formulaic manner. While a breach or any other type of liability for that matter would be disclosed during an acquisition, depending on the magnitude of the breach, associated response, and any potential future liability, it may or may not have a meaningful effect on valuation."

Raising capital for your cybersecurity venture

Strategic planning must address every aspect of the business. For best overall results, knowing how the market works and always thinking a few steps ahead is crucial.

To founders who find themselves at the strategic crossroads that is raising the next round of capital for their cybersecurity venture, Boukouris, who also teaches the Private Equity & Venture Capital course for MBA students at the University of California Berkeley – Haas School of Business, offers the following advice:

"Always consider that at each round you typically want a step up in valuation, which in turn brings in new investors at this higher valuation who will expect you to exit at an even higher valuation to make an exit worthwhile for them. This often raises the bar for the desired exit value by at least 2-3x at each round. As you raise the bar for an exit, your potential acquirer universe actually gets smaller and smaller since the number of companies who are able to do large deals naturally decreases as deal size goes up. Thus, you should evaluate all strategic options that are on the table every time you are raising their next round of capital, ensuring the risk

vs. reward profile of that next round is worthwhile for the company and for yourself as well."

Also: getting an incredibly high valuation does not mean they have to (or should) take it.

"While the thought of giving up a much smaller percentage of your company may seem appealing at the time of your capital raise, by doing so you'll only raise the bar that much higher when you go out for your subsequent round of capital," he explained.

"Future investors will expect that you've 'grown into' your (for lack of a better word) inflated valuation and will expect your company and associated operating metrics be solid enough to support this valuation. If they are not, you may have trouble finding new investors for the subsequent round, or you may have to raise the round at a decreased valuation (a 'down round') – both of which are worrisome outcomes."

Looking for strategic investors

Looking for strategic investors should be done well before you actually need them.

"Companies often think that they should search for strategic investors either concurrently with or after their search for a lead institutional investor. The reality is most strategic investors move quite slowly, and as such they often take a few months longer than a typical VC to make an investment in a company," he shared.

"Additionally, many companies don't get to know these strategic investors until they need them (meaning: until they are looking for funding). Instead, I always recommend reaching out to strategic parties well in advance of ever needing an investment to establish a relationship based on mutual strategic fit, thus organically starting the courting process months, if not years ahead of a potential investment."

Burner phones actually give attackers an opening to another, potentially more valuable, form of data: conversations that occur during key meetings in the vicinity of the device.

Burner phones are an eavesdropping risk for international travelers

AUTHOR_ Michael Campbell, Head of Government and Federal Business, Privoro

In recent years, burner phones have become an obligatory part of the international business traveler's toolkit. But though these devices are designed to minimize the amount of stored data available for capture by malicious actors in a foreign country, burner phones actually give attackers an opening to another, potentially more valuable, form of data: conversations that occur during key meetings in the vicinity of the device.

In this article, I'll explore the threat of mobile eavesdropping targeting the burner phones of executives and other corporate employees

traveling to high-risk countries and look at some mitigations for this emerging risk.

The evolution of technical eavesdropping

Though videoconferencing has made it possible for corporate executives to instantly traverse the globe, face-to-face meetings are still preferable for critical tasks like partnership discussions, sales and business development, corporate or legal negotiations, strategic planning, research-oriented conversations with colleagues, political meetings and more. In fact, these types of discussions are usually the main reason executives travel overseas in the first place. After all, the vast majority of people would spare themselves the time, money and hassle of international travel if they could get the same results with a video chat, a phone call or email.

Hacking the phone eliminates the need to use other techniques since executives voluntarily carry the spying device everywhere they go.

Within these sensitive, face-to-face meetings and conversations on foreign soil, an enterprise's most important information is often revealed, including information that hasn't yet been committed to writing. And corporate spies know this. In China, the epicenter of state-sponsored spying on foreign-owned businesses, spies have been known to bug conference rooms, hotel rooms, restaurants and even taxis. It's been alleged that Chinese spies have gone so far as to secretly plant listening devices inside the electronic key cards used to open travelers' hotel rooms.

Given that foreign spies have both the propensity to eavesdrop on conversations and the capability to do so via mobile spyware that remotely activates smartphone cameras and microphones, it's easy to understand why it happens – hacking the phone eliminates the need to use other techniques since executives voluntarily carry the spying device everywhere they go. Since burner phones are intended to provide a minimal data footprint in the likely event of compromise, they generally do nothing to mitigate the capture of data in vicinity of the device, including the sensitive conversations that occur in the closed-door meetings that brought the executive to the country in the first place.

The smartphone eavesdropping toolkit

Foreign security services have various means of screening incoming visitors and flagging CEOs and other corporate targets. Once the target is in country, there are a number of possible methods that intelligence agencies or sophisticated corporate competitors can take to install spyware on a target's burner phone, including examples such as these:

- **Malicious carrier updates:** In many countries, the entire telecommunications infrastructure is state-owned. The first time a targeted burner phone attempts to connect to a cellular network, spies can install spyware on that phone via a malicious carrier-level update.
- **Radio frequency (RF) hacking:** Airports, by design, have many chokepoints. In such close proximity to a user and their phone, it's possible to exploit Bluetooth and other RF vulnerabilities to install spyware.
- **Physical installation by customs agents:** If a traveler is chosen for secondary screening, their phone is often confiscated and examined. Physical access to a device opens up yet another avenue for device compromise and malware installation.
- **Fake cell towers:** It's also possible for spies to set up an IMSI catcher to simulate a cellphone base station. Once the burner phone connects to this fake cell tower, spies can perform spyware installations from the spoofed tower.
- **Infections via hotel WiFi:** As we saw with the DarkHotel spyware campaign, targeted business travelers can be infected through a hotel's WiFi network, typically via bogus software updates.

- **Evil maid attacks:** Hotel staff and government officials in China can access hotel rooms, including safes, to either install spyware directly onto the burner phone or use other techniques to compromise the phone.

Keeping private conversations private

Unfortunately, even savvy travelers who do the right things – disabling Bluetooth, not connecting to unknown networks, never leaving their phone out of sight – are still at risk of conversations being eavesdropped on through their burner phones. But instead of choosing a "dumb" phone or asking users to not bring their phones into critical meetings, security teams have the following options at their disposal for mitigating the risk of high-level conversations being captured.

- Invest in an anti-surveillance case for the burner phone that masks the surrounding audio in the vicinity of the phone, preventing spies listening on the other end from gaining any meaningful information.
- Purchase a burner phone that features a hardware kill switch for shutting off the microphones when not needed.
- If telephone calls aren't necessary, physically disconnect the microphones within the burner phone.

The theft of files and emails at the hands of foreign spies gets all the attention, but face-to-face conversations in the presence of a compromised smartphone can reveal information that's just as valuable. It's important for security teams to recognize this emerging threat and take the proper precautions.

Security world

Facial recognition hardware to reach over 800 million devices by 2024

A new report from Juniper Research found that facial recognition hardware, such as Face ID on recent iPhones, will be the fastest growing form of smartphone biometric hardware. This means it will reach over 800 million in 2024, compared to an estimated 96 million in 2019.

The new research, Mobile Payment Authentication: Biometrics, Regulation & Forecasts 2019-2024, however notes that the majority of smartphone facial recognition will be software-based, with over 1.3 billion devices having that capability by 2024.

This is made possible by advances in AI, with companies like iProov and Mastercard offering facial recognition authentication that is strong enough to be used for payment and other high-end authentication tasks.

Juniper Research recommends that all vendors embrace AI to drive further developments of capabilities and therefore increase customer acquisition.

Cyber attackers turn to business disruption as primary attack objective

Over the course of 2019, 36% of the incidents that CrowdStrike investigated were most often caused by ransomware, destructive malware or denial of service attacks, revealing that business disruption was often the main attack objective of cybercriminals.

Another notable finding in the new CrowdStrike Services Report shows a large increase in dwell time to an average of 95 days in 2019 — up from 85 days in 2018 — meaning that adversaries were able to hide their activities from defenders for longer, and that organizations still lack the technology necessary to harden network defenses, prevent exploitation and mitigate cyber risk.

Third-party compromises serve as a force multiplier for attacks. Threat actors are increasingly targeting third-party service providers to compromise their customers and scale attacks.

CIOs using AI to bridge gap between IT resources and cloud complexity

There's a widening gap between IT resources and the demands of managing the increasing scale and complexity of enterprise cloud ecosystems, a Dynatrace survey of 800 CIOs revealed.

IT leaders around the world are concerned about their ability to support the business effectively, as traditional monitoring solutions and custom-built approaches drown their teams in data and alerts that offer more questions than answers.

CIO responses in the research indicate that, on average, IT and cloud operations teams receive nearly 3,000 alerts from their monitoring and management tools each day. With such a high volume of alerts, the average IT team spends 15% of its total available time trying to identify which alerts need to be focused on and which are irrelevant.

This costs organizations an average of $1.5 million in overhead expense each year. As a result, CIOs are increasingly looking to AI and automation as they seek to maintain control and close the gap between constrained IT resources and the rising scale and complexity of the enterprise cloud.

How to govern cybersecurity risk at the board level

A report from University of California, Berkeley's Center for Long-Term Cybersecurity (CLTC) and Booz Allen Hamilton uses insights gleaned from board members with over 130 years of board service across nine industry sectors to offer guidance for boards of directors in managing cybersecurity within large global companies.

The report reveals that, while many boards regard cybersecurity risk as an "existential threat," they are not confident they have the information and processes in place to provide effective governance in this high-stakes area of oversight. Board members largely agree they are just getting started with oversight of cybersecurity and believe the cyber risk environment is not stabilizing or likely to do so in a predictable way over the next few years.

At the same time, boards are wrestling with difficult questions, including whether cyber risk should be addressed as a central part of overall business strategy discussions, and whether it should figure prominently in board-level investment or merger-and-acquisition decisions.

Fraud prevents a third of businesses from expanding digital capabilities

A recent report, conducted by Javelin Research, surveyed hundreds of respondents across the retail, restaurant, insurance, and financial industries and revealed more than 40% of businesses say fraud impedes their expansion into new digital channels and services. With the threat of emerging fraud and increasing expectations for a frictionless customer experience, businesses are challenged to balance revenue, expansion, and innovation priorities. Researchers found that 48% of consumers are more sensitive to anti-fraud measures that disrupt their online experience than they were a year ago. This means that retailers and restaurants have an increased imperative to balance fraud mitigation and customer experience.

NIST Privacy Framework 1.0: Manage privacy risk, demonstrate compliance

The NIST Privacy Framework is not a law or regulation, but rather a voluntary tool that can help organizations manage privacy risk arising from their products and services, as well as demonstrate compliance with laws that may affect them, such as the California Consumer Privacy Act and the European Union's General Data Protection Regulation. It helps organizations identify the privacy outcomes they want to achieve and then prioritize the actions needed to do so.

"What you'll find in the framework are building blocks that can help you achieve your privacy goals, which may include laws your organization needs to follow," said Naomi Lefkovitz, a senior privacy policy adviser at NIST and leader of the framework effort.

"If you want to consider how to increase customer trust through more privacy-protective products or services, the framework can help you do that."

