2019 Cyber Security Risk Report

What's Now / What's Next

Published: January 2019

Empower Results®

Table of Contents

8

Aon’s Cyber Solutions explores eight specific risks that organizations may face in 2019 no matter where they are on their digital journey.

2019 Cyber Security Risk Report: What's Now and What's Next

Every year technologists, security professionals, and risk managers comment extensively on the "unprecedented" level of change we have or will experience as we move from year to year. In fact, change - and the proliferation of new threats – has become the only constant we can expect. The digital transformation of the global economy continues to be an ever-accelerating evolution of the ways we conduct business, work, and life.

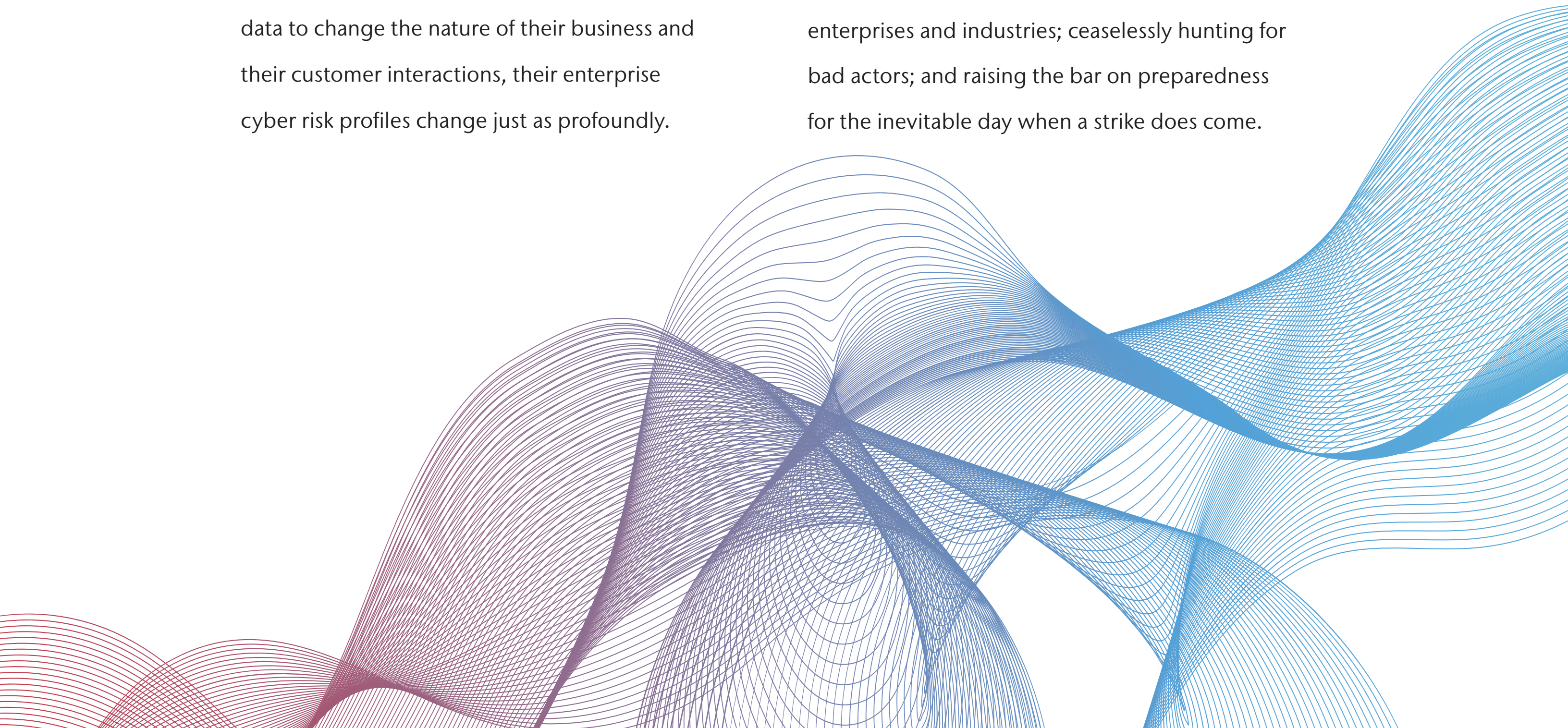
As we use technology to speed up the transfer of information, it creates amazing opportunity and, potentially, greater risk.

This digital shift comes with a second-order effect that is far less recognized: As industry after industry embraces digital technology and data to change the nature of their business and their customer interactions, their enterprise cyber risk profiles change just as profoundly.

In 2019, the greatest challenge organizations will face is simply keeping up with and staying informed about the evolving cyber risk landscape. The threats that can impact organizations vary widely by industry, size, and region. It is incumbent upon organizations to understand the risks they face, and to address them on a proactive basis.

2019

In this report, Aon's Cyber Solutions explores eight specific risks that organizations may face in 2019 no matter where they are on their digital journey. We believe the future of cyber risk management must be proactive, oriented around sharing threat intelligence, and collaborating within and across enterprises and industries; ceaselessly hunting for bad actors; and raising the bar on preparedness for the inevitable day when a strike does come.



