SPECIAL REPORT

A winning strategy for cybersecurity

TABLE OF CONTENTS

CYBERSECURITY: HOW TO DEVISE A WINNING STRATEGY

BY CHARLES MCLELLAN

IMAGE: ISTOCK/ KTSIMAGE

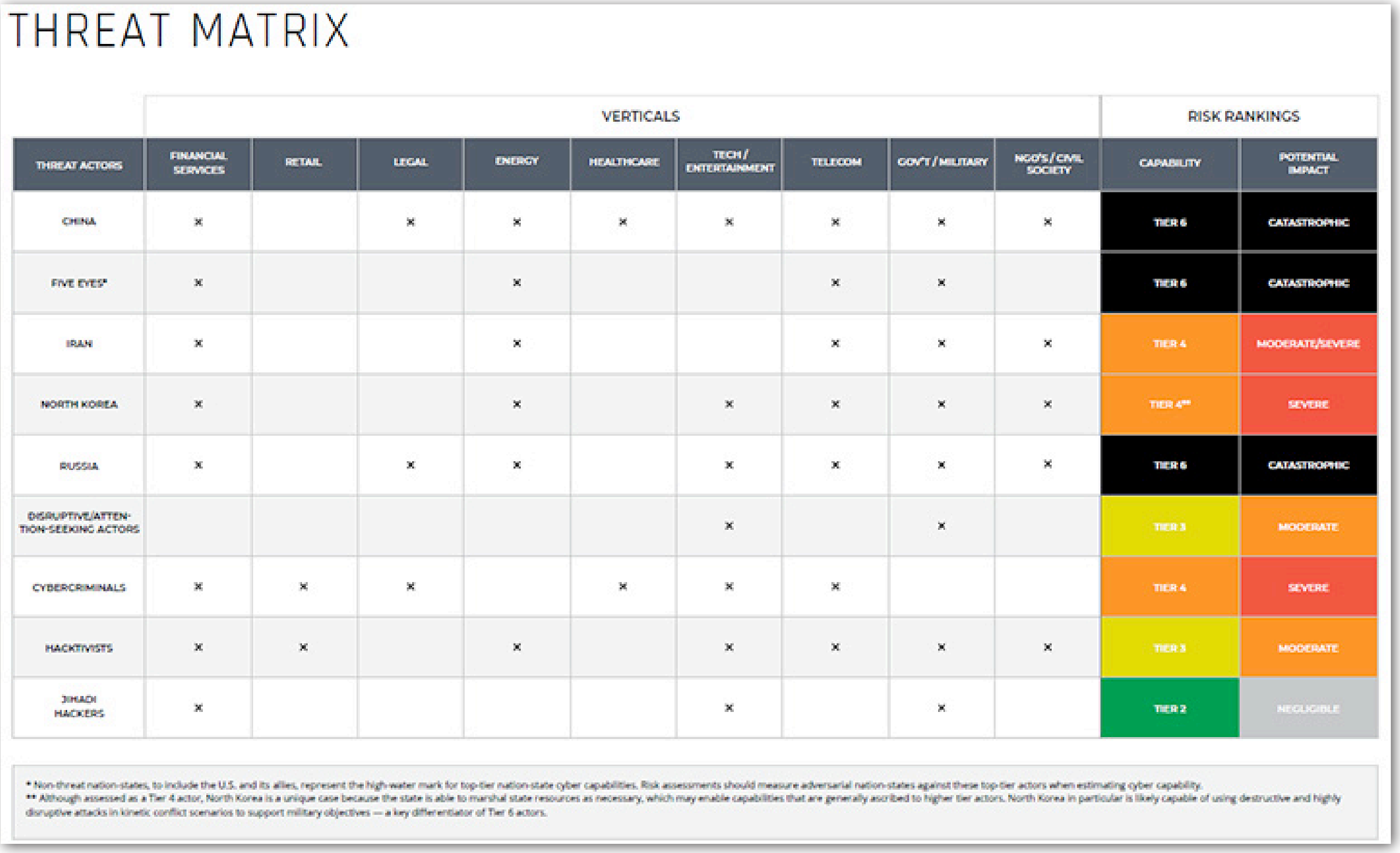
In 2018, as in previous years, cybersecurity incidents made the news on a regular basis, and there's no shortage of predictions for the ways in which bad actors may grab the headlines in 2019. Behind these prominent incidents and *modus operandi* is a continuous background level of cyber-activity that is the inevitable result of organisations failing to monitor and protect their networks, and of users neglecting basic security hygiene.

How should businesses respond to the clear, present and ever-evolving threat of cyber-attack? Completely locking down their IT systems isn't an option, but neither is complacency. Vulnerabilities will almost inevitably be discovered and exploited, and once security breaches have happened they're usually expensive and time-consuming to remediate, often resulting in lasting damage to the victim's reputation and bottom line.

The trick is to work out the attacks you're most likely to face, guard against them to the best of your ability, and review this process regularly. Where to start? Well, no military commander would charge headlong into battle without a clear strategic picture of the conflict, and the same applies in the cyber theatre. That's where business risk intelligence (BRI), or cyber threat intelligence (CTI), comes in. Here's BRI company Flashpoint on the subject, for example:

"Having a robust BRI program puts these threats into context for an organization and its risk management efforts. Cybercrime, fraud, insider threats, physical security, M&A security assessments and third-party risk can all be minimized with an adequate handle on intelligence."

Flashpoint's high-level summary of the 2017/18 global threat landscape—a matrix of threat actors and key verticals—looked like this (we've yet to see a 2018/19 update):



THREAT MATRIX

	VERTICALS									RISK RANKINGS	
THREAT ACTORS	FINANCIAL SERVICES	RETAIL	LEGAL	ENERGY	HEALTHCARE	TECH / ENTERTAINMENT	TELECOM	GOV'T / MILITARY	NGO'S / CIVIL SOCIETY	CAPABILITY	POTENTIAL IMPACT
CHINA	×		×	×	×	×	×	×	×	TIER 6	CATASTROPHIC
FIVE EYES*	×			×			×	×		TIER 6	CATASTROPHIC
IRAN	×			×			×	×	×	TIER 4	MODERATE/SEVERE
NORTH KOREA	×			×		×	×	×	×	TIER 4**	SEVERE
RUSSIA	×		×	×		×	×	×	×	TIER 6	CATASTROPHIC
DISRUPTIVE/ATTENTION-SEEKING ACTORS						×		×		TIER 3	MODERATE
CYBERCRIMINALS	×	×	×		×	×	×			TIER 4	SEVERE
HACKTIVISTS	×	×		×		×	×	×	×	TIER 3	MODERATE
JIHADI HACKERS	×					×		×		TIER 2	NEGLIGIBLE

* Non-threat nation-states, to include the U.S. and its allies, represent the high-water mark for top-tier nation-state cyber capabilities. Risk assessments should measure adversarial nation-states against these top-tier actors when estimating cyber capability.
** Although assessed as a Tier 4 actor, North Korea is a unique case because the state is able to marshal state resources as necessary, which may enable capabilities that are generally ascribed to higher tier actors. North Korea in particular is likely capable of using destructive and highly disruptive attacks in kinetic conflict scenarios to support military objectives — a key differentiator of Tier 6 actors.

IMAGE: FLASHPOINT

Threat actors are ranked on a six-point capability scale and a four-point potential impact scale, with Flashpoint's cast ranging from Tier 2 capability/Negligible potential impact (Jihadi hackers) to Tier 6/Catastrophic (China, Russia and Five Eyes). Cybercriminals—the main adversary of most businesses—are ranked as Tier 4/Severe:

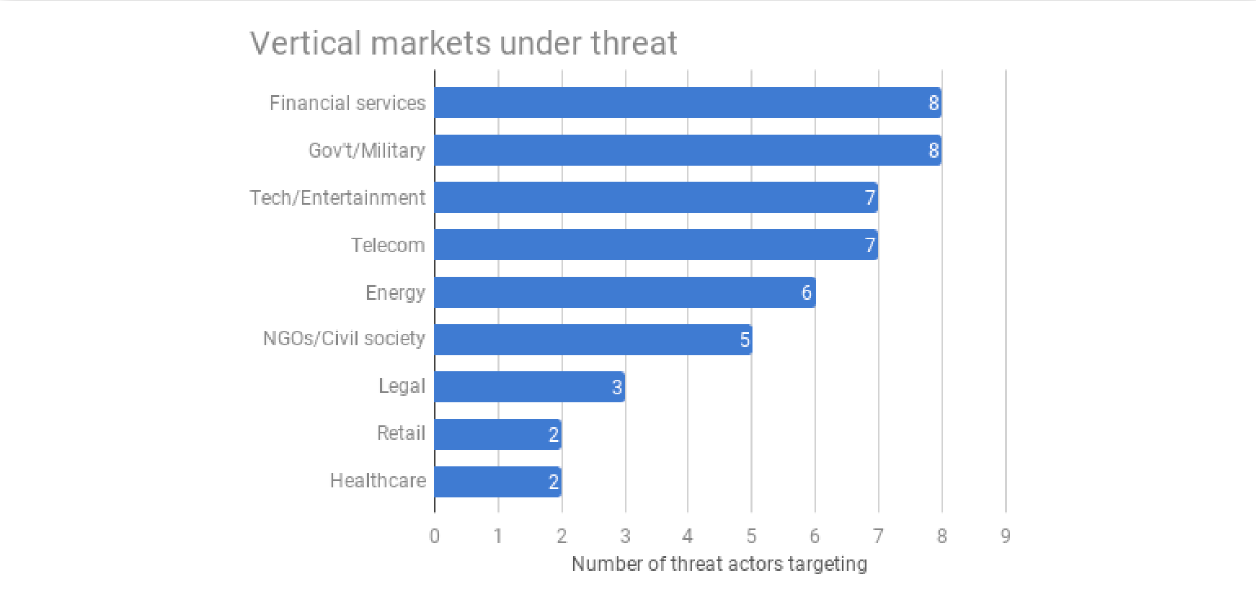
Tier 4 capability

"Attackers are part of a larger and well-resourced syndicate with a moderate-to-high level of technical sophistication. The actors are capable of writing custom tools and malware and can conduct targeted reconnaissance and staging prior to conducting attack campaigns. Tier 4 attackers and above will attempt to make use of publicly available tools prior to deploying more sophisticated and valuable toolkits."

Severe potential impact

"Cyber attacks at this level have the capacity to disrupt regular business operations and governmental functions severely. Such incidents may result in the temporary outage of critical services and the compromise of sensitive data."

Looking at the vertical industries targeted by these threat actors, financial services and government/military are the most threatened—bad actors tend to follow the money or the power, after all. Eight out of the nine categories of 'bad guys' have these sectors in their sights:



DATA: FLASHPOINT / CHART: ZDNET

Flashpoint's mid-2018 update to its BRI Intelligence Decision Report noted that political and social instability around the world is now affecting businesses, which must "contend not only with hackers targeting valuable corporate data, but also how geopolitical conflicts will affect the reliability of digital networks supporting commerce, how policy is formulated and enforced, and how investments are executed."

CEO DISCONNECT IS WEAKENING CYBERSECURITY
Centrify | WSJ. CUSTOM STUDIOS

Although businesses need a lot more detail before they can create their cybersecurity policies and deploy specific measures, it's essential to have a consistent company-wide view of the threat landscape. However, February 2018 research from security provider Centrify and Dow Jones Customer Intelligence suggested that CEOs and their front-line technical officers (CIOs, CTOs and CISOs) often have different perspectives.

Centrify's report was based on a survey of 800 senior executives in companies with at least 1,500 employees, covering 19 industries in the US and UK. Over 50 percent of the companies represented had over 10,000 employees. The key finding was that CEOs are focused on malware—perhaps influenced by headline-grabbing cyber-attacks—while their technical officers (TOs) cited identity breaches as the biggest threat.

> **"The disconnect between CEOs and TOs is resulting in misaligned priorities and strategies, as well as mis-investments in cybersecurity solutions, which are weakening security."**
> **—Centrify**

A clear majority (62%) of CEOs pointed to malware as the biggest cybersecurity threat, compared with only 35 percent of TOs. Meanwhile, 68 percent of executives from companies that had at least one serious breach said it would likely have been prevented by either privileged user identity and access management or user identity assurance. By contrast, only eight percent of companies said that anti-malware endpoint security would have prevented the breaches.

"The disconnect between CEOs and TOs is resulting in misaligned priorities and strategies, as well as mis-investments in cybersecurity solutions, which are weakening security," the report concluded.

So how can companies avoid such misalignments and mis-investments?

CYBER-RISK MANAGEMENT FRAMEWORKS

A coherent cybersecurity program requires a template or framework containing all of the important components. Organisations then need to work out which components are most applicable to their particular circumstances, a process that should point them towards the most appropriate security measures.

A number of industry-standard frameworks are available to guide organisations' cybersecurity policies, including AICPA, CIS, COBIT, ENISA, ISO 2700, NIST and—for those that handle payment card transactions—PCI DSS. There are also industry-specific frameworks such as those relating to the protection of healthcare data under the US HIPAA legislation.

Using these and other sources, security consultancy Mandiant (a FireEye company) developed a 10-component framework for creating a comprehensive cybersecurity program.

