Aon's Cyber Solutions

2018 Cybersecurity Predictions

A Shift to Managing Cyber as an Enterprise Risk

Published: January 2018

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

Table of Contents

Foreword

Preparing security professionals and business leaders to shift their thinking and manage cyber as an enterprise risk in 2018.

Since issuing our 2017 predictions, we've seen a dramatic rise in the sophistication, scale, and impact of cyber attacks. As companies strive to enrich their customer experiences through a spectrum of endpoints, ranging from mobile devices to automobiles, the attack surface has increased dramatically. With this ever-growing threat landscape comes a proportionate increase in the impact that cyber attacks have on enterprises, and the customers they serve. This report draws on our experience working with boards and C-suites, as well as security and risk professionals to plan for, mitigate, and manage the expanding impact of cyber risk across the enterprise.

Our 2017 Predictions: A year of large-scale cyber attacks with significant impact to organizations across sectors

The swift, public, and pervasive cyber attacks in 2017 demonstrated how cyber risk cannot be effectively managed solely as an information technology (IT) issue. The WannaCry ransomware attack hit over 200,000 computers in 150 countries,[1] taking businesses offline, disrupting sales and operations. Arguably the most significant data breach in U.S. history hit Equifax, exposing the sensitive data of 143 million people,[2] while subjecting the company to legal claims resulting in a dramatic loss of shareholder value and executive resignations.[3]

Additionally, as we predicted, criminals hijacked hundreds of thousands of Internet of Things (IoT) devices around the globe to attack third parties, and also advanced their social engineering and spear-phishing tactics.

Beyond large scale interruptions to global commerce,[4] 2017 witnessed the influence of cyber attackers on politics and policy. Russian hackers attempted to influence election outcomes around the globe, and Chinese hacker groups, known for targeting U.S. defense and aerospace companies, turned their attention to critical infrastructure across Asia.[5]

Data integrity attacks, where criminals seek to sow doubt over the accuracy and reliability of information, became a dominant issue in the public and private spheres as bad actors hit with false media reports and other misinformation campaigns. Major social media and technology companies came under fire as unwilling facilitators of these attacks.

As we anticipated, regulatory pressure for financial services institutions to conduct red-team testing increased in major markets including Hong Kong, the European Union (EU), and others. In our own experience working with clients, while some enterprises have begun to undertake proactive measures to test and remediate exposure, we continue to see a significant shortfall around conducting cybersecurity due diligence, particularly around M&A transactions.

"Today's silo-driven approach to cyber risk management will begin to disintegrate in 2018 in favor of a coordinated C-suite driven approach as leading companies begin to view the impact of cyber risk holistically across all functions of the enterprise."

Our 2018 Predictions: A shift to managing cyber as an enterprise risk

In our 2018 predictions, we examine how these and other dynamics will require companies to shift their approach to cyber risk management. Companies' increasing reliance on technology, regulators' focus on protecting consumer data, and the value of non-physical assets are causing a convergence of cyber exposures that will require security to be integrated into both business culture and risk management frameworks.

Global regulatory pressures will continue to intensify in 2018, with renewed enforcement of compliance and audit certificate requirements, as vanguard regulators pursue their missions to protect against the impact of cyber attacks. Mounting regulatory complexity will provoke calls for harmonizing this landscape.

Whereas past directors and officers (D&O) liability claims over cyber incidents have largely been dismissed, we expect to see more claims successfully brought against D&Os, holding them personally responsible for the handling of cyber incidents. In our predictions, we examine how the events of 2017 shifted this landscape. With cyber events now ranking among the top three triggers for D&O derivative actions,[6] we expect these claims to intensify in 2018. Heightened concern among executives over liability, and the financial and operational impact of cyber risk, will drive changes in the insurance market. As businesses demand more comprehensive cyber coverage, that coverage will reach beyond provisions in other policies, such as property, errors and omissions, and general liability.

We also anticipate 2018 will be a year of increased accountability over cyber attacks. Organizations facing risks from insider threats, IoT security, ransomware attacks and more, will have to demonstrate that they have followed best practices to protect consumers and employees. This will lead to an increased focus on proactive measures, such as better data hygiene, bug bounty programs, and multi-factor authentication (MFA) becoming standard practice for a broader and more diverse set of companies.

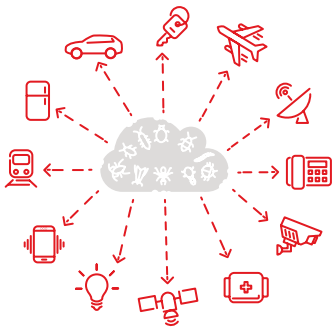
Today's silo-driven approach to cyber risk management will begin to disintegrate in 2018, in favor of a coordinated C-suite driven approach as leading companies begin to view the impact of cyber risk holistically across all functions of the enterprise.

We hope this year's predictions will be a useful launching pad to shift thinking and take action to mitigate and manage cyber risks.

Jason J. Hogg
Chief Executive Officer, Aon Cyber Solutions

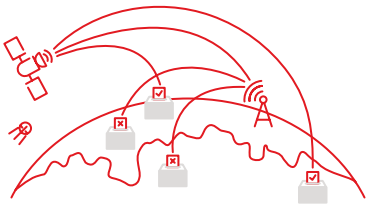
2017 Scorecard

True | Mixed | False



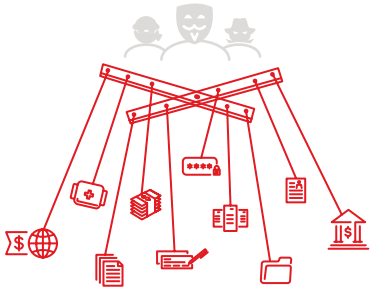
1. Criminals harness IoT devices as botnets to attack infrastructure

Hackers harnessed IoT devices as botnets, causing heightened concern over a potential DDoS attack on critical infrastructure. Security researchers identified new, rapidly growing botnets that hijacked millions of devices, including "Hajime" and "IoT_reaper". North Korea's "Hidden Cobra" operation aimed to use networks of devices to attack U.S. infrastructure.



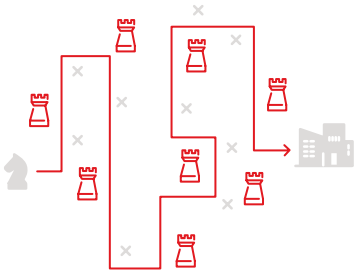
2. Nation state cyber espionage and information war influences global politics and policy

Hackers targeted elections and critical infrastructure, and conducted cyber espionage, impacting domestic politics and international relations. The U.S. investigation into Russian interference in the 2016 election continues. Qatar alleged that Abu Dhabi posted politically motivated fake news on its state news website. The U.S. started a formal probe into Chinese government cyber espionage.



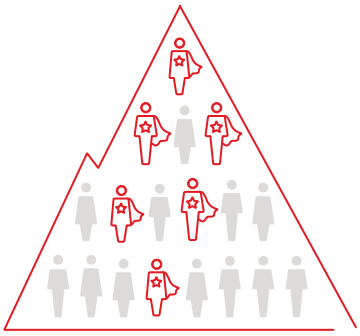
3. Data integrity attacks rise

The spread of misinformation continued; data integrity attacks rose. The spread of inaccurate, unverified information impacted the market value of companies, response to natural disasters, and swayed public opinion. Cyber attackers weaponized tech and media platforms, prompting calls for tech companies to actively address the problem of manipulated postings, bots, and ads.



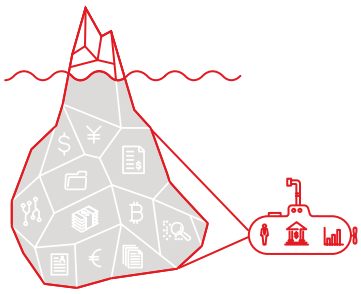
4. Spear-phishing and social engineering tactics become more crafty, more targeted and more advanced

Attackers deployed new spear-phishing tactics against organizations across sectors including major technology companies and government agencies. Hackers tricked employees at international energy companies into opening documents to harvest usernames and passwords, granting access to power switches and computer networks. Fraudsters targeted UK students with an email scam to steal personal and banking details.



