MARSH & McLENNAN ADVANTAGE
INSIGHTS

MMC Cyber Handbook 2020

Advancing Cyber Resilience

MARSH GUY CARPENTER MERCER OLIVER WYMAN

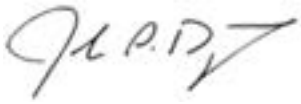
FOREWORD

Cyberattacks are viewed by business leaders as the number one risk in advanced economies for the second year in a row, according to the latest World Economic Forum executive opinion survey. This widespread and continuing apprehension about cybersecurity is reinforced by the results of the *Marsh | Microsoft 2019 Global Cyber Risk Perception Survey*, which found almost 80% of executive respondents ranking cyber risk among their top five concerns.

Cybersecurity is a top priority in the business community for a number of reasons. First, businesses are increasingly dependent on technology platforms to manage their core operations. This dependence heightens both the likelihood and severity of business interruptions stemming from cyberattacks. Second, digital innovation is now a top-line growth engine for many enterprises. However, the pace and nature of this innovation is introducing new types of technology risk that management practices and regulations have not yet fully addressed. Last but not least, many firms are operating in complex supply chains that expose them to the weaknesses in other companies who may not have the same focus on cyber risk management. This interdependency heightens the challenge of maintaining cyber resilience for all firms in the supply chain. Given these factors, business leaders increasingly recognize that cyber is a risk can be understood, measured and managed – but not completely eliminated.

Looking forward to 2020, we expect the cyber landscape to be more complex than ever before. *The MMC Cyber handbook 2020* features perspectives from business leaders across Marsh & McLennan Companies, as well as strategic partners who represent some of the best thinking about the cyber economy. We bring together the latest perspectives on how to take action in the face of growing complexity and uncertainty, and dive into some of the most significant cyber trends, industry-specific implications, and emerging regulatory challenges.

We hope this handbook provides you with new insights to advance your cyber resilience strategy in this increasingly complex and interconnected world.



John Drzik

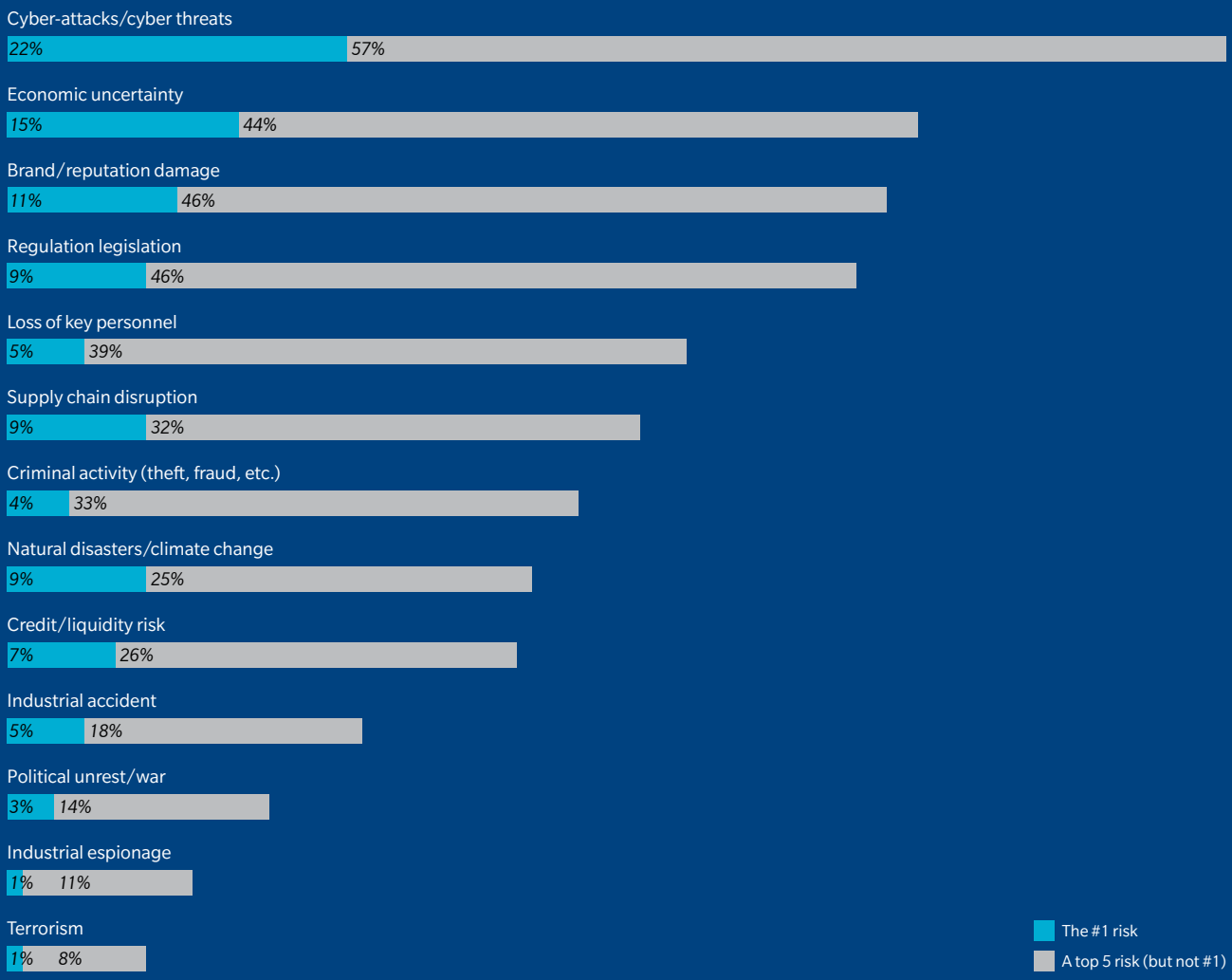
President, Global Risk and Digital
Marsh & McLennan Companies

TABLE OF CONTENTS

TREND WATCH

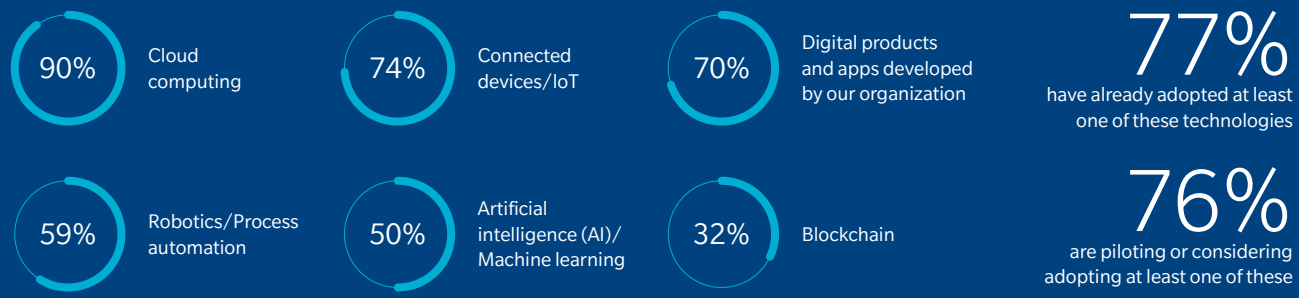
Cyber risks outrank all other risks by a wide margin[1]

Q: Out of the following business threats, please rank the top 5 that are the biggest concerns to your organization.



Most organizations are considering or using a range of new technologies[2]

Q: For each of the following technologies, please indicate which consideration or usage scenario best applies to your organization.



1. Base: all answering; n=1,512 (2019)

2. % of organizations that have adopted/are piloting/considering each technology. Base: all answering, excluding don't know responses; n=588-773 (2019)

Source: Marsh Microsoft Global Cyber Risk Perception Survey 2019, Marsh & McLennan Insights analysis

BEWARE OF THE RISKS OF SILENT CYBER

Siobhan O'Brien
Head of Cyber Center of Excellence for International and Global Specialties, Guy Carpenter

Cyber risk is one of the most dynamic challenges facing the insurance and reinsurance industry. **"Silent cyber"** is a term that is increasingly used to describe cyber-related losses stemming from insurance policies that were not specifically designed to cover cyber risk — meaning an insurer may have to pay claims for cyber losses under a policy not designed for that purpose.

THE SILENT CYBER THREAT

As a result, regulators are now formalizing capital requirements, as well as quantitative and qualitative measurements of risk appetite. In the UK, the Prudential Regulation Authority (PRA) is asking re/insurers to develop a silent cyber action plan by the middle of 2019. PRA will conduct deep-dives on select firms in the second half of the year to assess how well they are meeting expectations, as described in a 2017 supervisory statement. The PRA will then further assess affirmative cyber risk via an exploratory stress test later in the year.

As large-scale events and regulatory pressures increasingly test risk management strategies, this is a critical moment in the evolution of the cyber product, particularly regarding these silent exposures. Companies will need to enhance cyber underwriting and reinsurance strategies, leverage their innovative modeling capabilities, and develop technical and underwriting risk talent if they are to continue offering clients the best security possible.

TRYING TO DEFINE EXPECTATIONS

Regulators globally and other stakeholders are collaborating to define expectations for firms writing cyber policies to protect against attacks like WannaCry and NotPetya. These events demonstrated the speed at which a cyberattack can spread and the catastrophic potential of silent cyber. PCS Global Cyber attributes around 90 percent of the insurance industry's loss from NotPetya-related cyberattacks to silent cyber.

The systemic damages also shifted the conversation from data breaches, notification costs and third-party liability to first-party liability and business interruption. In 2017, the European Insurance and Occupational Pensions Authority (EIOPA), in its first attempt to quantify silent cyber, surveyed 13 re/insurers from across Europe based on their expertise and cyber exposures.

In 2018, EIOPA surveyed insurers on IT governance, their own system landscape and measures to respond to cyberattacks. The EU-U.S. Insurance Dialogue Project, started in 2012, aims to enhance understanding between the European Union and the United States, while a study by the U.S. National Association of Insurance Commissioners and the Center for Insurance Policy and Research titled Cyber Risk Insurance Market Advances, Challenges and Regulatory Concerns is forthcoming.