Technology

Risk 1

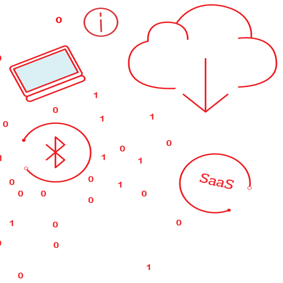
Embracing Digital Transformation Creates New and Unanticipated Risks

The publishing industry once manufactured newspapers and magazines, painting ink on paper and shipping it around the world. Some of that still goes on, but today publishing has fragmented into thousands of “information-as-a-service” businesses that mostly paint bits on web pages or sell subscriptions to online databases.

Or consider auto manufacturers. They still mostly create value by building cars, but those vehicles are racing toward a future of full autonomy and already include cellular, WiFi, Bluetooth, and infrared (key fob) networks– with others on the horizon. This translates into an expanding—and morphing—cyber-attack surface. Meanwhile, most auto manufacturers have nascent “mobility-as-a-service” offerings, in the form of car- and ride-sharing services, that many experts forecast as the future of the industry.

Such “X-as-a-service” (XaaS) opportunities are proliferating across most, if not all, industries, as each adopts digital technology and data and begins to realize that the information assets they are creating have value for customer cohorts, too.

As traditional “brick-and-mortar” companies rapidly evolve into digital economy XaaS providers, they face new and potentially not-yet-recognized exposures. Cyber risk management for web pages and online databases is radically different than for printed magazines; the risks inherent in a fully autonomous, multi-networked car are radically different than those of a circa-early-2000s car – or a ride-sharing service based on that autonomous vehicle. Organizations must carefully consider these new digital risks as continuous digital transformation drives them to embrace new ways of doing business.



Technology

> **As traditional “brick-and-mortar” companies rapidly evolve into digital economy XaaS providers, they face new and potentially not-yet-recognized exposures.**

Supply Chain

RISK 2

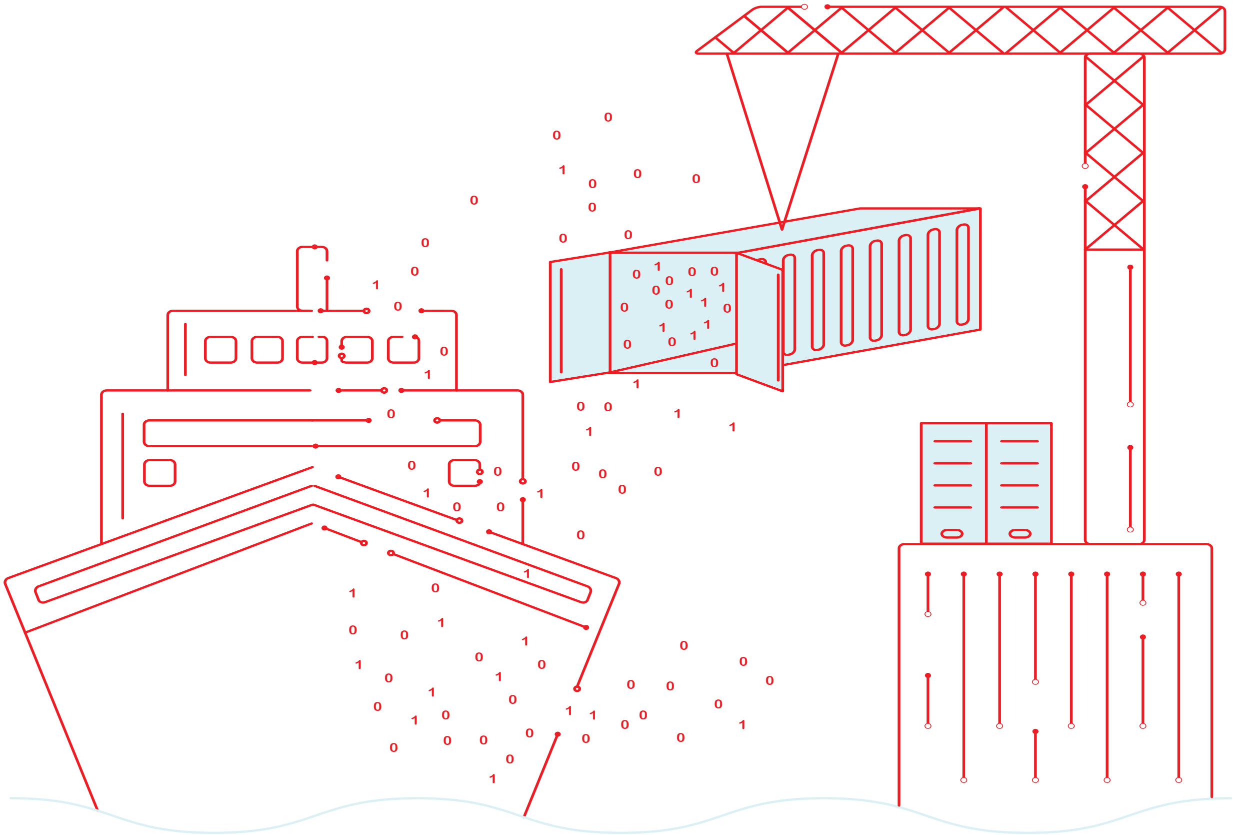
Supply chain security wake-up calls grow more insistent

Security is not always top-of-mind as companies build out increasingly complex, global supply chains. In C-suites and boardrooms, supply chain security still often struggles for attention. But expect wake-up calls to grow more insistent as two prevailing supply chain trends heighten cyber risks dramatically. One is the rapid expansion of operational data exposed to cyber adversaries, from mobile and edge devices like the Internet of Things (IoT) on up into the cloud. The second is companies' growing reliance on third-party—and even fourth-party—vendors and service providers, presenting attackers with new back doors into their supply chains.