5. Regulatory pressures make red teaming the global gold standard with cybersecurity talent development recognized as a key challenge

Global regulators in financial centers worldwide adopted regulation around red team testing, causing security talent shortages. EU financial market infrastructures will undergo testing through an EU red team testing framework. The Hong Kong Monetary Authority enforced the Cybersecurity Fortification Initiative (CFI), including its Intelligence-led Cyber-attack Simulation Testing framework.



6. Industry first-movers embrace pre-M&A cybersecurity due diligence

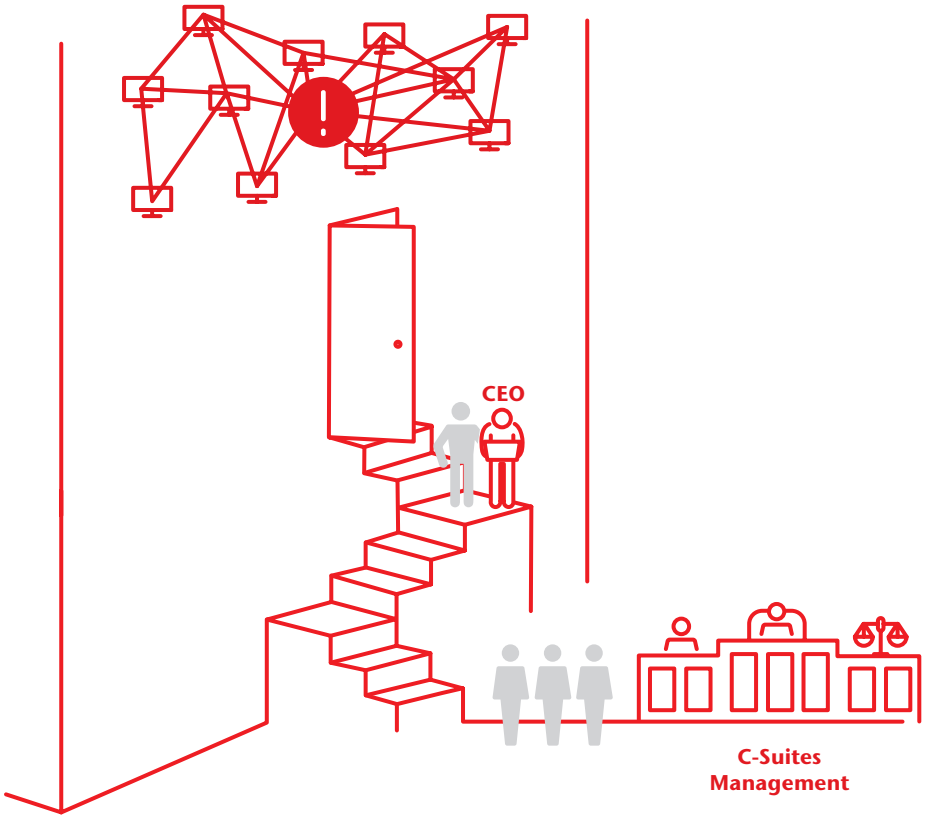
Pre-M&A cybersecurity due diligence is recognized as best practice across industries, but embraced only by first movers. The American Bar Association and others published guidance to help legal and business communities understand key requirements of cybersecurity due diligence that should be part of every M&A transaction.

1. Businesses adopt standalone cyber insurance policies as boards and executives wake up to cyber liability.

As boards and executives witness the material impact of cyber attacks, including reduced earnings, operational disruption, and claims brought against directors and officers, businesses will turn to tailored enterprise cyber insurance policies. At the same time, insurers will limit coverage of cyber-related losses in traditional property, casualty, and other business policies.

In 2017, businesses experienced significant material financial impact caused by cyber attacks, with at least six attacks requiring disclosure under U.S. Securities & Exchange Commission guidelines.[7] C-suite executives resigned and market capitalizations dropped following massive thefts of consumer data. Companies faced class-action lawsuits and regulatory investigations over the handling of breaches,[8] with cyber events now ranking among the top three triggers for D&O derivative actions.[9] The WannaCry ransomware and NotPetya malware attacks resulted in companies across industries reporting reduced revenue and profits due to operational problems.[10] These trends have emphasized boards' and executives' liability for ensuring effective cybersecurity controls are in place.

In 2017, C-suite executives resigned following massive data breaches.



In 2018, more companies will disclose severe cyber-related losses in financial reports or analyst calls, as companies face increased scrutiny over their handling of cyber incidents. As cyber attacks drag down earnings, disrupt operations, expose data, and hit share prices, it will no longer satisfy regulators, shareholders, and the public to mandate that a chief executive officer (CEO) or board member step down in the wake of a major compromise. Class-action lawsuits and liability claims will successfully be brought against D&Os, who will be held responsible for failing to uphold their fiduciary responsibility to protect shareholders and consumers from the effects of a breach.

The cyber insurance market will respond to concerns from boards and executives by offering policies reflecting the expanding impact of attacks. A 2017 Ponemon Institute survey found only 24 percent of risk management professionals said their companies had cyber insurance, despite 87 percent viewing cyber liability as one of their top ten business risks.[11] Companies cited inadequate coverage among the top reasons for not purchasing cybersecurity insurance, as well as having property and casualty insurance policies, which often provide limited elements of risk transfer protection from cyber exposures as a "silent" component.

This will change in 2018 as companies demand coverage for the full impact of cyber risk, and insurers explicitly exclude coverage for cyber-related losses in other business policies. As a result, insurers will craft enterprise cyber insurance policies that cover a broad spectrum of cyber-related exposures. Adoption will spread beyond traditional buyers of cyber insurance, such as the retail, financial, and healthcare sectors, to others vulnerable to cyber-related business disruption, particularly as we will see major material cyber incidents caused by system failures and outages impacting airports, airlines, power grids, manufacturing plants, oil and gas, utilities companies and others. Global scale cyber attacks like WannaCry will spur greater adoption, often among first time buyers, in Latin America, Europe, and other geographies outside the U.S., where most coverage is traditionally purchased.[12]

24%

of risk management professionals said their companies had cyber insurance

87%

of risk management professionals view cyber liability as one of their top ten business risks

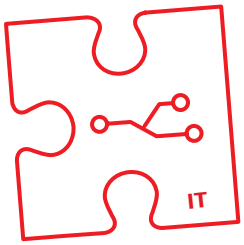
Bottom Line:

In response to the expanding impact of cyber risks on businesses across sectors and geographies and heightened executive concern over liability, the insurance industry will develop new cyber policies while restricting "silent" cyber coverage in other policies. Additionally, both insurers and reinsurers will push for increased scrutiny and improved quantification modeling to better understand potential correlated and systemic cyber perils that could aggregate catastrophic losses across multiple industries and geographies.

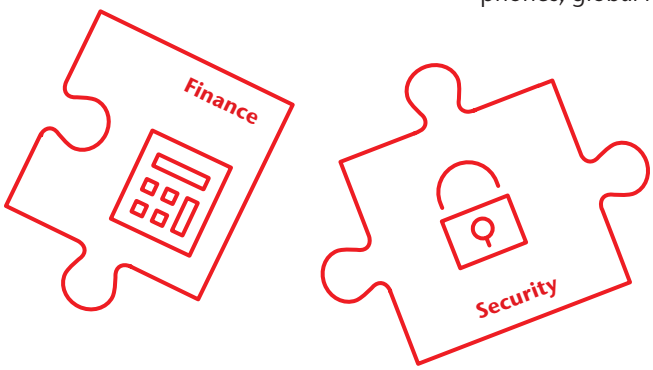
2. As the physical and cyber worlds collide, chief risk officers take center stage to manage cyber as an enterprise risk.