"There has been limited progress on modeling non-affirmative cyber risk, despite industry recognition of the need to continuously develop its cyber knowledge."

STRATEGIES ARE STILL EVOLVING

Between 2015 and 2016, the PRA asked the re/insurers it regulates to identify and assess their exposure to affirmative and silent cyber. The results showed that clear strategies, defined risk appetites and robust methods for quantifying exposures were still developing, along with a level of uncertainty regarding the response of reinsurance programs and a limited ability for risk managers to challenge business strategies.

At that time, the PRA also noted pricing had not developed sufficiently and there was insufficient investment in internal cyber expertise. In response, it issued a supervisory statement in 2017 detailing its expectations for managing non-affirmative cyber risk, setting clearly defined, board-approved cyber strategies and risk appetites and developing their expertise.

It also suggested addressing silent cyber by considering adjustments to premiums to offer explicit cover or introducing exclusions or sub-limits. In 2018, it conducted a follow-up survey that suggested progress had been made, but that more work was needed, particularly regarding silent cyber.

HIGHEST RISK IN CASUALTY, FINANCIAL, MOTOR AND A&H LINES

In January, the PRA issued a letter to CEOs outlining survey findings, including the high risk of silent cyber in casualty, financial, motor and A&H lines, although views of silent exposure within property, marine, aviation and transport and miscellaneous lines varied. The survey also found that firms' quantitative assessments of non-affirmative risk are underdeveloped, with only the most advanced companies conducting detailed analyses for all products by bringing together underwriting, risk, claims, IT and actuarial departments. This often included policy wording reviews.

The survey indicated a widening of affirmative cyber coverage for business interruption, contingent business interruption, and reputational damage, yet it also indicated a significant divergence in modeled losses among companies. There continues to be little evidence that reinsurance programs will respond as planned to a silent cyber event.

This underlines the inherent uncertainty in available cyber models and the lack of reliable claims data. The heightened need for formalized risk appetites and board-agreed cyber strategies increases the importance of developing bespoke scenarios for particular portfolios. But there has been limited progress on modeling non-affirmative cyber risk, despite industry recognition of the need to continuously develop its cyber knowledge.

THE INCREASING THREAT FROM INSIDE

A PROACTIVE TARGETED APPROACH TO MANAGING INSIDER RISK

Paul Mee
Partner and Cyber Lead,
Oliver Wyman

Rico Brandenburg
Partner,
Oliver Wyman

Insider threat, one of the greatest drivers of security risks that organizations face. It only takes one malicious insider to cause significant harm. Typically, a malicious insider utilizes their (or other employee's) credentials to gain access to a given organization's critical assets. Many organizations are challenged to detect internal nefarious acts, often due to limited access controls and the ability to detect unusual activity once someone is already inside their network.

A significant number of executives fall victim to common misconceptions about insider risk and, therefore, they typically do not believe that their organization's own workers pose a significant threat. Even those who do, find it challenging to make significant headway, as doing so requires tackling a host of thorny legal and HR issues. As a result, many organizations have underinvested in this area.

"In 2018, of the 5 billion records stolen or compromised, over 2 billion were a result of insider circumstances."

Risk based security: Data Breach Trends Report 2018

Organizations simply cannot afford to ignore the threat any longer. Companies are waking up to the fact that insider threat can pose considerable harm to their operational resilience, financial status, and reputation. Across industries, regulators, government agencies, and industry groups have signaled that organizations need to take insider threat seriously.

"75% of companies believe they have appropriate controls to mitigate insider threat — but more than 50% of companies had a confirmed insider attack in the past 12 months."

Crowd research partners: 2018 Insider Threat Report

Applying data loss prevention technology, monitoring software, or compliance surveillance tools is not enough. Organizations need to scale their diligence and defenses appropriately to their inherent insider risk exposure by integrating technology and organizational disciplines to identify, detect and mitigate risks before they materialize or cause harm.

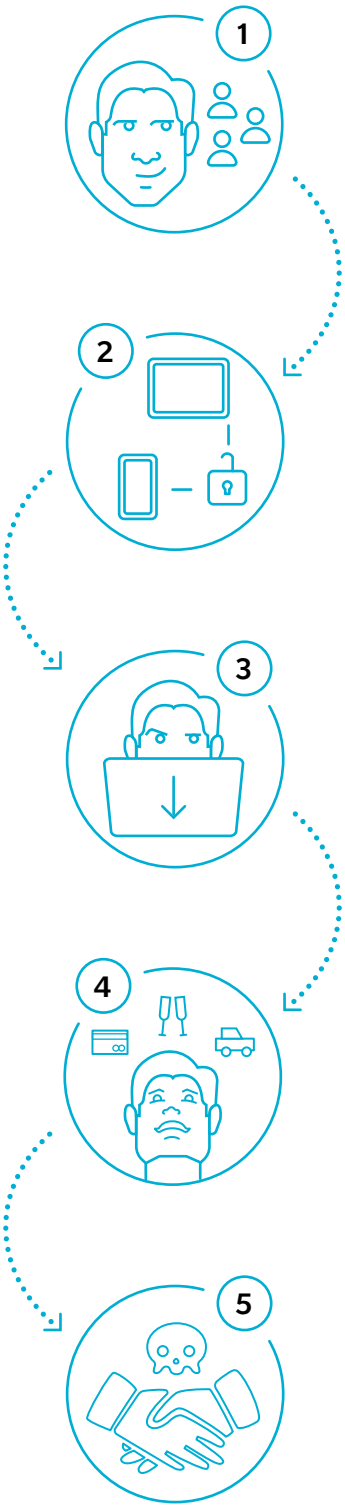
Leaders in this area tend to have the right level of senior stakeholder engagement; use a risk-based prioritization of what to monitor and protect; and most importantly, have implemented joined-up procedural arrangements with clear and tested roles and responsibilities to enable the right response when unusual behavior is identified.

Despite the growing consensus that insiders represent a considerable threat with potentially severe consequences, some organizations remain in denial. They fall victim to generally accepted myths that make them believe that "this won't happen to us" (see Exhibit 1).

EXHIBIT 1: MECHANICS OF A MALICIOUS INSIDER EVENT (ILLUSTRATIVE)

A SERIES OF SUSPICIOUS ACTIVITIES

by the talented Mr. Regal



- Through an internal transfer, Mr. Regal joins the Marketing Analytics team within the Wealth division
- He is excited by the potential of being associated with a lavish lifestyle
- He takes a particular interest in High Net Worth (HNW) clients

- Mr. Regal looks for the means to get access to customer PII/NPI
- When he knows his boss's boss is very busy, Mr. Regal asks him to approve access for some "new important campaigns"
- Mr. Regal secures broad privileged access

- Mr. Regal develops a set of queries to collect data on the most valuable clients
- Late at night, he runs scripts to pull the client data and uploads the datasets (each about 10,000 records in size) to a little-known file-sharing website

- Mr. Regal's "champagne lifestyle on a limited income" status weighs heavily on him and he explores means to monetize the HNW client data he continues to accumulate
- He approaches various potential FS and non-FS buyers
- His work suffers as he focuses on monetizing the data

- Mr. Regal contacts criminal groups through the dark web
- Mr. Regal shares the data and receives an agreed payment
- He is given a thumb drive for further data downloads that, unbeknownst to him, has malicious malware to allow undetected remote access by outsiders

EXHIBIT 2: MYTH BUSTERS - COMMON MISCONCEPTIONS ABOUT INSIDER THREATS

MYTH	TRUTH
A good company culture is enough to protect against insiders	A good company culture reduces the likelihood of disgruntled employees. But the motivation of malicious insiders can be driven by a variety of factors unrelated to the company's culture, e.g., financial gain, ideology, desire for recognition. Over 50 percent of companies confirmed insider attacks in the past 12 months.[1]
Insider threat comes from contractors	Permanent staff are typically with an organization longer and accumulate more access over time, so they represent a bigger threat. 56 percent of companies identified regular employees as the greatest security risk to organizations.[1]
Insider risk is mitigated through the general control environment	Controls designed for other purposes may not be as effective against insiders (e.g., requiring people to have valid credentials to enter a building or log in), but they can be leveraged in an effective program.
Malicious insider activity can be spotted right away	Many organizations have rules-based monitoring that will detect basic insider activity (e.g., an employee emailing large files to her personal email). But few organizations will detect more sophisticated insider activities (e.g., exploiting access they rightfully have, sending confidential information in the body of an email to a seemingly legitimate email address). On average, it takes organizations 72 days to contain an insider incident, with only 16 percent of such incidents contained in less than 30 days.[2]
Data loss prevention (DLP) is an effective insider risk program	DLP is a component of, but not the same as, an insider risk program. DLP can help prevent exfiltration of data by an insider. But it provides little protection against other malicious acts (e.g., destruction of assets, fraud).
Insider threat is only an issue for strategic industries	Many of the highest-profile events have been in "strategic industries" with leading-edge innovation or R&D, national defense capabilities, or highly valuable data (e.g., medical records). However, companies in all industries[2] and all sorts of government bodies have had material events caused by an insider.
Recruiting has a good process to filter out potentially malicious employees	People do not need to have malicious intentions from the start. Changes in personal or economic circumstances may create incentives for malicious activity over time.

1. Crowd Research Partners: 2018 Insider Threat Report
2. Ponemon Institute 2018 Cost of Insider Threats: Global. Includes accidental insiders, malicious insiders, and credential thieves

EXHIBIT 3: SUCCESSFUL DESIGN AND IMPLEMENTATION OF AN INSIDER RISK PROGRAM

Risk identification and assessment

- Classification of "crown jewels"
- Identification of internal threat vectors
- Development of business-driven risk scenarios

Pilot design and execution

- Definition of key risk factors and development of an employee risk rating
- Identification of a sub-group of high-risk employees as a pilot population
- Setting up an effective and efficient cross-functional governance to drive engagement
- Design of use cases around the target population
- Development of monitoring and reporting

Refinement and use case expansion

- Refinement of use cases and employee risk rating based on pilot results
- Identification of additional groups of high-risk individuals
- Integration of data sources
- Development of additional use cases

Roll-out to high-risk areas

- Roll-out planning and impact assessment
- Communication plan
- Development of maintenance and continuous improvement processes

TAKING A PRACTICAL APPROACH TO INSIDER RISK: START SMALL AND FOCUSED

Implementing an effective insider risk program requires a design tailored to the specific culture, processes, and risks of the organization. It's important to start small and focus on a clearly defined high-risk employee sub-group to work through the organizational issues that need to be solved. Our paper describes a practical approach to designing and implementing a successful insider risk program.