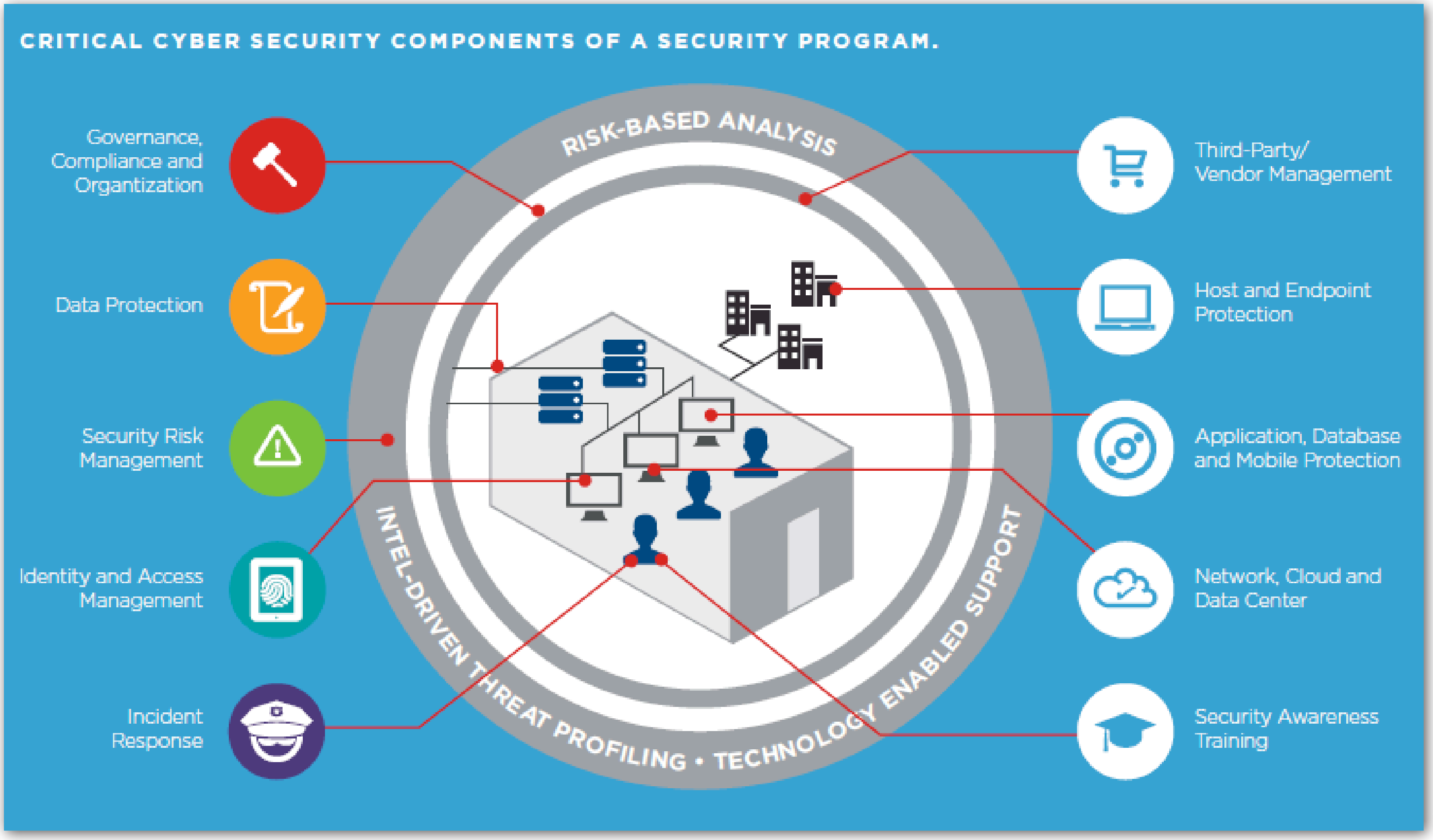
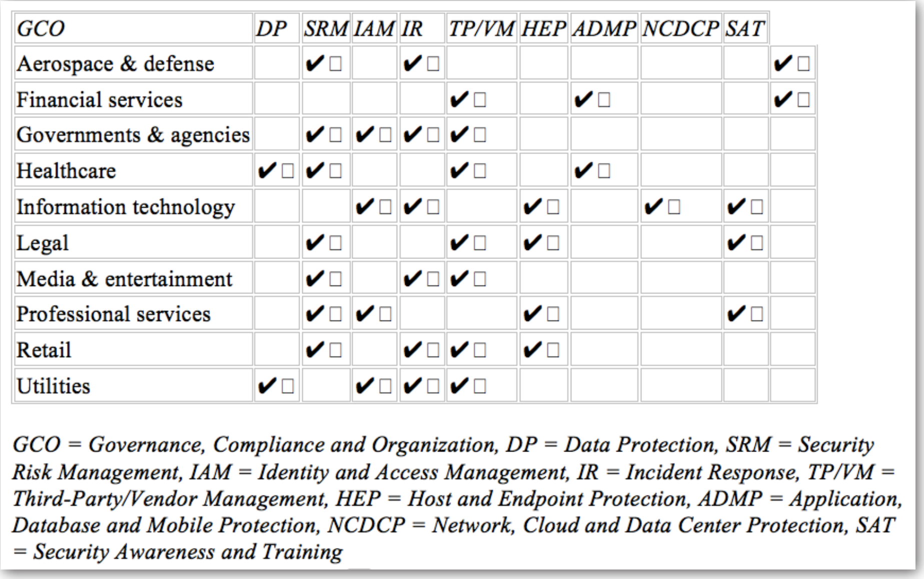

CRITICAL CYBER SECURITY COMPONENTS OF A SECURITY PROGRAM.
RISK-BASED ANALYSIS
INTEL-DRIVEN THREAT PROFILING • TECHNOLOGY ENABLED SUPPORT
Governance, Compliance and Organtization
Data Protection
Security Risk Management
Identity and Access Management
Incident Response
Third-Party/ Vendor Management
Host and Endpoint Protection
Application, Database and Mobile Protection
Network, Cloud and Data Center
Security Awareness Training

IMAGE: MANDIANT

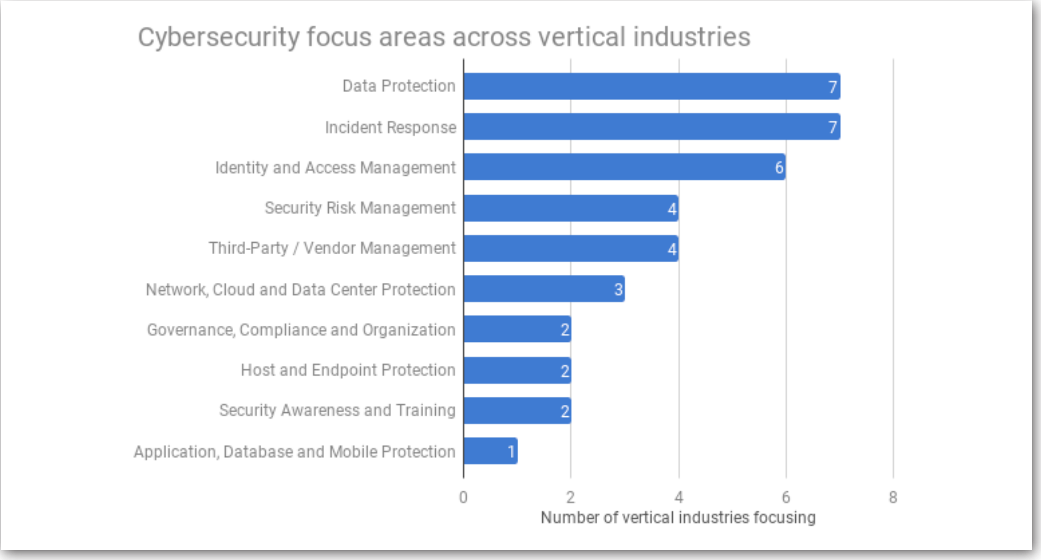
Different industries will tend to focus on different framework components, depending on the nature of their business and the particular threat landscape they face. Here's a summary of how Mandiant sees the security priorities for 10 vertical industries:



GCO	*DP*	*SRM*	*IAM*	*IR*	*TP/VM*	*HEP*	*ADMP*	*NCDCP*	*SAT*	
Aerospace & defense		✔□		✔□						✔□
Financial services					✔□		✔□			✔□
Governments & agencies		✔□	✔□	✔□	✔□					
Healthcare	✔□	✔□			✔□		✔□			
Information technology			✔□	✔□		✔□		✔□	✔□	
Legal		✔□			✔□	✔□			✔□	
Media & entertainment		✔□		✔□	✔□					
Professional services		✔□	✔□			✔□			✔□	
Retail		✔□		✔□	✔□	✔□				
Utilities	✔□		✔□	✔□	✔□					

GCO = Governance, Compliance and Organization, DP = Data Protection, SRM = Security Risk Management, IAM = Identity and Access Management, IR = Incident Response, TP/VM = Third-Party/Vendor Management, HEP = Host and Endpoint Protection, ADMP = Application, Database and Mobile Protection, NCDCP = Network, Cloud and Data Center Protection, SAT = Security Awareness and Training

As you might expect, the most commonly cited focus areas across these vertical industries are data protection and incident response, closely followed by identity and access management:



DATA: MANDIANT / CHART: ZDNET

THE COST OF CYBERCRIME

Cybersecurity has risen ever higher up the corporate agenda for the very good reason that incidents and breaches result in significant costs—money or intellectual property stolen, valuable data compromised, business disruption, impaired brand reputation, reduced revenue and/or lowered share price. Considerable research effort is expended every year to quantify those costs, a leading example being the IBM/Ponemon Cost of a Data Breach Study.

Ponemon Institute
2018 Cost of a Data Breach Study: Global Overview
Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC
July 2018
IBM.

The 2018 study, published in July, was based on responses from 2,200 IT, data protection and compliance professionals from 477 companies that had experienced a data breach in the previous 12 months; 17 industries were represented, the leading sectors being financial (16%), services (15%), industrial & manufacturing (14%) and technology (13%).

Headline findings were an average total cost per data breach of $3.86 million (up from $3.62m in 2017) with an average cost of $148 per lost or stolen record (up from $141 in 2017). The average number of records per data breach was 24,615 (up 2.2% from 2017), while the estimated probability that an organisation will have a 'material' data breach in the next two years was 27.9 percent (up from 27.7% in 2017).

The mean time to identify (MTTI) a data breach was 197 days (up from 191 days in 2017), while the mean time to contain (MTTC) a breach was 69 days (up from 66 days in 2017). Companies that responded rapidly, containing a breach in less than 30 days, saved over $1 million compared to those that took more than 30 days.

Two new cost factors were introduced in the 2018 report: security automation and the use of IoT devices. Fully deploying security automation lowered the average cost of a data breach by $1.55 million, while the extensive use of IoT devices increased the cost per compromised record by $5.

The 2018 study also quantified the cost of so-called 'mega' breaches involving over 1 million compromised records: a 1m-record breach cost $40m on average, rising to $350m for a 50m-record breach.

Among the many other useful findings in the IBM/Ponemon report is an analysis of the factors that influence the per capita cost of a data breach. A fully functional incident response team reduced the cost by $14 on average (down from $19.3 in 2017), while at the other end of the scale, third-party involvement increased the cost by $13.4 (down from $16.9 in 2017):

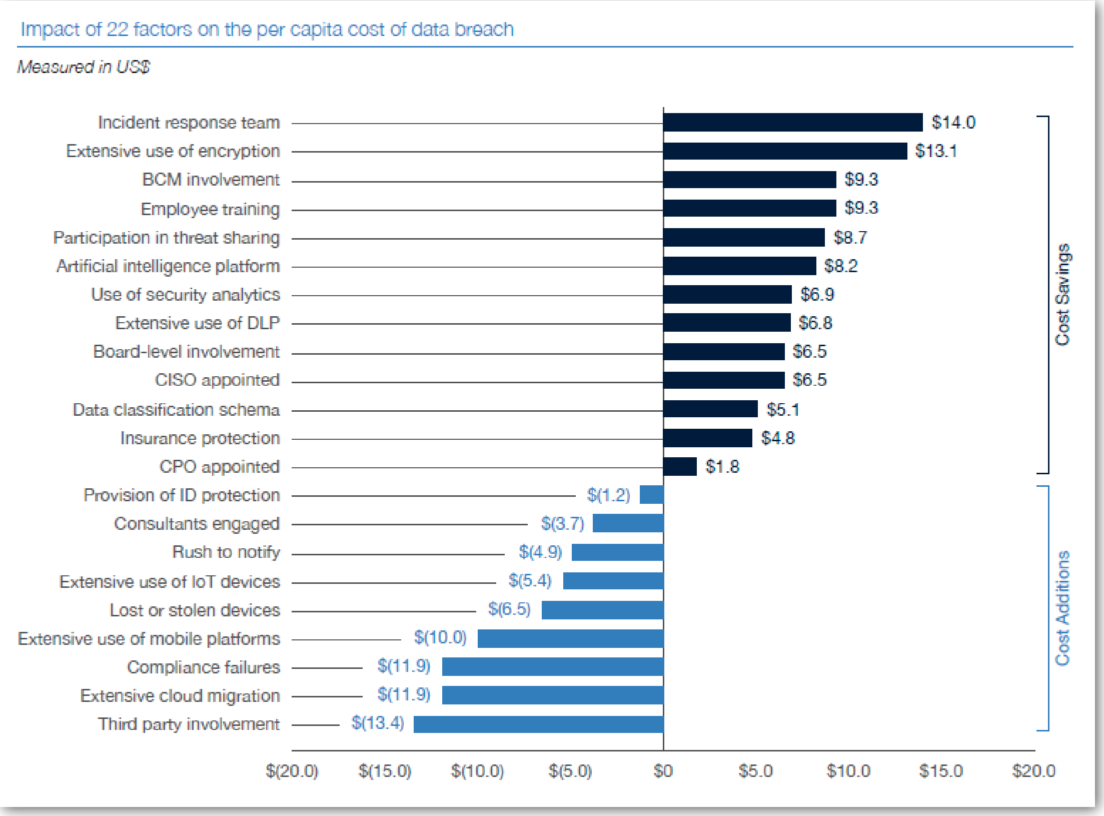


IMAGE: IBM AND PONEMON INSTITUTE

OUTLOOK

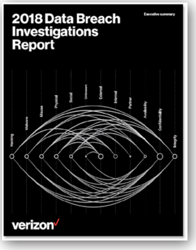
Cybersecurity incidents and breaches can seriously damage a company’s bottom line and brand image, making it imperative that security risk management is integral to corporate governance.