The ongoing migration from corporate data centers to the cloud makes useful supply chain management data more readily available, especially coupled with technologies like IoT. But it is also changing cyber risk. New kinds of potential security issues arise from "direct-to-cloud" employee access and illicit crypto mining in the cloud. And while cloud service providers are considered better than most companies at protecting data, IDG Research[1] still reports that 25 percent of companies don't have a cloud-first policy, mainly due to security concerns. For many, the hurdle is to design security into their side of the configuration.

Cyber due diligence and oversight of suppliers out to the third, fourth—or nth degree—is also a challenge, such as when a company's accounting firm uses a third-party data hosting company that works with a fourth-party systems integrator. In a 2018 Ponemon[2] Institute survey, 59% of companies in the U.K. and U.S. said they experienced a data breach via a third party, but only 35% rate their third-party risk management program as highly effective. The consequences continue to grow as cyber security regulations increasingly hold breached companies responsible even when their suppliers are at fault. For example, the Federal Energy Regulatory Commission issued supply chain cyber security standards in October 2018, mandating that energy companies mitigate third-party risk. And by March 2019, any banks operating in New York will come under strict third-party risk management rules set by the New York State Department of Financial Services.

With the combined impact of accelerated innovation and multiplying cyber threats, supply chains require board-level, forward-looking risk management in order to help sustain reliable and viable business operations.



Supply Chain

59%

of companies in the U.K. and U.S. said they experienced a data breach via a third party,

ONLY

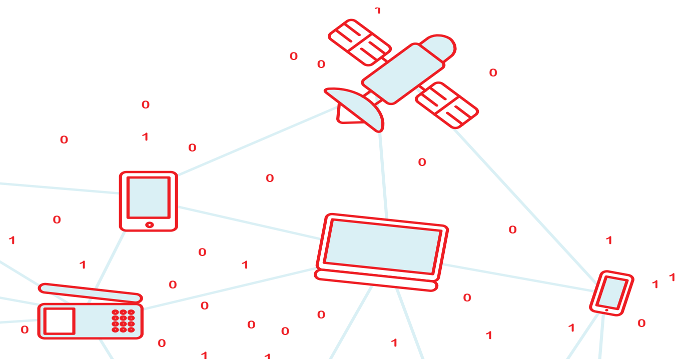
35%

rate their third-party risk management program as highly effective.

RISK 3 IoT (Internet of Things)

IoT is everywhere, and it is creating more risks than companies realize

IoT devices are everywhere in the workplace—even though many businesses may not realize it—and each device is a potential security risk. Network-connected IoT devices such as conferencing systems, security cameras, printers, and building automation sensors and controls can easily outnumber the organization's managed IT assets; in a 2018 Ponemon Institute survey, 52% of organizations that maintained an IoT inventory said they had at least 1,000 IoT devices—while the actual study average was much higher, at more than 15,000.[3]



Yet most companies don't securely manage or even inventory all of their IoT devices. This is partly because many corporate IoT devices are supplied and remotely managed by third parties, a practice that contributes to increased risk. Inadequately secured IoT devices are already leading to breaches. In the Ponemon survey, 21% of companies had experienced an attack or breach due to unsecured IoT devices in the last year—and 18% said the attacks were caused by third-party devices. As IoT devices are increasingly used in industrial systems, there is also an increased risk that IoT infections can disrupt manufacturing processes as well as other critical business operations.

The number of IoT endpoints will increase dramatically over the next few years, facilitated by the current worldwide rollouts of cellular IoT and the forthcoming transition to faster 5G networks. However, those networks will also provide new attack vectors. The combination of faster networks and vulnerable IoT devices may open the door to more destructive threats, such as botnets that use hordes of compromised IoT devices to overwhelm targets in Distributed Denial of Service (DDoS) attacks. New botnet malware continues to surface, as well as variants of the Mirai software that infected hundreds of thousands of insecure devices and blocked access to some Internet services in 2016.[4] It is important for organizations to monitor and inventory their IoT endpoints—and to assess the risk associated with these devices.

52% of organizations that maintained an IoT inventory said they had at least **1,000 IoT devices**—while the actual study average was **much higher, at more than 15,000.**