With insider threat only increasing in prominence, organizations simply cannot afford to ignore the threat. Getting it right will deliver clear benefits, but delays could be costly. Take a proactive approach to managing insider risk – start small, but start now.

THE THREAT FROM THE CLOUD

HOW CYBER INTRUDERS EXPLOIT THIRD PARTIES

Kevin R. Brock
Founder and Principal,
NewStreet Global Solutions,
LLC

David X Martin
CEO and Expert Witness,
David X Martin,
LLC

There's a growing concern within intelligence communities that hostile governments could cyber-invade financial institutions, not to steal money — but to pollute, destroy and manipulate data. Data manipulation is difficult to detect, and hackers might even target data in backup storage to ensure that recovery is impossible. Cyberattacks that create chaos in record keeping, transaction precision and currency valuations could corrode public trust to such an extent that it threatens the stability of the financial system.

THE CLOUD AS A POINT OF ENTRY

One of the biggest exposures lies in the cloud. As supply chains become ever more complex, financial institutions are relying on third parties to provide scale and agility. However, third-party providers are often the vector that cyber intruders exploit in order to reach the intended target. This dramatically increases the attack surface that companies have to worry about. Trusting that third parties will attend to your security needs in the manner you would is not a prudent strategy.

If you rely on a weak set of interfaces to interact with cloud services, security issues can arise concerning confidentiality, integrity, availability and accountability. A few examples: Attackers now have the ability to use your (or your employees') login information to remotely access sensitive data stored on the cloud; falsify and manipulate data through hijacked credentials; or inject malware, which gets imbedded in the cloud servers. And, if operating in tandem, attackers can eavesdrop, compromise the integrity of sensitive information and even steal data.

THE VULNERABILITY OF APIs

Secondly, the services provided are elastic in that there are different degrees or levels of service and security. This fosters an inconsistent security model. Application programming interfaces (API) give users the opportunity to customize features of their cloud services to fit business needs — but also allows users to authenticate, provide access and effect encryption, which can create vulnerabilities. The biggest vulnerability of an API lies in the communication that takes place between applications — creating exploitable security risks and new attack surfaces.

Case in point: In January of this year, researchers revealed a design feature common in most modern microprocessors that could allow content — including encrypted data — to be read from memory using malicious Javascript code. Two variations of this issue, called Meltdown and Spectre, permit side-channel attacks because they break down the isolation between applications.

EMPLOYEES CAN ACCESS THE CLOUD

In addition, data stored on a cloud provider's server could potentially be accessed by an employee of that company — and you have none of the usual personnel controls over those people. In a recent breach of an online bank, the attacker was a former employee of the web-hosting company involved and allegedly used web application firewall credentials to obtain privilege escalation.

Data on cloud services can also be lost by an erroneous data wipe by the service provider — as happened recently at a large online retailer. Making matters worse, most businesses do not have recovery plans for data stored on the cloud. The bottom line is that companies need to take ownership of their risk all the way down the line.

"Threat-aware companies build cybersecurity environments similar to the immune system of the human body."

DEVELOP A DATA-CENTRIC APPROACH

It is important for business leaders to develop strategies that are tailored to their institution's unique imperatives and seek the highest level of risk mitigation reasonably achievable. Most businesses think of cybersecurity as protection of the digital environment encompassing networks, servers and applications. The problem with this paradigm is that the security deployed is not necessarily related to the data it's trying to protect.

Security that focuses on protecting crucial data asks: "What is our most important data? What people, processes and technology, if any, are deployed to protect the data? What would be the impact of a specific breach of this data on the organization, and how would we respond?"

Consider the use of data loss prevention solutions that can encrypt your important data with high assurance; provide automated backup and accurate audit information regarding the movement and handling of sensitive data; and even block the transfer or delete the data when found on unauthorized endpoints. Perimeter security without data security is false security.

STRENGTHEN YOUR IMMUNE SYSTEM

Threat-aware companies build cybersecurity environments similar to the immune system of the human body. When a germ breaches the body's natural barriers, the immune system mounts a three-step defense: It sounds the alarm, attacks the problem and then recovers and remembers.

Managing the very real risks to critical infrastructure like our financial systems will take determined, strategic effort — largely by the private sector. For the first time in recent history, the U.S. and other governments are unlikely to be able to provide an effective deterrent to a significant criminal threat. Don't expect the government to come to the rescue when your company experiences a cyberattack. Instead, the best place to find a helping hand is likely to be within your own company.

D&O LIABILITY

THREE EMERGING AREAS TO WATCH

Sarah Downey
D&O Product Leader,
Marsh

As business risk evolves, the pressures on company boards and officers are growing. Gone are the days when the main concerns of directors and officers were related to company mismanagement and misrepresentation claims.

Chief among potential risks that boards must now deal with are: emerging technologies, cyber-risk issues and ever-expanding litigation against companies and their boards. Given the emergence of these three threats, it is imperative that board members review their directors and officers liability (D&O) insurance for any lapses in coverage.

EMERGING TECHNOLOGIES

Technology is advancing like never before, and businesses are using innovative technological tools to revamp everything from back-office processes to the products and services they deliver to customers. But with the excitement of new and arguably better solutions come a lot of unknowns.

Although artificial intelligence, blockchain technology, digital assets and quantum computing are all emerging technologies with business value, each also presents potential exposures that must be understood and addressed. These new innovations can give rise to exposures that are now only being discovered by courts of law and insurance companies alike, whether that is due to lack of regulation, the evolution of existing regulations to keep up with new technology, a company's inability to keep up with the times or a board's failure to properly disclose associated risks or costs. For example, the failure to adequately disclose the potential risks associated with the implementation of AI or misrepresentations about those risks could lead to a D&O insurance claim.

CYBERSECURITY AND PRIVACY-RELATED ISSUES

In the short history of cybersecurity exposure, boards have generally considered cyber-related loss to be a top risk for companies. The threats these incidents can pose to organizations, directors, and officers are becoming more apparent. The threats include an increase in:

- Securities class-action filings as stock drops associated with data breaches continue
- Derivative lawsuit filings against directors and officers for alleged mismanagement or false or misleading statements related to cyber incidents

Over the past year, we've seen greater regulatory scrutiny and activity in the cyber exposure space, and it is not limited to civil litigation. The Securities and Exchange Commission (SEC), for example, has settled enforcement proceedings arising from matters such as a company's purported material misstatements and omissions regarding a large data breach and alleged failures in cybersecurity policies and procedures surrounding such a breach that compromised the personal information of thousands of customers.

We expect that the SEC and other regulators will continue to focus on cybersecurity threats and breaches going forward. In addition to breaches, privacy regulations — such as the General Data Protection Regulation in Europe — are a priority for all boards and a major area of focus for regulators. For example, the Federal Trade Commission's recent acknowledgment that it has the ability to penalize individuals for their respective companies' privacy law violations is a reminder that individuals are not immune to these types of exposures.

In addition to liability concerns, cyber- and privacy-related issues can cause reputational harm. A rating agency recently downgraded its outlook on a company in large part because of breach-related issues. The impacts of cyber- and privacy-related exposures on companies and their directors and officers are only beginning to play out.

"The market has seen 14 years of generally soft conditions, however over the last few quarters, we've seen a dramatic switch."

LITIGIOUS ENVIRONMENT

One need not look far to find significant litigation risks for businesses and their boards of directors. According to an analysis by NERA Economic Consulting, 83% of completed company mergers are met with litigation,

and one in 12 publicly traded companies are expected to be sued in a securities class action suit this year.

What's more, following the March 2018 U.S. Supreme Court decision in Cyan, Inc. v. Beaver County Employees Retirement Fund, companies going through initial or secondary public offerings are now more likely to be met with litigation in both state and federal court than before.

The world of corporate governance has changed. Business decisions are now closely scrutinized by the public. The use of email among company individuals forever preserves a record of discussions that once might have remained private. And actions taken in the public eye — including those through social media — can expose a company and its officers and directors to some form of liability.

Plaintiffs' attorneys, meanwhile, become more resourceful every day; even those firms that were previously not feared have turned filing lawsuits into a factory business. And smaller to midsize companies that once barely caught the eye of the plaintiffs' bar are now squarely in their crosshairs.

THE RISE OF SECURITIES CLASS ACTIONS

According to NERA, 441 new securities class actions were filed in 2018, the most in any year since the aftermath of the 2000 dot-com crash. 2018 was also the fourth consecutive year of growth in the number of filings, exceeding the 434 filings in 2017. In the first quarter of 2019, 118 securities class actions were filed; that puts us on track for 472 class actions this year and a fifth consecutive year of growth.

The heightened pace and total of securities class action filings that has continued into 2019 is, in part, attributable to the growing number of follow-on, event-driven securities litigation filings, as opposed to cases involving accounting misrepresentations and financial restatements that have historically made up the bulk of securities litigation.

Event-driven litigation occurs when some adverse event at a company triggers a securities claim — based either on a stock drop following the announcement of such an event or in the form of a derivative action thanks to an alleged breach of fiduciary duty. In addition to cyber-, privacy-, and sexual harassment-related, event-driven litigation, an array of other incidents have led to securities claims, including mass torts, product defects, product recalls, food safety issues, anti-corruption scandals and the California wildfires. These types of risks are difficult to predict.

THE COST OF LITIGATION

The cost of litigating even a baseless case that is dismissed or settled early on can be significant, which has not gone unnoticed by D&O insurers. The more litigious environment coupled with years of falling premiums and expansions in coverage have brought the D&O market to a crossroads.

The market has seen 14 years of generally soft conditions, providing buyers with favorable premium pricing and broad coverage enhancements. Over the last few quarters, however, we've seen a dramatic switch. Premium increases are now commonplace, and policy negotiations have become more difficult as insurers face pressure on primary, excess, and Side-A — or personal asset protection — differences in condition pricing.