Detailed analysis of the threat landscape for a company’s particular business sector should lead to the adoption of an appropriate framework within which to develop a security policy, which in turn should suggest the best combination of security measures to deploy. Policies must be revisited and updated as the threat landscape evolves. Extensive use of IoT devices increases an organisation’s attack surface, increasing the likelihood and level of breach-related costs.

As well as covering the basics, companies need to consider deploying advanced security technologies such as AI-driven automation, in order to give themselves the best chance against the ever-nimble ‘bad guys’.

Cybersecurity trends in 2018/19

Numerous reports and surveys are published every year, analysing the state of the cybersecurity arms race and allowing interested parties to keep up to date with the changing threat landscape. The table below lists some of the most influential ones, summarising the key content areas and recommendations.

Report	Key subject areas and findings	Recommendations, best practices, and predictions
Verizon 2018 Data Breach Investigations Report  2018 Data Breach Investigations Report Executive summary verizon	**It will probably be you one day** Most cybercriminals are motivated by cold, hard cash. If there's some way they can make money out of you, they will. **So who are you up against?** Almost three-quarters (73%) of cyberattacks were perpetrated by outsiders. Members of organized criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12%. **People make mistakes** Malicious employees looking to line their pockets aren't the only insider threat you face. Errors were at the heart of almost one in five (17%) breaches. **Don't get held to ransom** Cybercriminals don't have to steal data to make money—they can just stop you using it.	Be vigilant Make people your first line of defense Only keep data on a need-to-know basis Patch promptly Encrypt sensitive data Use two-factor authentication Don't forget physical security

Report	Key subject areas and findings	Recommendations, best practices, and predictions
Booz Allen Hamilton 2019 Cyber Threat Outlook Booz | Allen | Hamilton 2019 CYBER THREAT OUTLOOK Eight ways threat actors will make waves in 2019 CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER	Companies in the cross hairs of information warfare IoT devices broaden state espionage operations Chip and pin may fall short The weaponization of adware networks Deepfakes in the wild—AI in information warfare State-sponsored threat actors double-down on deception Water utility targeting bubbles to the surface	States may use their burgeoning information warfare capabilities to influence consumers and harm companies, just as they already target voters and foment civil strife. State-linked groups could find new uses for Internet-of-Things (IoT) botnets, such as Tor-like communication infrastructure. Adversaries might develop novel attack vectors that exploit the growing pervasiveness of non-WiFi wireless protocols, especially among IoT devices. Adware networks, a long-standing security nuisance, could be leveraged for more harmful targeted attacks. Increased adversary emphasis on misattribution will likely result in more examples of confident attribution by the private sector later being disproved, further undermining public confidence in attribution. Government-backed adversaries may increasingly penetrate the industrial control systems (ICS) of water utilities to conduct reconnaissance and generate fear and uncertainty, mirroring their historical focus on frequent intrusions and rare disruptions at energy firms.

Report	Key subject areas and findings	Recommendations, best practices, and predictions
EY Global Information Security Survey 2018-19 Is cybersecurity about more than protection? EY Global Information Security Survey 2018-19 The better the question. The better the answer. The better the world works. EY Building a better working world	The future state of cybersecurity Protect the enterprise Optimize cybersecurity Enable growth	**Protect** Cybersecurity needs to be in the DNA of the organization / Build awareness around phishing and malware / Focus the security strategy and program on the entire eco-system of the organization / Increase cybersecurity budgets now (instead of after the fact) and focus the spend on threat detection and response. **Optimize** Consider investments in analytical capabilities / It may be difficult to quickly build up forensic capabilities in house / Focus on where investment will be most effective / Be more open around security operations. **Grow** Put cybersecurity at the heart of corporate strategy / Cybersecurity must be an ongoing agenda item for all executive and non-executive boards / Focus on cybersecurity as part of digital transformation strategy / Continue the focus on emerging technologies.

RESEARCH: EMPLOYEE COMPLIANCE IS THE MAIN CHALLENGE TO IMPLEMENTING CYBERSECURITY STRATEGY

BY AMY TALBOTT

It's one thing for a company to create a cybersecurity strategy, but it's another thing to put strategy into practice. Recently, ZDNet's sister site Tech Pro Research conducted a poll to see what security tactics companies are using and how they're working out.

Just as many respondents (39%) said their company has a formal, regularly updated cybersecurity policy as those who said their company has no policy. Others said their company has a policy, but it doesn't get regular updates.

In terms of what's covered in those policies, automatic software updates and employee training were the two most common cybersecurity tactics used by respondents' companies. Among respondents whose companies had added security measures in the past year, new firewall or antivirus products and additional employee training were most common.

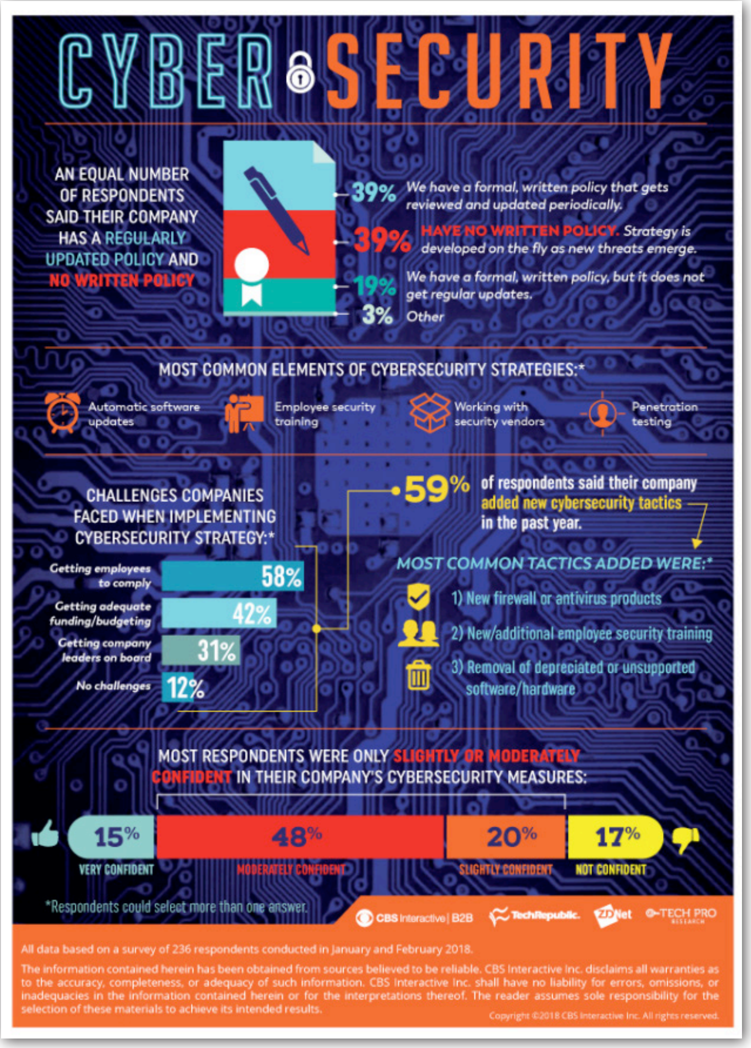


IMAGE: ERIK UNDERWOOD/TECHREPUBLIC

This shows that businesses do realize the importance of getting employees involved in cybersecurity. However, when asked about any challenges to implementing strategies, 58% said the hardest part was getting employees to comply. The infographic above contains selected details from the research. To read more findings, plus analysis, download the full report: Cybersecurity strategy: Common tactics, issues with implementation, and effectiveness (Tech Pro Research subscription required).

5 EMERGING CYBERSECURITY THREATS YOU SHOULD TAKE VERY SERIOUSLY IN 2019

BY ALISON DENISCO RAYOME

The cyberthreat landscape continues to evolve, with new threats emerging almost daily. The ability to track and prepare to face these threats can help security and risk management leaders improve their organization's resilience and better support business goals.

The number of high-profile breaches and attacks making headlines has led business leaders to finally take cybersecurity seriously, said Sam Olyaei, senior principal and analyst at Gartner.

"Today, not only are business leaders and the business community understanding cybersecurity, they know it's important to their business outcomes and objectives," Olyaei said. "The problem is, there is still a lack of understanding as to why it's important."

Firms must work to bridge the gap between communicating the technical aspects of cybersecurity and the business outcomes, such as customer satisfaction, financial health, and reputation, Olyaei said.

Keeping track of new threats and not just established ones like ransomware is key for a strong security posture, said Josh Zelonis, senior analyst at Forrester.

"Whenever we develop our strategies for how we're going to protect our organizations, it's really easy to look at things that you're familiar with, or that you have a good understanding of," Zelonis said. "But if you're not looking ahead, you're building for the problems that already exist, and not setting yourself up for long-term success. And that is really the number one reason why you need to be looking ahead--to understand how attack techniques are evolving."

Here are five emerging cybersecurity threats that business, technology, and security leaders need to take seriously this year.

1. CRYPTOJACKING

Ransomware has been one of the biggest threats impacting businesses in the past two years, exploiting basic vulnerabilities including lack of network segmentation and backups, Olyaei said.

Today, threat actors are employing the same variants of ransomware previously used to encrypt data to ransom an organization's resources or systems to mine for cryptocurrency—a practice known as cryptojacking or cryptomining.

"These are strains of malware that are very similar to strains that different types of ransomware, like Petya and NotPetya, had in place, but instead it's kind of running in the background silently mining for cryptocurrency," Olyaei said.

The rise of cryptojacking means the argument that many SMB leaders used in the past--that their business was too small to be attacked--goes out the window, Olyaei said. "You still have computers, you still have resources, you still have applications," he added. "And these application systems, computers, and resources can be used to mine for cryptocurrency. That's one of the biggest threats that we see from that standpoint."

2. INTERNET OF THINGS (IOT) DEVICE THREATS

Companies are adding more and more devices to their infrastructures, Zelonis said. "Organizations are going and adding solutions like security cameras and smart container ships, and a lot of these devices don't have how you're going to manage them factored into the design of the products."

Maintenance is often the last consideration when it comes to IoT, Zelonis said. Organizations that want to stay safe should require that all IoT devices be manageable and implement a process for updating them.

3. GEOPOLITICAL RISKS

More organizations are starting to consider where their products are based or implemented and where their data is stored, in terms of cybersecurity risks and regulations, Olyaei said.

"When you have regulations like GDPR and threat actors that emerge from nation states like Russia, China, North Korea, and Iran, more and more organizations are beginning to evaluate the intricacies of the security controls of their vendors and their suppliers," Olyaei said. "They're looking at geopolitical risk as a cyber risk, whereas in the past geopolitical was sort of a separate risk function, belonging in enterprise risk."

If organizations do not consider location and geopolitical risk, those that store data in a third party or a nation state that is very sensitive will run the risk of threat actors or nation state resources being used against them, Olyaei said. "If you do that then you also impact the business outcome."

4. CROSS-SITE SCRIPTING

Organizations struggle to avoid cross-site scripting (XSS) attacks in the development cycle, Zelonis said. More than 21% of vulnerabilities identified by bug bounty programs are XSS areas, making them the leading vulnerability type, Forrester research found.

XSS attacks allow adversaries to use business websites to execute untrusted code in a victim's browser, making it easy for a criminal to interact with a user and steal their cookie information used for authentication to hijack the site without any credentials, Forrester said.

Security teams often discount the severity of this attack, Zelonis said. But bug bounty programs can help identify XSS attacks and other weaknesses in your systems, he added.

5. MOBILE MALWARE

Mobile devices are increasingly a top attack target, a trend rooted in poor vulnerability management, according to Forrester. But it said many organizations that try to deploy mobile device management (MDM) solutions find that privacy concerns limit adoption.

The biggest harbinger of pain in this space is the Android installed base, Zelonis said. "The Google developer site shows that the vast majority of Android devices in the world are running pretty old versions of Android," he said. "And when you look at the motivations of a lot of IoT device manufacturers, it's challenging to get them to continue to support devices and get timely patches, because then you're getting back to mobile issues."

Organizations should ensure employee access to an anti-malware solution, Forrester recommended. Even if it is not managed by the organization, it will alleviate some security concerns.

THE HACKING STRATEGIES THAT WILL DOMINATE IN 2019

BY DANNY PALMER

If an organisation is connected to the internet and holds any type of data, it's almost inevitable that it's going to end up in the sights of hackers.

Pretty much any data from personal information and bank details to email addresses and passwords can be attractive to cyber attackers. They could take this information and sell it to others on the dark web, they could use it as a jumping-off point for larger campaigns — they could even dump it in public view, just to cause chaos.

The types of potential attacker are also broader than ever. Some large organisations will need to have the ability to fight off skilled cyber criminal gangs and nation-state backed hacking campaigns. But, for the most part, it's likely that those attempting to breach an organisation won't be the most advanced attackers in the world, especially now many cyber criminal marketplaces sell do-it-yourself kits. All of this is visible in the two very different hacking trends that will likely dominate this year. First, the mass adoption of sophisticated attacks by much less skilled attackers, and second, hyper-targeted attacks going after particular companies or even individuals.

Strategies and hacking techniques that may have once required specialist expertise are now sold in easy-to-use bundles, complete with tutorials for the non-tech savvy.