IoT

RISK 4

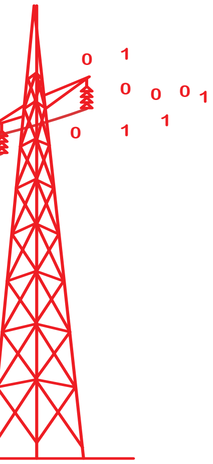
Business Operations

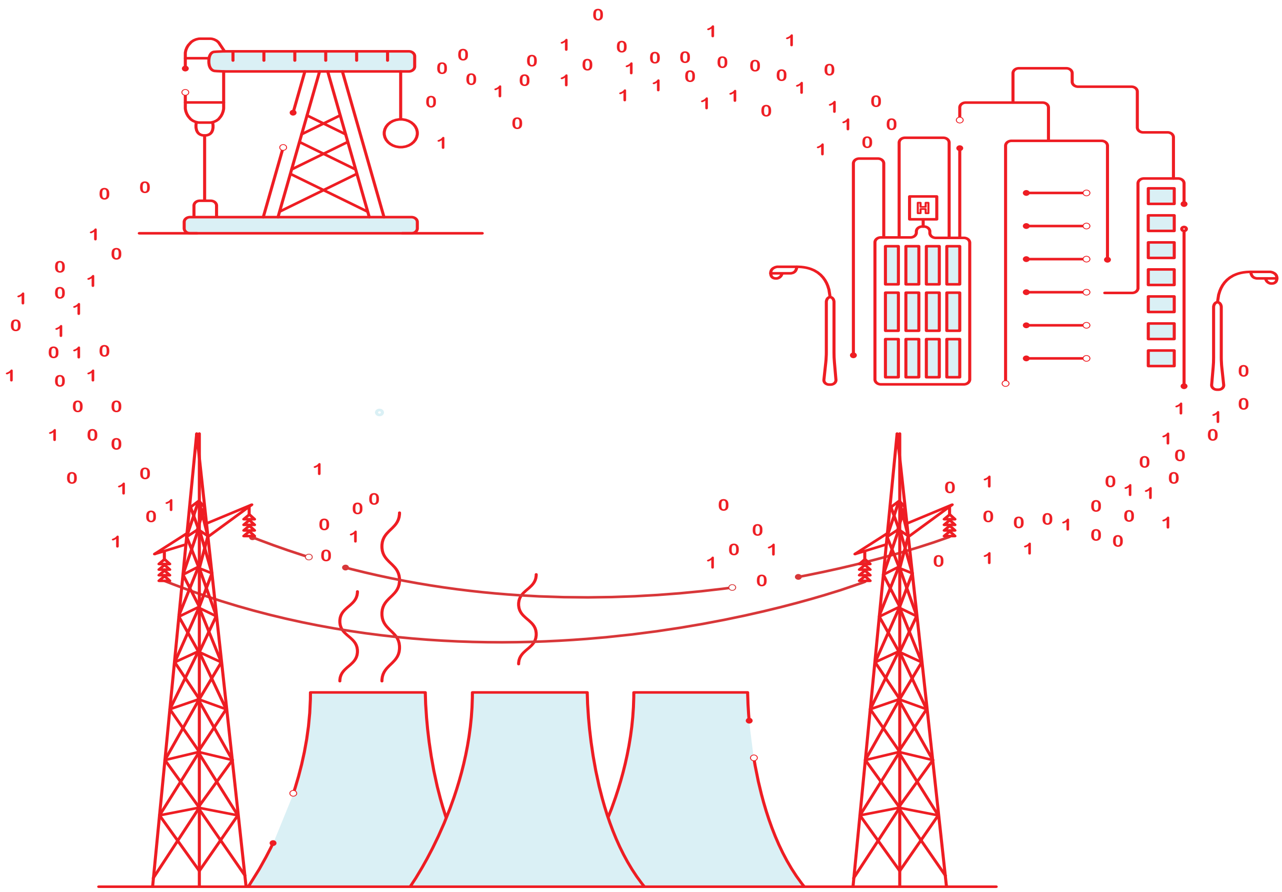
Technology for operational efficiencies can lead to security deficiencies that disrupt organizations

Increasingly, companies rely on technology to run critical day-to-day business operations. This reliance can create a painfully disproportionate risk of operational disruption. Malware infections can shut down manufacturing systems or potentially even a power grid; ransomware can bring business operations to a halt by encrypting the company's data.

Industrial control systems and public utility infrastructure have traditionally operated as standalone networks, but are increasingly connecting to the Internet and being integrated with traditional IT environments. While this connectivity increases operational efficiency, it also creates new security risks by greatly expanding the attack surface and making it easier for attackers to move laterally across the entire network. Worse, industrial control systems often include older equipment that wasn't designed with network security in mind. The Trisis malware, which shut down a major petrochemical plant, illustrates this very danger. It was designed to attack a logic controller that operates as a safety system for equipment used in industrial environments—such as nuclear power plants and oil and gas facilities—thus potentially causing not only significant physical damage but even loss of life.[5]

Increased connectivity also underpins the smart-city trend, in which municipalities are using technology to deliver new services—often in partnership with private companies, which may share the responsibility for ensuring the services are secure. The expanded network of connections increases the potential that a threat may cascade through city infrastructure; compromised smart street lights could be used to gain access to systems that control utilities or contain personal information about citizens.[6]





Business Operations

Meanwhile, destructive malware and ransomware continue to cause painful operational disruption. The NotPetya malware caused billions of dollars in damage at organizations in many different industries, including multinational shipping, pharmaceutical, construction, and manufacturing companies, bringing operations to a halt by irreversibly encrypting key data.[7] The WannaCry ransomware, which encrypted data and demanded a bitcoin ransom for making it accessible again, attacked more than 230,000 computers and caused worldwide chaos.[8] In such attacks, operational shortcuts or ineffective backup processes can increase the impact; for example, if backups are stored on network-attached drives instead of offline media, ransomware may find and encrypt backups as well as operational data, making data recovery practically impossible.[9] The disruptive effect of cyber events can threaten business continuity, and it is critical that companies understand the potential impact.