Email security industry miss rates when encountering threats are higher than 20%

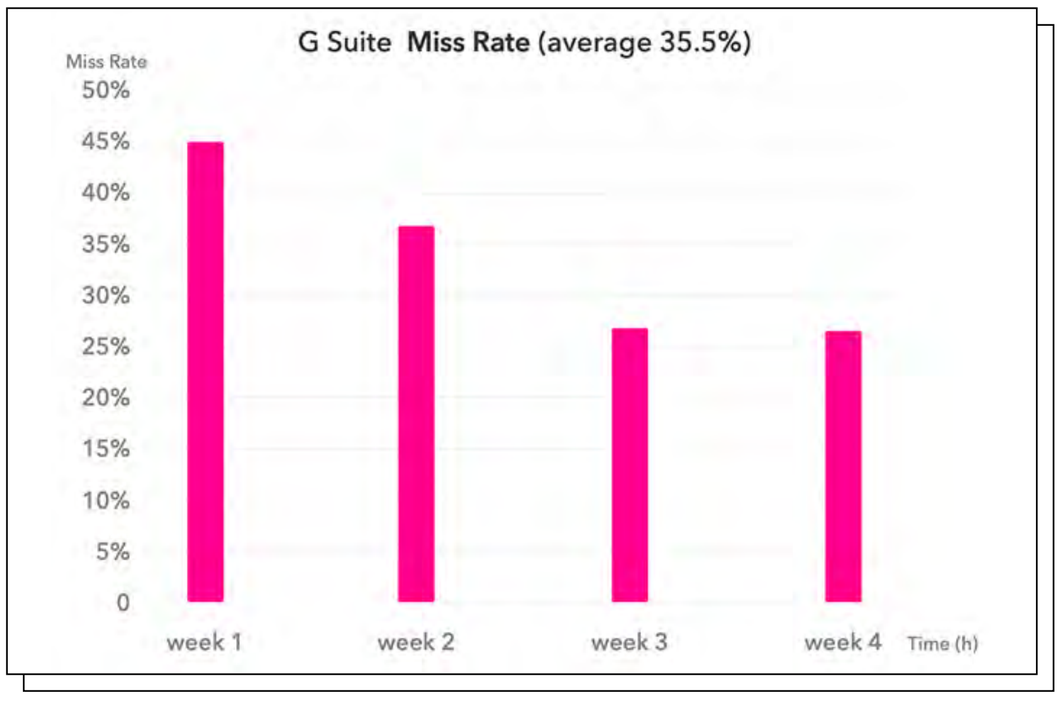
BitDam conducted an empirical study to measure leading email security products' ability to detect unknown threats at first encounter. Unknown threats are produced in the wild, sometimes hundreds in a day.

The study employs the retrieval of fresh samples of malicious files from various feeds and sources, qualifying them as unknown threats, and sending them to mailboxes protected by leading email security products. The miss rate at first encounter was then measured, as well as the Time to Detect (TTD).

According to the study's findings, for Office ATP, the miss rate over seven weeks in late 2019 was about 23% and the TTD average was about 48 hours. About 20% of missed unknown threats took four or more days to be detected. Office 365 ATP was "blind" to selected unknown threats it did not detect at first encounter.

For G Suite, the miss rate was 35.5% over four weeks in late 2019. The TTD average was about 26 hours with about 10% of missed unknown threats taking three days or more to be detected.

These massive detection gaps provide proof of how enterprises are often unprotected against unknown threats, which leads to successful email-based attacks such as ransomware, phishing, and malware.

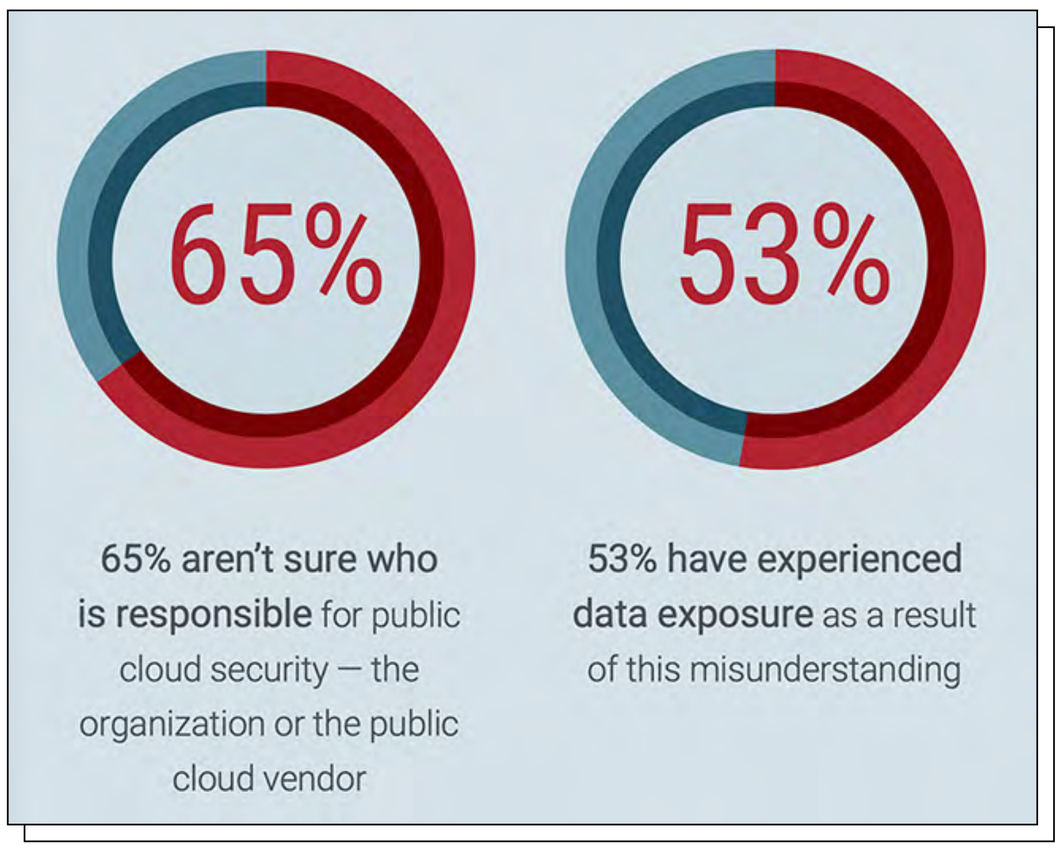


Companies increasingly reporting attacks attributed to foreign governments

More than one in four security managers attribute attacks against their organization to cyberwarfare or nation-state activity, according to Radware. In 2018, 19% of organizations believed they were attacked by a nation-state. That figure increased to 27% in 2019. Companies in North America were more likely to report nation-state attribution, at 36%.

As organizations adapt their network infrastructure to enjoy the benefits of these new paradigms (such as microservices and multi-cloud environments), they increase their attack surface and decrease the overall visibility into their traffic.

For example, 22% of respondents don't even know if they were attacked, 27% of those who were attacked don't know the hacker's motivations, 38% are not sure whether an IoT botnet hit their networks, and 46% are not sure if they suffered an encrypted DDoS attack.



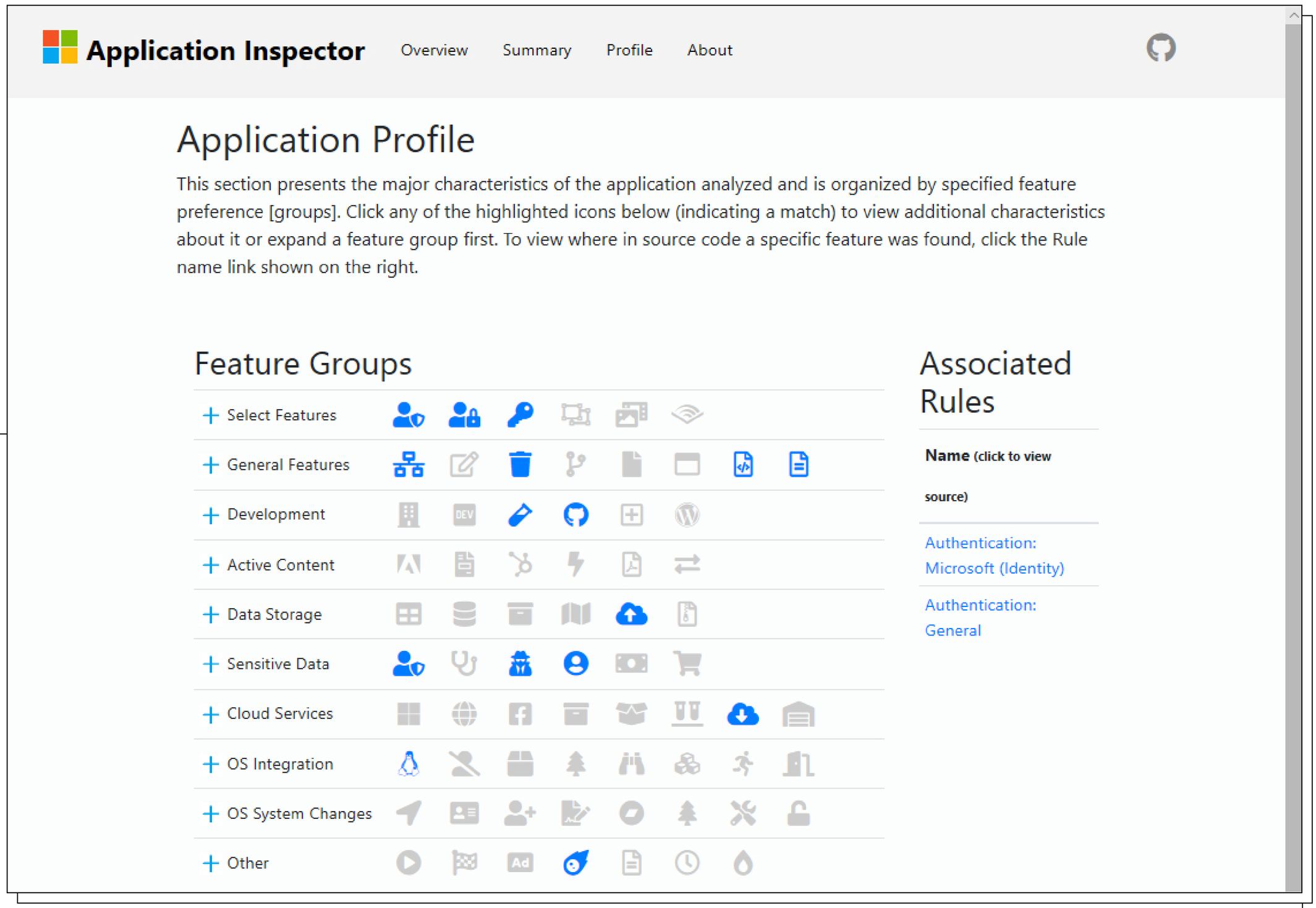
Researchers create OT honeypot, attract exploits and fraud

Trend Micro announced the results of research featuring a honeypot imitating an industrial factory. The highly sophisticated Operational Technology (OT) honeypot attracted fraud and financially motivated exploits.

The six-month investigation revealed that unsecured industrial environments are primarily victims of common threats. The honeypot was compromised for cryptocurrency mining, targeted by two separate ransomware attacks, and used for consumer fraud.

To better understand the attacks targeting ICS environments, Trend Micro Research created a highly realistic, industrial prototyping company. The honeypot consisted of real ICS hardware and a mix of physical hosts and virtual machines to run the factory, which included several programmable logic controllers (PLCs), human machine interfaces (HMIs), separate robotic and engineering workstations and a file server.

Trend Micro urges smart factory owners to minimize the number of ports they leave open and to tighten access control policies, among other cybersecurity best practices. In addition, implementing cybersecurity solutions designed for factories can help further mitigate the risk of attack.



Microsoft Application Inspector: Check open source components for unwanted features

Want to know what's in an open source software component before you use it? Microsoft Application Inspector will tell you what it does and will spot potentially unwanted features – or backdoors.

The Microsoft Application Inspector:

- Is a client .NET Core-based tool that can be run from a command line in Windows, Linux or macOS.
- Uses static analysis and a customizable JSON-based rules engine to analyze the target code. Users can add/edit/remove default rule patterns (there are over 500) as well as add their own rules.
- Is able to analyze code written in a variety of programming languages.
- Once the tool does its work, it generates a HTML "report" that shows the features, project summary and meta-data detected. JSON and TEXT output format options are supported for those who prefer them.