"There's an entire as-a-service ecosystem and it's really everywhere. It started as malware as-a-service, but now there's also phishing as-a-service, exploit kits as-a-service, botnets as-a-service. Anyone can mix-and-match their own attacks, almost without knowing anything," says Maya Horowtiz, director of threat intelligence and research at security company Check Point Software.

There are various examples of , malware and other malicious as-a-service campaigns that haven't been conducted by criminal masterminds, but have still caused plenty of damage

"These tools are available on the open web, not even the dark web -- you can really easily get your hands on them," says Horowitz.

When it comes to the entry point for cyber attacks, phishing emails are still the most common means of forcing a way into the network.

Even simple phishing attacks can be surprisingly effective—lures like fake invoices or phoney requests from colleagues or customers are tried-and-tested techniques used by hackers to dupe victims into letting them in.

But with social media profiles and the wider internet providing attackers with vast and free resources to gather operational intelligence about victims, it's entirely possible to scope out individual targets and tailor phishing attacks directly towards them.

Dubbed 'rose phishing', this could potentially supercharge phishing attacks by making it almost impossible for the victim to ignore the bait.

"With rose phishing, people are utilising social media to do that reconnaissance and really digging into it. The reconnaissance provides a much higher return on investment — you have a much higher probability of that person clicking on something of a personal nature about them," says Amanda Fennell, chief security officer at Relativity.

For example, if someone publicly posts that they're on a business trip to a specific city, perhaps even staying at a specific hotel, attackers could take that information and use it to craft a highly specific lure.

"If you travel and post you're at company headquarters in Chicago, next thing you know you could get a targeted email stating you left a document at O'Hare airport. You'd get really worried, it could be very compelling to click on," Fennell explains.

"Or if you post about checking into a hotel in Chicago and then you get an invoice phishing attack [that] references that hotel. That's enough for somebody who is savvy enough to use it to their advantage," she adds.

As with any phishing attack, targeting the right person or people could give attackers the keys to the kingdom, allowing them to slowly but surely make their way across the network for whatever malicious goals they intend to carry out.

But it won't end here: hackers are always looking for new and ingenious ways to conduct campaigns. While organisations may not be able to predict every type of attack vector hackers could use, they can develop a cybersecurity strategy that does the utmost to prevent attacks from being successful, no matter how they're delivered.

HOW AI AND MACHINE LEARNING CAN HELP YOU DEFEND THE ENTERPRISE FROM CYBERATTACKS

BY JAMES SANDERS

Security measures have increased significantly in the last several years, and malicious actors have similarly advanced their techniques to keep pace, particularly with advances in attack methods such as fileless malware. Likewise, the security model of "serverless" computing platforms like AWS Lambda are completely different from traditional computers. These itinerant computing concepts are not effectively secured by the traditional model of checking file hashes against known malware samples.

For a robust, modern defense, an adaptive monitoring solution that leverages machine learning to identify anomalous patterns indicative of an attack in its infancy is necessary to defend enterprise systems from cyberattacks.

Much of the groundwork for this has been laid over the last several years, with endpoint detection services analyzing system events. "Network connection opened, registry key modified, process created… You build this catalog of really security relevant behaviors. The challenge becomes to map known malicious behaviors that essentially do the same thing," said Forrester Senior Analyst for Security and Risk Josh Zelonis, "You have to have two people in the room in order to build this: a data scientist who understands the map and can build these models… [and] an expert in offensive techniques in order to help them build the model and understand the abstraction of what they're doing, so they can statistically identify when an adversary does something that looks similar."

Accurately connecting aggregations of system events to anomalous activities is just one step on the security staircase—determining the difference between legitimate changes in workflow and malicious activity is a higher-level-order task for machine learning or artificial intelligence. A variety of approaches for security information and event management (SIEM) that leverage ML/AI are available from a variety of vendors.

LEADING VENDORS FOR AI/ML-POWERED SOLUTIONS

ExtraHop

ExtraHop's Reveal(x) platform provides network traffic analysts for enterprise networks, providing insight into connections, and identifies potential threats using rule and behavior based analytics paired with logical device groups. The platform also touts "full context and one-click investigation workflows for every detection."

Vectra Networks

Vectra Cognito is an AI-powered security platform that uses an analysis of known malware payloads and techniques to inform the machine learning models to detect future or unknown threats. It also analyzes user behavior and local networks, or attributes specific to a customer environment, in order to gain a baseline understanding of normal, against which to set parameters that identify anomalous behavior.

CoreLight

Corelight's 1U rack-mountable network security appliances are intended to produce comprehensive and actionable logs based on a variety of factors. CoreLight's platform can be used to track DNS queries and responses, as well as potentially problematic environmental factors, such as out-of-date or vulnerable software, abnormal keyboard settings for an environment, self-signed, expired, or soon to expire SSL certificates, as well as detecting what systems in a network have accessed a file found to be malicious.

DataVisor

DataVisor's offerings are targeted more toward transactional security than network security, with products targeted toward content moderation and filtering, transaction fraud (including promotional abuse and loyalty program fraud), account opening and monitoring, and money laundering detection and prevention.

The company touts their ability to provide detailed information about why patterns are flagged as anomalous, citing a tendency for competing AI/ML models to be treated as "black boxes."

PerimeterX

Like DataVisor, PerimeterX targets detection of automated platform abuse, in essence, bots. The PerimeterX platform can be added to existing websites through the use of javascript, and uses " hundreds of indicators from the browser such as features, sensor data, and visual and audio rendering," which are compared against known profiles to detect when requests are not typical of normal users. Likewise, it also collects user behavior patterns "such as mouse clicks, screen touches, cadence and timing."

LOOKING FORWARD (AND BACKWARD) IN ENTERPRISE CYBERSECURITY

For all of the advancements that AI/ML promise for improving cybersecurity, it is not a replacement for the traditional groundwork needed to establish basic security hygiene in a given organization. "In terms of what people need to worry about when they're deploying is how control systems get used or accessed.. that is the gateway to all the other devices. If someone is checking their email on [an industrial control system] then you're going to have a bad time." said Zelonis. "There really isn't a technological solution for in-depth social engineering."

Moving forward, SIEM is likely to integrate user data, according to Eric Ogren, Senior Analyst for Information Security at 451 Research. "The first step is who's accessing [a device]? And are they accessing at normal hours with normal protocols? Do they have permissions? Are they authorized? I'm starting to see a lot of the same vendors integrate with identity information, for access control."

IMPROVE YOUR CYBERSECURITY STRATEGY: DO THESE 2 THINGS

BY JASON HINER

Over 77% over businesses suffered a cybersecurity attack last year, according to an IT security economics report from Kaspersky Lab.

That percentage is consistent with lots of other security research, and the number of companies admitting that they have been attacked has continued to move upward each year over the past several years.

Every company, no matter how big or small, is now a target. The question is what can you do to best protect yourself with the resources you have?

The answer is two things.

1. TAKE A RISK MANAGEMENT APPROACH

The organizations with the best track record in cybersecurity have long figured out that they can't secure everything or have a perfect security posture. Instead, they approach cybersecurity like an insurance company, by taking a risk management strategy.

They audit their organization to understand where their most valuable data lives and then prioritize their resources to protect it—whether that data is at rest, in transit, or anywhere that it flows.

2. WRITE GOOD SECURITY POLICIES

Once you have a deep understanding of where your most valuable data lives and how attackers could potentially do the most damage to your company, then you need a set of good policies to protect it.

These policies need to be updated annually and you need to communicate them in a way that your employees clearly understand why they should care and what they can do to be part of the solution. And if you need help drafting your cybersecurity policies, our sister site Tech Pro Research offers a lot of different templates that can help you get started.

10 WAYS TO DEVELOP CYBERSECURITY POLICIES AND BEST PRACTICES

BY MARY SHACKLETT

In January 2018, UK businesses were victimized 7,073,069 times. On January 3, 2018, the US Department of Homeland Security informed 247,167 of its employees that their data had been breached.

It's been an auspicious beginning for cyber hackers in 2018, so it comes as no surprise that security and risk management were rated as the number one priority for CIOs in a November 2017 NASCIO survey.

But are companies ready?

"We are in the fifth generation of cyber security," said Gabi Reish, vice president of marketing at Check Point, a security provider.

Reish lists the cybersecurity generations as follows:

- Gen 1: Developed when PCs with floppy disks were first introduced in the 1980s, with viruses as the first cyberattacks.
- Gen 2: Emerged during the mid-1990s, with cyberattacks focused on data and network security; the solution was firewalls.
- Gen 3: Began in the early 2000s with the exploitation of applications, browsers, and networks. This was the beginning of network intrusion detection.
- Gen 4: Began around 2010, with more sophisticated cybersecurity attacks that embedded malware in email, documents, and images. This generated security technology that "sandboxed" these occurrences to contain them and prevent them from spreading to other areas of the network.
- Gen 5: Broad scale attacks that involve ransomware, phishing, content exploitation, and/or any number of combinations.

Unfortunately, Reish also says that most companies "are only at generation two or three" cyber protection levels, and a recent survey by Radware, which provides DDoS attack prevention, firewalls, and network load balancing solutions, supports this. According to the Radware survey, "Despite one in four (24%) businesses reporting cyber-attacks daily or weekly, nearly 80% of surveyed organizations have not come up with a calculation for the costs of attacks, and one in three lack a cyber emergency response plan."

One approach to tightening up cybersecurity is to implement the most effective technologies—but those technologies are only as effective as the companies and people who operate them. This makes policy setting and enforcement a paramount objective for CIOs and CSOs.

So what are the best ways to go about developing sound cybersecurity policies and practices in 2018? Here are 10 recommendations.

1. UPDATE SOFTWARE AND SYSTEMS

After Spectre struck in January 2018, Apple issued security fixes for its iOS 11 operating system. This is no different from what other IT vendors do when they discover a security vulnerability. However, the rub for IT is making sure that the diversity of devices that are in the hands of users are all updated with the latest versions of a bevy of OSes. This requires centralized policy making in IT that likely adopts a "push " methodology, forcing new security updates onto a user's device when they connect to the network, instead of a "pull" methodology, which notifies the user that a new security patch is available and gives them the option to load this new software when it's convenient.

I have been a proponent of pull updates to software in the field because you never know when a user needs their device, and these updates can get in the way. But the volume and velocity of today's cyberattacks require tougher guidelines, since it is also true that many users never bother to pull an update to their devices. Consequently, in 2018's security environment, push is the surest security protection policy.

2. CONDUCT TOP-TO-BOTTOM SECURITY AUDITS

If your company hasn't already done so, it should conduct a thorough security audit of its IT assets and practices. This audit will review the security practices and policies of your central IT systems, as well as your end-user departments and at the "edges" of your enterprise, like the automated machines and IoT you might be employing at remote manufacturing plants. The audit should look not only at the software and hardware techniques you have in place to protect security but also at remote site personnel habits and compliance with security policies.

3. DON'T FORGET SOCIAL ENGINEERING

As part of your end-to-end IT audit, you should include social engineering, which reviews whether your employees are demonstrating vulnerability when it comes to offering up confidential information.

This social engineering can be as simple as someone shouting a password to a co-worker over an office partition—or it could be a user who pulls up a Website at work and surrenders passwords or other vital information that ultimately gets into the wrong hands.

"Requests for social engineering audits have increased," said Stuart Chontos-Gilchrist, CEO of E3 Technology, an IT security audit firm. "Companies are recognizing that it is people, more often than machines, who generate security breaches."

4. DEMAND AUDITS FROM VENDORS AND BUSINESS PARTNERS

According to a 2017 report by Commvault and CITO Research, more than 80% of companies see the cloud as integral to their technology. But with the move away from internal data centers, it's also become more important to demand regular IT audit reports from your vendors and business partners. Companies should have policies in place that require regular security audit reports from vendors they are considering before contracts are signed. Thereafter, vendors, as part of their SLAs, should be expected to deliver security audit reports on an annual basis.

5. PROVIDE NEW AND CONTINUING SECURITY EDUCATION

Cybersecurity education should be a staple of every new employee orientation, with new employees signing off that they have read and understood the training. On an

annual basis, a refresher course in cybersecurity practices should also be given to employees company-wide. This ensures that security policies and practices stay fresh in employees' minds, and that they understand any policy additions or changes.

6. WATCH THE EDGE

Manufacturing 4.0 and other remote computing strategies are moving computing away from data centers and out to the edges of companies. This means that a manufacturer with a remote plant in Ireland is likely to have manufacturing personnel operate automated robots and production analytics with local servers in the plant. Software and hardware security must be maintained on these devices, but the devices must also be locally administered under accepted cybersecurity policies and procedures by personnel who are asked to do these jobs without an IT background. This is a security exposure point for the company and for IT that requires training of non-IT personnel in IT security policies and practices, as well as oversight by IT and auditors.

7. PERFORM REGULAR DATA BACKUPS THAT *WORK*

If your data is compromised or held hostage in a ransomware attack, a nightly data backup will at least enable you to roll back to the previous day's data with minimal loss. It's a simple enough policy and practice to enact. Unfortunately, a bigger problem for companies is not so much that they don't perform data backups—it's that the backups don't always work. One of the most important cybersecurity policies that corporate IT can put in place is a requirement that data backups and disaster recovery minimally be full-tested on an annual basis to ensure that everything is working properly.

A successful cybersecurity strategy is one where you never find yourself in front of the CEO or the board having to explain how a cyber breach happened and what you are doing to mitigate it.

8. PHYSICALLY SECURE YOUR INFORMATION ASSETS

Even if software, hardware, and network security are in place, it doesn't help much if servers are left unsecured on manufacturing floors and in business units. Physical security, like a locked "cage" for a server in a plant that is accessible only to personnel with security clearance, is vital. Security policies and practices should address the physical as well as the visual aspects of information.