As sophisticated cyber attacks generate real-world consequences that impact business operations at increasing scale, C-suites will be rudely awoken to the enterprise nature of cyber risk. Chief risk officers (CROs) will take center stage, working with information security teams, treasurers, chief financial officers (CFOs), and general counsels (GCs) to improve risk modeling and paint a more holistic picture of the business' exposure.

In 2017, large-scale cyber attacks alerted businesses to the operational impact of technical vulnerabilities, beyond data breaches. Manufacturing companies were taken down; hospitals were extorted by bad actors who held systems for ransom and endangered patient lives; and cyber criminals gained access capable of blacking out U.S. electric power.[13] These attacks and others occurred despite the fact that security spend was up 7 percent in 2017 to $86.4 billion.[14] Despite the impact of cyber risk extending to compliance, technical, finance, human resources, legal and other departments, organizations continued to manage it as if it were only an IT issue. Silos abounded in cybersecurity risk management, and criminals exploited the gaps.



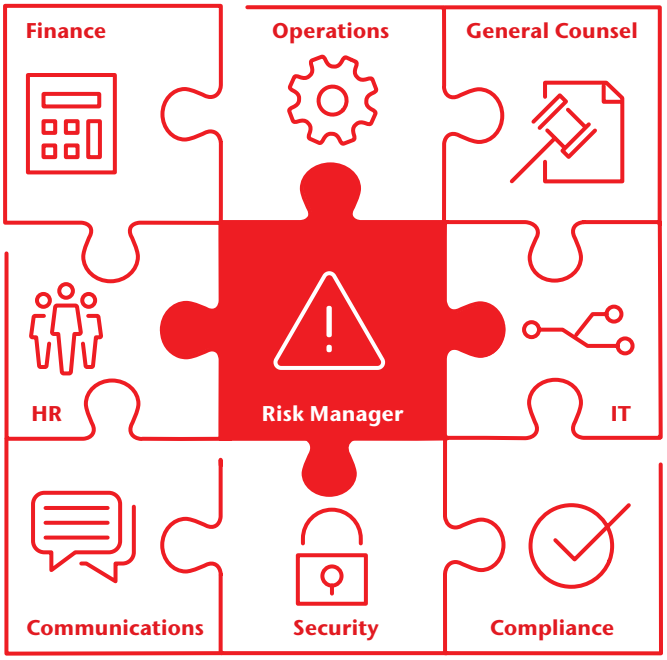
In 2018, C-suites in industries beyond the retail, financial services, and healthcare industries will react to the impact that exploited cyber vulnerabilities can have on their business' ability to operate, weaving cybersecurity into all areas of business risk and breaking down organizational risk management silos. For instance, connected grid systems, infrastructure, supervisory control and data acquisition (SCADA), and industrial control systems, have expanded cyber exposures beyond risks to personally identifiable information (PII) in almost every industry. The C-suites of mature organizations will empower the CRO to enter the cybersecurity spotlight, aligning them closely with information security teams. In 2018, the CROs and chief information security officers (CISOs) will become risk collaborators to better understand their organization's cyber risk exposures and potential "real-world" operational consequences. For example, global logistics companies will gather multidisciplinary teams to anticipate cyber vulnerabilities in applications on drivers' phones; global marketing services firms will look at how cyber vulnerabilities



Silos abounded in cybersecurity risk management, and criminals exploited the gaps.

affect crisis management and business continuity planning; shipping firms will address how cyber impacts operations, such as tankers and goods being remotely diverted. Shipping companies will also continue to assess the potential benefits of smart contracts and block chain technologies with regard to goods and inventory tracking and manifest verification.

As the impact of digital risk and technical vulnerabilities on companies' bottom lines grows through lost sales, business downtime, or product safety concerns, CISOs' visibility into a company's cybersecurity posture will become a major component in how CROs work with CFOs and GCs to assess risk and allocate resources towards insurance solutions. In 2018, CROs will be expected to articulate how digital business operations affect financial exposure. Using the CISO's specialized knowledge of a company's information security posture, alongside sophisticated modeling tools leveraging big data, CROs will improve an organization's ability to model how cyber risk could propagate across the entire enterprise. This will also provide C-suites and boards with a broader picture of the impact of risk on the business as a whole.



Bottom Line:

In 2018, the role of the CRO will be redefined, as they work more closely with CISOs to help company leadership understand the holistic impact of cyber risk on the business. This unique perspective will make the CRO one of the CEO's most valuable assets, as they provide a more meaningful risk story for boards and executive leadership, enabling more effective investment in cybersecurity measures and cyber insurance.

$86.4B

was spent on security in 2017, up 7% from the previous year

3. Regulatory spotlight widens and becomes more complex, provoking calls for harmonization. The EU holds global company to account over GDPR violation; big data aggregators come under scrutiny in the US.

In 2018, regulators at the international, national, and local levels will more strictly enforce existing cybersecurity regulations and increase compliance pressures by introducing new ones. Companies burdened by multiple rules and regulations will mount a campaign to harmonize the complex cybersecurity regulatory landscape.

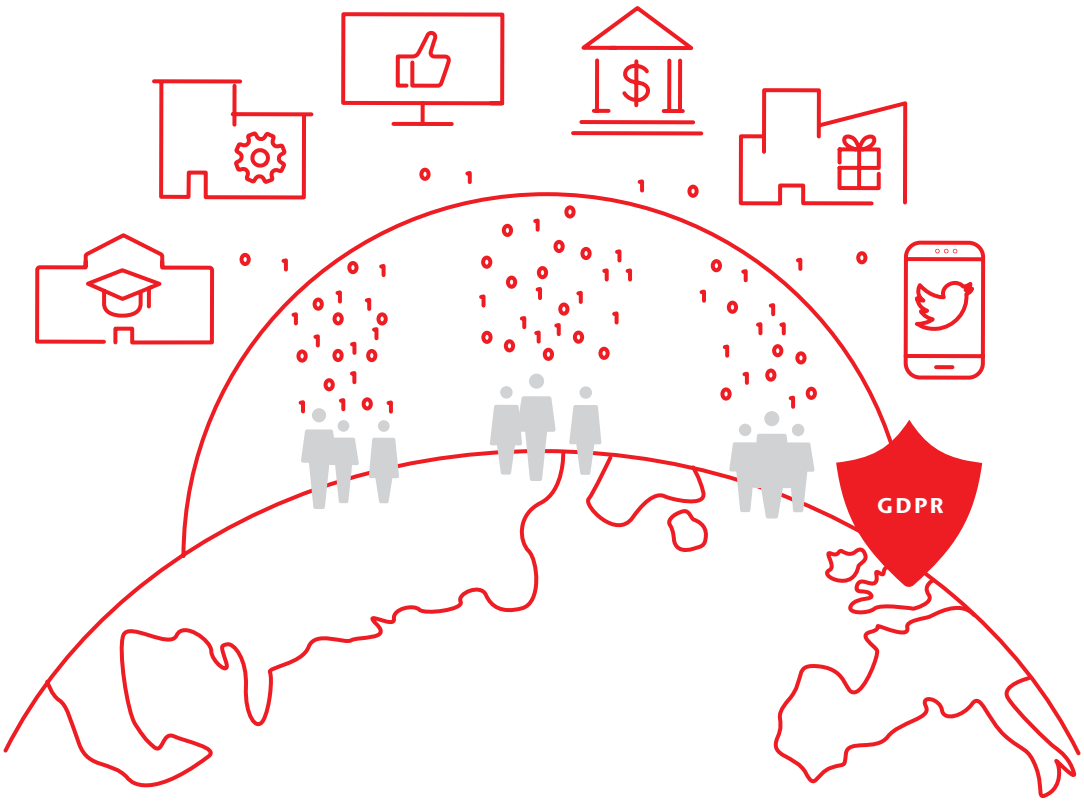
In 2017, new cyber regulations were introduced to address the broad impact of cyber risk across business activities, sectors, and jurisdictions. The EU's focus on setting a universal standard for consumer data privacy now has worldwide significance with the General Data Protection Regulation (GDPR), governing all companies that collect data of EU citizens. Asia-Pacific governments such as Australia, Japan, and South Korea are largely aligned with the EU's approach, albeit with more moderate enforcement and penalties. In the U.S., the New York Department of Financial Services (NYDFS) cybersecurity regulations had major implications for the financial services industry globally.