Each discovered feature can be broken down into more specific categories and receives a confidence indicator. Users can see for themselves the source code snippets that produced each "discovery".

Hardware hacks: The next generation of cybercrime

AUTHOR_ Nathan Palmer, Security Researcher, Raytheon's Cyber Offensive and Defensive group

Every 39 seconds there is a cyber attack affecting one out of three Americans. All organizations need to take proactive measures and think like the attackers that are infiltrating their networks.

Despite the fact that businesses around the world are deploying new cybersecurity tools to fend off these persistent attackers, cybercriminals are working around the clock to find new ways to get around them and compromise software and hardware.

Physical access requirements are a thing of the past. A somewhat recent example includes UEFI/BIOS implants, which were weaponized by nation-states and installed remotely by exploiting vulnerabilities in the underlying UEFI system. It's a form of cyber-espionage where attackers thrive off of access, stealth, and persistence to manipulate low-level software embedded in the hardware to gain control over the system. Once hackers gain control, they sit

and wait for the most opportune moment to create the most extensive destruction possible.

Specifically, hackers wait until they have the opportunity to infiltrate every facet of the system, without detection, in order to access as much valuable data as possible. Once they are in, they make it extremely difficult for the security team to track them, let alone remove them altogether.

> *Hardware has always been inherently trusted, meaning that the hardware design doesn't always include security features itself, but instead relies on higher level software to provide protections.*

The shift from physical to remote access hacking

Attackers have and always will go for the low-hanging fruit, the easiest point of access, whether it be on a weapons system, laptop, or automobile. In the past, they have primarily targeted the software running at the application layer such as email, web browsers, and development tools. One layer deeper, attacks take place on the operating systems, such as Windows, Linux, macOS, and iOS. Hackers are well aware that operating systems are often vulnerable to bugs, which makes infiltrating these systems even easier.

Developers have gotten more security savvy in the last five to 10 years and, as a result, so have their cybersecurity tools. As additional layers of protection have been added to the operating system, these once-considered "easy" attacks are now more difficult for cybercriminals. Once one method becomes harder, attackers then look for other - easier - ways to disrupt operations.

They bypass software and target hardware through the supply chain, insider threats, system updates, firmware updates and hardware errors. For example, Spectre and Meltdown are a trio of flaws that arose from features that are part of nearly every modern computer CPU and some CPUs as far back as 20 years. The consequences are very real.

Hackers can get access to memory, including passwords, encryption keys, or other sensitive information, by leveraging hardware design flaws to leak data between applications. Even mechanisms that are designed to prevent these vulnerabilities, such as allowing firmware updates for the CPU, can be used as "backdoors" that allow attacks against hardware. Organizations need to take proactive measures, like adopting a Zero Trust framework, to reduce the risk of a successful attack.

The strategy behind a Zero Trust cybersecurity approach is to trust no one and nothing and verify everybody and everything.

Hardware has always been inherently trusted, meaning that the hardware design doesn't always include security features itself, but instead relies on higher level software to provide protections. Unfortunately, if an organization falls victim to a hardware attack, there isn't much that can be done. Hardware hacks are often very difficult to detect as the payloads often sit quietly and wait for the best opportunity to spring into action. Organizations often don't know they have been hit until the hacker pivots from hardware to the OS and applications and the damage is already done.

A Zero Trust strategy gives organizations the ability to take action against this risk.

Hardware hacks: Plan A, when there isn't a Plan B

Because hardware hacks are so difficult to detect and mitigate it is important for organizations to do everything possible to thwart them.

The first priority is ensuring hardware verification is a top priority. Because hackers are able to mimic an admin once they have access, having a Zero Trust framework in place is a necessity. A Zero Trust approach leverages hardware root-of-trust solutions that enforce advanced security technologies in commercial systems in a way that prevents them from being disabled or bypassed, even by insiders or attackers that have administrator privilege on the system.

> *Because hardware hacks are so difficult to detect and mitigate it is important for organizations to do everything possible to thwart them.*

Software updates are an important part of a strong security posture, and this goes for hardware/firmware updates as well. Critical security patches should be applied as soon as possible to address evolving threats. Even in this process, back doors are created for firmware to act which increases the attack surface. Every update should be verified as authentic from a trusted provider, preferably by some cryptographic methods like signed packages. Organizations must also have a secondary process to independently verify the updates before they're applied.

No area of the security perimeter goes unnoticed by hackers, so organizations must ensure all equipment is protected. This means verifying that peripheral and support hardware – not just the obvious major targets – are protected from these attacks as well. Hackers get more sophisticated by the day.

The best crisis plan is one you never have to use, but it is critical that every organization has one in place. This is especially true with hardware hacking when a reactive approach is not an option. Knowing this will be our reality, we need plans, processes and tools in place to detect, protect and mitigate attacks.

California's IoT cybersecurity bill: What it gets right and wrong

AUTHOR_Charles Eagan, CTO, BlackBerry

California state lawmakers should be lauded for SB 327, their well-intentioned legislative attempt at tackling one of the most pressing issues in the tech sector: IoT security. But as the law went into effect at the start of the year, they will also (unfortunately) soon be faced with the reality that it is inadequate for today's security threat landscape.

The most significant issue to be addressed is the law's ambiguity.

To its credit, SB 327 – popularly known as the IoT security law – provides a good first step towards much-needed and extensive cybersecurity legislation: with an estimated 22 billion connected devices worldwide (and as many as 75 billion connected devices by 2025), the very existence of an IoT security law is encouraging. And further

praise is warranted because the scope of the bill includes all devices that can connect directly or indirectly to the internet, as well as all connected devices sold in California – not just manufactured there.

But ultimately, the specifics of SB 327 fail to fully support its good intentions, as rapid technological development has outstripped legislative intent. And while it's unlikely that legislation can fully catch up with cybersecurity development, the emphasis should be on incremental improvements – we must focus on the fruit we can reach, even as new buds sprout on higher branches. If some of these specific concerns are met, we can drive iterative advancements, and force IoT device manufacturers to invest the appropriate time and money into the security of their products.

In the interest of proactivity, what changes could be implemented to further strengthen this IoT security law?

The most significant issue to be addressed is the law's ambiguity: it requires all connected devices to have "a reasonable security feature" (appropriate to the nature of the device and the information it collects) that is designed to protect the user's data from unauthorized access, modification, or disclosure. Beyond that vague prescription, the law only specifically states that each connected device must also come with a unique hard-wired password, or it must otherwise require a user to set their own unique password before using the device.

Some experts maintain that meeting the password requirements is all that's needed to satisfy the regulation; in effect, the password is the "reasonable security feature." If this interpretation is validated, it's wholly insufficient for securing the IoT – especially for those connected systems that reside in our appliances, vehicles, and municipal infrastructures. And, if it's deemed that a simple password will not meet SB 327's requirements, it remains unclear what specific measures are necessary to meet the definition of a "reasonable security feature."

The law's terminology might have a saving grace, though: because the verbiage is so ambiguous, the bill could be subject to extensive amendments as cybersecurity deficiencies become clearer. So, in the interest of proactivity, what changes could be implemented to further strengthen this IoT security law?

First, the law should mandate that all data – both at rest and in transit – should be secured or encrypted. It should also specify security measures for data transport services.

Second, the law should require that all connected devices have updatable software and operating systems, and a commitment to deliver frequent updates – so that old vulnerabilities don't expose an entire network to an attack. Because malicious software and firmware updates are common attack vectors, software updates should also be required to use secure boot and code-loading operations. These systems use digital signatures to verify that the device software comes from a trusted source and has otherwise not been tampered with.

To ensure these specific advancements are included in future cybersecurity legislation, we must use the power of our collective wallets. As users and consumers of IoT devices, we can use our buying power to demand secure, trustworthy devices – and, in the process, demand that manufacturers build security into these devices from the very start, not as a last-minute, ineffective add-on. California SB 327 is a good start out of the gate, but further legislation – and our collective consumer voice – can help us win the race.

7 signs your cybersecurity is doomed to fail in 2020

AUTHOR_Marcus Chung, CEO, BoldCloud

While most enterprises have come to terms with the fact that a security incident is not a question of "if," but rather "when", many are still struggling to translate this into the right security architecture and mindset. FireEye's Cyber Trendscape 2020 report found that the majority (51%) of organizations do not believe they are ready or would respond well to a cyberattack or data breach.

Old security paradigms are predicted to force many victimized companies out of business. Will you be one of them?

Under an increasingly evolving threat landscape, old security paradigms are predicted to force many victimized companies out of business. Will you be one of them?

If you are guilty of these common mistakes, your cybersecurity may be doomed to fail in the year ahead:

1_You think your business is too small to be a target

Verizon's 2019 Data Breach Investigations Report revealed that 43% of all cyberattacks are aimed at small businesses. According to insurance carrier Hiscox, more than half of all small businesses suffered a breach within the last year and 4 in 10 have experienced multiple incidents. Further, the US National Cyber Security Alliance reports an estimated 60% of small companies go out of business within just six months of a cyberattack - illustrating the real-world consequences of inadequate cybersecurity measures.

> *Smartly allocate your security budget by focusing on the end goals.*

Businesses of all sizes need to make high-tech security a top priority in 2020. While many small business owners believe they can't afford to keep their companies safe, the cost of a breach can be significant. IBM reports that companies with less than 500 employees suffer losses of more than $2.5 million on average.

It's better to start spending a portion of that money on proactive security measures. Just remember that doubling your security budget doesn't double your security - it's not a one-for-one trade-off when it comes to cybersecurity investments.

Smartly allocate your security budget by focusing on the end goals - whether that be protecting client data, safeguarding intellectual property or avoiding network outages. This will help you prioritize your investments and make the appropriate business compromises between security, usability and cost.

2_You're unable to defend against zero-day, multi-vector or polymorphic attacks

Since the 1980s, we've seen an evolution of cyberattacks, which continuously force us to update the way we protect digital assets. First generation attacks included viruses and were mainly contained using anti-virus software.

In the 90s, threats became more sophisticated as hackers targeted networks - making firewalls an essential security defense. The 2000s ushered in the mass use of applications along with the exploitation of their vulnerabilities, which made intrusion prevention systems (IPS) popular. Starting in 2010, we began to see zero-day threats, which use highly evasive polymorphic content to bypass traditional defenses. Behavioral analysis tools have helped us tackle these threats.

Currently, we're witnessing the proliferation of large-scale and multi-vectored attacks, like WannaCry and NotPetya. In these attacks, hackers attempt exploits on multiple fronts -including network, cloud and mobile devices - at the same time. This makes cybersecurity much more complicated. Today, only 3% of the world is prepared to defend themselves from zero-day, multi-vector or polymorphic attacks.

Cybersecurity is not something that you can set once and forget about it. Cybercriminals keep gaining ground because they are financially incentivized and willing to innovate. As we enter 2020, expect to see even more sophisticated attacks, capable of causing more damage, while being much harder to defend against.

In response, you need to ramp up your defenses with multiple layers of modern cybersecurity solutions. There are potentially game-changing products in development, like autonomous security services and blockchain-based data breach protection, that deserve consideration as attack vectors evolve and these new technologies prove themselves enterprise ready.

3_You're drowning in data

Hunting for signs of an attacker on your network can be like searching for a needle in a haystack. In many cases, it takes companies months to detect a data breach. Obviously, you need data to find an attacker. But many companies go overboard by trying to capture everything, at enormous infrastructure and workforce cost, and then find they can't effectively analyze or operationalize that data in a crunch.

More than ever, your security team needs the right tools to detect and investigate critical security threats. This includes security software that provides tools for hunting and performing diagnostics as well as heuristics that study patterns. New adaptive security tools that use machine learning and AI can help you find attackers, halt their intrusion or the exfiltration of data within milliseconds and prevent the next attack.