9. MAINTAIN INDUSTRY COMPLIANCE

Especially for companies in highly regulated industries like healthcare, insurance, and finance, regulatory compliance that concerns IT security should be closely adhered to. Companies in these industries should annually review security compliance requirements and update their security policies and practices as needed.

10. INFORM YOUR BOARD AND CEO

A successful cybersecurity strategy is one where you never find yourself in front of the CEO or the board having to explain how a cyber breach happened and what you are doing to mitigate it. Unfortunately, great security systems are "invisible," because they never give you problems.

This makes it important for CIOs, CSOs, and others with security responsibilities to clearly explain cybersecurity technologies, policies, and practices in plain language that the CEO, the board, and other nontechnical stakeholders can understand. If the nontechnical people in your organization can't understand why you are enacting a certain policy or asking for a sizable investment for a cybersecurity technology, you're going to have trouble making your case—unless you're all suffering through an embarrassing security breach that could end careers and put the entire company's survival on the line.

ELECTRONIC COMMUNICATIONS: WHAT NEEDS TO BE IN A GOOD POLICY

BY NATALIE GAGLIORDI

When it comes to essential security requirements for businesses, the electronic communications policy is decidedly unsexy. A painstakingly detailed document is rarely read in full outside of the employee onboarding process, and often languishes, unchecked, in the abyss of corporate paperwork.

That said, an electronic communications policy serves as the foundation for basic internet safety guidelines, business instant messaging practices, email standards, and general corporate policy for today's digital workplace. Without a solid policy in place, businesses open themselves up to a bevy of security issues, potential employee mishaps, and sometimes serious legal challenges.

WHAT DOES A GOOD POLICY LOOK LIKE?

In general, an electronic communications policy needs to be comprehensive, meaning it covers all forms of electronic communication, and well-defined.

"It's important to identify scope and purpose to help employees understand what you mean by electronic communications, and why this policy exists," said Heidi Shey, a senior analyst with research firm Forrester. "Does this only apply to email? What about VoIP calls, or texting, chat and messaging apps? Without a well-thought policy, everyone makes their own assumptions about what is acceptable use, and people may not know what they don't know about risks to the enterprise with using different forms of electronic communications."

Shey said it's also important to avoid making assumptions about the reader and to use clear, concise language that employees understand. A policy document should also provide a date for when it was last updated and a contact person for employees to go to if they have questions or concerns.

The most comprehensive, well-defined communications policies are usually written by a team of experts within an organization, spanning the departments of human resources, legal, audit and compliance, and information technology.

"That's because the document isn't about any one of these things individually," said Sean Pike, program VP for IDC's security products group. "It's about reducing risk throughout the business."

As far as terminology goes, the common bullet points in an electronic communications policy include:

- Guidelines on the appropriate use of email and other communication platforms
- Retention policies
- Proper internet usage

The policy should also contain clear language about prohibited uses of email, messaging platforms, internet and other electronic communications, as well as consequences and disciplinary actions for policy violations.

THE SECURITY RATIONALE

When it comes to email usage, the communications policy should set standards for appropriate content to send under the company banner, as well as rules for acceptable use and behavior, like avoiding personal messages and maintaining professionalism.

Precise guidelines are also needed to ensure that certain types of information remain within the confines of the business and only reach the eyes of intended recipients.

"The drivers are are often risk or regulation," said Pike. "Accidentally leaking corporate crown jewel intellectual property via email could be devastating, and accidentally emailing unencrypted personally identifiable information of customers could also create challenges."

Proper email usage is also key to preventing phishing scenarios. Corporate employees should be well-trained to avoid email that looks suspicious, and up-to-date anti-phishing training should be part of the email regimen in an effort to reduce security risks.

Policies surrounding email retention are needed to help companies ensure that they meet various data protection or retention requirements for relevant regulations, explained Shey. In healthcare, for instance, the Health Insurance Portability and Accountability Act (HIPAA) requires health care businesses to encrypt health data in transit and storage.

For financial services, the Financial Industry Regulatory Authority (FINRA) has issued guidance for social media and digital communications that requires archiving text messages for records retention purposes.

"This is so employees who are communicating with each other or clients using text messaging or a chat app for business purposes don't put the company at risk of non-compliance and possible data leakage," Shey said.

Both usage and leakage are important for internet guidelines as well. For the most part, companies want to make sure that users only go to approved web resources to reduce the risk of viruses or downloading unapproved software. Some companies even have policies that dictate behavior on an employee's personal social media accounts to reduce brand risk.

The exact details of a communications policy will vary depending on an organization's precise needs, but Pike noted that modern policies have trended toward being longer and more specific to ensure that every calculable risk is managed.

"There are plenty of ways to be destructive with communication, whether that's leaking information—accidentally or purposefully—or creating hostility toward a coworker," said Pike. "At the end of the day, these policies are in place to establish the way companies believe employees should act, or must act, given corporate culture or legal and regulatory obligations."

SAMPLE POLICIES

- If you need a place to start in creating or updating your company's policies, these templates from our sister site Tech Pro Research (a paid resource) can help:

- Electronic communication policy
- Internet and email usage policy
- Electronic Retention Policy
- Social media policy

DATA STORAGE AND ACCESS: WHAT YOU NEED TO APPLY IN ORDER TO ENSURE A GOOD, SECURE DATA POLICY

BY DANNY PALMER

Hacking, data breaches, malware, ransomware and more; no matter the size of organisation it can sometimes appear as if there's a cyber security related threat looming around every single corner, given how prolific and important data has become to the modern business.

But whether you are a global corporation or a small business there are best practices which can be applied in order to ensure that those responsible for handling, storing, transferring and using data are doing everything possible to keep it safe.

Organisations need to ensure they have taken the time to set out best practice and good policy on data storage to make data as secure and resilient as possible, at every level.

"It starts with understanding your data. Not just where it lives, but also classifying that data" said Julie Cullivan, CIO at network security form ForeScout told ZDNet.

"Focus on understanding what your most critical services and data is and making sure you really understand where it lives and that you have the right controls and policies around that as priority. Companies which try to address everything if it's all created equally, suddenly end up in this situation where you've protected nothing." she said.

In addition to different types of data having different levels of sensitivity, organisations also need to consider different strategies for data in different scenarios. That might be at rest, when it is physically stored on a device, be it a data warehouse, a network of computers, or even a single smaller device like a smartphone or a flash drive.

There's data in use, which specifically refers to data actively being processed , and then there's data in transit, which is when data is flowing from one place to the other, be it over the internet or in a local area network.

When thinking about all those states of data, organisations need to determine the potential risks to it, then use that decide what action needs to be taken to protect all of that data.

"It sounds really basic, but it's about understanding what you have or what you come into contact with," Emma Wright, Commercial Technology Partner at law firm Kemp Little told ZDNet.

"Because your information security policy shouldn't be one-size-fits-all, it should be a multi-layer approach which takes into account both physical and cyber security measures apply to the data".

For example while it isn't necessarily essential to encrypt all forms of data—although it should certainly be applied to sensitive information such as credit card information, personal details and other critical data—a good policy is to take stock and examine how data is stored.

In some instances, sensitive data can be anonymised, but even then, you should be asking yourself if there's any reason why encryption shouldn't be used. "Your starting position around personal data should be 'why is it not encrypted'?," said Wright.

But a data storage policy isn't just about encrypting it and hoping for the best, because not every individual in an organisation needs access to all of the data it holds. That's why access controls over who can access and use data—and for how long—need to form part of good data storage policy.

In some instances, sensitive data can be anonymised, but even then, you should be asking yourself if there's any reason why encryption shouldn't be used. "Your starting position around personal data should be 'why is it not encrypted'?" —Emma Wright

"Most organisations that have identity and access management policies start with a standard image—every employee has access to these systems and this data. Then you start just narrowing it down to role-based access and depending on the risk and the data and the applications they have access to," Rashmi Knowles, EMEA Field CTO for RSA Security told ZDNet.

The idea is that only users who are required to handle sensitive information have access to it, reducing the risk of it being mishandled by other users. And this isn't a one-time job; organisations should be regularly reassessing who needs access to what data and what they need it for, especially if sensitive data is involved.

"If you have privileged users, who have access to sensitive data and it's critical to the business, typically you'd revisit that every three months to check that access is still relevant to that role. Then from a compliance perspective, you'll have visibility of that fact," said Knowles.

Even if you set out good policy around data control based around of knowing what you have, encryption and access within the boundaries of your organisation, the nature of the modern business means it's highly unlikely that all of your data is going to be contained within just your walls.

If your organisation has suppliers or contractors, they will end up handling your data in some way.

They too, will therefore need to ensure that their policy is up to scratch - perhaps even more so, considering how the supply chain is viewed by many hackers as a soft underbelly for attacks—so it could be up to you to help them comply with that.

"Companies are engaging with suppliers and they're not seeing their information security as something which needs to be extended down the chain," said Wright.

"They think the information security stops within their systems when in fact if you can access a system or you're sending your information to someone else's system, you've got to apply the same level of controls from the third party," she added.

It's understandable that all of this might sound somewhat intimating, but there are government issued guides such as the Networks and Information Systems (NIS) directive which contains detailed, but step by step guides on implementing strategies around data security policy.

But while having a good data storage policy is good practice in any case, there's a looming deadline for organisations which have policies which aren't up to scratch—that's the introduction of General Data Protection Regulation (GDPR) as law across the European Union on May 25.

It might sound Europe-centric, but the legislation will apply to to any organisation in the world which does business in EU countries.

While some are fearful of GDPR, given the potential for huge fines if organisations are found to have suffered a data breach while being non-compliant, it could be viewed as an opportunity for organisations to revisit what data they have and assess what it is, why it has been collected, what consent they have for processing it—and if there's no good reason to keep it, delete it.

"Policy and process is the biggest burden in GDPR, but it's a good opportunity for organisations to start from scratch and ask what data do we collect," said Knowles.

"It gives them an opportunity to start from scratch and get their house in order so they have really good visibility of where they are, where their third parties are, how their data is protected and what that data lifecycle is, all the way from when it is collected to it being deleted".

HOW TO WRITE A GOOD SECURITY POLICY FOR BYOD OR COMPANY-OWNED MOBILE DEVICES

BY TEENA MADDOX

Mobile devices are among the most vulnerable tech items we own, because they're easily exploited and can be quickly compromised by hackers.

It's essential for a company to have a solid security policy in place for mobile devices, whether bring-your-own-device (BYOD) or company-provided. Allowing employees the option to buy their own devices can save a company money, and employees can benefit from the familiarity of using their own smartphone or tablet. But it does open up a company to security risks.

According to Tech Pro Research's Scott Matteson, "Since employees use their devices for personal and/or recreational activities, this can pose more risk for the organization than the exclusive use of business-owned devices."

CBS Interactive, parent company of ZDNet, TechRepublic, and Tech Pro Research, has created a list of best practices for securing a mobile device for its employees:

- Keep the software up to date
- If you lose it or it's stolen, report it immediately
- Use a secure PIN
- Don't connect to public Wi-Fi networks
- Back up your device
- Encrypt your device

The greatest risk comes from BYOD devices, according to Engin Kirda, Ph.D., co-founder and chief architect of malware protection provider Lastline.

"It is important to make sure that BYOD devices can only be used in so-called 'demilitarized zones' within the organization. That is, the devices should not be able to directly access sensitive resources, and access should only be allowed to some organizational resources through VPNs. It is also important to be able to monitor the use of such devices through the network, and keep track of when, where, and how these devices connect," Kirda said.

Galina Datskovsky, CEO of Vaporstream, said, "In order to reap the benefits of BYOD while mitigating physical and digital security risk, corporate leaders and risk managers must provide a BYOD Acceptable Use Policy that specifies how employees can use their own devices to access and process corporate data. This policy should also include which specific applications may be used to share or discuss corporate information."

> **"User awareness and education is also a very important component when it comes to BYOD type of work environments. With great power comes great responsibility."**
> **—Engin Kirda**

Datskovsky added, "Most importantly, company leadership must hold their employees accountable for following such policy. With 90% of all cyberattacks beginning with phishing, organizations are under constant threat of complex attacks targeting employees that can easily bypass gateways and land in email or text inboxes. Since employees use their devices for email and text to conduct business, a secure messaging strategy must be considered an essential component to any BYOD initiative."

Company-owned devices are easier to secure, since the organization can control them.

"For example, the company can make sure that these devices are not rooted, and can also check which programs the user has installed and is running on the company-owned system. There is also the option of installing security software (such as end-point monitoring agents) on these company-owned devices," Kirda said.

Datskovsky said, "It is more manageable to secure company-owned devices than it is to secure devices used via BYOD policies. Through the use of mobile device management (MDM), IT departments can limit the application and program options that employees can use in order to restrict downloads, block websites and monitor network traffic for suspicious activity. To keep corporate-owned devices protected from potential security threats, IT departments must ensure that all applications offered on company-owned devices are secure, meet compliance standards and offer encryption. Policies must also be in place to help ensure proper use by employees to protect from the ever-changing hacking landscape."

Some of the potential problems stem from rogue Wi-Fi in public venues, since a typical user can't easily determine whether the network is authentic and belongs to the organization.

"We have seen attacks in the past where rogue Wi-Fi routers have played an important role. Such attacks can sometimes take place if the device automatically connects to known networks. By automatically deactivating Wi-Fi when the device is not in use, such automatic connections can be prevented. Also, the user can be encouraged to create profiles that are used based on the physical location of the device. User awareness and education is also a very important component when it comes to BYOD type of work environments. With great power comes great responsibility," Kirda said.

Larry Lunetta, vice president of marketing for security solutions for Aruba, a Hewlett Packard Enterprise company, said, "Rogue clients and ad-hoc networks add to a company's risk profile. One possible solution is to utilize intrusion prevention system (IPS) functionality built into the network infrastructure itself. Clear policies for rules and network traffic, paired with an alerting detection system, give network administrators information and options to react.