230,000

computers and caused worldwide chaos

RISK 5 Employees

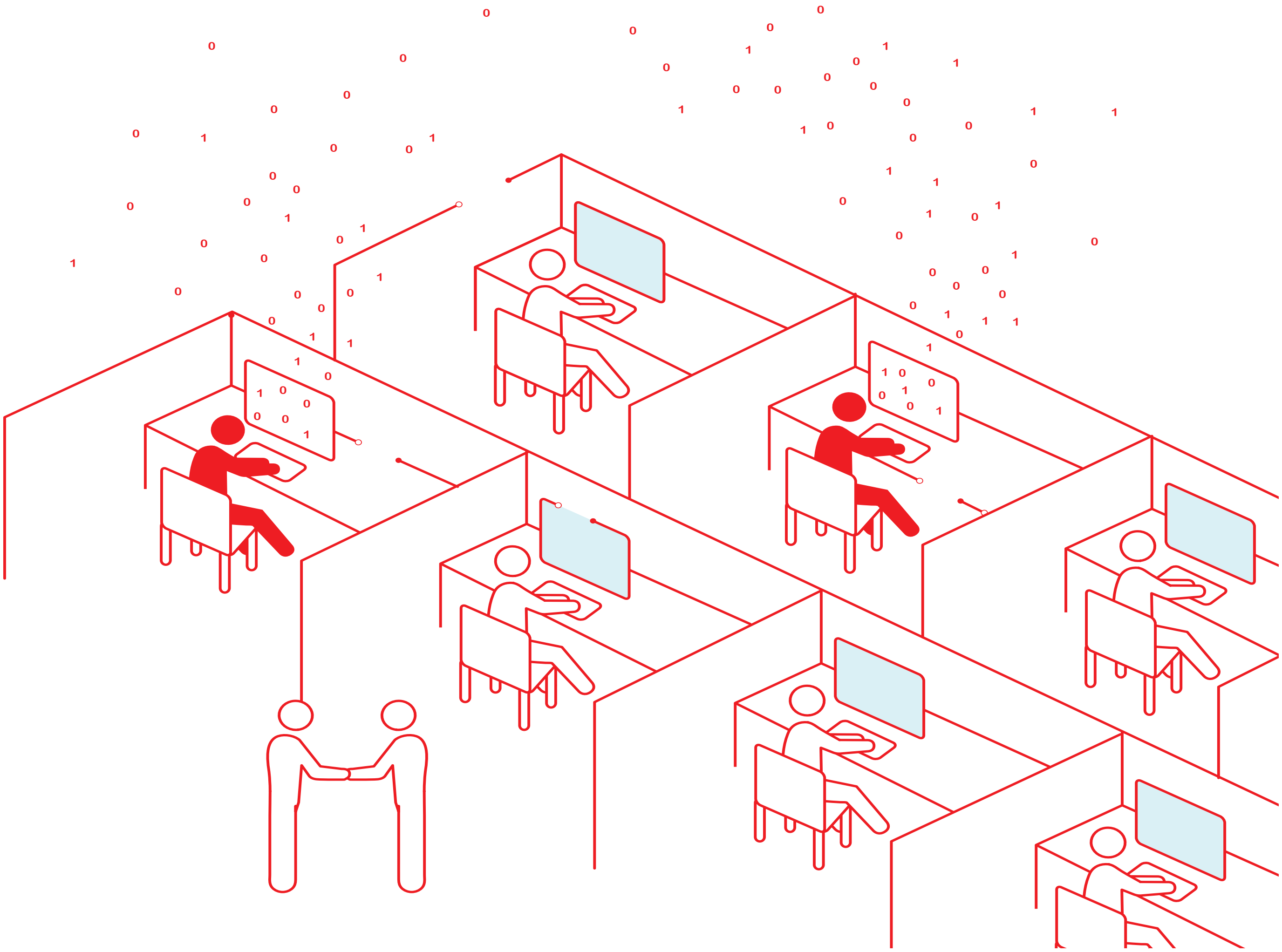
Excess privileges and shadow IT increase employee risk

Whether through malicious acts or negligence, employees remain one of the most common causes of security breaches. In a 2018 survey of cyber security professionals, 53% said their organizations had experienced an insider-related attack within the last year. And respondents were split nearly even on whether they worried most about accidental mistakes such as clicking on phishing links (51%) or malevolent employee behavior (47%).[10]

As companies seek to increase efficiency through technology, they often give users more robust access privileges than may be needed, which can increase risk. For example, system administrators tasked with managing more systems need correspondingly broader privileges, which increases the potential damage if those privileges are misused or compromised. Technology also enables employees to capture more sensitive information—by recording videoconferences or taking screenshots, for example—potentially increasing risk exposure.

At the same time, cloud computing is intensifying the "shadow IT" problem, in which departments or business units independently adopt technology without telling the central IT organization. It's often faster and easier for departments to directly establish accounts for cloud-based applications and services than to submit technology requisition requests to a central IT group. That can expose the organization to new, unknown risks, since IT may not even know which services are being used and is therefore unable to assess their security or enforce the use of strong login credentials.[11]

As privacy regulations increase in response to the digital economy transformation, the consequences of compromised personal and business data are growing. It's becoming even more important to establish a comprehensive approach to mitigate insider risks—including strong data governance, communicating cyber security policies throughout the organization, and implementing effective access and data-protection controls.