Regulators are increasingly looking at third-party risks.

4_You don't have an incident response plan

Incident response plans provide a set of instructions that help IT staff detect, respond to and recover from network security incidents. IBM found that companies with an incident response team that also extensively tested their incident response plan experienced $1.23 million less in data breach costs on average than those that had neither measure in place.

Your incident response plan should address issues like cybercrime, data loss and service outages that can threaten to disrupt daily business operations at a high cost to the business. If you don't have an incident response plan, it's time to develop one.

SANS Institute's Incident Handlers Handbook is a good place to start. It provides an overview of the six steps that should be taken by your incident response team to effectively handle security incidents.

5_You aren't taking third-party risk seriously

The weak link in your enterprise security may actually be your partners and suppliers. Supply chain attacks, also called value-chain or third-party attacks, occur when someone infiltrates your system through an outside entity that has access to your systems and data.

Human error still remains one of the greatest threats to your organization's well-being.

Breaches originating from a third-party cost companies $370,000 more than average. According to Ponemon, 56 percent of organizations have had a breach that was caused by one of their vendors. Meanwhile, the average number of third parties with access to sensitive information is increasing.

In response, regulators are increasingly looking at third-party risks. Last year, New York State financial regulators began requiring financial firms with a presence in New York to ensure that their suppliers' cybersecurity protections are up to par. Next year Europe will do the same.

To protect your company and avoid any penalties, you will need to closely vet the security of the companies you do business with in 2020, align your security standards and actively monitor third-party access.

6_Security is not a boardroom imperative

The size of fines assessed for data breaches in 2019 suggest that regulators are getting more serious about punishing organizations that don't properly protect consumer data. In the UK, British Airways was hit with a record $230 million penalty, while Equifax

agreed to pay a minimum of $575 million for its 2017 breach in the US.

With the industry calling for an Americanized version of Europe's GDPR, businesses should be prepared for the pace and size of fines to increase in 2020. With the cost of fines rising, security will forcefully become a mainstream issue.

If your board hasn't already taken notice of the evolving cybersecurity and regulatory landscape, they should. According to research by Infosys Knowledge Institute, 48% of corporate boards and 63% of business leaders are actively involved in cybersecurity strategy discussions.

In response, the CISO role must evolve from squeaky wheel to strategic advisor. Security leaders must be ready, willing and able to assemble and execute a sound security strategy that includes the right talent, services and technologies to defend against today's sophisticated threat environment.

7_Your employees aren't held accountable for cybersecurity

Human error still remains one of the greatest threats to your organization's well-being. With just 3 in 10 employees currently receiving annual cyber security training, it's all too easy for enterprising con artists or email scammers to circumvent even the most cutting-edge digital safeguards.

Ninety-one percent of all company breaches come from phishing. While email security tools can provide a first line of defense against phishing, the best way to prevent a phishing breach is to treat cybersecurity as workplace culture issue, rather than an IT issue.

For this type of cybersecurity initiative to be a success, you must not only weave good security habits into the fabric of your organization, but also hold employees accountable and responsible for corporate security. Formal security training programs can help teach employees how protect themselves and the company against cyberattacks but changing the attitudes and habits of your workforce can be more challenging. For this you will need to properly leverage change management models to successfully build an all-inclusive security culture.

Conclusion

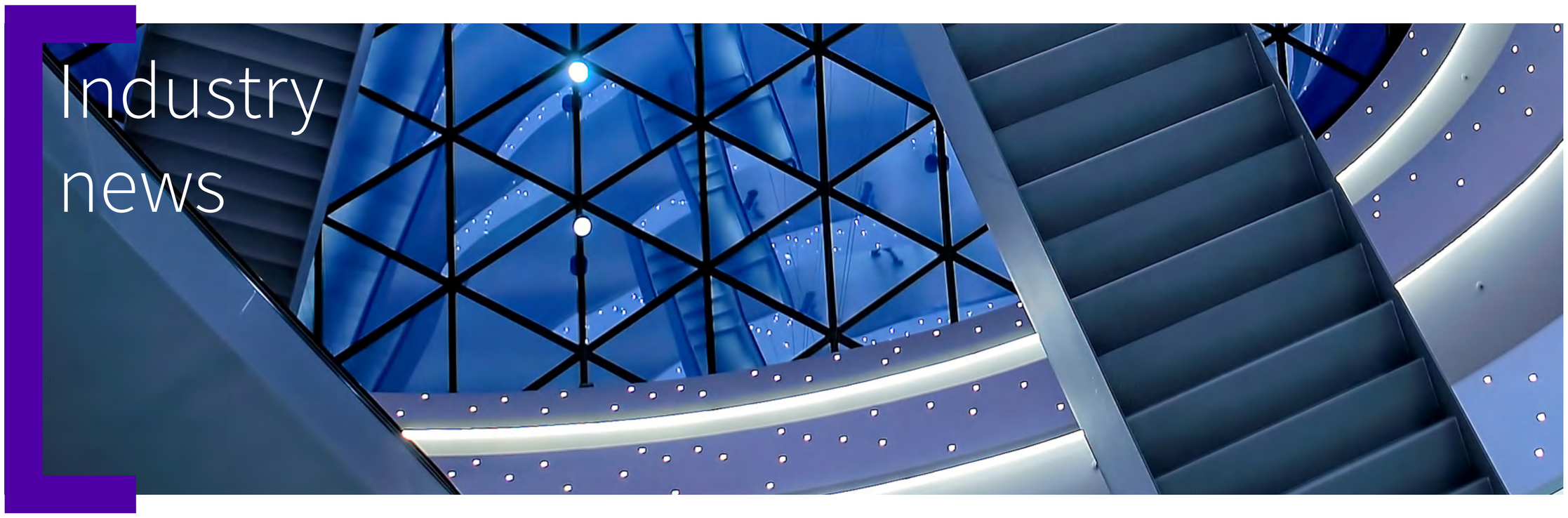
Attackers are getting smarter, attacks are occurring faster and incidents are becoming more complex. It's now guaranteed that virtually every modern organization's high-tech perimeters will eventually be breached. If you are still haphazardly or reactively approaching security with disconnected point tools, manual processes and inadequate staffing, be prepared to spend most of 2020 fighting cybersecurity fires.

As we move into an era of increasing connectivity, cybersecurity is a business-critical, extremely dynamic, massively scalable and highly specialized discipline. In 2020, you must be prepared to embrace AI and autonomous services, implement real-time cybersecurity tools and encourage every person on staff to play a role in combating online threats.

As cybercriminals become more innovative, make sure your executive team is aware of the full financial and operational impact that a data breach can have—and be ready to present a clear cut strategy on how to manage the risk using a multi-faceted approach to cybersecurity that leverages a robust set of adaptive security measures.

Your strategy should include a range of measures—with security software, vulnerability management and employee training topping the list of ways your organization can increase its resilience against cyberattacks in the year and years ahead.

Industry news



Cloudflare for Teams: Protecting corporations without sacrificing performance

Cloudflare for Teams is a set of solutions that will secure corporations and their employees globally, without sacrificing performance. Cloudflare for Teams is centered around two core products: Cloudflare Access and Cloudflare Gateway. Cloudflare Access is a Zero Trust identity and access management solution that secures, authenticates, and monitors user access to ensure that employees and devices are who they say they are. To do this, Cloudflare is working with identity providers, including Okta, OneLogin, and Ping Identity.

Cloudflare Gateway is a new solution being developed that will secure and filter outbound Internet traffic to protect employees from threats on the public Internet. Gateway will also ensure that Internet-browsing employees don't bring malware or vulnerable code into the organization.

CyberArk's new just-in-time access capabilities help reduce risk and improve operational efficiency

CyberArk unveiled new just-in-time access capabilities that help reduce risk and improve operational efficiency as organizations implement broader least privilege strategies.

Some privileged accounts are granted standing, "always on" access despite only requiring access for brief periods of time – increasing the attack surface. This is particularly true in the case of SSH keys, which are often mismanaged and easily compromised. New CyberArk capabilities feature short-lived SSH certificate authentication to secure access to existing or newly created instances in Linux systems without the need to manually manage accounts and credentials.

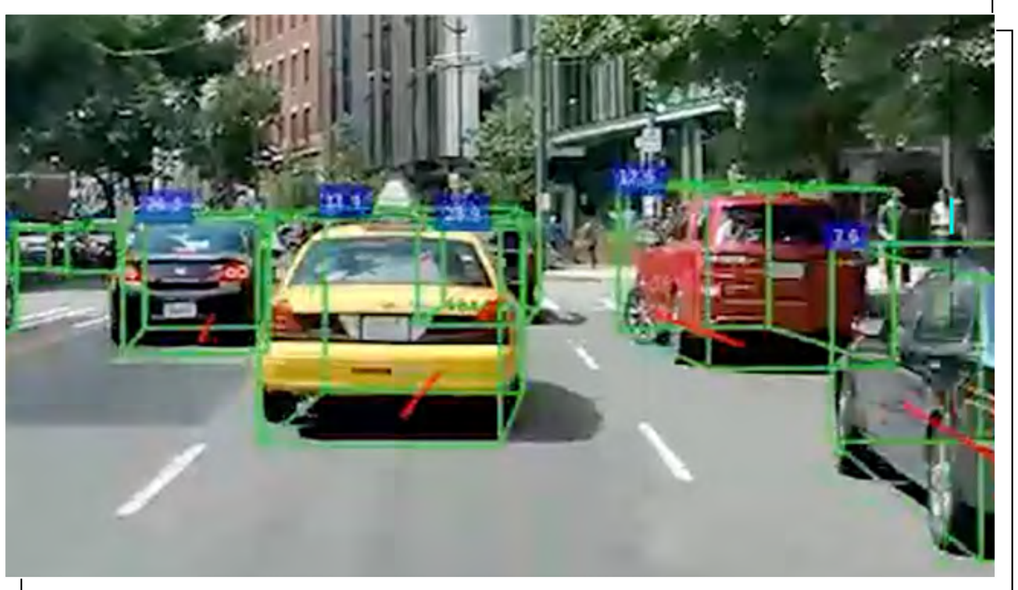
Skyview Capital acquires Fidelis Cybersecurity to expand portfolio and accelerate growth

Global private investment firm Skyview Capital has added to its software technology portfolio with the acquisition of Bethesda, MD-based Fidelis Cybersecurity from a consortium of investors in a stock transaction.

"We see a great opportunity to continue evolving our solution that will further differentiate us by providing a holistic approach to keeping organizations safe in an increasingly threatening environment," said Nick Lantuh, President and Chief Executive Officer of Fidelis Cybersecurity.

3D sensing platform for access control and smart video security announced

The Ambarella CV25 AI vision SoC powers depth processing, anti-spoofing algorithms, 3D facial recognition algorithms, and video encoding on a single chip, significantly reducing system complexity while improving performance.



Ambarella's CV25 chip includes a powerful ISP, native support for RGB-IR color filter arrays, and advanced high dynamic range (HDR) processing, which results in exceptional image quality in low-light and high-contrast environments. CV25's CVflow architecture delivers the computational power required for liveness detection and 3D face recognition, while running multiple AI algorithms for advanced features such as people counting and anti-tailgating. CV25 includes a suite of advanced security features to protect against hacking including secure boot, TrustZone, and I/O virtualization.