Lunetta added, "We also counsel organizations to create public Wi-Fi safety measures. Using public and open Wi-Fi is fraught with risk and any devices that have connected to these networks can easily bring malware into an organization's network. This is another area where focused IPS functionality can aid in the detection of odd network behavior."

Another potential problem is public USB ports, since many attacks can be launched over USB.

"In a secure environment, public USB ports are often disabled so that an attacker cannot launch a physical attack (e.g., by attaching a fake keyboard), or booting a version of Linux that has been specifically-created for launching attacks," Kirda said.

George Avetisov, CEO of HYPR, said, "Public USB ports are a security no-no and should be avoided. A USB port is a common delivery method for malware and that is why internal security policies at enterprises often disable USB ports on company-owned devices. Some companies actually ban USB sticks entirely and may even reprimand employees for bringing them in."

And then, there is the risk from broken or lost mobile devices.

Lunetta said, "If a mobile device is broken or lost, endpoint and MDM solutions can help. Whether installed on a BYOD or a company-owned device, these platforms can provide fencing around work-related emails and documents. These platforms also offer the ability to push a remote system wipe, as a last resort, should a device with confidential or sensitive files go missing. With BYOD, network administrators can only impact company owned information such as e-mails or documents delivered through work systems. With company owned devices, the entire device can be wiped remotely, removing all data and access."

PASSWORD SECURITY TIPS: HOW TO CREATE A BETTER SECURITY POLICY

BY NICK HEATH

In recent years the received wisdom on passwords—that they need to be complex, lengthy and changed frequently—has begun to be challenged.

These type of passwords are not only potentially insecure, but following these guidelines can open up major holes in an organization's defences.

Leading security figures in the US and the UK have said it's time for businesses to look beyond the traditional advice and consider approaches to password security that work in practice, not just in theory.

Here's what you need to know to put together a robust password policy for your firm.

DON'T REQUIRE REGULAR PASSWORD CHANGES

Although many organizations follow the advice of forcing staff to change passwords every 30 to 90 days, the practice "carries no real benefit", according to guidelines from the UK's National Cyber Security Centre (NCSC), due to the fact stolen passwords are generally "exploited immediately".

Such a policy can even reduce security, due to users using variations of the same or similar passwords, or choosing the simplest password possible in order to minimize the hassle. That employees would choose the most straightforward password they can is hardly surprising, according to Dr Ian Levy, technical director at the NCSC, who says that once you take into account the myriad services the average person uses each day, forcing staff to make frequent changes is akin to asking them to "remember a different 660-digit number every month".

One way to limit password reuse is by forbidding choices too similar to previous passwords.

"Storing password history and checking their next password against their previous password gives companies a bit more ability to enforce, to ensure that every password is in fact unique from the previous one," says Merritt Maxim, principal analyst serving security and risk professionals at Forrester.

However, instead of forcing frequent changes on workers, the NCSC advises monitoring log-ins to detect unusual activity and notifying users of attempted log-ins—with the expectation they report any they weren't responsible for.

Basically, you should only ask users to change their password if you suspect it has been compromised, according to the NCSC.

CHOOSE TECHNICAL DEFENCES OVER COMPLEX PASSWORDS

The NCSC says that requiring users to devise lengthy and complex passwords composed of multiple types of characters often fails to achieve the desired security, due to people using predictable strategies to meet the requirements.

"The security benefit is marginal while the user burden is high," the NCSC guidelines state.

People will typically look for shortcuts when asked to choose complex passwords, reusing the same option multiple times or choosing predictable strategies, such as replacing the letter 'o' with a zero.

Attackers are aware of this behavior and seek to exploit it via brute-force attacks, which will prioritise frequently used words and common character substitutions.

Instead of enforcing a complex password, the NCSC recommends systems that:

- Defend against automated guessing attacks, such as locking the account after a certain number of failed guesses or limiting the rate at which passwords can be submitted. When locking accounts in the event of multiple password guesses, allowing 10 attempts strikes a good balance between security and usability.
- Blacklist common password choices.
- Monitor log-ins to detect unusual use and to notify users with details of logins, successful and unsuccessful.

ENCOURAGE THE USE OF THESE TYPE OF PASSWORDS

Good choices for striking a balance between memorability and security are passphrases, four random dictionary words or CVC-CVC-CVC (consonant-vowel-consonant) passwords.

TRAIN STAFF TO AVOID COMMON PITFALLS

Even if your company requires a complex password, that doesn't prevent users from undermining security by choosing easy-to-guess options.

Training and post-training FAQs should warn staff about common mistakes when choosing passwords, like:

- Basing it on personal information.
- Using simple dictionary words.

- Relying on predictable keyboard sequences, for example, QWERTY.
- Reusing passwords across multiple services—especially between work and home. This is particularly an issue in the modern world where the average adult is estimated to have about 25 online accounts.

Forrester's Maxim says firms should also stress the reasons for changes to password policy.

"If context is provided around the reason for the changes, users are much more accepting of it," he says.

It's also important to ensure that your outsourcing companies meet internal data protection and password security standards by stipulating compliance in their contracts.

MINIMISE YOUR USE OF PASSWORDS

Do everything you can not to overload staff with password-protected systems.

- Only password protect systems where access needs to be securely controlled.
- Consider alternatives that make it easier for staff to manage passwords, such as single-sign on or password synchronisation.
- Help staff remember passwords by providing a suitable way for them to store passwords, either physically, in a secure filing cabinet, or digitally, via password management software. Gartner highlights LastPass Enterprise, Keeper Business and Dashlane Business as being among the few business-targeted password managers available. Forrester singles out Lieberman Software and ManageEngine, while also recommending checking for integration with other Identity and Access Management Systems (IAM) and, in the case of Microsoft shops, with Active Directory. However, be aware that password management software is a tempting target for hackers. Buying a separate password management tool may not be needed as these tools are often included as part of web access management products or identity-as-a-service and IT service desk offerings.
- Consider using Privileged Access Management technologies to help control and manage passwords and secure access to systems.

PICK THE RIGHT KIND OF MACHINE-GENERATED PASSWORDS

If your company is choosing to issue staff with machine-generated passwords, it's important to be aware of the potential downsides.

Choose a system that generates passwords that are easy for users to remember while still being relatively secure, otherwise you increase the risk of users storing passwords in an insecure fashion.

As with user-chosen passwords, examples of the type of passwords that strike the correct balance, according to the NCSC, are passphrases, four random dictionary words or CVC-CVC-CVC (consonant-vowel-consonant) passwords. It recommends letting users choose the password they find the most memorable from those generated.

DON'T SHARE PASSWORDS BETWEEN USERS

Sharing passwords is not only a security risk but removes the ability to reliably audit a user's actions in the event of an issue.

The NCSC recommends using a hardware token, such as an RFID badge, as a better alternative to passwords for controlling access to shared systems.

CHANGE DEFAULT PASSWORDS

Always change factory-set or default passwords on systems before they are deployed. Where you're uncertain over whether they've been changed, run a check for any instances of default passwords being used.

PUT EXTRA PROTECTIONS IN PLACE FOR REMOTE USERS AND ADMINS

Given administrator accounts will have broad permissions to make changes across the corporate network, these accounts should not be used to

IMAGE: ISTOCK/RTIMAGES

carry out less important and potentially risky day-to-day tasks, such as browsing the internet and checking mail. Instead create a separate account with fewer privileges for admins to use for non-administrative, everyday activities.

According to the Gartner report *Four Kinds of Password Management*, it's not only the passwords that need to be carefully considered, but also the reset policy, with a requirement that reset policies are designed to resist social engineering and other attacks against administrators.

Users logging into systems remotely over VPN or to systems such as webmail should also be required to log in using some form of two-factor authentication (2FA) alongside their password.

PASSWORDS SHOULD NEVER BE STORED AS PLAIN TEXT

Passwords should be hashed and salted, that is be mixed with random data before being run through a one-way cryptographic function that converts them into a 'hash'.

Run periodic searches within documents, emails and spreadsheets for plain-text passwords. These can often be located out by searching for tell-tale strings such as 'password'.

Only use approved public algorithms such as AES, RSA public key cryptography, and SHA-256 or better for hashing. Do not use weak algorithms, such as MD5 or SHA1.

MAKE SURE YOUR PASSWORD POLICY MEETS REGULATORY STANDARDS

Remember to check that your password policy meets the applicable regulatory and audit requirements for your firm.

DON'T FORGET ABOUT LEGACY SYSTEMS

Forrester's Maxim points out that large companies need to consider whether older systems can meet the firm's password requirements, for example demanding use of special characters.

"Those kind of passwords may not work for some legacy systems," he says.

"So you need to understand whether your policy will be supported in every kind of system in your environment, and if there are ones where it doesn't work, you need to find ways around that."

TRAVEL AND REMOTE ACCESS: WHAT NEEDS TO BE IN A GOOD POLICY

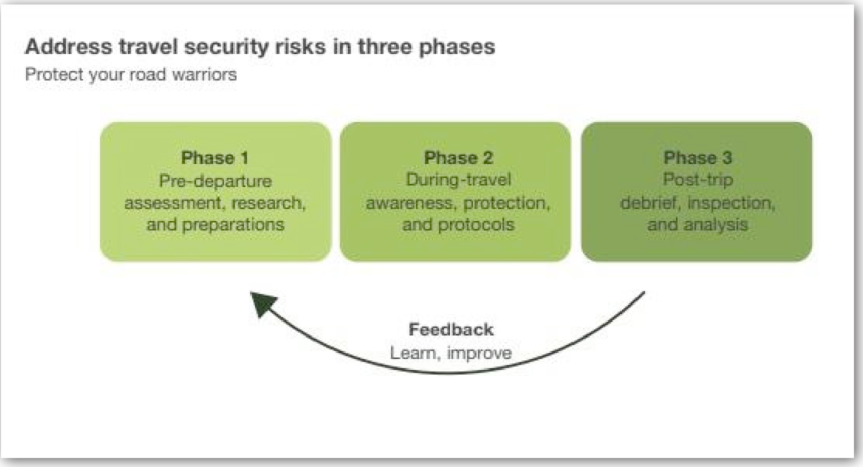
BY STEPHANIE CONDON

Thanks to growing connectivity and the increasing mobility of devices, working outside of the office has become more and more commonplace. Large enterprises and small businesses alike have employees who are taking their work on the road. And as the world becomes more connected, a company of any size may need employees to pursue business in different cities or different countries.

Business travelers, however, face a unique set of risks. Travelers in an unfamiliar place -- and without their company's infrastructure to support them—could be more susceptible to incidents like theft or weather-related disasters. Outside of the office, they could find themselves more vulnerable to state-sponsored or nonstate-sponsored actors with malicious intentions. Even in a home office or a local Starbucks, workers could be putting corporate data at risk.

"Companies with more distributed and global workforces are sussing this out on a daily basis," Forrester analyst Merritt Maxim said. Travel protocol, he said, "is not just about employee safety, it's about data and businesses doing their best to protect themselves from breaches, whether they're malicious or inadvertent."

In response to companies asking for advice on securing business travelers, Forrester has produced a guide for security and risk professionals called "Best Practices For Minimizing Business Travel Risk." It offers detailed guidance on preventing cybertheft, espionage and physical harm. The guide advises companies to create a security program for travelers that includes three phases: pre-departure, during travel, and post-trip.


Address travel security risks in three phases

Protect your road warriors

Phase 1
Pre-departure assessment, research, and preparations
Phase 2
During-travel awareness, protection, and protocols
Phase 3
Post-trip debrief, inspection, and analysis
Feedback
Learn, improve

IMAGE: FORRESTER

PRE-DEPARTURE BEST PRACTICES

- Assess your threat level
- Avoid stereotyping and assumptions
- Implement device management
- Enable secure communication methods
- Manage people, not just devices

The first step in preparing for business travel is assessing the threats and risks involved. That means throwing out any unfounded assumptions about where your employees are going.

When it comes to security breaches, “usually people think these are things that only happen when they go to a far flung country,” Maxim said, “but there’s still the ability to exfiltrate data from devices from users in public or semi-public places anywhere.”

That said, some nation states present greater risks, Maxim said. “Even if you’re a low-level employee without much access to information, your machine may still be useful as a machine to load malware onto, which could be used to infect other systems and allow them to do reconnaissance and gain information about your company in the future.”

Along with assessing the threats of a particular location, businesses should consider the identity of the traveler. What is their job title, and what information do they have? Do those factors make them more of a target?

The next step is to equip your employees with the right tools. According to a survey from the Association of Corporate Travel Executives (ACTE), employees are increasingly pressing their managers about corporate communications policies. In the survey, which polled the ACTE’s global membership, 37 percent of managers reported seeing a rise in the past year in inquiries about on-trip connectivity and communications.

“Companies are starting to look at what devices do we want our folks to travel with, what access should they have on the road,” said ACTE executive director Greeley Koch.

Some businesses, he said, give employees loaner devices that are scrubbed by the IT department following a trip. Others take stock of where an employee is going and what they’re doing on the road, and they restrict their device usage accordingly.

The Forrester guide suggests preparing devices for travel by enabling full disk encryption, disabling USB ports, enabling VPN access, installing IT management tools that enable remote wiping if necessary and ensuring a recent backup of the device is available.

Additionally, device management can include methods to ensure a device is "tamper evident." Something as simple as putting stickers and glitter nail polish over the screw holes of a device can add a helpful layer of security to make it obvious if someone tried to tamper with it.

"You might hear about devices that are tamper resistant, but tamper resistant is not as important as tamper evident," Maxim said.