In 2018, we expect the European Commission will hold major U.S. and global companies to account for GDPR violations, through one or more major enforcement actions demonstrating its seriousness to enforce the regulation internationally, including through fines – a maximum 4 percent of worldwide annual revenue or €20 million (US$23.8 million)[15] – which are uninsurable under most country laws. While there is historically less litigation outside the U.S., consumer businesses in particular could also face the prospect of GDPR-related class action lawsuits, and other impacts such as reputational damages.

In the U.S., while the outcome of the Federal Trade Commission (FTC) versus LabMD litigation will impact whether the scope of the Commission's authority extends to enforcement of cybersecurity standards,[16] in 2018 we will see other regulatory bodies, such as NYDFS, enforcing existing regulations and launching targeted interventions in response to concern over major breaches. For example, big data organizations (aggregators and resellers) will come under renewed scrutiny over how they are collecting, using, and securing data. New regulations will mean that companies in sectors beyond healthcare, financial services, and retail— for example, education—will be forced to address cybersecurity compliance requirements.

Under the burden of significant and ever-increasing regulatory pressures, industry organizations will push back on regulators, calling for the alignment of cyber regulations. Business bodies like the U.S. Chamber of Commerce have already begun lobbying the U.S. government to harmonize regulations with the voluntary framework developed in public-private collaboration under the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).[17] The DigitalEurope trade association has also called for "full consistency" between the GDPR and other legislation in Europe.[18] In general, however, the compliance burden for companies across sectors will get tougher in 2018 before it gets better.

Companies across sectors will therefore need to optimize their compliance programs by leveraging external experts, automation, analytics, and other tools to drive actual, risk-based cybersecurity improvements.



Bottom Line:

As regulators seek to protect against the impact of data breaches and large-scale cyber attacks, with the implementation of GDPR we will see strict enforcement of existing regulation and fines, as well as new rules and guidelines introduced. Companies across sectors, forced to examine the controls in place to comply with multiple regulations, will call for greater alignment to ease the regulatory burden.

4. Criminals look to attack businesses embracing the IoT, in particular targeting a small to mid-sized company providing services to a global organization.

In 2018, global organizations will need to factor into third-party risk management the increased complexities in how their business partners are using the IoT. However, we will not see this happen, and as a result we predict a large company will be brought down by an attack on a small vendor or contractor that targets the IoT as a way into their network. This will be a wake-up call for large organizations to update their approach to third-party risk management, and for small and midsized businesses (SMBs) to implement better security measures or risk losing business.

Enterprises continue to interconnect endpoints, objects, and platforms to their networks, disintegrating traditional network perimeters, converging the digital and the physical worlds, and creating new security challenges. Businesses are expected to have employed 3.1 billion connected things in 2017.[19] Beyond devices, companies are linking more business processes to the Internet to gather data, drive efficiencies, and automate, monitor, and control operations.

This boom in usage could generate up to $11.1 trillion a year in economic value by 2025.[20] Yet, IoT devices are notoriously unsecured and proper patch management programs will continue to be overlooked in 2018. The security vulnerabilities introduced by how businesses are utilizing the IoT therefore present substantial risks, and even if a company's own IoT ecosystem is relatively secure, the impact of how third parties are deploying IoT is neglected. In a 2017 Ponemon study,[21] only 25 percent of respondents said the board of directors ask for assurances that IoT risks among third parties are being assessed, managed, and monitored appropriately.

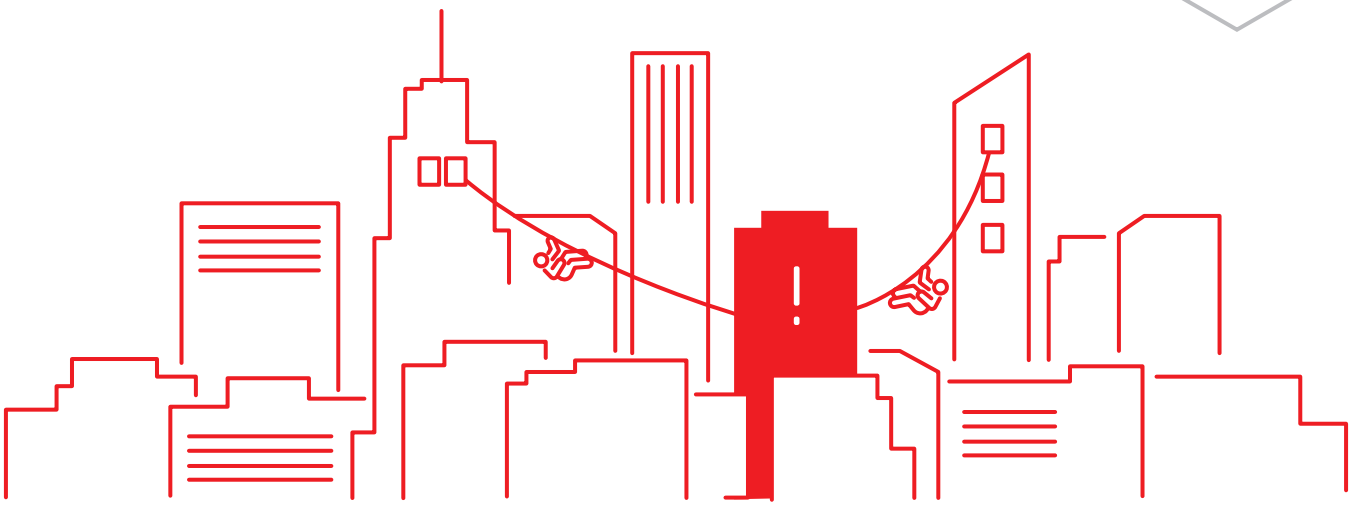
The security vulnerabilities introduced by how businesses are utilizing the IoT present substantial risks. Even if a company's own IoT ecosystem is relatively secure, the impact of how third parties are deploying IoT is neglected.

This is a particular concern for large organizations working with SMBs, given their lower prioritization of cybersecurity. Another recent Ponemon study found that 55 percent of small businesses reported to have been breached in a 12-month period between 2015 and 2016,[22] yet a tiny minority said they view it as the most critical issue they face.[23] As enterprises derive more efficiencies from working with SMBs in 2018, hackers will pinpoint smaller businesses that utilize IoT platforms and devices to gain entry into larger businesses. For example, we will see criminals targeting ATM manufacturers and maintenance vendors working with large banks. Additionally, organizations face risks from smaller service providers of printers or copy machines, security camera systems, and other connected endpoints through which client data can be exposed if hacked. As a result, demand for visibility into third-party security will increase and smaller vendors bidding for contracts will have to demonstrate stronger cybersecurity measures around IoT.

55%

of small businesses reported to have been breached in a 12-month period between 2015 and 2016

...yet a tiny minority said they view it as the most critical issue they face.



Bottom Line:

In 2018, we will see an attack on a SMB that has not properly integrated security into its IoT ecosystem, and this attack will extend into the network of a large organization causing exponentially more damage. In response, large organizations will broaden third-party risk management programs and due diligence processes so that they account for weaknesses in vendor IoT security. SMBs bidding to work with them will be forced to improve and document their cybersecurity measures.

5. As passwords continue to be hacked, and attackers circumvent physical biometrics, multi-factor authentication becomes more important than ever before.

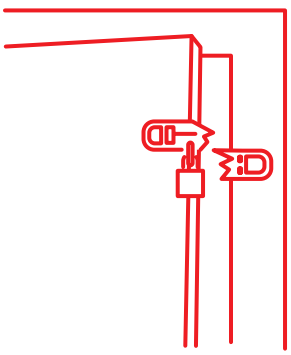
While passwords alone do not provide adequate levels of security, their convenience means that they are still widely deployed. Although they will be phased out as the primary method of authentication on mobile and IoT devices in 2018, they are unlikely to disappear completely. As companies implement biometrics to authenticate identity, criminals will advance their attacks to override these new technologies. In 2018, as more credentials are compromised, and biometrics are hacked, we will see the rise of MFA.