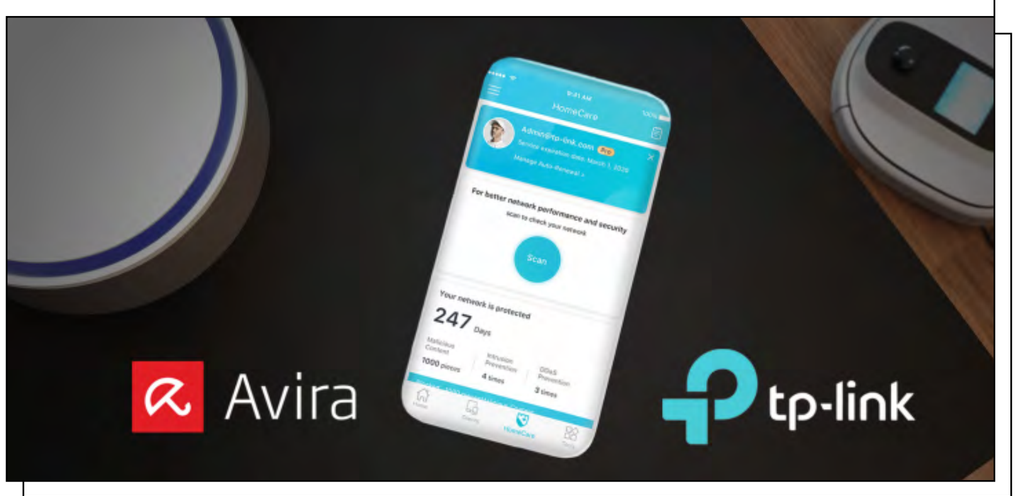
Fingerprint Cards adds two capacitive touch sensors to its fingerprint authentication portfolio

The FPC1020 and FPC1024 touch sensors feature high biometric performance and a small physical footprint. They are water resistant and can be used by devices and applications where a secure and smooth way to authenticate users is desired. The sensors have low power consumption and come with features for an excellent everyday user experience.

Stellar Cyber's new app applies machine learning to firewall data to spot anomalies

With Stellar Cyber's Firewall Traffic Analysis (FTA) Application, security analysts get an automated assistant to detect firewall misconfigurations, malicious users and abnormal traffic to gain new value from firewall data, typically improving analyst productivity over 20x. The FTA Application supports firewalls from many vendors including Cisco, Check Point, Fortinet, Palo Alto Networks and Sophos.

TP-Link HomeCare Pro: A smart home IoT security solution powered by Avira



Powered by Avira, Homecare Pro can identify smart home devices and check to determine if they are safe. Users will be notified if a related security function needs to be enabled or optimized to protect not only endpoints like laptops or smartphones, but also IoT devices like smart bulbs, smart thermostats, smart plugs and more.

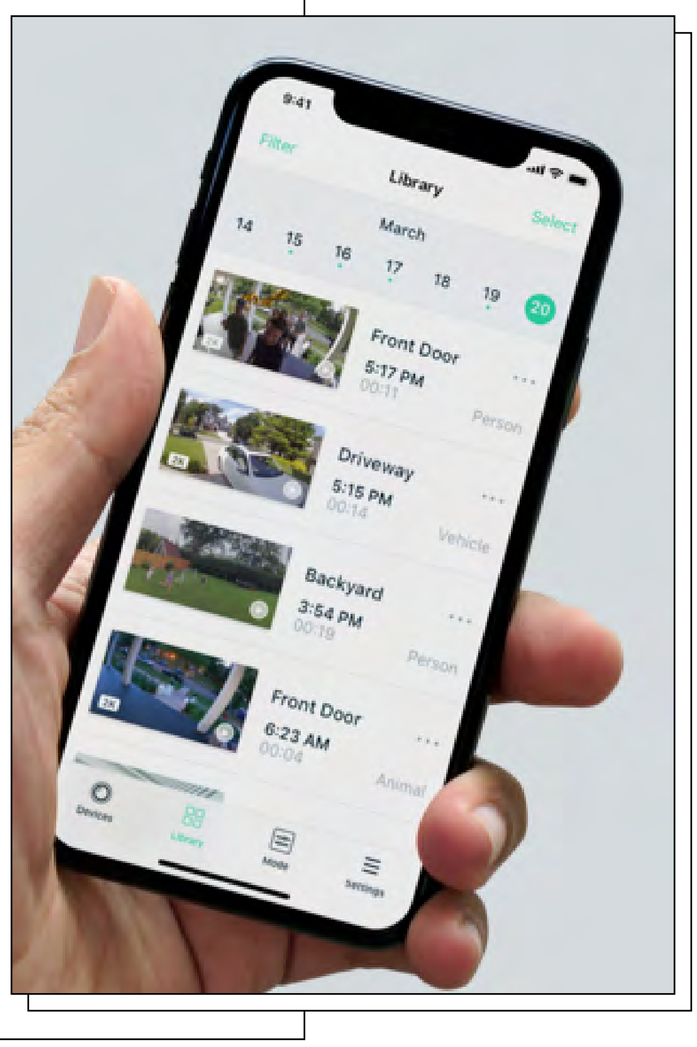
Waterfall Security Solutions secures significant new funding round

Waterfall Security Solutions, the OT security company, announced a major expansion into new markets and industry verticals. In support of this expansion, Waterfall has secured a significant new funding round to enable aggressive growth.

Waterfall's priorities for expansion are rail transport and Building Automation System markets for large facilities, including airports, casinos and large government installations. Waterfall reports several tier-1 customers in these arenas already, in addition to a large installed base in existing markets, including electric power, oil & gas, and critical infrastructures across the globe.

Arlo SmartCloud: A SaaS solution securing cloud services for businesses

Arlo SmartCloud is a fully managed global platform built for security, scalability and reliability that can be deployed as part of subscription services for hardware companies, automotive companies, service providers, insurance companies, home builders, smart communities, smart cities, traditional security companies, and other related verticals.



GoSecure adds Insider Threat Detection and Response to its portfolio

Offering more than 50 unique insider threat event types, GoSecure Insider Threat Detection and Response provides almost unlimited flexibility in creating the exact rulesets required for any organization. By combining personnel with actions, the solution can detect user behavior and respond immediately with a variety of potential actions.

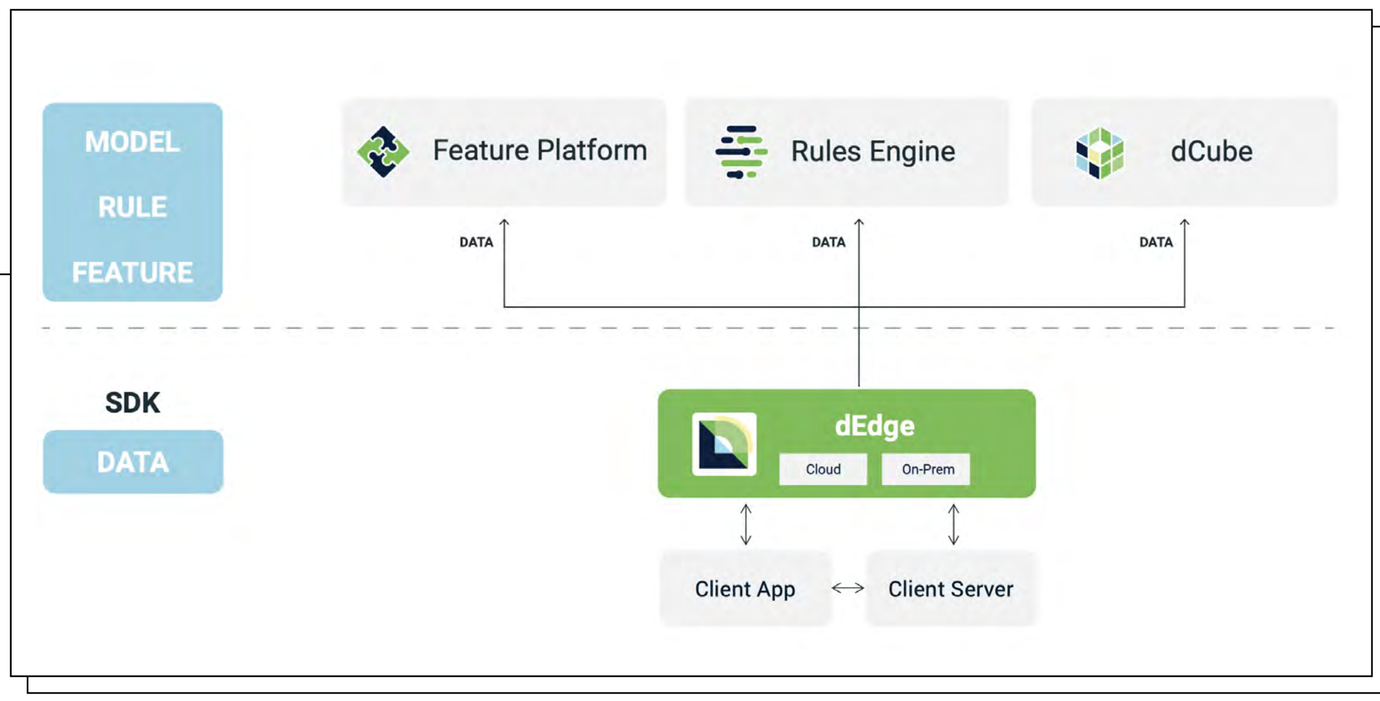
STEALTHbits StealthINTERCEPT 7.0 strengthens enterprise passwords and AD security

The latest enhancements delivered in StealthINTERCEPT 7.0 aim to provide organizations advanced capabilities to thwart attacks against AD and provide progressive password policy and complexity improvements that boost security without causing poor user and administrator experiences. The solution can now detect successful and failed Kerberos pre-authentication events in order to provide security analysts visibility into nefarious activities.

Micro Focus AD Bridge 2.0: Extending security policies and access controls to cloud-based Linux

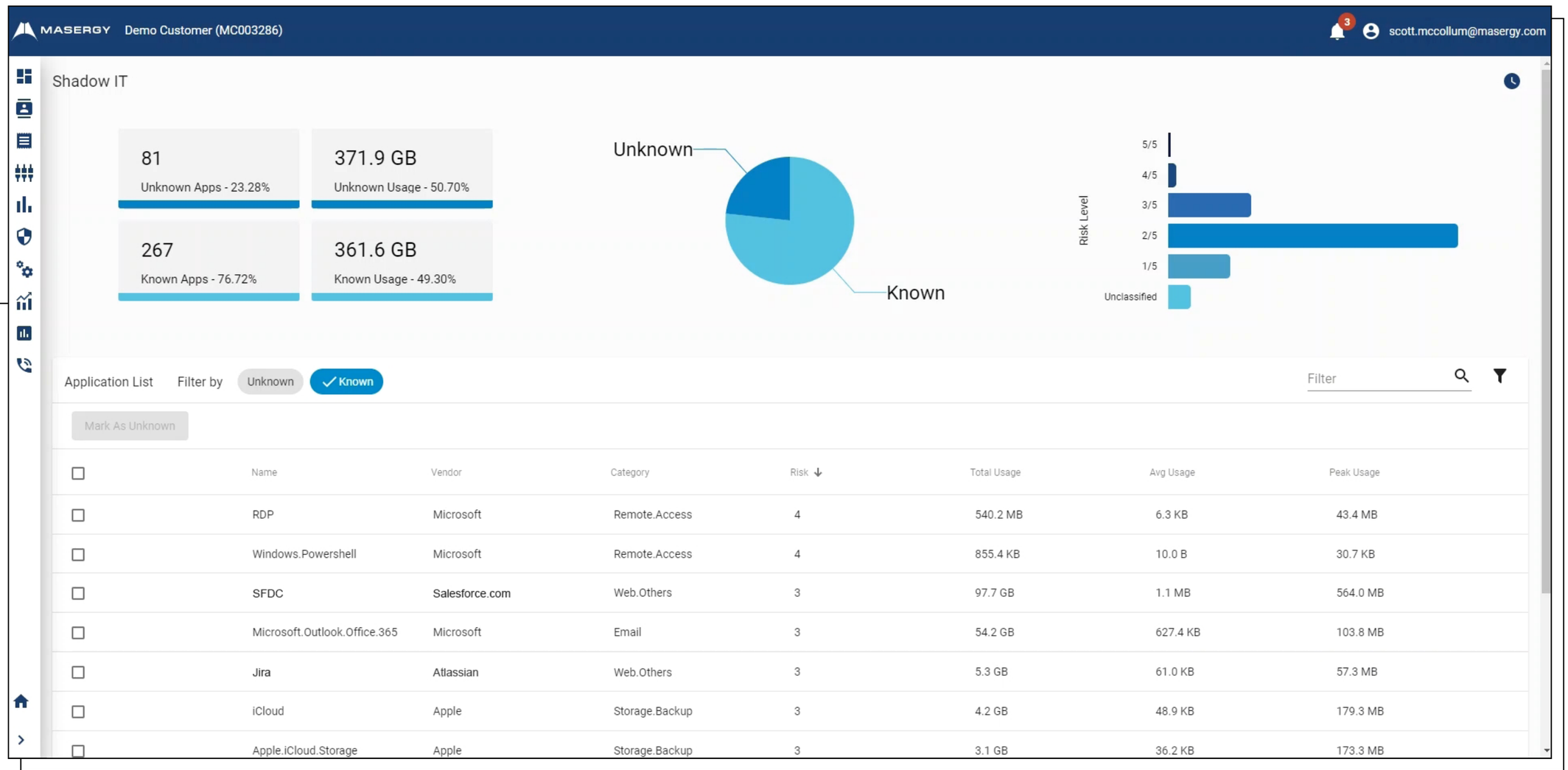
Micro Focus AD Bridge 2.0 offers IT administrators the ability to extend Active Directory (AD) controls from on-premises resources, including Windows and Linux devices to the cloud – a solution not previously offered in the marketplace.