With the risks for directors and officers constantly becoming more numerous and complex, insurance is more important than ever. It's vital to consult closely with your insurance and legal advisers to ensure the companies you serve have robust D&O insurance programs that protect both corporate and personal assets against these — and other — potential threats.

INDUSTRY DEEP DIVE

IS THE ENERGY SECTOR'S RISK MANAGEMENT KEEPING UP WITH THE PACE OF DIGITALIZATION?

Kevin Richards
Global Head,
Cyber Risk Consulting,
Marsh

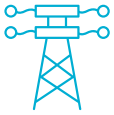
Expanding digitalization is a core characteristic of the energy sector's ongoing transformation. However, while enjoying all the benefits, the sector may not be adapting its risk management approaches quickly enough to manage the exposures and risks associated with the pace of digital change.

EXHIBIT 4: ENERGY SECTOR'S EXPANDING DIGITAL FOOTPRINT

Downstream companies use supply-demand matching smart grids and complex algorithms constantly adjust flows helping companies improve margins and identify necessary predictive maintenance

Oil and gas companies depend on data networks to track data from thousands of oil and gas wells and thousands of kilometers of pipelines, manage facilities, and interpret operating conditions

Upstream companies use digital technologies or reservoir modelling, drilling resource dispatching, production optimisation, and more



Electric transmission companies depend on automated controls to run their networks

Utilties rely on data networks to manage complex combinations of centralised grids and decentralised resources to analyse and efficiently meet customers' needs on a minute-by-minute basis

Source: Marsh and McLennan Companies

SPEED OF RESPONSE

Digitalization enables agile and responsive energy infrastructure, but the energy sector will need to likewise adopt dynamic resilience concepts to respond to evolving risks. A critical aspect of building resilience includes capacities for speed of response in the event of a cyber breach or digital breakdown.

The adoption of intelligent, sophisticated technology, including artificial intelligence for control and monitoring systems, is enabling new business models and more efficient asset management. New synergies are being realized by linking operational, information technology, and communication systems within organizations and across the energy supply chain. For example, oil and gas companies depend on data networks to track data from thousands of kilometers of pipelines, manage facilities and interpret operating conditions.

Utilities rely on vast data networks to manage complex combinations of centralized grids and decentralized resources to analyze and efficiently meet customers' needs on a minute-by-minute basis. In many aspects, digitalization increases the resilience of the energy sector as it enables the use of a complex and widening array of decentralized resources, improved efficiency and enhanced abilities to detect maintenance needs. Ultimately, this increases operational accessibility, productivity, sustainability and safety.

DIGITALIZATION IS CREATING NEW RISKS

At the same time, digitalization creates new cyber risk exposures, including business interruption, due to digital complexity. The energy sector's digital backbone is vulnerable to a range of failures. These can include non-malicious human errors or software failures in systems within the sector's increasingly complex supply chain or operations, insider threats from disgruntled employees, malicious external cyberattacks, and even the impact of space weather or geomagnetic storms.

Interconnectivity and complexity create vulnerabilities to malfunction or sabotage that can cascade across the energy sector and impact the broader economy. This was highlighted by the recent widespread blackout impacting approximately 48 million people in Argentina and Uruguay. The cause is still unknown, but the complexity of the system is such that "Just milliseconds had passed from the 'destabilization' of the grid to the power being

cut." Trains and subways were halted, traffic lights did not function and the water company's distribution system was compromised.

In the face of these challenges, the energy sector must build its dynamic resilience capabilities, as a new report from World Energy Council shows. An essential component of dynamic resilience is preparing for response to and recovery from events. For example, if a cyberattack occurs, an organization's ability to isolate the problem and then mitigate and restore normal activities promptly could define future business success.

NOT PREPARED FOR CYBERATTACKS?

However, survey data suggests the energy sector may be lagging in preparation for cyberattacks. A recent survey identified that respondents in the energy and power sector were relatively confident in their understanding of their cyber risk exposure, as well as preventing such attacks, but had less confidence about their ability to recover from cyber incidents. Preparation exercises may be particularly valuable in the energy sector, where experience and expertise in working in a digital ecosystem may be lagging.

Eight in 10 organizations in the energy sector, are not actively recruiting skills to support digital transformation, automation or AI. In general, the energy sector lacks sufficient skilled talent due to an aging workforce, workers who left the industry because of layoff fatigue and younger potential employees whose value propositions are more in line with those of tech firms and startups.

STRESS-TESTING THE RESILIENCY OF RECOVERY PLANNING

Exercises such as scenario planning and "gaming" workshops are essential to identifying specific vulnerabilities and understanding where the organization needs to improve cyber incident response plans and response capabilities as well its overall cyber risk management framework. Such exercises teach leaders how to manage through and after the attack to remediate damage. Cyber scenario exercises often identify vulnerabilities across a number of areas, including response implementation, response governance, and intra- and inter-sector coordination.

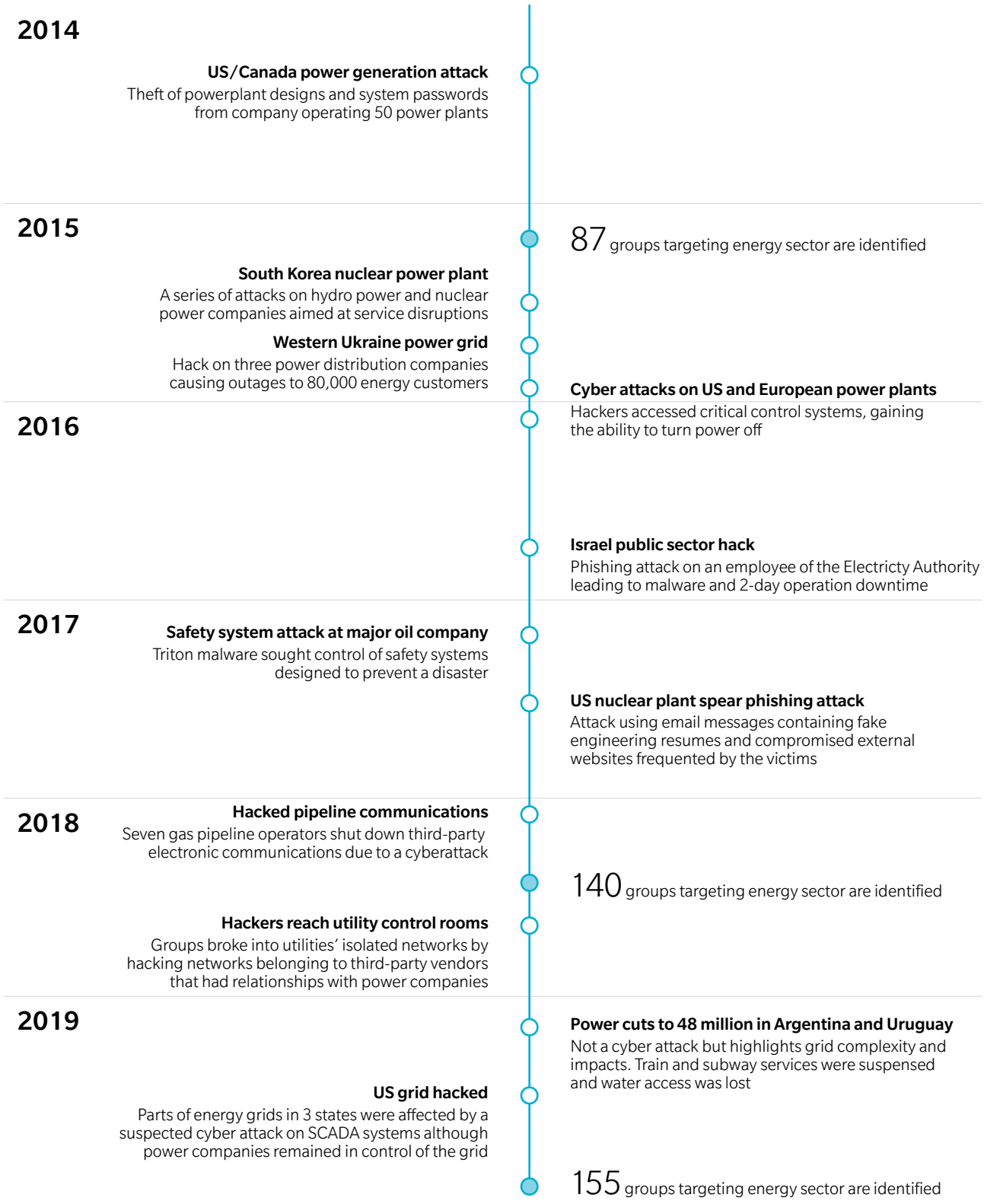
Digital disruptions or cyberattacks can impact communication capabilities vital to the implementation of standard response protocols. For example, a cyber response plan housed only on the corporate network may be of little use in a malicious ransomware attack that limits access to company networks and laptops — and along with that, vital technical information, telephone numbers and contact points. During the 2019 cyberattack on the aluminium maker Norsk Hydro, plants were able to continue production by relying on the knowledge of retired workers and paper manuals.

WHO IS THE DECISION-MAKER?

Gaming exercises also test the governance for decision-making during an event and whether there are clearly defined and pre-established roles, responsibilities and authorities at all levels of the organization to make necessary decisions. Responding to an event will be a shared responsibility of system operators, control engineers, information technology staff and cybersecurity professionals, as well as business leaders from an array of functions, such as government relations and customer service.

Organizations must consider which executive will be the decision-maker for critical decisions such as shutting down systems or determining when business systems can be restored. Will it be operational leaders such as the chief operating officer, the chief information officer or the chief information security officer? Who has the authority in a given unit or geography? What happens if a key executive is on vacation or medical leave?