In 2017 we saw companies continue to fall victim to brute force and phishing attacks. A recent study found 81 percent of hacking-related breaches leveraged stolen or weak passwords.[24] As attackers continue to exploit passwords, innovative companies, such as mobile and IoT device manufacturers, are deploying biometrics as an alternative way to authenticate identity. For example, Apple's iPhone X uses facial recognition technology instead of passwords, and banks in financial centers including the UK and Hong Kong are rolling out biometrics in specific situations, such as voice recognition to authenticate customer service calls with high-net-worth individuals.

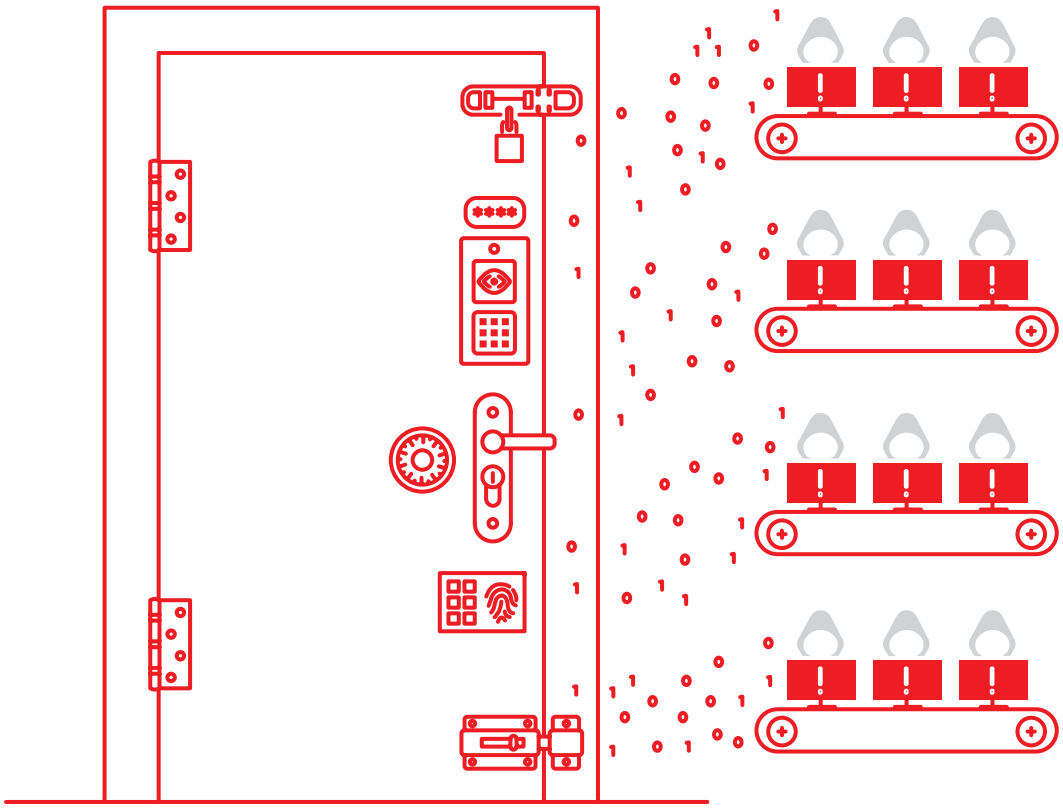
In 2018, these authentication methods, once requisite only for individuals with security clearances, will move mainstream. Physical biometrics, such as facial recognition, iris patterns, or fingerprints will extend beyond mobile devices to everyday usage, for example, replacing access badges to offices. However, even advanced biometrics will not be bulletproof as a single layer of authentication. The hash value behind fingerprints in a device can be stolen and attackers can use forged physical copies of a fingerprint to hack systems. In 2018, we will see a theft of biometrics that creates a lifetime of exposure for consumers, highlighting the challenges inherent in biometrics having no "re-set" process.

To combat the assault on passwords and attacks targeting biometrics, major financial institutions beyond FinTech companies will adopt MFA technologies in earnest, for example using voice recognition plus a PIN or password to authenticate all customer service calls. Individuals will be required to present at least two of the following pieces of evidence to an authentication instrument: knowledge (something they know), possession (something they have), and inherence (something they are). Banks will run behavioral biometrics authentication technologies in the background of online banking websites, continuously collecting information about a user's interactions, like keystroke and mouse movement, to create a unique user template on that device – and asking for more information if the behavior doesn't match the template. Major cloud providers will push for users of their platforms to put MFA into practice.

Even as companies adopt MFA, hackers will devise techniques to penetrate new authentication technologies, just as they devised methods to break two-factor authentication with "SIM swap" attacks. In 2018, we will see new smartphone-based malware targeting MFA applications on mobile phones.



While passwords alone do not provide adequate levels of security, their convenience means that they are still widely deployed.



Bottom Line:

Companies will widely adopt MFA as criminals successfully target single factor authentication, such as usernames and passwords, and biometrics. Even with MFA, companies will need to commit to a proactive, continuous process of testing and improving their defenses, as attackers will continue to evolve their techniques.

81%

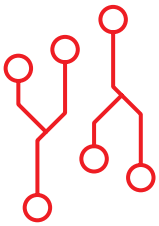
of hacking-related breaches leverage stolen or weak passwords

6. Criminals will target transactions that use points as currency, spurring mainstream adoption of bug bounty programs.

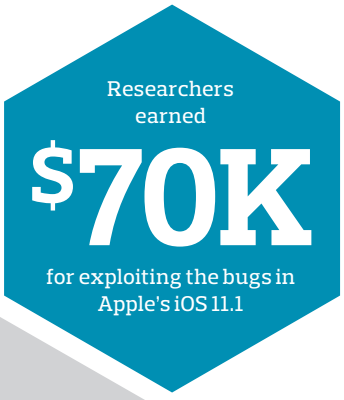
In 2018, companies beyond the technology, government, automotive, and financial services sectors will introduce bug bounty platforms into their security programs. Businesses with loyalty, gift, and rewards programs, such as airlines, retailers, and hospitality providers, will be the next wave of adopters as criminals target transactions that use points as currency.

In 2016 and 2017, we saw organizations in the technology,[25] government,[26] automotive,[27] and the financial services[28] sectors lead the pack in deploying bug bounty programs, crowdsourcing the expertise of skilled security researchers to root out vulnerabilities in exchange for money and recognition. Shortly after Apple's release of iOS 11.1 in 2017, researchers at Tencent Keen Security Lab quickly exploited two bugs,[29] earning $70,000 in rewards — a far lower price than Apple could have paid had the vulnerability been exploited by a malicious attacker.