With AD Bridge 2.0, organizations can leverage existing infrastructure authentication, security as well as policy, in order to simplify the migration of on-premises Linux Active Directory to the cloud, resulting in fully secured and managed Linux virtual machines in the cloud.



DataVisor dEdge: Uncover known and unknown attacks early

DataVisor dEdge is an anti-fraud solution that detects malicious devices in real-time, empowering organizations to uncover known and unknown attacks early, and take action with confidence. dEdge provides complete visibility into digital attacks, generating unique device IDs and accurate fraud scores – no matter how fraudsters manipulate devices.



Masergy Shadow IT Discovery: Automatically identify unauthorized SaaS applications

Masergy Shadow IT Discovery immediately scans and identifies all applications, providing clients visibility through the SD-WAN management portal. Until now, IT departments have had to rely on a variety of endpoint security solutions and guesswork to access this information. The time savings and decreased threat exposure will help IT organizations increase their security posture and keep up with the blind spots created by unsanctioned usage.

Vicarius raises $5 million to accelerate international growth and operating scale

Vicarius announced seed funding of $5 million. Founded in 2016, by Michael Assraf, Roi Cohen and Yossi Ze'evi, Vicarius is the first cybersecurity platform globally to empower companies with proactive attack mitigation strategies for software vulnerabilities in real-time. Vicarius detects exposures in software before hacks occur and offers customers built-in solutions and prioritization tools in a functional "risk-snapshot" dashboard to securely reinforce threat zones.

OneLogin launches Trusted Experience Platform, a complete IAM solution for enterprises

OneLogin introduced the Trusted Experience Platform, an identity foundation that enables companies to provide secure, scalable and smart experiences. The platform is a complete identity and access management (IAM) solution that leverages OneLogin's investment and expertise in AI, seamlessly managing all of an enterprise client's digital identities for its workforce and customers.

How to test employee cyber competence through pentesting

AUTHOR_ Michael Schenck, Director of Security Services, Kaytuso

Social engineering hacking preys on the vulnerabilities inherent in human psychology.

Take the Nigerian (419) scams as an example: the scammer tries to convince the victim to help get funds out of their own country into a safe bank by offering a percentage of the money for their participation. While senders of “Nigerian prince” emails have been scamming people for decades, people still regularly fall for it.

If they’re not properly trained and educated on their role and cybersecurity responsibilities, employees pose a huge threat to their organization and it is therefore vital for organizations to test employee cyber competence. To weed out the vulnerable workers that may require extra learning, organizations can utilize social engineering pentesting.

Employees are the first line of defense

Your employees are truly the first line of defense to keeping your company safe and secure. Employees need to understand how their personal social media habits and information oversharing can have a direct impact on the safety of their companies. With the amount of information shared on platforms such as LinkedIn, Facebook, Twitter, and Instagram, hackers can gather enough of it to build trust with the victim or even assume the identity of someone in their social circle.

Employees also often lack the knowledge to identify cyber threats. Phishing emails, tailgating, and baiting may seem legit to an employee who has no reason to be skeptical. Why wouldn’t they open an email from their boss on vacation, asking them to transfer money for him/her? Why wouldn’t they open the door for a colleague who happened to leave their keycard at home that day?

Social engineering hacks infiltrate organizations by "hacking" the human brain and taking advantage of its vulnerabilities. Without a general understanding and training on how to identify cyber threats, employees will remain a target for cybercrime.

Make employee training a priority

Seek out comprehensive training services to prepare your employees to recognize and avoid the latest cybersecurity threats. You'll want to find a cybersecurity training program that addresses your organization's vulnerabilities and risks. Organizations in different industries have different needs and compliance standards.

> *The training program that focuses on your industry should also be customizable so that it can be adapted to an employee's role within the company*

For example, law firms and others in the legal services field have strict, mandated compliance requirements regarding both the handling of paper documents and digital security. Custom employee training programs for legal services will help staff adapt to the latest technologies and reduce liabilities with best practices in data hygiene and physical security.

The training program that focuses on your industry should also be customizable so that it can be adapted to an employee's role within the company (e.g., paralegals must beware of spoofed emails from court systems, wait staff at a restaurant should focus on credit card theft or identify fraud, and financial advisors need to be cautious when wiring money to and from their clients' accounts).

Another crucial aspect of employee cybersecurity training is teaching your staff the importance of digital hygiene and how to keep their online data organized, safe, and secure from outside threats. This can be established through digital hygiene practice and data-loss prevention methods. Educate your employees on the value of information and how to properly share it at different levels - this will help protect against accidental disclosures.

Going back to oversharing on social media: training can help employees better understand social media hygiene and better gauge when and where it is appropriate to share personal information. If employees are aware of how the information they post can be used, they'll be less likely to make that information so easily accessible to hackers.

One-time-training isn't going to cut it. Frequent training sessions for employees are crucial to highlight new social engineering hacks flagged by experts as well as to keep best practices fresh in employees' minds. Regular sessions keep information active in the brain and not pushed to long-term memory.

Also: non-technical employees will absorb more information via 5 to 10-minute-long micro-training sessions than via the typical annual one-hour training session.

> *Hiring an outside penetration testing firm to run your security preparation through the paces is ideal since a third party can bring to light issues that may be in your company's blind spot.*

Test employee cyber competence

Your employees have gone through training programs and are more aware of their responsibilities. It's time to put them through the

test. You can do this by utilizing social engineering pentesting to evaluate your employee's level of cyber awareness through simulations. Hiring an outside penetration testing firm to run your security preparation through the paces is ideal since a third party can bring to light issues that may be in your company's blind spot.

The value of social engineering pentesting is that it will uncover security weaknesses in the following areas:

- Physical security (of the entire building)
- Corporate security policies regarding proper usage and disposal of sensitive data
- Employees' security awareness and implementation – you will discover whether the staff needs additional security training

> *Pentesting also provides valuable metrics – education and training without metrics fail to show whether people are learning and putting what they've learned to use.*

Social engineering pentesting can be used on your employees, either offsite or on-site. Offsite testing is designed to make employees divulge information intended for internal use only. You can attempt to compromise employees through phone phishing, email phishing or SMS phishing. A pentester can send employees an email with a link to files containing malware. For example, staff members may receive an email that informs them they've won a vacation. If they click on the link, they give the pentester access to the target's corporate account. A test of this nature will provide the organization with analytics on how many employees clicked the link and which employees are the biggest threat to company security.

On-site penetration testing includes various techniques aimed at gaining physical access to the office of the target company. This can include impersonation of employees or clients, dumpster diving, and physical honey pots. One way to test employee cyber competence through this method is to try out impersonation. Have a pentester impersonate a tech support worker to gain access directly to the company's network. The pentester can launch a USB thumb-drive on the target computer and compromise the company within seconds. Employees that were easily tricked can get additional training.

Take a dumpster dive into your employee's trash bins. Have they left printouts and pieces of paper with critical information? Was the paper shredder not used to get rid of data? This is an effective way to see which employees may not be cautious with sensitive corporate information.

Takeaway

You may think your organization is safe, but it only takes one individual to jeopardize the security of the whole company. Social engineering pentesting is an efficient way to identify where your employees stand when it comes to cybersecurity best practices. Making employees aware is the key, and results from pentests can help drive this awareness.

Pentesting also provides valuable metrics – education and training without metrics fail to show whether people are learning and putting what they've learned to use. Testing employees when they don't know they're being tested enables real insight into their cyber awareness and how you can best train them. With your employees being your biggest cybersecurity vulnerability, training is the most cost-effective way to safeguard your organization.

RSA® Conference 2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

EXPLORE THE HUMAN ELEMENT OF CYBERSECURITY.

What's the most important weapon in the fight against cyberthreats? New software? Faster equipment? Smarter computers? At RSA Conference, we believe it's people.

Attend RSA Conference 2020, February 24-28, and join thousands of security professionals, forward-thinking innovators and solution providers for five days of actionable learning, inspiring conversation and breakthrough ideas.

Register today to save your spot at the world's most comprehensive cybersecurity event.

rsaconference.com/helpnet-us20

#RSAC

FOLLOW US

To cope with increasing populations and tightening budgets, civic managers are looking at better ways of doing more with less through automation technologies.

Smart cities are on the rise: What are the dangers?

AUTHOR_ Galina Antova, Chief Business Development Officer, Claroty

A combination of job prospects, local amenities and other attractions is drawing more people to city living than ever before. Indeed, the UN estimates that by 2050 two-thirds of the global population will be living in cities, up from just over half currently. At the same time, central governments' investment for urban areas continues to shrink, with UK cities being on "life support" due to lack of funding from Westminster (for instance).

To cope with increasing populations and tightening budgets, civic managers are looking at better ways of doing more with less through

automation technologies. While the creation of these “smart cities” has the potential to drive efficiencies and improve services, their implementation needs to be coupled with robust cybersecurity solutions and practices to mitigate the vulnerabilities that would make them attractive targets for threat actors.

In addition to the physical impact of a cyber attack, these systems run on a significant amount of data, including personal information, which presents another tempting target for thieves.

What’s at risk?

Frost and Sullivan has predicted that there will be at least 26 fully fledged major smart cities around the world by 2025.

Tempted by the possibilities of being able to remotely control and monitor assets and processes throughout their districts, city administrators are implementing smart technologies across a whole host of services. These include street lighting, transportation, traffic control and utilities.

However, through greater connectivity comes greater risk and the results of a successful cyber attack on smart city infrastructure can be catastrophic. For instance, an attack against a city’s electricity grid could knock out power for an extended period resulting in businesses not being able to operate and residents having to be without heating, lighting and cooking facilities.

Another example: IoT sensors used to notify refuse collectors when to pick up waste could be taken down and rubbish could end up piling up for weeks at a time and creating a public health risk.

In addition to the physical impact of a cyber attack, these systems run on a significant amount of data, including personal information, which presents another tempting target for thieves.

How severe is the threat?