EXHIBIT 5: CYBER INCIDENTS INCREASING IN BOTH FREQUENCY AND IMPACT



Source: Marsh and McLennan analysis

BUILD COALITIONS

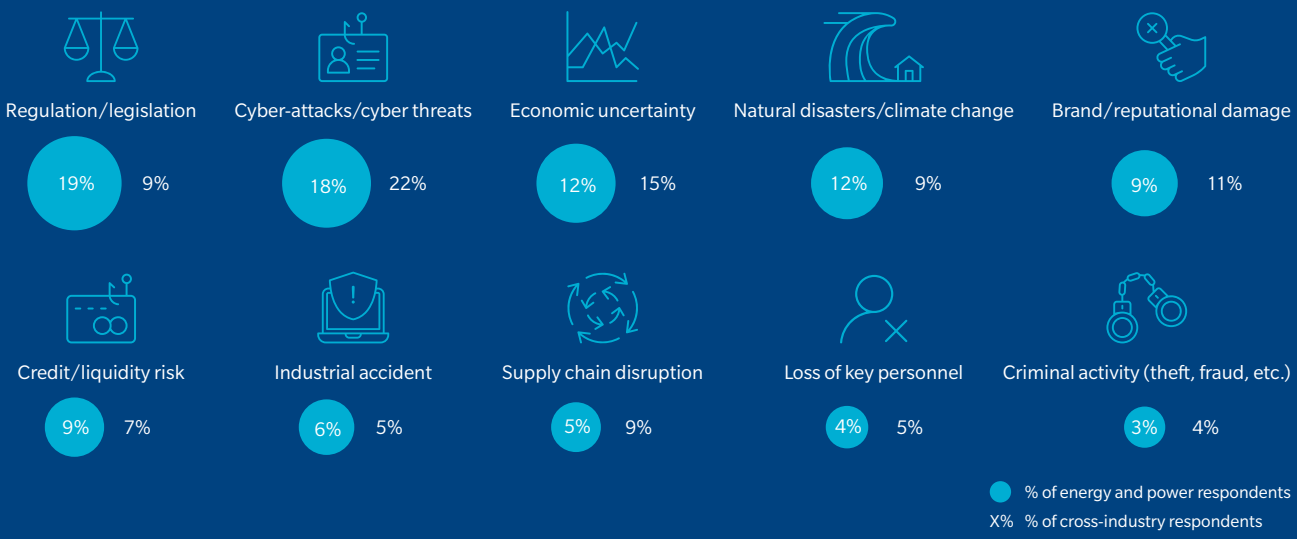
With highly networked supply chains, cultivating the right relationships is critical to building dynamic resilience. Coalitions with industry peers, regulators, industry associations, strategic partners and law enforcement are critical elements of baseline capabilities.

These coalitions can help to establish predefined channels and mechanisms to improve situational awareness during an attack and facilitate agility and speed of response. For example, in the U.S., the Cyber Mutual Assistance program provides a pool of utility cybersecurity experts who volunteer to share their expertise with other utilities in the event of a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency.

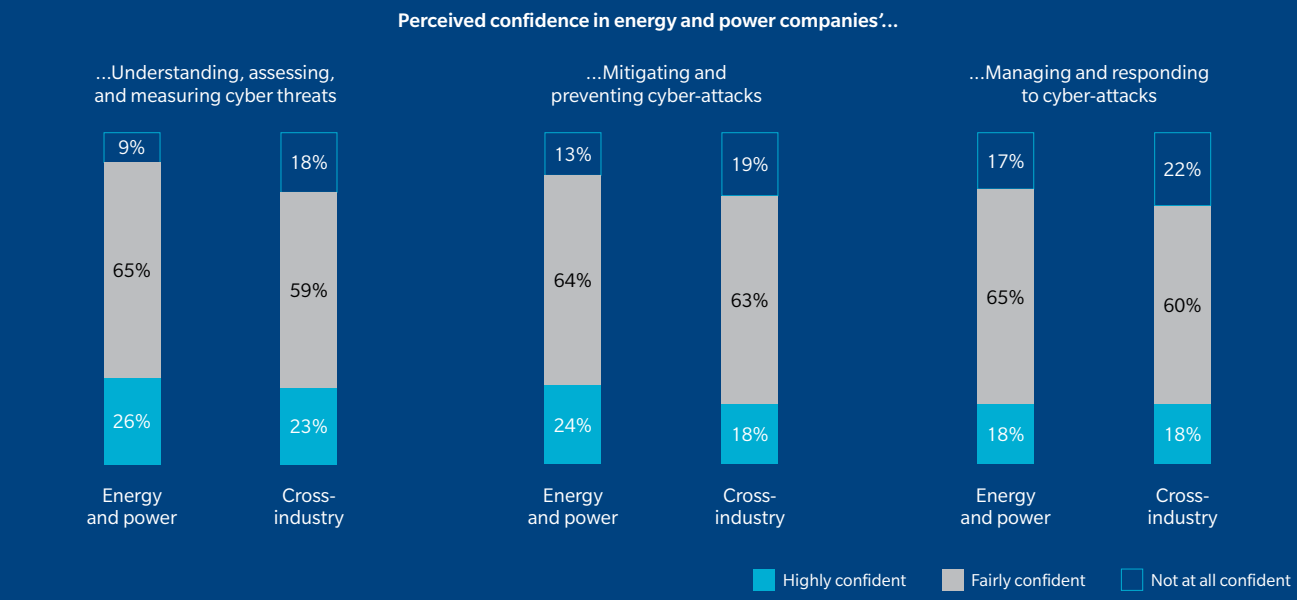
The 24/7 resilience of the digitized energy sector depends on the decisions and processes applied by countless individuals working throughout its supply chain. Exercises structured around risk scenarios can help leaders envision how they would handle different risk scenarios and manage through and after the event to remediate damage and build dynamic resilience.

Digital advancements across the energy sector will bring significant benefits: optimized assets, more efficient delivery and a more resilient ecosystem. Building and exercising response programs across the organizations within the ecosystem will help build the muscle memory to react at speed and at scale to remain truly resilient.

Biggest threats/concerns to energy/power organizations



Energy/power organizations' self-assessed ability to understand, prevent, and manage cyber-attacks



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2019, Marsh & McLennan Insights analysis

CYBER RESILIENCY

A CLEAR AND URGENT NECESSITY FOR MODERN RAILROADS

Paul Mee
Partner and Cyber Lead,
Oliver Wyman

Brian Prentice
Partner,
Oliver Wyman

Patrick Lortie
Partner & Rail Practice Leader,
Surface Transportation,
Oliver Wyman

The World Economic Forum's most recent Regional Risks of Doing Business report lists cyberattacks as the top concern of corporate executives in 19 countries, including advanced economies in North America, Europe, and Asia. These concerns, according to the report, "highlight the growing reliance of global commerce on digital networks that are the target of increasingly sophisticated and prolific attacks."

Many highly digitized industries and companies, having experienced these consequences firsthand, are incorporating cybersecurity into their cultures, while building advanced cyber defenses and resiliency programs. Rail and other industries with legacy infrastructure assets built long before the Internet age, however, appear to be lagging in terms of cyber resiliency, even as they increasingly rely on expanded digital systems and connectivity.

Globally, rail offers a relatively soft and highly tempting target for those looking to wreak havoc, as rail is often closely tied to a country's economic infrastructure and mobility. In the US and elsewhere, rail freight is used to move dangerous industrial goods, while passenger rail is a common mode of travel in many countries – including into densely populated urban cores.

The rail sector has witnessed its share of cyber events. While not crippling, they hint at the potential for damage. In 2008, a 14-year-old Polish boy modified a TV remote to change junction-box controls and derailed four trams in the city of Lodz, causing injuries to passengers. The UK rail network was attacked four times in 2015-2016 by hackers exploring its vulnerabilities, while Canada's Metrolinx thwarted a 2017 cyberattack originating in North Korea. Ransomware and DDoS (distributed denial of service) attacks have shut down systems ranging from scheduling and information to internal communications and ticket selling at the San Francisco Muni, Deutsche Bahn in Germany, and Danish train operator DSB.

RAIL'S CYBER RISK

There are as many as 300,000 hackers worldwide and that number is growing. Organized crime, hacktivists, and nation states are part of the mix and constantly innovating, meaning that the severity and frequency of attacks can be expected to increase.

Rail networks are particularly at risk because they are extensive, dispersed, and complex. Despite modernization, critical infrastructure is still made up of legacy components not originally designed and deployed with cyber resilience in mind. Transportation systems also are increasingly interconnected and no longer air-gapped (separated from the Internet). The continued introduction of new and connected technologies, such as IoT (Internet of Things) sensors and tools further widens the "surface area" vulnerable to cyberattack. The introduction of machine learning and artificial intelligence is expected to lead to even more potent and targeted cyberattacks in the future.

In the United States, the rollout of positive train control (PTC) on 65% of the rail network – which hauls 90% of rail freight – could be of notable interest to bad actors. PTC represents a new application of a complex web of technologies (GPS, wireless, cellular, radio communication, etc.), and have largely eliminated legacy signal systems that were air-gapped. PTC is designed to improve rail safety by preventing train collisions and derailments, yet its cyber vulnerabilities and security weaknesses might be easily exploited, thus creating new safety concerns.

Other liabilities include the use of open-source software and software with outdated security patches (which WannaCry exploited). In addition, railroads, like other asset-intensive industries, typically do not have a culture of cyber awareness, which makes their workforces vulnerable to social engineering (such as phishing) and the misuse of portable storage and other intrusion-enabling devices.

Finally, technology architectures typically comprise legacy components from third- and fourth-party providers, making vulnerabilities, often deep in the technology stack, difficult to discern and address. Hardware as well as software is exploitable; for example, the Chinese government reportedly infiltrated the

networks of major US corporations by inserting nearly undetectable microchips into computer servers built by Chinese companies. This has led to US lawmakers expressing concerns over state-owned China Railway Rolling Stock Corp. (CRRC) bidding on a contract to supply new rolling stock for the Washington Metro. In response, the Metro has tightened up cybersecurity requirements for the tender, but some doubt these go far enough.

CYBERATTACK CONSEQUENCES

The cyber risks for rail are many, including financial losses, compromised infrastructure, scheduling and communications breakdowns, theft of private data, safety liabilities, and reputational risk. In the EU, scheduling and information blackouts have shut down trains and stranded passengers, leading to lost revenues and network disruptions. The most serious concern, of course, is the physical safety of the rail network. PTC, digitally controllable locomotives and train components, and expanding wireless data streams all make the threat of a hacker-caused train collision or derailment real and plausible.