Employees

In a 2018 survey of cyber security professionals, 53% said their organizations had experienced an insider-related attack within the last year. And respondents were split nearly even on whether they worried most about accidental mistakes such as clicking on phishing links (51%) or malevolent employee behavior (47%).

RISK 6

Mergers & Acquisitions

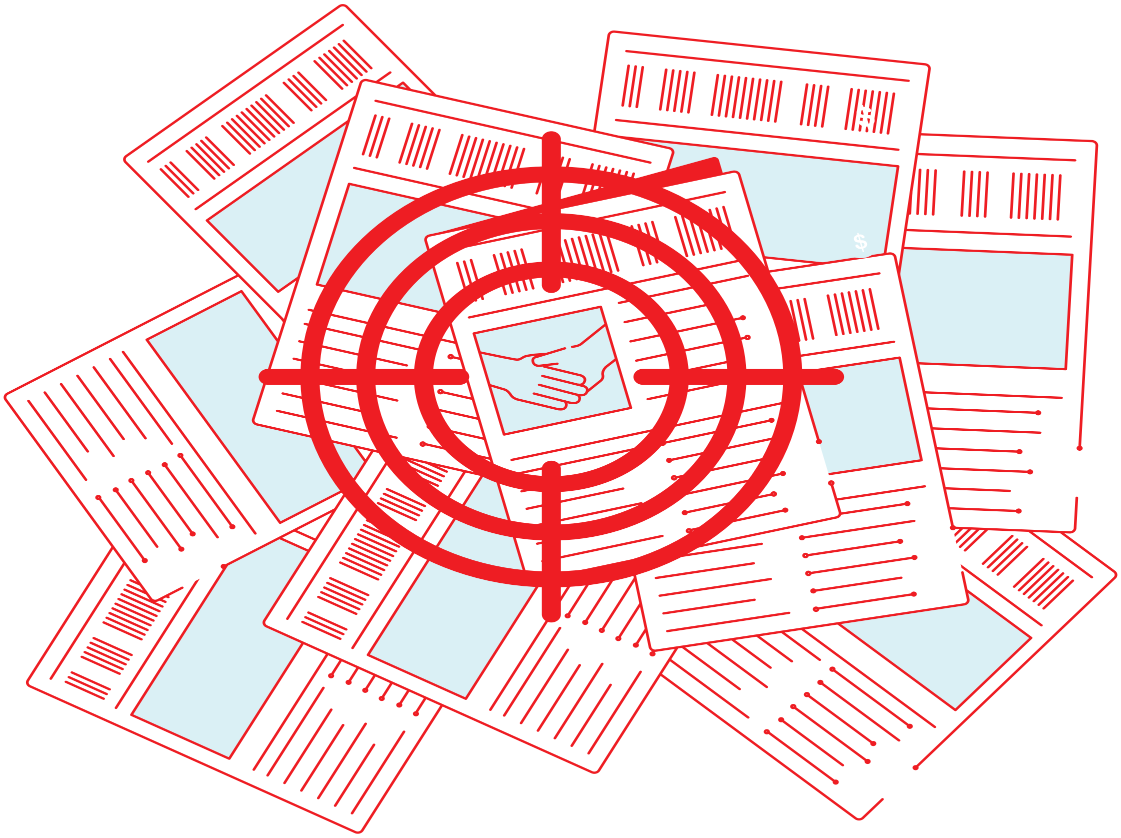
Vulnerabilities from deal targets increases as dramatically as M&A value.

As 2018 came to a close, global M&A deal value for the year was projected to top $4 trillion,[12] a rarely-reached watermark and the highest level in four years. But even with all that value at stake, many organizations don't recognize that every new M&A deal comes with new potential security vulnerabilities that are exceedingly hard to assess.

M&A cyber security risk is not theoretical. In 2017, an acquisition target from the media industry was forced to lower its deal price by $350 million when an attack was revealed between deal announcement and closing. And in the healthcare industry, nearly 80 million patient records ended up in the hands of a foreign government due to a persistent attack that began with a phishing email opened by an employee of a large insurer's acquisition target.[13]

The conundrum faced by acquiring companies is that while they may run a tight ship when it comes to cyber security enterprise risk – diligently patching security vulnerabilities, for example – there's no guarantee that the M&A target does the same. So, through the acquisition of another company, organizations also acquire all of that company's vulnerabilities. And the fast-moving timelines associated with most deal scenarios often challenge the ability of the acquiring company to gain insight into the cyber security posture of the target organization. How can companies confirm that necessary cyber security controls are in place? And who is responsible for that risk – and the potential cost of remediation?

As deal-making continues to grow, related cyber security risk may rise even faster. That's because cyber forensics leaders[14] report a trend in which bad actors target companies being acquired by larger enterprises in between deal announcement and closing. Dealmakers must make a plan to meet this rising challenge.



Mergers & Acquisitions

$4 TRILLION

As 2018 came to a close, global M&A deal value for the year was projected to top $4 trillion, a rarely-reached watermark and the highest level in four years.