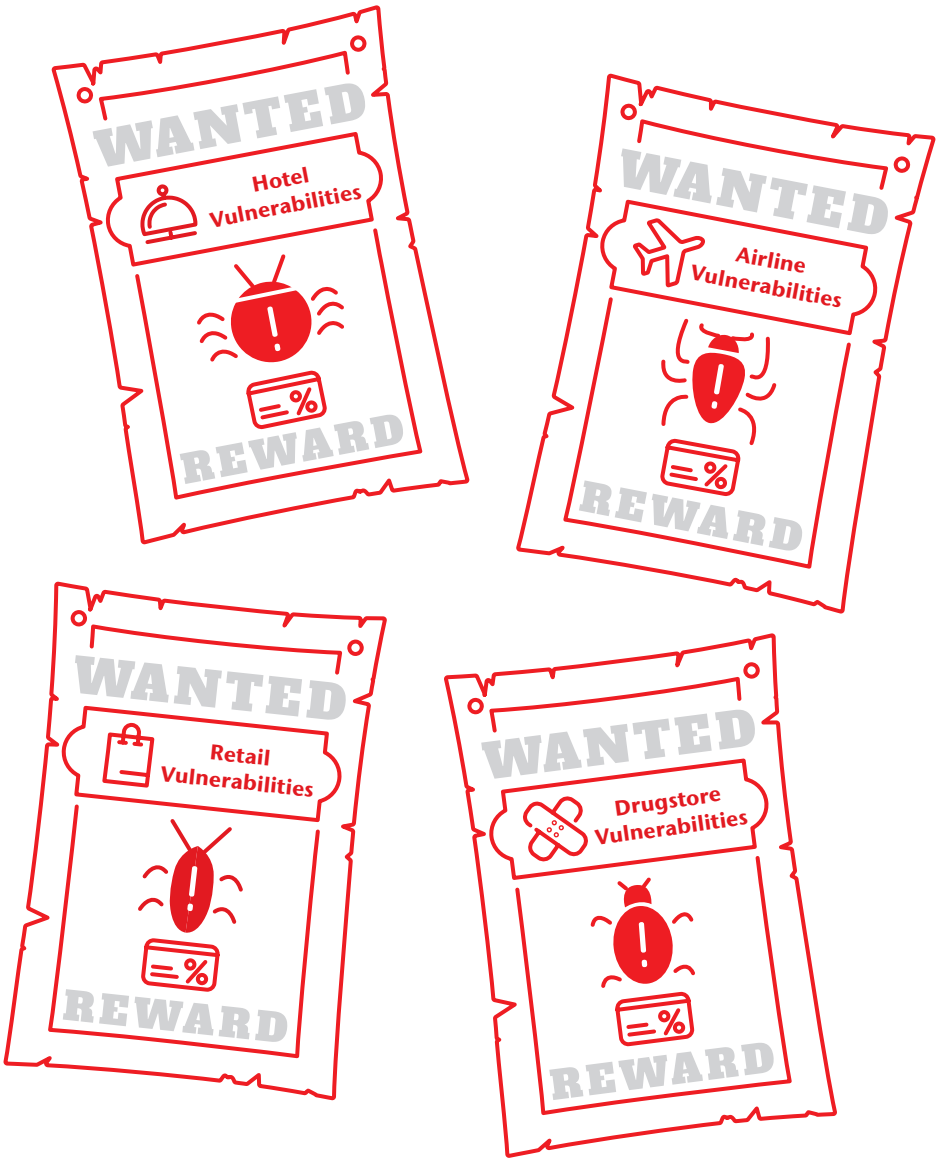
Enterprises with over 5,000 employees accounted for the fastest growth of program launches on the Bugcrowd platform over the past 12 months.[30] In 2018, we will see companies beyond the few early adopters in the airlines industry, as well as retail and hospitality, and other sectors operating rewards programs, adopt bug bounty programs to protect "points as currency". As credit cards become more secure, and criminals target more "card-not-present" transactions like gift cards and rewards points, bug bounty programs will be implemented as an extra layer of defense.



As the threat environment drives broader adoption, bug bounty programs will become part of the standard security lifecycle.



As the threat environment drives broader adoption, bug bounty programs will become part of the standard security lifecycle. Enterprises across industries will be expected to run bug bounty programs to prove they have done everything possible to protect themselves from cyber attacks. As bug bounties go mainstream, more companies will turn to external providers of private bug bounty programs and cybersecurity experts to implement best practices, such as setting up payments, defining the scope of the program, quantifying and remediating vulnerabilities, and managing the program in relation to simultaneous security testing. To meet demand, major cybersecurity and information security service providers will partner with, or acquire, private bug bounty program providers to offer these capabilities.



Bottom Line:

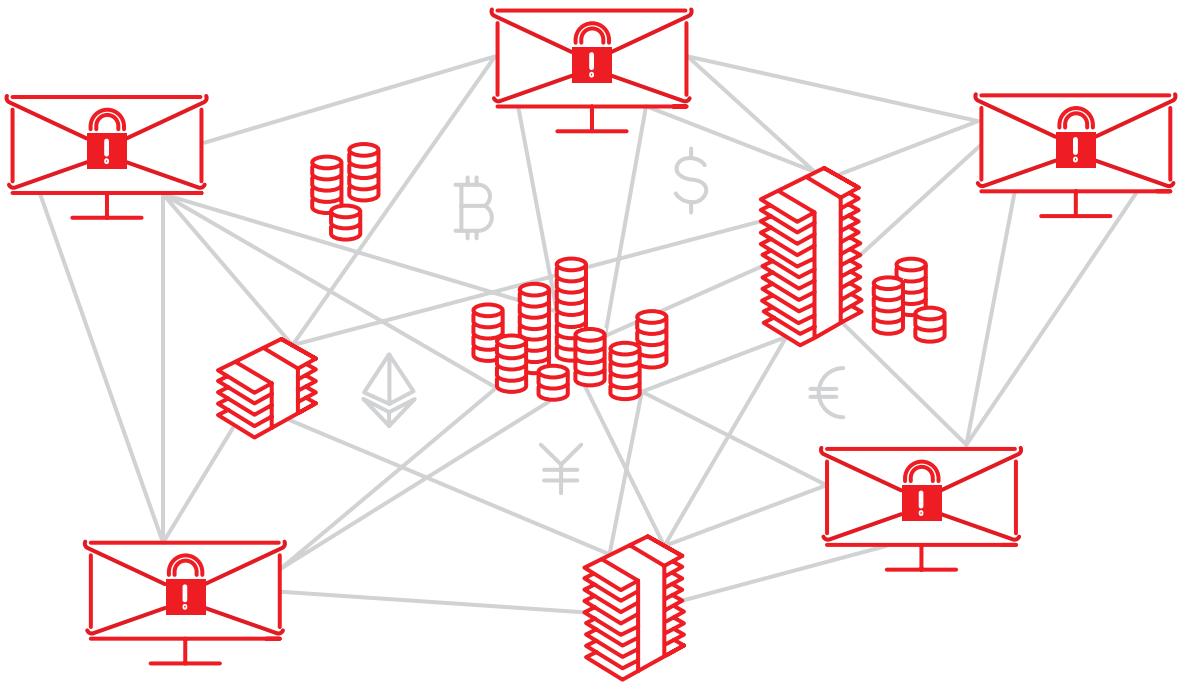
In 2018, bug bounty programs will expand to the wider airline industry, and retail and hospitality sectors, to protect points used as currency. As more organizations embrace bug bounty programs, they will require support from external experts to avoid introducing new risks with improperly configured programs.

7. Ransomware attackers get targeted; cryptocurrencies help ransomware industry flourish.

By the end of 2017, the global cost for organizations of ransomware attacks is estimated to reach $5 billion, up 400 percent from 2016.[31] The WannaCry ransomware attack impacted more than 300,000 people across 150 countries in less than two days. In 2018, criminals will evolve their tactics, including launching well-researched, targeted attacks intended to infect specific high-value assets known to hold critical data.

In the past few years, ransomware attacks relied on infecting systems by taking advantage of vulnerabilities. However, in mid-2017 the perpetrators of the NotPetya ransomware attack changed this landscape. Attackers gained admin credentials which then granted access to infect the non-vulnerable systems of the victim organization, thereby affecting almost all accessible systems in the network. In 2018, we will continue to see large-scale ransomware attacks that target admin credentials to gain access to, and infect, wider networks. With the expected increase in ransomware attacks designed to spread through a network, businesses in 2018 will urgently need to segment their networks. Companies that fail to do so will be impacted by ransomware attacks at a larger scale than necessary.

Attackers will also evolve their tactics in 2018, utilizing forms of benign malware—such as software designed to cause distributed denial-of-service (DDoS) attacks, or launching display ads on thousands of systems— to unleash huge outbreaks of ransomware. Botnet operators will grant ransomware attackers with access to botnet nodes in exchange for payments, allowing them to significantly expand the scope of a ransomware attack.