Beyond direct financial losses, post-attack recovery can be costly: When the world's largest shipping company, A.P. Moller-Maersk, was hit by ransomware in 2017 that disrupted operations at terminals in four countries for weeks, generating recovery costs of up to $300 million.

Concerns over the potential impacts of cyberattacks also raise the threat of additional regulation or shipper requirements that railroads guarantee the integrity of product and transportation data. Stricter cybersecurity laws may be in the offing for infrastructure considered critical to a country's economy and security. The EU, for example, has implemented a Network and Infrastructure Security directive to standardize cybersecurity protocols for "essential services," while the US in late 2018 created the Cybersecurity and Infrastructure Security Agency (CISA) as a new federal regulatory agency.

ENHANCING CYBER RESILIENCE

Cyber resilience – the ability to prepare for, react to, and move past a cyberattack – must be high on the agenda of rail executives and board members. Most critically, an organization's outlook in terms of preparedness for cyberattacks needs to be "when" – not "if." Railroads should assume a cyberattack will happen and develop a robust and responsive risk-management system. This starts with asking the right questions to fully understand the threat landscape and all the components of risk and response that must be developed and managed.

Effective cybersecurity begins by articulating a strategy in response to these questions, supported by an assessment of the company's current preparedness, appetite for risk, and quantification of economic exposure. A cyber operating model can be used to assign roles and responsibilities, while a cyber dashboard can monitor threat metrics and elevate discussion to the executive/board level. Finally, cyber playbooks need to be developed that step through how to handle major incidents, including accountabilities and response/recovery actions.

A valuable input to this process can be simulating various attacks on the organization, based on the threat landscape and prior attacks on other companies, to determine preparedness and resiliency. Working sessions with employees can uncover their knowledge about specific security weaknesses and gaps in oversight, controls, and access.

EXHIBIT 6: CYBERSECURITY QUESTIONS FOR RAILROADS (NOT EXHAUSTIVE)

Asset criticality

- Which assets are most important? To a specific railroad and its supply chain/ecosystem? To the sector? For service continuity/ safety in general?
- What are the principal assets that need to be preserved/protected?
  - Infrastructure/ communications
  - Digital services, instrumentation, and controls (hardware and software)
  - Data (e.g. sensor information, maintenance guides, logs, personal)

Threats

- Which assets are attractive to different threat actors? What bad outcomes might they be motivated to orchestrate or enact? How might they achieve this?
- What does the threat landscape look like for a specific railroad?

Preparedness

- What cyber-related policies and control frameworks should be in place?
- What governance arrangements are needed?
- What mechanisms will be used to detect an attack?

Response

- What playbooks are needed? How should these vary based on the assets under seige and the nature of the attack?
- How will communications and coordination be managed? For a specific railroad and across the sector? With third parties, customers, and the media? With law enforcement and government agencies?

Recovery

- Under what circumstances can an "all clear" be declared?
- What are the special considerations/controls needed for resumption?
- What are the arrangements or task force constructs for recovery and clean-up? (e.g. when data has been manipulated/destroyed)

Source: Holding Healthcare to Ransom: Industry perspectives on cyber risks. Marsh and McLennan Companies' Global Risk Center

Ultimately, a cyber risk assessment must include the following six themes to ensure effective cyber defenses and resiliency for a railroad:

- **Risk measurement:** Fully understand cyber risk exposure and the underlying drivers of losses
- **Risk management:** Ensure that cyber risk can be comprehensively managed across the organization
- **Response:** Be prepared to respond quickly and in a structured way to a cyberattack, to minimize stakeholder impact
- **Investment portfolio:** Evaluate investments across the cyber risk mitigation spectrum and relative to other investment demands
- **Executive oversight:** Continuously monitor cyber risk exposure status, trends/outlook, and the impact of investments
- **Insurance:** Determine cyber coverage strategy and the nature/extent of premiums

Railroads are complex, unique environments. Managing cyber risk and building appropriate defenses for railroads are not easy tasks, given the mix of legacy components that railroads have inherited and the advanced technologies they are embracing. But make no mistake: cyber resiliency is a clear and urgent necessity in today's digital world.

THE MARRIOTT DATA BREACH
LESSONS LEARNED FOR BOARDS

Paul Mee
Partner and Cyber Lead,
Oliver Wyman

Rico Brandenburg
Partner,
Oliver Wyman

Marriott International recently announced that it was the victim of one of the largest data breaches ever reported. Based on their disclosures, the private information of up to 500 million Marriott customers was stolen via a sustained compromise of the network that apparently started four years ago. Marriott has now joined the league of largest companies in the world having systems breached and customer information compromised, a peer group that includes Yahoo, Target, Facebook, Equifax, eBay, Sony, and Home Depot, among many others.[1] To put things in context, in the first half of 2018, a staggering 4.5 billion records were compromised worldwide.[2]

If you sit on the board of a company, or are part of the executive management team, this latest hack is yet another reminder that cyber risk needs to be at the top of your agenda. This data breach should lead you to ask some particularly hard questions about your company's cyber preparedness, and cyber risk appetite.

1 http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

2 https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx

IF THEY WANT TO, THEY WILL GET IN

Corporate networks are rife with legacy technology that was never designed with security in mind. In some cases, these legacy systems were a result of company mergers or acquisitions. Many business networks are flat, often consisting of thousands of applications and databases and file shares with limitations to access control mechanisms. This leaves sensitive data potentially exposed to adversaries once they are able to gain access and navigate the network.

And then there are your workers (employees, contractors, and other third parties), who can represent the weakest link in any cyber defense strategy as they can fall for phishing attacks, social engineering, and the temptation to 'go rogue' for monetary gain or as a form of revenge.

"Your cyber team needs to be successful 100% of the time. A hacker only needs to be successful once."

If you accept that a motivated hacker will find a way **around** your defenses, then your cyber strategy needs to be more than just protecting the perimeter — you need to develop an active defense culture. It also needs to focus on catching bad actors when they breach your walls, and if breached, how to identify and eradicate persistent presence prior to bad actor exfiltration. This includes identifying, segregating, and hardening your most valuable data assets or 'crown jewels', deploying advanced internal detection capabilities, integrating threat hunting as part of business as usual, and performing continuous Red Team[3] exercises to test your internal network identification and response capabilities.

THE MOTIVATION AND INTEREST OF HACKERS VARY

The goal of an attack is not always the direct monetization of valuable customer information. It can also include things like targeting the whereabouts of customers and staff for espionage purposes, understanding the business practices and IT architecture to launch subsequent attacks on the company, or manipulating information to cause reputational damage.

Organizations need to take a focused and robust approach to identifying non-public data assets that they hold which could be valuable if sold (e.g. ID scans, credit card data), or are valuable because of the information they contain (e.g. systems and network maps, travel records). Once identified, a corporation can make sure these assets are stored in a hardened state, make it increasingly more difficult to access them based on how sensitive the information is, and ensure the associated data is not moved from a more secure to a less secure format (e.g. extracted from a protected database to an Excel file and then emailed).

"A given corporation needs to ensure that its most valuable assets or 'crown jewels' are subject to the most hardened of defenses."

3 Red Team exercise: An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization (NIST Special Publication 800-53 Rev.).

It is also critical that you think like a hacker when performing an evaluation of the data assets your company holds and how attractive they might be. While a company may not immediately consider that travel plans would be valuable information, nation-state actors or criminal groups would certainly consider the check-in and check-out data for important people of interest and worth going after.

PLAN FOR A CYBER EVENT, THEN DRILL AND TEST

As we wrote a year back[4], the time to determine how to respond to a cyber event is not when it happens, but long before there is an actual event involving your company. GDPR requires businesses to report a cyber breach involving personal data in 72 hours. The SEC requires public companies who are listed in the US to report material cyber events in a timely fashion. While the SEC is not yet as prescriptive as in the European Union, anything that could impact shareholders needs to be reported quickly or the company could be accused of hiding information that would impact share price (Marriott's stock value was off over 7 percent directly following their announcement, a market cap reduction of over $2.7 billion dollars).

"It is crucial that cyber incident and crisis response plans consider all practical aspects and the associated decision making relevant to the situation."

Therefore, corporations should have cyber response plans and protocols in place that consider how management will respond, communicate (internally and externally), recover from and assess the impact of a large scale cyber-attack. It is crucial that the plans consider all practical aspects relevant in a given cyber response scenario (e.g. How do we contact customers with missing contact details? How do we handle capacity in the contact centers? What is the communication protocol of contact center staff?).

The board needs to ask management to rigorously review and challenge their cyber incident response plans to ensure they are comprehensive and well thought out. And don't forget you need to drill the organization on the plan, just writing it down is not enough.

FOCUS ON CRITICAL BUSINESS PROCESSES

Even if your company has thought through all of this, has the right insurance and reserves, and drills cyber events at least quarterly, it is likely you are missing a substantial amount of the cyber risk your organization faces.

Most organizations still take a relatively technically-centric view of cyber risk, considering their networks, infrastructure, databases, identity and access management (IAM), etc. But state of the art in cyber risk identification and risk management is to take a business view, rather than a technical view, and go step-by-step across your critical business processes to identify where cyber risk is introduced and how effective your controls are. By following the process steps that your people take to do their work, a significant amount of hidden cyber risk can be identified that cannot be found through other means.