Forrester also lays out steps for establishing secure communications methods. "This can be as simple as establishing email as the main point of communication or having your business travelers download Secure Chat, Signal, Telegram, or WhatsApp," the guide says.

Device management is a "crucial" step for securing data, according to Max Saltonstall, technical director of the Google Cloud CTO Office. The next step, he said, is "knowing your people."

While some companies limit travelers' devices, Google uses its employees' identities as a means of limiting information, in or out of the office.

"It can be hard for some companies to know, for instance, that Alice joined in finance but then she switched to legal -- should she have the access of someone in finance, or legal or both?" Saltonstall said.

Google, he said, "had to take a hard look at how we track hires, fires, transfers, how we understand when someone has shifted teams, or shifted roles -- how do we communicate that person's role to give them the appropriate amount of access and trust."

BEST PRACTICES DURING TRAVEL

- Help employees stay productive
- Consider government policies and border policies
- Stay vigilant of human threats

Identity is one key element behind Google's custom-built security system, BeyondCorp. The other key element is device inventory. BeyondCorp routes all traffic through a proxy to determine who the user is and what internal data they're allowed to access. It also determines whether they're using a Google-approved device that's clear of any malware.

"We've shifted from giving you access based on where you're sitting," Saltonstall said. "Instead, I know who you are and what you're using."

Google developed BeyondCorp about eight years ago, after growing into a massive company with a highly-mobile workforce. At that point, VPN-based security models were "hampering people's ability to get work done whether it was inside or outside the office," Saltonstall said.

VPNs can be hard to use on tablets and smartphones, he said. Meanwhile, if a bad actor gets past traditional, perimeter-based security systems, they'll get access to everything on the device.

Google has taken what it's learned from building BeyondCorp to develop a product called Identity Aware Proxy (IAP) for Google Cloud customers.

The security model is premised on the notion that "anybody should be able to work from any device, from any location, without special VPN software," Saltonstall said.

Forrester's research shows that an effective travel policy should indeed keep in mind worker productivity. In a 2016 survey asking workers why they sometimes go around company security policies, 46 percent cited efficiency.

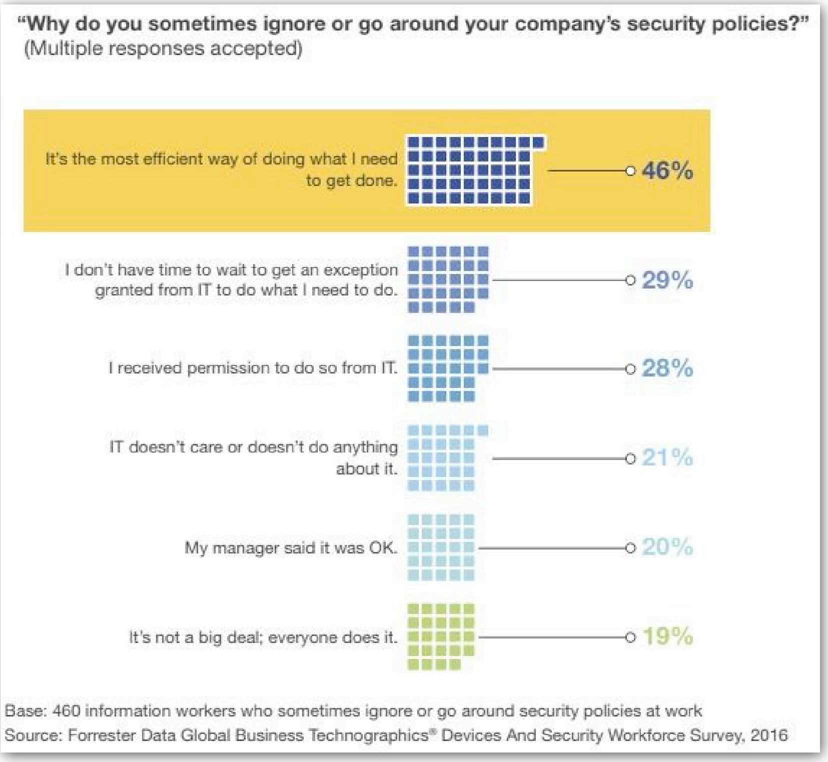


IMAGE: FORRESTER

Beyond device access, travelers need to think about the context of their surroundings. For international travel, a sound policy should consider different government rules and regulations, the ACTE's Koch said. Last year, when the US banned electronics from airplane cabins on flights to the Middle East, many ACTE members had to reevaluate their device policies, he said. Companies should also advise their workers on how to proceed through borders, where government officials may try to access their devices.

"Rules are changing all the time, threats are coming in different ways," Koch said. "Companies need to stay up to speed."

Travelers also need to think about their in-person interactions.

Travelers need to keep in mind that people may be listening in on their conversations or snooping over their shoulders.

"Our interviews revealed that the human threats, a.k.a. honey traps, are often ignored altogether," the Forrester guide says. "This translates into a need for caution with interactions, such as being approached in a hotel bar by a stranger offering them a free drink. Encourage travelers to keep their devices with them at all times if possible."

Travelers need to keep in mind that people may be listening in on their conversations or snooping over their shoulders. They should be on the lookout for common criminals who may want to snatch a device simply to resell it. Also, they should make sure they don't lose their devices while on the road.

POST-TRIP BEST PRACTICES

- Implement a post-trip checklist
- Debrief, even if nothing went wrong
- Keep policies up to date

Once a traveler is back from a trip, Forrester suggests running through a list of actions such as changing passwords or running a device through forensics. Businesses should also debrief employees to find out, for instance, about any suspicious behavior encountered on the trip.

Even if a worker travels without incident, a debrief can provide valuable information for future travelers, Maxim noted.

Lastly, policies should be regularly updated. Data theft is an ongoing, evolving risk, Maxim said.

"Businesses are changing as well," he said. "They're making acquisitions, which could alter where their travelers are going... Make sure you have an understanding of how those policies need to adapt."

SAMPLE POLICIES

If you need a place to start in creating or updating your company's policies, these templates from our sister site Tech Pro Research (a paid resource) can help:

- Remote access policy
- Encryption policy
- Travel and business expense policy
- Information security policy
- Data classification policy

VENDOR SELECTION: WHAT NEEDS TO BE IN A GOOD POLICY

BY CONNER FORREST

Operating a company in the modern enterprise landscape requires a reliance, to some degree, on third-party vendors. It's unavoidable. But the addition of each new vendor brings with it a certain amount of risk.

In the past few years, vendors have been at the center of high-profile breaches at major firms like Target and Verizon. However, companies don't have to accept data breaches as the status quo for working with outside partners, and can take steps to mitigate the risk of bringing on a third-party provider. It all starts with a proper policy that accounts for vendor security audits.

Starting small is key. Company leaders should work with their CISO or CSO to determine their minimum acceptable security standards, and use that as baseline criteria, according to Gartner research director Mark Horvath. This should be done even before a request for proposal (RFP) or request for information (RFI) is written, Horvath said.

IMAGE: ISTOCK/ FIZKES

"Every organization will have a set of requirements which are informed by the relevant industry standards and the unique needs of the organization. These should be written as a policy long before any vendor inquiries are made, so that they can be addressed up front with the vendors. The goal is to avoid the problem of buying a product and then discovering later that it violates privacy or security policies in a way which hinders the business case for the purchase."

Once those minimum requirements are determined, the company must look at each vendor individually. There will not be a standard approach that will work with each type of vendor, according to Daniel Kennedy, research director at 451 Research.

A good place to start with separating the needs of different kinds of vendors is by creating a risk quotient around each vendor's product or service. This will help a company better decide how much time to spend on an assessment.

Kennedy recommended asking the following questions: "Is the vendor handling or managing some type of critical data, whether intellectual property or customer personal information? Is the vendor product/service involved with a critical business function, or directly affect revenue or expenses? Is the vendor's service a single point of failure?"

Once these questions have been answered, a company can begin its due diligence, Kennedy said. Companies should send questionnaires, interview key employees at the vendor, request materials, and try to schedule a site visit if possible. According to Kennedy, these are some additional questions a company should be asking the vendor:

- Is the vendor mostly free of negative publicity?
- Can the vendor provide references to confirm that it delivers on contractual obligations?
- Does the vendor have a security officer and clear security policies in place?
- Does the vendor have a realistic business continuity or disaster recovery plan?
- Is the vendor financially viable? (i.e. Are they profitable, or are they still running on investor funds? Do they have other large clients? What is their exit strategy?) Can they turn over a SSAE 18, SOC 2 report if appropriate?
- Does the vendor perform third-party vulnerability assessments of their services, and will they share the results?
- Will the vendor agree to additional testing?
- What provisions can the vendor support for ongoing assessment of their controls once the contract is signed?

Horvath also recommended that companies ask the vendor to provide a manifest of the open-source code they use in their product or service.

"Open source code is widely used in application development, which is fine, but OSS libraries are often updated in response to security evens (e.g. Heartbleed), so knowing what open source code is in a product is critical to being able to maintain it," Horvath said.

Of course, there are also the standard contract elements that must be considered, Kennedy said. Enterprises should work with their IT leaders and executive team to draw up SLAs for availability, quality, and responsibility. Other factors to consider include insurance needs, non-disclosure agreements (NDAs), and what will happen in the event of a data breach.

Unfortunately, Kennedy said, many companies think they are covered under state laws, but those often don't protect an impacted firm from having to notify its own end users.

Understanding a vendor's data retention, attribution, privacy, and deletion processes, and whether or not company data will be deployed to the cloud, is critical.

"Those customers don't blame the tiny supplier they didn't even know about, they blame you," Kennedy said. "Under what terms can you get out of the contract, or reduce its scope if conditions change?"

Prior to purchasing, a company should be able to validate the vendor's testing processes, including their methods for testing application security, Horvath said. Knowing how the vendor will notify their customers in the event of an outage is also helpful, as it allows the purchasing company to more effectively alert their own users, and to remain compliant with regulations like the EU's General Data Protection Regulation (GDPR), Horvath said.

Speaking of compliance, Horvath also noted that vendors should be required to provide a policy for protected data, and proof of compliance with appropriate standards for the company's industry. Understanding a vendor's data retention, attribution, privacy, and deletion processes, and whether or not company data will be deployed to the cloud, is also critical.

In considering the vendor security audit as a whole, Forrester Research principal analyst Duncan Jones recommended integrating that audit with other assessments such as service reliability and financial stability.

"Too often I see discrete assessments by different functions, which overloads suppliers and creates gaps through which risks can enter the organization," Jones said. "You need one single platform to manage and record all the assessments, including security."

Adapting the audit to the context of the vendor and what product or service is on the table is also important, Jones said. However, don't write off startups and smaller companies, he added. Rather, "refine the process so that you can work with emerging suppliers on innovation and pilot projects without completing a full audit, because being overly risk averse stifles innovation," Jones said. "Try to defer the assessment until you are ready to scale up the relationship."

Finally, consider the data. Companies should look to providers that collect risk data about certain vendors, and "syndicate that out to multiple clients—a sort of community-based approach, rather than an egocentric one just for yourself," Jones said. "That reduces the workload for the suppliers and for you, and improves the reliability of the intelligence collected."

INCIDENT RESPONSE: WHAT NEEDS TO BE IN A GOOD POLICY

BY ALISON DENISCO RAYOME

It's almost completely certain that your organization—no matter its size or industry—will at some point experience a cyberattack. As such, it is imperative that every company create and routinely test incident response policies to keep systems operating and reputations intact.

"Whenever there's a breach or an incident, the way that the organization responds is going to be judged critically by their customers, their peers, and their board," said Josh Zelonis, a senior analyst serving security and risk professionals at Forrester Research.

In many cases, "organizations are caught flat-footed, and the consequence is that it moves very quickly from an impact on an IT system to a more meaningful impact to the organization, including reputational damage," said Matt Stamper, research director of risk and security management programs at Gartner, pointing to the Equifax breach.

Organizations need an incident response policy, and, perhaps most importantly, a number of playbooks that allow them to think through a variety of different incident scenarios, Stamper said.

When employees work through an attack scenario, they realize that cybersecurity is not an issue that only impacts IT, but also human resources, vendor management, and lines of business, Stamper said.

"We do need to be engaged in the process," Stamper said. "Planning for it is better than reacting to it."

The most fundamental part of the policy is an organizational document that outlines what the plan will be, how it's going to be created and maintained, and who they key stakeholders are, Zelonis said. Incident response plans are often very high level, he added: Some of the best he's seen are only a couple of pages long. "It's almost a statement of how we're approaching this process," Zelonis said.

The document and language used should be simple to read under pressure, and focus on managing the consequences, rather than the causes, of an incident, according to a Gartner report.

Playbooks, on the other hand, are more granular, and describe in detail how to respond to specific threats like ransomware. "You usually have multiple playbooks and one overall incident response policy that governs how you will go, building the team and maintaining this body of work," Zelonis said.

A good incident response policy should include the following, according to Stamper:

- The lines of business in scope.
- Who is authorized to remove or contain a compromised system, and how doing so might impact the availability of a higher level function.
- The response priorities in an organization. For example, an COO's goal may be to return a system to operational availability as soon as possible, while a legal counsel's goal may be to investigate and gain evidence. "Having those types of scenarios evaluated and fleshed out in a policy, more appropriately in the documents that are related to that, your playbooks and your plan is really critical," Stamper said.
- The level of risk tolerance that is appropriate to the organization.

The policy should also detail at what point an organization engages its legal counsel, its cyber insurance provider, and its public relations (PR) team to handle messaging, Zelonis said.

"As we've seen, particularly in the last year with Equifax, the C-level drops when you have bad PR around a breach," Zelonis said. "It escalates a bad situation out of control, and people will have to lose their jobs."