Attacks against the IT systems of public sector authorities are happening almost continuously, with UK councils being hit by 800 every hour (according to a freedom of information request submitted by Gallagher Insurance Brokers). This should be cause for concern to those in charge of smart cities as once a threat actor has infiltrated the IT environment, they could move laterally into an OT system if they are not properly segmented from each other.

While such an attack against an OT network has not yet affected the infrastructure of a smart city on a wider scale, businesses in the industrial sector have witnessed them to their cost. The likes of WannaCry and NotPetya infected production environments via the IT systems of companies including Merck and Renault, severely disrupting operations.

Unfortunately, risks are seemingly built into connected city systems. For instance, there are vulnerabilities inherent in the operating systems used in the OT and IoT devices common in smart cities. One such example is IPnet, an old TCP/IP stack that has not been supported since 2006 but is still being used in real-time operating systems, leaving them open to attack. Further, those designing the architecture of smart devices look to make them as lightweight as possible, meaning that security is often an afterthought.

Security teams need to know every detail about everything on their networks from make and model of a device through to IP address, patching schedule and risk level.

These risks are magnified by the fact that there are potentially hundreds of thousands, if not millions, of devices connecting to the OT network, all of which increase the attack surface for threat actors. The advent of 5G is adding to this, offering not only IoT devices new and better ways of connecting to the OT network, but cybercriminals too.

Mitigating the risks

To ensure they reap the benefits of creating smart cities without putting the safety of infrastructure, data and citizens at risk, city administrators must take a cybersecurity-first approach. They need to recruit and train security specialists who understand the different requirements for managing and protecting IT and OT networks.

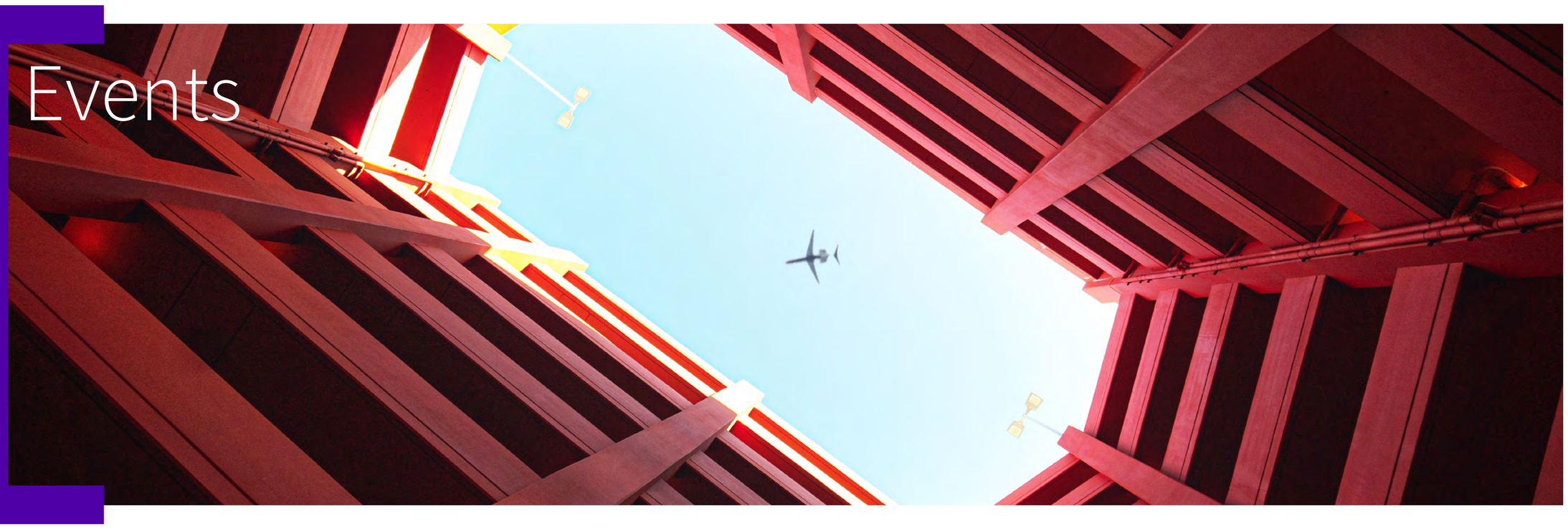
To be effective, automated monitoring should run continuously 24/7, providing security teams with contextualized alerts that are prioritized based on how urgently they need to be acted upon.

City administrators should also look to implement robust processes and invest in the right technologies. Such technology should offer total visibility of what is running on a city's network, as this is vital to keeping it safe. After all, you cannot protect something if you don't know it's there. Security teams need to know every detail about everything on their networks from make and model of a device through to IP address, patching schedule and risk level. Armed with this information, security professionals will be able to see where the vulnerabilities are on their networks and take steps to remove them. In OT and IoT environments this can only be achieved through specialized solutions that are able to recognize the unique communication protocols used in production networks.

There is also the need to know how every asset on the network should behave when functioning normally. This will enable any unusual activity to be detected and acted upon. To be effective, automated monitoring should run continuously 24/7, providing security teams with contextualized alerts that are prioritized based on how urgently they need to be acted upon. In this way, security teams will have all the necessary information they need to deal with potential risks in order of severity, cutting down on the number of hours wasted in investigating low-level risks or false positives.

Ultimately "smart" cities need to think of themselves as "cybersecurity" cities, building security into their OT networks, in the same way they build safety into their road networks.

Events



RSA Conference 2020

February 24-28, 2020
Moscone Center, San Francisco, CA, USA
http://helpnet.pro/rsaconf2020

Expert-led track sessions. Thought-provoking keynotes. Cutting-edge innovation. Valuable networking opportunities. RSA Conference is where the world talks security, and you can be a part of this important conversation.

Join industry leaders and peers at RSAC 2020 in San Francisco, February 24 – 28. Learn about the latest trends that are most relevant to your needs while helping to shape the future of the industry.

HITB Security Conference Amsterdam 2020

April 20-24, 2020
NH Kasnapolsky, Amsterdam, The Netherlands
https://conference.hitb.org/hitbsecconf2020ams/

HITBSecConf is an annual must attend event in the calendars of security researchers and professionals around the world. It is a platform for the discussion and dissemination of next generation computer security issues.

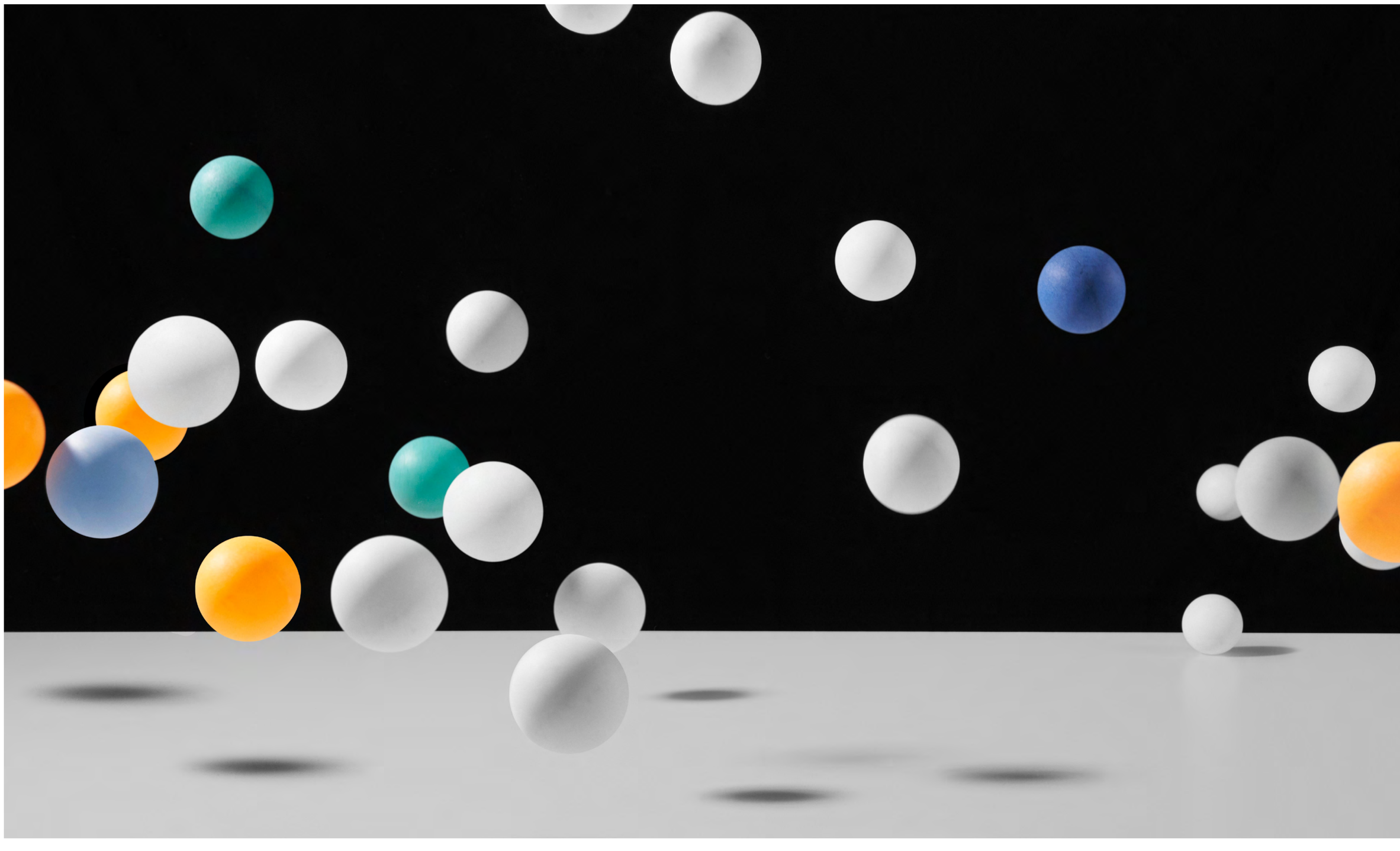
The event features two days of trainings and a two-day multi-track conference with cutting-edge technical talks delivered by some of the most respected names in the computer security industry. HITBSecConf is a place where ideas are exchanged, talent discovered and genius celebrated.

SOAR without limits

Think you can't have it all? With Swimlane's security orchestration, automation and response (SOAR) solution, you can. Don't put limits on what your security team can do and automate nearly any use case based on what, how and when you need it.

SWIMLANE

Orchestrate. Automate. Respond.



Achieving certifications against standards like Common Criteria or its related cryptographic validation standard FIPS 140-2 are industry and government procurement table stakes.

Modern security product certification best practices

AUTHOR_ Jason Lawlor, President, Lightship Security

IT security product manufacturers are required to achieve government-mandated, standards-based certifications to get their product in market. One of the most common, aptly called Common Criteria (CC), was introduced more than two decades ago to help standardize the evaluation criteria used to validate a product's conformance to a variety of functional security requirements.

Its goal is to ensure that a certified product meets the rigorous level of conformance required by the internationally adopted CC standard, thereby providing end users with assurance about the product's security posture prior to deployment.

Achieving certifications against standards like Common Criteria or its related cryptographic validation standard FIPS 140-2 are industry and government procurement table stakes. Without these independent, third-party certifications, product vendors are limited in their ability to sell into government agencies or other regulated industries.

When it comes to cybersecurity product development, the industry is agile by design, but certification methods haven't kept pace with modern development methods and release cycles. As many developers or product managers will attest, trying to integrate legacy certification processes on top of modern development on your own is complex, expensive and often frustrating.

Nothing will slow a fully automated pipeline down faster than legacy, manual product certification.