While attackers will continue to launch scatter-gun-style attacks to disrupt as many systems as possible, we will also see increasing instances of attackers targeting specific companies and demanding ransomware payments proportional to the value of the encrypted assets. To achieve stronger returns in these targeted attacks, criminals will hit environments where access to data and systems is mission critical, such as hospitals, transportation companies, and manufacturing companies. We also expect to see an increase in the use of ransomware to infect IoT devices, which come with a diminished set of security features by default to facilitate out-of-the-box functionality, and users tend to maintain these original settings once the devices start functioning. We have already seen the Mirai botnet that harnessed IoT devices to launch DDoS attacks, and anticipate ransomware to infect smart thermostats and other smart devices in 2018.

$5B

is the estimated global cost for organizations of ransomware attacks in 2017 – up 400% from 2016

In addition, cryptocurrencies will continue to support the flourishing ransomware industry overall, despite law enforcement becoming more advanced in their ability to trace attacks, for example, through bitcoin wallets.

To protect themselves in 2018, companies will have to go beyond the vital step of creating backups. Companies will need to utilize systems that can create snapshots in time, or maintain multiple versions of files created over the course of the day, to enable restoration to a specific point in time prior to the backup with minimal loss of productivity. Security professionals will need to routinely test if their backups allow them to restore the data and files in a specific timeframe to ascertain the downtime the company can withstand if a ransomware attack is realized.

In 2018, we will also see more companies recognizing the need to implement the *Principle of Least Privilege*—limiting file access rights for users to the bare minimum permissions they need to perform their work to reduce the number of files that could be encrypted in the event of a ransomware attack. Advanced companies will grant employees only the access needed for the business activities of a specific function, rather than providing automatic access to everything.

Bottom Line:

With perpetrators carrying out wide-scale, profitable, and disruptive attacks in 2016 and 2017, the number of attackers, the volume of ransomware families, and the number of infections increased dramatically. In 2018, we will see attackers continuing to launch large-scale attacks, but also evolve their tactics to implement targeted attacks with demands for greater payments proportional to the value of the assets. This activity will be supported by the continued rise of cryptocurrencies. A company's ability to protect against and recover from ransomware attacks in 2018 will rely on implementing proactive technical measures and business continuity plans.

8. Insider risks plague organizations as they underestimate their critical vulnerability and liability, and major attacks continue to fly under the radar.

Since we predicted the rise of the "insider" in 2016, we have seen organizations severely impacted by actions taken by malicious, careless, negligent, and unaware employees, contractors, leavers, consultants, and others with access to information, systems, and networks. Despite this, in 2017 we saw businesses underinvest in proactive insider risk mitigation strategies and 2018 will be no different. With a continued lack of security training and technical controls, coupled with the changing dynamics of the modern workforce, the full extent of cyber attacks and incidents caused by insiders will not even become fully public.

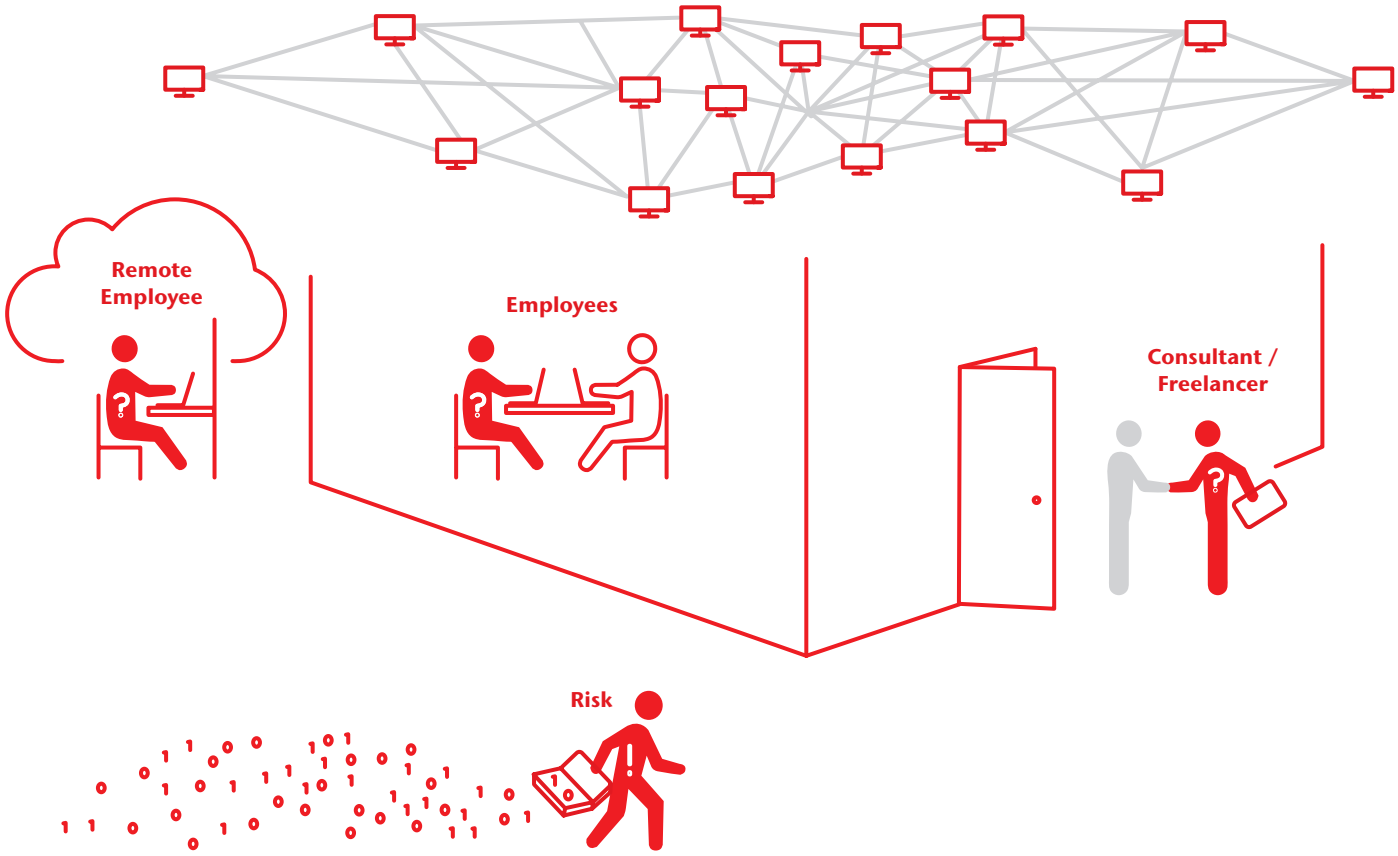
Disruptive technologies and the changing employer-employee relationship is challenging the security of organizations in unprecedented ways. The rise of the gig economy, consulting, and freelancing[32] means the definition of an "insider" has changed, and boundaries between internal and external employees are fluid. Corporations depersonalizing the workforce and creating more virtually connected ecosystems has impacted the level of an employee's psychological investment and engagement in their organization.[33] Media hunger for private documents such as those publicized in the Panama and Paradise Papers attacks is fueling the motivation to expose and leak information from inside sources. These factors contribute to why companies will continue to be impacted by actions—both intentional and unintentional—taken by members of their own workforce next year.

In 2018, too many organizations will continue to manage insider risk reactively, and insiders will cause major cyber incidents such as misappropriating intellectual property (IP), or providing criminals with access to sensitive data and systems to get inside security controls and infiltrate an organization's perimeter. Employees will find workarounds for security policies or unwittingly fall victim to social engineering and phishing attacks. Criminals will target insiders in sophisticated sectors that are required and trusted to ensure information and data remain private, such as professional services, healthcare, financial services, automotive, entertainment, and technology. Bad leavers, many of whom see work products as their own to take, will intentionally misuse access to an organization's network or data.

However, only a fraction of these incidents will be publicly reported, and much of the resulting theft will be difficult to detect—given that many of the most valuable corporate assets today are in the form of IP,[34] trade secrets, research and development, or business strategies—that can be copied without being physically stolen. The dark web, encryption, and virtual currencies will continue to facilitate concealed transactions, communications, and storage of stolen data.