These plans are often created by a CISO or chief risk officer, Zelonis said. But legal counsel should also be involved in the creation of the policy, especially with GDPR and other regulations looming, he added.

The policy should detail at what point an organization engages its legal counsel, its cyber insurance provider, and its public relations (PR) team to handle messaging.

"As soon as you realize that an incident needs to be escalated, the people who should be running things are actually attorneys," Zelonis said. "Whatever region or country that you're in, you need to have specific legal expertise in that area."

While most organizations have an incident response plan, those plans are often never tested, Stamper said. He recommends doing tabletop exercises to have employees work through the process, and evaluate its strengths and weaknesses.

"When you're dealing with a security incident, there's this inherent asymmetry—I don't know what the attacker is after, I don't know how much my environment has necessarily been compromised yet. I'm in this kind of very acute, highly reactive environment. I don't know if I'm authorized to make this decision, or the impacts of all of the sudden the news reporting the fact that a critical business unit has been compromised and we're not prepared for it," Stamper said.

"You want to get as much of that muscle memory in learning accomplished in a safer exercise, like a tabletop, sooner rather than later."

Running real-world drills beyond tabletop is also a good way to test your incident response plan, according to Bruce Beam, director of infrastructure and security at the nonprofit (ISC)². This way, you implement your crisis action team and go through the full process of an attack, he said.

One way to do this is by hiring a third-party vendor to oversee running the drill, to avoid internal bias and create a report that can be used for later assessment, Beam said. "You work with them to come up with a realistic scenario that's actually something that you've seen in the news or something that would have a real true impact," Beam said. "Then you take this scenario up to upper management, ensure that they're okay with looking at critical times to exercise this."

For example, this might involve injecting the system with a containable, known malware, and include prompts to ensure that HR, PR, and legal teams are all involved in the process so they can see it from beginning to end. Ultimately, you want to critique and realign your processes and policies to correct any deficiencies, Beam said.

Ideally, an organization's plan should be tested on a quarterly basis, Stamper said, even in an informal tabletop exercise within a small group or department.

While many companies do have a policy, they often don't have top-level buy-in, or it is not used appropriately, Beam said. To fix this, companies need to invest in their security personnel, to make sure they are able to brief executives and board members on risks and responses.

"It's very important that a company has someone in that position that can articulate from the senior level down to the security team and ensure that everything's being captured in the proper way and reported back up and down as necessary," Beam said.

SECURITY TRAINING IS USELESS UNLESS IT CHANGES BEHAVIOURS

BY STILGHERRIAN

Security training is useless unless it changes behaviours Many corporate security awareness programs fail because there's no real motivation for employees to even care, according to Laura Bell, founder and chief executive officer of SafeStack.

"You can teach somebody the technical bits and pieces till you're blue in the face, whether it's electronically or in person, but unless you can get them to care about the why, you'll never see a change in their behaviour," Bell told ZDNet.

James Turner, security advisor with consulting firm IBRS and founder of CISO Lens, agrees. He says it's all about the organisation's staff engagement level.

> **"If you're just going to be pumping out an awareness campaign and you've got low engagement, stop and let the HR people focus on engagement first."**
> **—James Turner**

"If you have a low engagement level with your staff, you're effectively saying, 'I want you to change your behaviours, and I know you don't give a s*** about the company, but do it anyway.' You're asking staff to behave completely altruistically for a company that they feel no connection with," Turner told ZDNet.

"If you're just going to be pumping out an awareness campaign and you've got low engagement, stop and let the HR people focus on engagement first."

Turner says some of the top security executives have started making security training a core part of the organisational change process by firstly training staff in personal e-safety. Topics include the privacy issues in using Facebook and communications platforms like WhatsApp, safe internet banking, and how to talk to their kids and teenagers about internet safety and cyberbullying.

"[These are] issues that are directly relevant to them in their home lives [and] their families," Turner said. That provides an opportunity for the HR team to start improving engagement.

"The company is going, 'We actually give a damn about you as a human being. This stuff is important. As much as we need you to change your behaviour here at work, we're recognising that we actually need you, as one of our valued staff, to be safe at home.'"

It's also important, however, that creating an awareness of the risks doesn't turn into fear mongering.

"It's the difference between recognising that you're driving a car, and that there's other moving objects and so on around you, and that there's a safety issue but you should be fine provided you understand what you're doing and what everyone else around you is doing," Turner said.

"We're interested in just making sure that you don't think that the internet is a bouncy castle where nothing's going to go wrong."

For Bell, it's also about storytelling, as well as the "click-less training" and the workplace posters that act as reminders. The stories have to tap into how people think and what they care about.

"I don't mean horror stories, because we're not the scariest monster in the room for most people. Security is a big problem, but it's not the only problem, and for most people it's not the worst, either," Bell said.

"For example, if I'm teaching technical developers, we'll be talking about, 'Well, let's look at this horror story of what happened, and let's not look at the scary part of it. Let's talk about it like a Hollywood movie. How would we have done this? Could we do this in here?"

IMAGE: ISTOCK/G-STOCKSTUDIO

It's an interactive process that becomes an engaging, creative process, rather than one that induces fear.

Or, as Turner explained it, "This entire thing about security awareness is all about education ... That's not new. We know how to do that. There's an entire world around that one."

Cybersecurity researchers have continually found that when it comes to building an organisation's cybersecurity resilience, cultural factors are more important than technical factors.

A research team from Australia's Defence Science and Technology Group (DST) and the University of Adelaide, for example, found that employees might be better able to spot a phishing email if they were allowed to exhibit more individualism in the workplace and question the authenticity of emailed instructions.

Sometimes it can be as simple as giving employees the cultural permission to ask a colleague for a second opinion, and reinforcing that doing so is a sign of taking care of the organisation, rather than a sign of weakness. Ask out loud, suggests the Australian government's Stay Smart Online program.

"Talking through your concerns out loud with someone else can reassure you and help to identify messages that may be fake before you click a malicious link or give away any personal information."

Another DST-Adelaide research team found that employees had better information security awareness skills if they were more personally resilient, and suffered less workplace stress. Organisational changes that reduce stress would of course have many other benefits besides improving security.

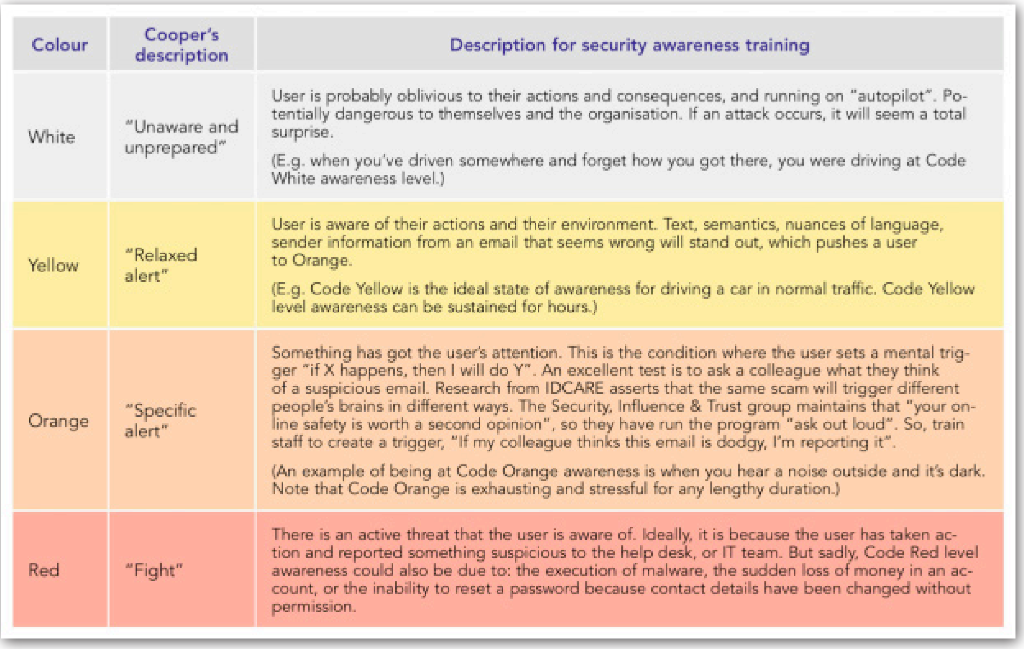
Research presented by the University of Otago in 2015 showed that when employees fell for a phishing attack, they were usually away from their desk, using mobile devices that didn't necessarily display the email in full. It usually happened outside business hours, too, either late at night when they were tired, or first thing in the morning when they were busy starting their household's daily routine.

"This expectation that we're going to ask people to work long hours, be on call to answer emails and queries at any time, has a huge downside, and that's about managing expectations," said Mark Borrie, the university's information security manager.

The lesson is that organisations won't fix their cybersecurity problems unless they fix those workplace problems first.

Turner says that IBRS has been explaining these attention issues to clients in terms of colour codes, a system adapted from Jeff Cooper's colour code for the combat mindset.

Under the IBRS version of the code, employees in condition White are “unaware and unprepared”, probably oblivious to their actions and consequences, and potentially dangerous to themselves and the organisation.



Colour	Cooper's description	Description for security awareness training
White	"Unaware and unprepared"	User is probably oblivious to their actions and consequences, and running on "autopilot". Potentially dangerous to themselves and the organisation. If an attack occurs, it will seem a total surprise. (E.g. when you've driven somewhere and forget how you got there, you were driving at Code White awareness level.)
Yellow	"Relaxed alert"	User is aware of their actions and their environment. Text, semantics, nuances of language, sender information from an email that seems wrong will stand out, which pushes a user to Orange. (E.g. Code Yellow is the ideal state of awareness for driving a car in normal traffic. Code Yellow level awareness can be sustained for hours.)
Orange	"Specific alert"	Something has got the user's attention. This is the condition where the user sets a mental trigger "if X happens, then I will do Y". An excellent test is to ask a colleague what they think of a suspicious email. Research from IDCARE asserts that the same scam will trigger different people's brains in different ways. The Security, Influence & Trust group maintains that "your online safety is worth a second opinion", so they have run the program "ask out loud". So, train staff to create a trigger, "If my colleague thinks this email is dodgy, I'm reporting it". (An example of being at Code Orange awareness is when you hear a noise outside and it's dark. Note that Code Orange is exhausting and stressful for any lengthy duration.)
Red	"Fight"	There is an active threat that the user is aware of. Ideally, it is because the user has taken action and reported something suspicious to the help desk, or IT team. But sadly, Code Red level awareness could also be due to: the execution of malware, the sudden loss of money in an account, or the inability to reset a password because contact details have been changed without permission.

IMAGE: SUPPLIED

You want your staff members to be operating at Yellow, says Turner, a “relaxed alert” state where employees are aware of their actions and their environment. Text, semantics, nuances of language, and sender information from an email that seems wrong will stand out, which pushes them to the Orange state.

Orange is a “specific alert”, where something has got the employee’s attention. The action of asking out loud puts both parties into the Orange state.

“You don’t want them in Orange [continuously] because that’s mentally exhausting. But Yellow, with training and practice you can maintain that for hours at a time,” Turner said. Providing, that is, that staff members are taking breaks and doing “a lot of good occupational health and safety and ergonomic things” like standing up, going for a walk, and drinking water.

While an organisation’s culture is a key to success, the content of security awareness training is still important.

Staff members need to understand what that technology means to the organisation, and how that organisation is winning—or not—by using that technology, according to Nigel Phair, director of the Centre for Internet Safety at the University of Canberra.

“Instead of saying users are our weakest link, which everyone says at every conference, I spin that around and say you are the greatest strength to the organisation when it comes to online security. You’re the one that is the eyes and ears,” Phair told ZDNet.

Staff members need to understand the reasons behind security decisions, and the relative risks involved in different transactions. They need to understand, for example, that while the data on a device might be encrypted, losing that device still means losing an expensive corporate asset.

According to CERT Australia critical infrastructure protection reports, around one in five cybercrime incidents are connected with an insider.

“Most of those were a silly insider, not a malicious insider. We want to stop that silliness,” Phair said.

Programs need to help employees become aware of the accidental risks as well as the malicious ones, and according to Bell that’s another cultural issue. It’s not about secrets being written on whiteboards for all to see, but the assumption that bad things won’t happen because everyone is a good person.

“That’s a red flag for me, because there’s a lot of reasons bad things happen in security,” Bell said.

“Some of it is malicious intent. Some have gone rogue and decided they’re going to become an evil genius, and great. But then there’s also ‘My toddler threw a shoe out of the window on my way to work in the morning and I’m just distracted today’, or ‘I’m dealing with s*** in my life and I’m not quite on my A game’, or ‘I’m actually a little bit nervous about this job because I don’t really know how to do it well enough and I’m a bit too scared to ask’.”

Or as an IBRS advisory paper says, “A disempowering message is more likely to result in either no behavioural change or, potentially, an undesirable change. Instead, security awareness programs should focus on helping staff develop and sustain the skills and knowledge required to execute on their work, and also maintain a mind state of ‘relaxed alert’.”

Disclosure: Stilgherrian receives payment from the Centre for Internet Safety for editorial work on their advisory newsletter DirectorTech.

CREDITS

Editor in Chief
Bill Detwilerr

Editor in Chief, UK
Steve Ranger

Associate Managing Editor
Mary Weilage

Editor, Australia
Chris Duckett

Senior Features Editor
Jody Gilbert

Senior Editor
Alison DeNisco Rayome

Senior Writer
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Macy Bayern

Associate Editor
Melanie Wachsman

Multimedia Producer
Derek Poore

ZDNet TechRepublic

ABOUT ZDNET

ZDNet brings together the reach of global and the depth of local, delivering 24/7 news coverage and analysis on the trends, technologies, and opportunities that matter to IT professionals and decision makers.

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.