RISK 7

Regulatory

Managing the intersection of cyber security policy and enforcement

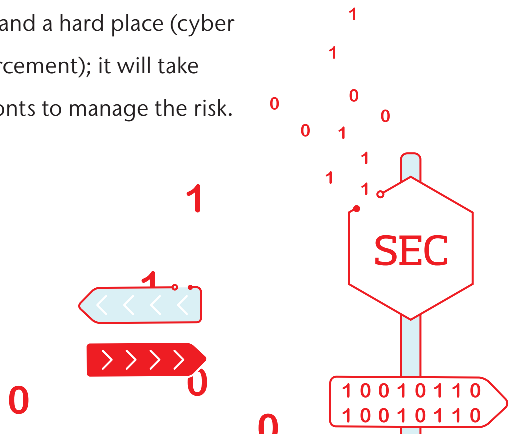
Cyber security regulation has gone viral. Proposals, principles, laws, rules, standards, and guidelines are spreading in global forums, federal agencies, state legislatures, and the business world—from the law of the land to sector-specific regulations to government purchasing requirements, and from public-private partnerships to accounting associations to technology industry consortia. The U.S. Securities and Exchange Commission (SEC) became involved in 2018, requiring cyber security disclosures in financial statements. The pace of cyber regulation enforcement grew more aggressive, as well, with the SEC issuing its first fines. The stage is set for heightened compliance risk in 2019.

What's more, proliferating and overlapping cyber-regulation runs the danger of actually creating more cyber risk, not less, as compliance obligations overwhelm the Chief Information Security Officer (CISO), and a "check-the-box" mentality replaces best cyber security practices. On top of it all, even knowing which box to check, in which jurisdiction, has become much more complex.

In a clear sign of the times in 2018, California passed a consumer privacy act and an Internet of Things privacy law. If past is prologue, businesses must prepare for a new wave of similar state legislation across the country, as happened with the California Data Breach Notification Law of 2002. Meanwhile, some are pressing for U.S. federal legislation.

No discussion of the cyber security regulatory environment could be complete without the European Union's General Data Protection Regulation (GDPR) and its fines for noncompliance of up to 4% of annual revenue. Since the May 2018 deadline for implementation, the few GDPR enforcement actions, fines, and civil suits to date represent what is perceived to be the tip of the iceberg. Media reports[15] surrounding 2018 mega-breaches have speculated that each company involved could face a potential fine of $500 million to over $1 billion if regulators uncover associated GDPR violations.

Companies today find themselves between a rock (cyber threats) and a hard place (cyber regulation and enforcement); it will take vigilance on both fronts to manage the risk.



Regulatory

$500 MILLION to over $1 BILLION

Media reports surrounding 2018 mega-breaches have speculated that each company involved could face a potential fine of $500 million to over $1 billion if regulators uncover associated GDPR violations.

RISK 8

Board of Directors

Directors and Officers face growing personal liability relative to cyber security oversight

Proposals, Managing cyber security risk has quickly become one of the biggest oversight challenges facing board directors and officers—and it's a growing personal risk, too. Shareholders[16] have been bringing claims against directors in some of the highest-profile data breaches.

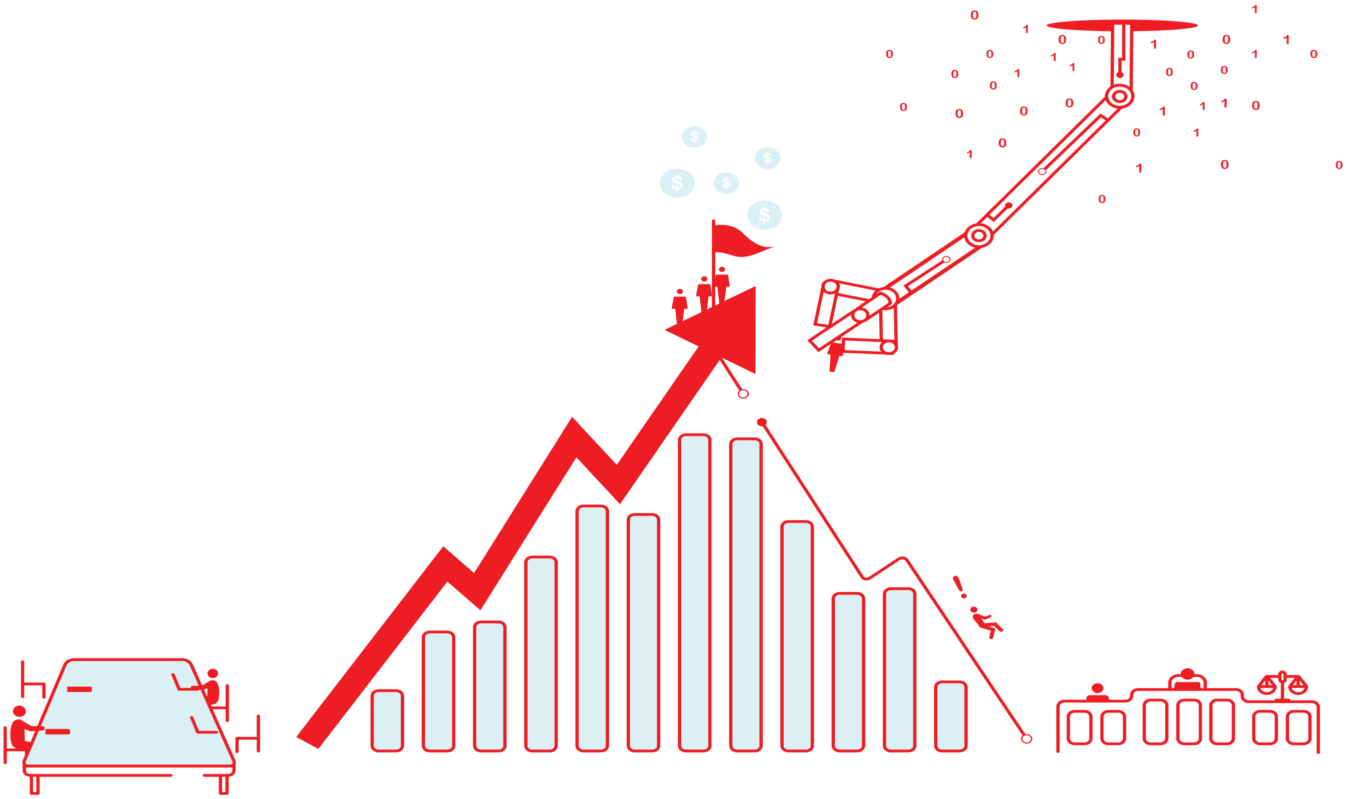
As of print, a majority of litigation against directors and officers has not been successful, but the story will likely not end there. Plaintiffs' attorneys are expected to learn from initial failed claims, reframe arguments, and continue bringing cyber security suits against directors and officers, as well as the companies they govern. The stakes are high, considering the $47 million settlement[17] one online services company announced in late 2018 to end three cyber-suits, including derivative shareholder litigation.