To complicate matters, standards-based certification programs are expanding in scope, rigor and prevalence. This means the DevOps toolchain has drastically changed the speed at which teams can bring product to market thanks to process automation. But nothing will slow a fully automated pipeline down faster than legacy, manual product certification. Why are these processes so out of sync? At best, the intricate testing and evaluation process usually takes months to achieve certification with a product that is ready to certify. At worst, it can lead a product back to the drawing board for fixes if problems are identified through the evaluation, thereby delaying time to market. The process is time consuming and costly for development teams implementing fixes against the prescriptive requirements. This is also one of the few remaining non-automated test processes within the development environment and whether you're managing it internally or outsourcing to a lab, the entire process is typically managed in a very manual way.

For years, security was often a last consideration in product development, but today manufacturers and regulators recognize the importance of security at design – and that security by design must include preparing for certification during design and development. Standards-based testing will benefit by a modern approach; new automation capabilities and certification process innovation means continuous iterative testing will help teams certify at the speed of development.

Many industry players are working to modernize the process. Meantime, here are five steps product managers and developers can take to manage the certification process more smoothly:

1_Fully vet an accredited lab partner to help you manage the test process. Ask your lab before contracting if you (as the vendor) need to develop any test harnesses or use your own resources to do any of the testing and show the results. With few exceptions, your lab should be able to do close to 100% of the Protection Profile testing with their processes and tools. Set expectations in advance on your team's required level of involvement to avoid surprises.

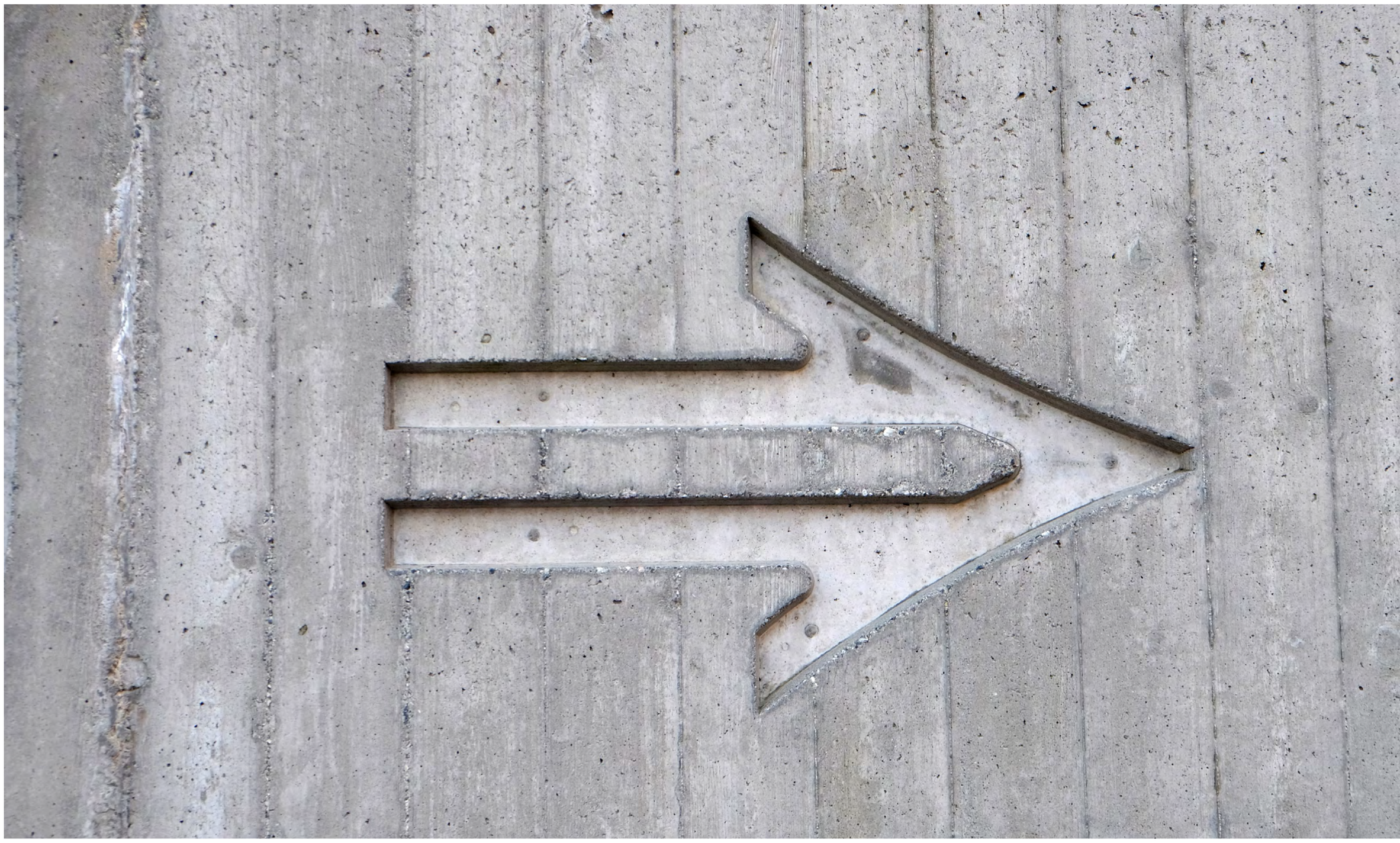
2_Confirm how much pricing contingency the lab is building into their model for testing. Historically, labs did not know how many rounds of testing they would need to do, because the testing was done at the end of an evaluation project with little advance insight into possible issues. This resulted in labs building in a significant risk premium. If you, as a vendor, undertake an automated Functional Gap Assessment approach to ensure product readiness before formal testing, you can confidently enter into a contract with a lab that only includes one full pass of testing. Don't pay for unnecessary testing cycles.

3_Ask your lab how they do their gap analysis. If it's a paper-based exercise or checklist, be aware that the process will likely miss granular details that may end up costing re-development cycles and slow your time to market. A lab that relies solely on a paper-based gap analysis may only uncover additional problems during the official testing phase, at which point you are forced to remediate the problem. The best way to determine gaps is to execute actual test cases using customized tools against the target early and often to dramatically reduce re-development risk.

4_Confirm with your lab how long the entire process takes before signing the contract. Be wary of broad or loose time frames. Armed with the results of a Functional Gap Assessment, the lab should be able to confidently commit to testing and finalization duration. There are some caveats around specific CC-scheme policies, such as the US scheme requiring last minute technical interpretations or requirements to be applicable right up until submission. A standard NDcPP formal evaluation can be completed in 60 days or less if the lab has the FGA results as inputs and is able to be "one and done" with formal testing. Don't agree to an extended multi-month process without understanding why it will take so long and slow your time to market.

5_Check with your lab on the ownership of the project deliverables. Be wary of labs that don't provide the consulting or documentation deliverables as works for hire. You have paid for the work and should have ownership of the documents for future use with that lab or another of your choosing.

At the end of the day, product managers and developers are equally responsible for driving better security assurance outcomes and the move to a modernized approach will yield greater results. Common Criteria can and should be a key tool in the toolbox to get us there.



Why outsourcing your DPO is an effective insurance policy

AUTHOR_ Dyann Heward-Mills, CEO, HewardMills

Organizations are starting to take a much more considered approach to data protection as high-profile regulatory action for data mishandlings has raised both the stakes and interest in data privacy operations.

Since the EU General Data Protection Regulation (GDPR) came into force in May 2018, data protection has risen to the top of the news agenda. Simultaneously, the GDPR has raised the profile and highlighted the importance of the data protection officer (DPO) internationally as, under this legislation, certain entities are under legal obligation to appoint a DPO.

Investor activism and customer scrutiny – over the way their data is collected, processed and used – is putting the pressure on organizations to act ethically.

Noncompliance with the GDPR carries hefty fines and is generally associated with a wave of negativity when public trust is compromised. Moreover, there is a growing global awareness that data protection matters, and people expect organizations to handle their personal data with care. It is for this reason that legislators around the world are actively seeking new ways to protect the security and privacy of personal data.

Organizations should strive for ethical handling of personal data

The global movement for an ethical handling of personal information is multidimensional. Investor activism and customer scrutiny – over the way their data is collected, processed and used – is putting the pressure on organizations to act ethically and on legislators to enact laws that effectively deal with rapid technological changes. Issues related to corporate governance and accountability are at the center of this movement.

Every day at HewardMills we speak with more and more organizations recognizing the value of in-depth knowledge and the need for total autonomy in this area. Businesses understand that their reputation is closely aligned with the processes around privacy and data protection in place. As a result, clearer lines are being drawn around departmental responsibilities to better operationalize data protection regulations.

Organizations may have good intentions to achieve best practices and meet their legal obligations, but the data protection process does not stop there.

Similar to other data specialist skill sets, demand for qualified and experienced DPOs is raising. This is a result of the role being both legally required for certain entities and organizations realizing the value of fostering a data protection culture.

DPOs are the cornerstone

The DPO can be internal or external, but they must be allowed to function independently. They are the link between the organization, the supervisory authorities and the data subjects. Thus, it is important that the DPO strike a careful balance to meet their own obligations toward all parties involved.

DPOs play a pivotal role in an organization's data management health and are required to report directly to the highest level of management. Some tasks that fall under the DPO role include advising on issues around data protection impact assessments (DPIAs), training, overseeing the accuracy of data mapping and responding to data subject access requests (DSARs). These things are all mandated under the GDPR.

Even the best intentions fall flat without the right execution

Organizations may have good intentions to achieve best practices and meet their legal obligations, but the data protection process does not stop there. Practical knowledge on how to operationalize legal obligations is the key to success. For example, if an organization is not adequately prepared to respond to DSARs, it may miss the one-month GDPR deadline or respond in an incomplete manner.

Since the GDPR came into effect, supervisory authorities have actively sought greater transparency. This means that there is a particular focus on accurate privacy notices, data protection impact assessments and legitimate interest

assessments. Given the global trend toward accountability, it is safe to argue that investing in data protection and privacy will win the trust of individuals, be the customers or employees. Organizations that foster a culture of integrity are at a competitive advantage in a world where privacy and data protection matter. For those that do not, the financial, legal and public opinion risks can be significant.

Getting ahead of the risks

Being responsive to GDPR data subject requests helps to build trust with individuals and demonstrates a serious dedication to data protection obligations. The DPO is the contact point for data subjects who are exercising their rights. As such, DPOs must be easily accessible, be it by telephone, mail or other avenues. Lack of resources is not an excuse for neglecting legal obligations and denying data subjects their rights. A consultant or outsourced DPO function can provide a cost-effective way to fill this gap. DPOs help organizations to prioritize risks. While they themselves must address highest-risk activities first, they must also educate on how DPIAs are reached. This allows controllers to know which activities should be prioritized. Ultimately, ensuring data controllers are informed about the perceived risks relating to different processing activities. For instance, the DPO could flag data protection audits, the need for enhanced security measures, or gaps in staff training and resource allocations.

To maintain the level of autonomy needed to act as an independent body, job security has been built into the DPO appointment.

The insurance policy of an autonomous partner

To maintain the level of autonomy needed to act as an independent body, job security has been built into the DPO appointment. The DPO can be disciplined or even terminated for legitimate reasons. However, they cannot be dismissed or penalized by the controller or processor as a result of carrying out their duties. In other words, the organization cannot direct the DPO or instruct them to reach a certain desired conclusion. The DPO must also be given the resources required to achieve this level of independence and carry out their duties. Typically, these resources are budget, equipment and staff.

One of the benefits of using an external DPO is that conflicts of interest are less likely. Organizations should strive to give the DPO the necessary autonomy to successfully act as a bridge between data subjects, the organization and the supervisory authorities. The DPO should not be assigned tasks that would put them in a position of “marking their own homework”. Used correctly, the DPO is a partner that helps navigate the organization toward an ethical handling of personal data.

Faced with meeting strict obligations under GDPR, organizations controlling and processing personal data must empower and embrace their DPOs and work closely with them. Organizations should view DPOs as a type of insurance policy for data risk and not think of them as the regulators’ undercover watchmen.