While the full extent of these attacks, and the true cybersecurity cost that insider threats pose, will go underreported, in the proportion of attacks that do become public we will start to see more companies being held legally liable for their poor handling of incidents caused by insiders, as in the landmark 2017 case brought against Morrisons Supermarkets in the High Court in the UK.[35]

In 2018, too many organizations will continue to manage insider risk reactively, and insiders will cause major cyber incidents. However, only a fraction of these incidents will be publicly reported.



Bottom Line:

Companies cannot eliminate the cyber risks caused by even well-intentioned employees, and while it is difficult to measure the full impact of insider risk, they can no longer afford to deprioritize this risk over those they face from external factors. Organizations will need to attend to this vulnerability, and implement effective insider risk programs. If ignored, they could be held liable in 2018 for failing to protect staff and consumers if an incident occurs.

??%

The full extent and the true cybersecurity costs of insider attacks will go underreported

Contacts

Jason J. Hogg
CEO, Aon Cyber Solutions
E: jason.j.hogg@aon.com

Eric Friedberg
Co-President
Stroz Friedberg, an Aon company
E: efriedberg@strozfriedberg.com
T +1 212.981.6536

Edward Stroz
Co-President
Stroz Friedberg, an Aon company
E: estroz@strozfriedberg.com
T: +1 212 981 6541

United States

Rocco Grillo
Cyber Resilience Leader
Stroz Friedberg, an Aon company
E: rgrillo@strozfriedberg.com
T: +1 212 981 2674

Kevin Kalinich
Global Practice Leader,
Cyber/Network Risk
Aon Professional Risk Solutions
E: Kevin.Kalinich@aon.com
T: +1 312 381 4203

CJ Dietzman
Vice President, Security Advisory
Practice Leader
Stroz Friedberg, an Aon company
E: cdietzman@strozfriedberg.com
T:+1 347.283.4861

Cassio Goldschmidt
Vice President, Proactive Services
Stroz Friedberg, an Aon company
E: cgoldschmidt@strozfriedberg.com
T:+1 310.623.3270

Christian E. Hoffman
Aon Risk Solutions, Financial Services
Group, Professional Risk Solutions,
National Practice Leader
E: christian.hoffman@aon.com
T: +1 484 343 3740

Jibran Ilyas
Managing Director, Incident Response
Stroz Friedberg, an Aon company
E: jilyas@strozfriedberg.com
T:+1 312.216.8107

Stephanie Snyder
National Sales Leader, Cyber Insurance
Aon Professional Risk Solutions
T: +1 312 402 6038

Carolyn Vadino
Chief Communications Officer and
Marketing Leader
Stroz Friedberg, an Aon company
E: cvadino@strozfriedberg.com
T: +1 646 524 8454

United Kingdom

Justin Clarke-Salt
Justin Clarke-Salt
Co-Founder, Gotham Digital Science,
A Stroz Friedberg Company
E: justin@gdssecurity.com
T: +44 330 660 0720

Alex Carte
Managing Director,
Engagement Management
Stroz Friedberg, an Aon company
E: acarte@strozfriedberg.co.uk
T: +44 20.7061.2302

References

1. https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX
2. https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html?utm_term=.7eba7c991ffd
3. https://investor.equifax.com/news-and-events/news/2017/09-26-2017-140531280
4. https://www.programbusiness.com/News/Shipping-Giant-Maersk-Could-Lose-Nearly-450M-Due-to-Recent-Cyber-Attack
5. https://www.ft.com/content/c8e634fa-2a31-11e7-9ec8-168383da43b7
6. http://riskandinsurance.com/ponemon-go/
7. Securities and Exchange Commission, Cybersecurity Disclosure Guidance, October 13, 2011.
8. The Washington Post, Equifax faces hundreds of class-action lawsuits and an SEC subpoena over the way it handled its data breach, November 9, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach
9. http://riskandinsurance.com/ponemon-go/
10. Infosecurity Magazine, Pharma Giant Merck Sees Petya Profit Hit for Rest of 2017, https://www.infosecurity-magazine.com/news/pharma-giant-merck-petya-profits/
11. Ponemon Institute, 2017 Global Cyber Risk Transfer Comparison Report, April 2017. http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp
12. http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp
13. Wired, Hackers Gain Direct Access to US Power Grid Controls, September 6, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/
14. Techcrunch, Global cybersecurity spending to grow 7% to $86.4BN in 2017, says Gartner, August 16, 2017 https://techcrunch.com/2017/08/16/global-cybersecurity-sending-to-grow-7-to-86-4bn-in-2017-says-gartner/
15. "Questions and Answers – Data Protection Reform Package," European Commission; http://europa.eu/rapid/press-release_MEMO-17-1441_en.html
16. https://www.bna.com/oral-argument-labmd-n73014453538/
17. "2017 Cybersecurity Policy Priorities," U.S. Chamber of Commerce; https://www.uschamber.com/2017cyberpriorities
18. "DigitalEurope urges MEPs to Bring ePrivacy Closer to Digital Reality," DigitalEurope; http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2549&language=en-US&PortalId=0&TabId=353
19. https://www.gartner.com/newsroom/id/3598917
20. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
21. www.ponemon.org/library/the-internet-of-things-iot-a-new-era-of-third-party-risk
22. Ponemon Institute, "2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)," June 2016, https://signup.keepersecurity.com/state-of-smb-cybersecurity-report/.
23. CNBC Small Business Survey, April 2017. https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html
24. 2017 Data Breach Investigations Report (DBIR), Verizon, July 2017. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
25. https://www.facebook.com/whitehat
26. https://www.defense.gov/News/Article/Article/710033/hack-the-pentagon-pilot-program-opens-for-registration/
27. https://bugcrowd.com/tesla
28. 2017 State of Bug Bounty Report, June 2017, Bugcrowd. https://www.bugcrowd.com/resource/2017-state-of-bug-bounty/
29. ios11 Hacked by Security Researchers Day After Release, Zach Whittaker, Zero Day, November 2, 2017, ZDNet. http://www.zdnet.com/article/ios-11-hacked-by-security-researchers-day-after-release/?utm_source=hs_email&utm_medium=email&utm_content=2&_hsenc=p2ANqtz-88NIeQpAvpVDiDqbehjhWYOuq-
30. 2017 State of Bug Bounty Report, June 2017, Bugcrowd. https://www.bugcrowd.com/resource/2017-state-of-bug-bounty/
31. https://go.druva.com/2017-Survey-Ransomware-Report-SEM.html?utm_medium=cpc&utm_source=paid-search&utm_campaign=US-inSyncRansomware-Ransomware&utm_content=&utm_adgroup=General&utm_term=ransomware&gclid=Cj0KCQjwsZHPBRCIARIsAC-VMPD9UVi_IC780BzYjlBAYk
32. https://s3.amazonaws.com/fuwt-prod-storage/content/FreelancingInAmericaReport-2017.pdf
33. http://www.aon.com/unitedkingdom/attachments/trp/2017-Trends-in-Global-Employee-Engagement.pdf
34. http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp
35. http://www.telegraph.co.uk/business/2017/12/01/victory-morrisons-workers-data-leak-compensation-claim/

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

About Stroz Friedberg

Stroz Friedberg, an Aon company, is a specialized risk management firm built to help clients solve the complex challenges prevalent in today's digital, connected, and regulated business world. A global leader in the field of cybersecurity, with leading experts in digital forensics, incident response, proactive security, investigations, intellectual property, and eDiscovery, Stroz Friedberg works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Founded in 2000 and acquired by Aon in 2016, Stroz Friedberg has thirteen offices across nine U.S. cities, London, Zurich, Dubai, and Hong Kong. Stroz Friedberg serves Fortune 100 companies, 80% of the AmLaw 100, and the Top 20 UK law firms. Learn more at https://www.strozfriedberg.com/.

www.aon.com | www.strozfriedberg.com

STROZ FRIEDBERG
an Aon company

AON
Empower Results®