4 Please see the 2017 Oliver Wyman report, "Practical Cyber Response: Being fully prepared for the inevitable."

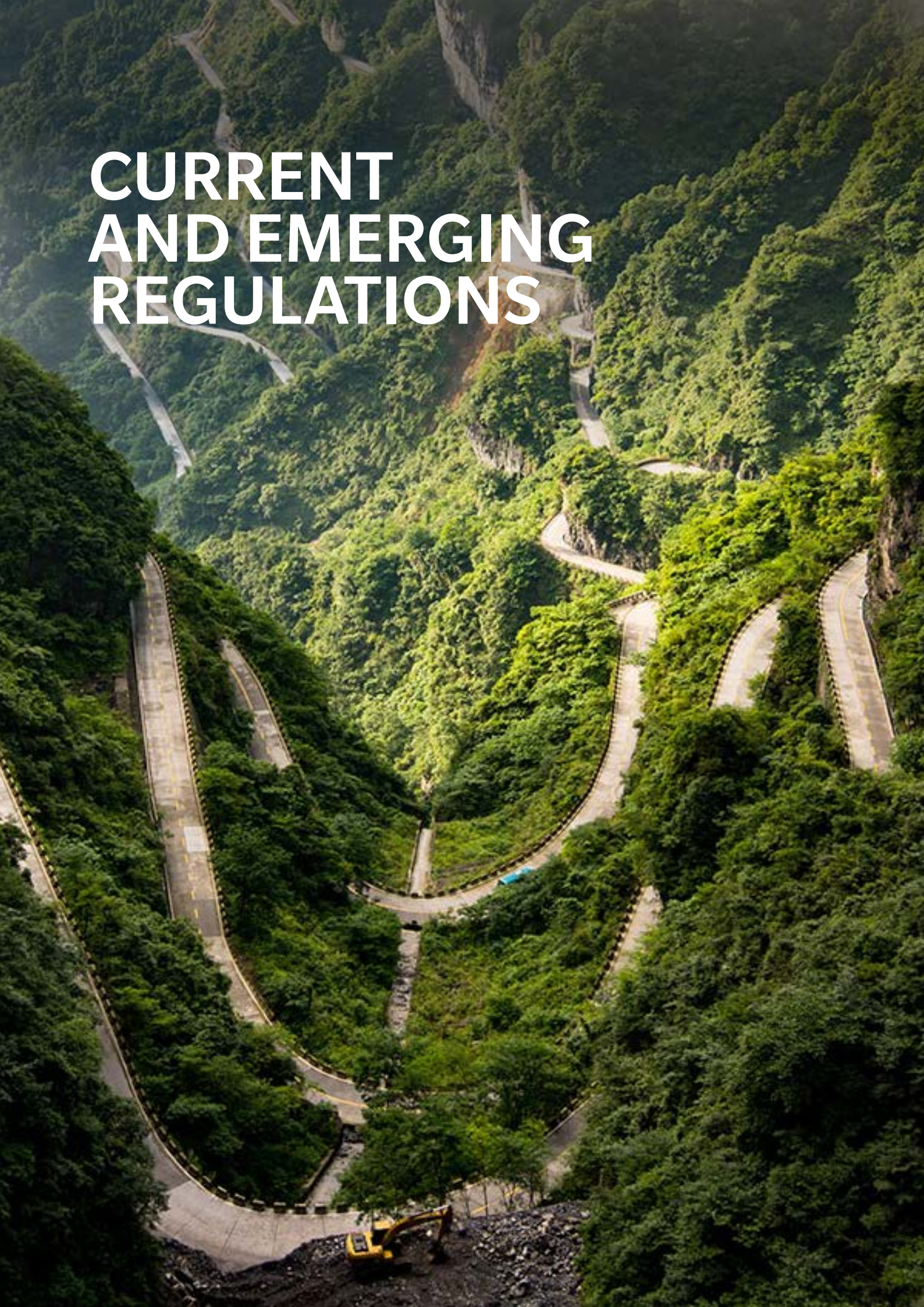
Making business decisions without considering the impact on an organization's cyber risk posture can have dire consequences. Many of organizations still prioritize speed-to-market over adequate security, without fully analyzing or understanding the impact of increased cyber risk to the enterprise.

YOU ARE NEVER DONE

The one thing that the never-ending announcements of data breaches should reinforce in every board and executive team is that no matter how much you have invested in your cyber risk management program, you are never done. New technical vulnerabilities are discovered every day, every business process change can create unintended process vulnerabilities, and every new worker in your organization is increasing the cyber risk exposure that needs to be managed.

We expect cyber risk to stay pinned on the agendas of board risk committees. The key is to not let your guard down, actively defend, and continue to challenge the organizations you are responsible for to think way out of the box — the bad guys certainly are.

CURRENT AND EMERGING REGULATIONS



Fewer than half of businesses globally regard government regulations or industry standards as being effective in improving cybersecurity.

Q: For each of the following pairs of statements, please indicate which choice most closely reflects your organization's views.

37%[1]

"**Soft industry standards** and guidance, such as NIST and ISO, are very effective in helping us **improve our cybersecurity posture.**"

- 29% <$100 million revenue
- 48% >$5 billion revenue
- 56% Financial institutions

28%[2]

"**Government regulation and laws** are very effective in helping us **improve our cybersecurity posture.**"

- 39% Communication and Technology
- 44% Financial institutions
- 44% Aviation

Organizations looking to government for help addressing nation-state cyber-attacks.

Q: For each of the following pairs of statements, please indicate which choice most closely reflects your organization's views.

54%[3]

"We are **highly concerned** about the potential harm that **nation-state cyber-attacks** could have on our organization."

- 60% Energy and power
- 69% >$5 billion revenue
- 71% Communication and Technology

55%[4]

"Governments **need to do more** to help protect private enterprise from **nation-state cyber-attacks**."

- 61% Board & C-suite
- 66% Financial institutions
- 69% Professional services

1. Base: all answering; n=822 (2019)
2. Base: all answering; n=828 (2019)
3. Base: all answering; n=825 (2019)
4. Base: all answering; n=821 (2019)

Source: Marsh Microsoft Global Cyber Risk Perception Survey 2019, Marsh & McLennan Insights analysis

IGNORE THE SEC'S STRENGTHENED STANCE ON CYBERSECURITY AT YOUR OWN PERIL

Robert A. Parisi, Jr.
Managing Director,
Network Security & Privacy Risk,
Marsh

Chris Hetner
Managing Director, Cyber Risk,
Marsh Risk Consulting

As recent events have shown, the pace and scale of cyberattacks continue to grow, as do the financial stakes — revenue losses, recovery expenses, liability costs, and potentially severe regulatory fines are all consequences facing companies. The specter of 2017's NotPetya event, the most devastating cyber event in history, continues to haunt business leaders: the malware caused more than $10 billion in economic damages and disrupted business operations, production, and logistics for major global firms. The insured losses from that attack alone have been estimated at more than $3 billion.

Incidents such as these are forcing companies to make cyber risk a corporate priority. In the recently released Global Risks Report 2019, those in advanced economies again rank cyberattacks among their top risk concerns. That recognition has evolved from viewing cyber risk as a problem to be solved by spending more on technology to seeing it as a risk that must be actively managed across many areas of the company. That shift in mindset has brought cyber insurance into the overall equation of how a firm manages its technology risk.

But cyber risk is an increasing concern not just for c-suites and boards: regulators also are more actively looking at how organizations address cyber risks and how they manage their responsibilities to key stakeholders. So even as the financial costs of cyber threats grow, the regulatory stakes are likewise poised to rise as more regulators — and particularly the US Securities and Exchange Commission (SEC) — begin to impose stricter requirements on businesses.

THE SEC STRENGTHENS ITS STANCE

Cybersecurity has been on the SEC's agenda for several years. In 2011, the commission's Division of Corporation Finance issued guidance calling on companies to assess their disclosure obligations regarding their cybersecurity risks and cyber incidents.

While a good starting point, the guidance did not go far enough in setting clear expectations for both proactive and reactive cyber-risk management and oversight. The SEC's 2018 interpretative guidance outlines requirements for publicly traded companies to disclose cybersecurity risks and material incidents.

The SEC guidance focuses on five main areas:

- **Pre-incident disclosure:** The guidance calls for transparency around the identification, quantification, and management of cyber risks by the C-suite and oversight by the board of directors. Often, growth in technology and the global operating environment impede 360-degree visibility into a company's vulnerable spots, with lack of data contributing to compromised security
- **Board oversight:** The board is expected to understand, quantify, and oversee cyber risk. The SEC advises companies to disclose in their proxy statement the board's role and engagement in cyber-risk oversight. Board members have to be privy to and understand the company's overall cybersecurity exposure, with a particular focus on the impact on the company's financial condition, integrating this insight into their 360-degree view of the company's risks
- **Incident disclosure:** Companies are required to "inform investors about material cybersecurity risks and incidents in a timely fashion." To do so, companies must have structures in place to identify and quantify cyber risk — tools that allow the organization to rapidly determine whether the impact of a compromised system was, in fact, material and requires disclosure to regulators and investors
- **Controls and procedures:** The guidance also tasks companies with assessing whether their enterprise risk management (ERM) process is sufficient to safeguard the organization from cyber disasters. This requires a step-by-step playbook for cyber events, including identifying who needs to be contacted and how and with whom the business will share information about a breach. Given the evolving nature of cyber risk, ongoing due diligence exercises should occur to identify and manage new risks — especially during a merger or acquisition

- **Insider trading:** New to the 2018 guidance is a reminder to companies, directors, officers, and other parties of insider trading prohibitions. In practice, this means that directors, officers, and other executives who are aware of a company's cyber vulnerabilities or a breach could be liable if they sell company stock, or instruct anyone else to do so, before such a breach or vulnerability is divulged

The cost of non-compliance can be substantial. Last year the SEC leveled a $35 million penalty against a large technology company it said misled investors when the company failed to disclose the theft of the personal data from hundreds of millions of user accounts.

Congress, which holds the SEC's purse strings, is placing mounting pressure on the agency to improve cybersecurity, and private investors are also pressing for more stringent cybersecurity controls at the companies they hold. It is, therefore, likely the SEC will start coming down on companies with more vigor, especially in the wake of recent — and, inevitably, future — major breaches.

RISK TRANSFER AS A CORE CYBER-RISK MANAGEMENT TOOL

Given the nature of the majority of risks, businesses recognize that technology and other solutions alone can't respond to the full spectrum of risks they face. Insurance has historically stepped in to provide the financial backstop for that residual risk that cannot be managed to zero through process, procedure, and mitigation.

Cyber risk is no different in this sense, and organizations are now recognizing that cyber risk also cannot be managed through technology alone. It is an operational risk that needs to be incorporated into the firm's overall ERM processes — one that includes risk transfer, as well as mitigation and resilience planning.