Class-action suits will likely increase, especially in cases where data incidents cause precipitous stock drops. The general rise in European class-action lawsuits is also leading to GDPR-fueled legal challenges. And at print time, a data privacy suit that pre-dates GDPR, involving a class-action complaint by employees against a U.K. supermarket chain, was already headed for the U.K. Supreme Court.[18]

Directors and officers also face regulatory liability. In 2018, for example, wide-reaching new cyber security rules from the New York State Department of Financial Services began requiring annual certifications of compliance by directors or other senior officers. Further, the SEC has become active, policing cyber security disclosures in financial reports—and has been known to single out directors and senior officers when enforcing other areas of its portfolio. In egregious cases, the SEC has levied monetary penalties and lifetime bans on acting as a director or officer of a public company.

3/4

The good news is that nearly three-quarters of board directors say they are more involved with cyber security than they were a year ago.



Board of Directors

The good news is that nearly three-quarters of board directors say they are more involved with cyber security than they were a year ago, according to a 2018 survey[19] by the BDO Center for Corporate Governance and Financial Reporting. Still, there is room to grow: While many boards make significant cyber security spending decisions after a cyber incident, it is all too common that cyber security remains a capital expense and is not provided adequate operating budget support once the crisis has passed.

Expanding personal as well as business risk from cyber security oversight has raised the stakes for board directors and officers, who must continue to expand their focus and set a strong tone at the top to drive their company's cyber policy and procedures.

2019

It’s a modern digital twist on a story as old as time: with great opportunity comes great risk.

2019 Outlook: With great opportunity comes great risk

The eight risks discussed in this report point to the fact that as digital transformation proliferates, the "attack surface" of global business expands rapidly, and in sometimes unexpected ways. It's a modern digital twist on a story as old as time: with great opportunity comes great risk. To mitigate that risk, corporations must exercise constant vigilance over their fast-changing enterprise cyber risk profiles—from the boardroom to the supply chain, and from IT infrastructure to every other facet of business operations. That means organizations must stay informed, understand their risk profile and be proactive in their defense: share threat intelligence to help keep the entire business community safe, hunt to detect bad actors before they cause damage and, perhaps above all else, be prepared for a cyber attack.

8

The eight risks discussed in this report point to the fact that as digital transformation proliferates, the "attack surface" of global business expands rapidly, and in sometimes unexpected ways.

Contacts

References

1. https://www.cio.com/article/3018156/cloud-computing/cloud-adoption-soars-but-integration-challenges-remain.html
2. 2018 Ponemon Study on Global Megatrends in Cybersecurity; https://www.ponemon.org/blog/ponemon-institute-announces-the-release-of-the-2018-megatrends-study
3. Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk, Ponemon Institute
4. https://www.zdnet.com/article/meet-torii-a-new-iot-botnet-far-more-sophisticated-than-mirai/
5. https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos/
6. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/smart-cities.html
7. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
8. https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/
9. https://www.csoonline.com/article/3075385/backup-recovery/will-your-backups-protect-you-against-ransomware.html
10. http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf
11. https://www.cio.com/article/3139396/security/the-evolving-insider-threat.html
12. https://imaa-institute.org/mergers-and-acquisitions-statistics/
13. https://www.bitsighttech.com/blog/security-breaches-healthcare
14. https://imaa-institute.org/mergers-and-acquisitions-statistics/
15. https://www.healthcareitnews.com/news/hacking-and-mega-breaches-2018-worst-year-yet
16. https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2018-insurance/written-materials/cyber-attack.pdf
17. https://www.bizjournals.com/sanjose/news/2018/09/17/altaba-yahoo-data-breach-settlement-vz.html
18. https://www.theregister.co.uk/2018/10/23/morrisons_loses_court_appeal_data_theft/
19. https://www.rtinsights.com/fresh-data-bdo-sees-some-boards-preparing-for-cyber-risks-others-blind/

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

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.

Visit aon.com/cyber-solutions for more information.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.