The insurance market now offers risk transfer solutions for cyber risk that address both ever-evolving technology risk and the recent retreat of traditional insurance products from adequately addressing firms' evolving cyber-risk profile. Cyber insurance starts with the premise that all of a firm's technology-driven risk should be insurable. These risks include both the direct loss that a firm can suffer in terms of lost revenue or assets, as well as the liability that can arise from a data breach or failure to comply with myriad new domestic and international regulations.

Cyber insurance has also been at the forefront of pushing for better understanding of this risk's financial implications to help the industry improve modeling of potential loss scenarios. That financial assessment is a critical foundation for businesses' risk management planning as well: Cyber-risk quantification helps the firm assess the economic impact of a range of cyber events, and on that basis, make informed investments in technology, insurance, and response resources. Quantification of cyber risk also allows for cyber risk to be analyzed within the firm's overall risk framework and integrated into its overall risk management planning.

The assessment, evaluation, and modeling processes that are essential foundations for purchasing cyber insurance are, in many ways, aligned with the practices called for by the SEC in its recent guidance. Given the likelihood of an increasingly active regulatory agenda, organizations are advised to align their policies and practices to abide by the SEC's recommendations and to consider insurance market coverage that can help protect against cyber event-related losses and regulatory liabilities.

THE ACDC ACT OPENS THE DOOR TO A HACK-BACK HIGHWAY TO HELL

Anne Toomey McKenna
Distinguished Scholar of Cyber Law & Policy, Penn State Dickinson Law and Institute for CyberScience

Due to the nature of cyberspace and the vast number of malicious cyberattacks, law enforcement is ill-equipped and understaffed to respond to, disrupt and prosecute most cybercrime. To address this, in the United States, the proposed Active Cyber Defense Certainty Act of 2019, (the ACDC Act), introduced by Rep. Tom Graves (R-Ga.), would allow private entities in the U.S. to "hack back" when their systems are being attacked, provided certain conditions are met. The idea sounds brilliant, but its initial sparkle hides some danger zones. As written, there are major problems with the act.

THE ACDC ACT'S KEY PROVISIONS

ACDC is designed to harness the power of the private sector to investigate, identify, defend and deter cyber hackers, although it requires companies who want to use ACDC's provisions to legally hack back against attackers to notify the FBI Cyber Investigative Joint Task Force and receive acknowledgment of notification before hacking back.

According to Rep. Graves, ACDC's key provisions would permit these "authorized" companies to "leave their network" (a euphemism for accessing an attacker's systems without authorization) and

- Establish attribution (identify the attacker)
- Disrupt or stop the cyberattack without damaging other computers along the way
- Retrieve the victims' stolen files or destroy the files on the attacker's system
- "Monitor the behavior of an attacker"
- Use beaconing technology

These actions are described as Active Cyber Defense Measures (ACDMs) — and make for a strong, proactive policy. But there are some major problems lurking in the language.

Not only is the language of the act vague and confusing, but it also creates dangerously murky areas around when and what cyber-defense activities are appropriate. This vagueness and murkiness will not work to the benefit of authorized companies. Instead, they can spell significant economic and legal exposure.

The congressional findings in ACDC admonish hacked businesses to: First, report the cybercrime to law enforcement and second, improve defensive measures. Many information security officers would reasonably disagree with that order of priority when their companies' systems are under malicious cyberattack.

WHO CAN HACK BACK, AND WHEN?

The act defines a "defender" as a person or entity who is a victim of a persistent unauthorized intrusion of the defender's computer. One might reasonably ask: When is an intrusion persistent? Do two system access events without authorization qualify as persistent? Does persistent refer to how long an intruder remains within a defender's systems, or how many times an intruder has breached a system? Unfortunately, the proposed legislation fails to define what constitutes a persistent intrusion. This creates a big gray area for companies and courts.

Moreover, only after notifying the FBI and receiving acknowledgment from the FBI of the notification does the act permit qualified defenders to use ACDMs. In sum, hacking back is permitted only when the FBI is onboard and when the victim/defender has a high degree of confidence about who the attacker is. To help with achieving a high degree of confidence in attribution, ACDC would legalize the use of beacon technology.

Beacons are programs, codes or commands embedded in files that signal back to the defender's systems when a file embedded with the beacon is removed without authorization from the defender's systems. This allows the defender to track down the path and location of the beacon (and hence the stolen file), providing potentially stronger evidence of attribution if the beacon is discovered in another entity's systems.

This part of the act is very helpful, because some argue — incorrectly — that the use of beacon technology is unlawful, as it is unauthorized access into another system. The act provides clarification on this point, without which companies would be reluctant to use the technology.

WHAT CAN BE DONE DURING A HACK BACK?

The act permits qualified defenders to use ACDMs to combat cybercrime, but it defers to the Department of Justice on defining details about which ACDMs are lawful and appropriate. It charges the DOJ "to clarify the proper protocols for entities who are engaged in" ACDMs.

To its credit, the act does specify some things that can't be done: It prohibits defenders from destroying data on the attacker's computer system (unless it's the defender's own files), impairing the operation of the attacker's computer systems, or creating a backdoor into the attacker's systems. However, it also lacks any protocols or technical guidelines for what can be done.

> "ACDC, with its vague language, will create a sea of litigation and hack-back hell, all without any demonstrable benefit."

LIABILITY FOR HACK BACK

It is critical for companies to understand that although ACDC would modify existing U.S. computer crime legislation to decriminalize ACDMs, the act does not provide any protection whatsoever from civil lawsuits for defender activities under the act. It also potentially leaves open a swath of state computer crime laws that criminalize hack-back type activities.

Moreover, ACDC places the burden on the system defender to avoid violating laws of other nations. It should come as no surprise that many other nations besides the U.S. outlaw hacking back against an attacker. Under ACDC, companies are civilly liable for their actions, and that's a costly proposition when there is such a lack of clarity in the proposed bill.

TOO MANY QUESTIONS RAISED BY HACKING BACK

Section 5 of ACDC requires any defender to notify the FBI and to receive back from the FBI an acknowledgment of the notification before using an ACDM. This creates a legal quagmire. When a company acts at the direction of law enforcement to investigate a suspected criminal, they can become an agent of the government for Fourth Amendment purposes. The FBI would typically need a warrant to enter an alleged attacker's systems and hang out in the system monitoring the behavior. Thus, ACDM arguably creates a sidestep to normal legal processes; this is fraught with peril for both law enforcement and the defender.

In addition, what if the attacker is a nation-state or an agent of a nation-state? Is the ACDM permitting defender companies under FBI oversight to engage in acts of retribution under international norms and the laws of armed conflict? Think back to the Sony hack, allegedly perpetrated by North Korea. Hypothetically, if the FBI were to consent to and oversee Sony's use of ACDMs against North Korea, what would the international implications be?

MAKING A MESS OF EXISTING LEGISLATION

In the U.S., our primary federal "hacking" law is the Computer Fraud and Abuse Act, (CFAA), which prohibits accessing any "protected computer" (defined as any computer attached to the internet) without authorization (this usually means an outside hacker) or in excess of authorization (usually an inside hacker).

The CFAA clearly makes hacking back unlawful — and in addition to its criminal penalties, the CFAA also permits individuals to bring a private cause of action against anyone who violates the CFAA's prohibitions. The CFAA's private cause of action generates a significant amount of civil litigation, and verdicts in CFAA cases can be substantial. The CFAA's long litigation history and amendments over the years have created a strong law that is clearly understood by the private sector.

We all want and benefit from certainty in our laws and legal system. ACDC, with its vague language, lack of clear protocols and weakening of key CFAA provisions will create a sea of litigation and hack-back hell, all without any demonstrable benefit — except for the FBI potentially gaining more knowledge of vulnerabilities and oversight of hack backs.

Debate will continue to swirl around the passage of ACDC — as it should. Perhaps we should be grateful that at the moment, govtrack.us only gives the ACDC a 5% chance of being enacted into law.

THE US IS LEAVING DATA PRIVACY TO THE STATES — AND THAT'S A PROBLEM

Carsten Rhod Gregersen
CEO and Founder,
Nabto

One year in, the impact of the General Data Protection Regulation (GDPR) has been widespread. Europe's new data protection laws have resulted in 281,000 breaches and 55 million euros ($61 million) in fines to some of the world's biggest tech companies over the mishandling of personal information. Furthermore, the legislation has drawn a line in the sand as to what companies can and cannot do when it comes to sensitive user data.

While GDPR has somewhat clarified the murky rules surrounding consumer data in Europe, the same cannot be said in the United States. Legislation in the U.S. varies from state to state, rather than having unified standards from country to country. As states like California and New York begin to legislate for consumer data rights, the risk of differing rules could result in weaker federal data laws.

Why? Because a patchwork of protections legislated at the state level makes for an uneven and confusing legal environment. Without a formal federal position, differing state rules could translate into privacy that is complex and onerous for any company.

CALIFORNIA MAKES THE FIRST MOVE

No movement on the federal front means U.S. states must take privacy protection into their own hands, and California is the first to take a stand. The California Consumer Privacy Act comes into effect in 2020 and grants consumers insight into and control over their personal information collected online.

As reported by Wired, the sweeping law gives Californian residents the ability to request the data that businesses collect on them, demand that it be deleted and opt out of having that data sold to third parties. Tech companies are clearly worried about the changes and have lobbied hard for their watering down — with legislative bodies, backed by major tech bodies, advancing a series of changes in April that would offer exemptions for certain categories of businesses.

The law will ultimately result in strict control of consumer data use from corporate entities, as well as major fines for tech companies that do not comply. Fines will total $7,500 per violation and $750 for each record compromised — which could add up to a considerable sum for smaller business. Major corporations have already begun to prepare for the incoming rules, but smaller online businesses could be hit hard if they are not ready when the laws come into effect.

NEW YORK FOLLOWS WITH A TOUGH APPROACH

The Californian overhaul has been praised by privacy advocates for its hardline stance on the issue — though the law has since been overshadowed by the even tougher stance made by the state of New York. The New York Privacy Act entered the state senate last month and, if approved, would grant the strictest controls over personal data in the U.S.

This bill shares similarities with the Californian law in that the user can better understand who holds what data and request that any such information be deleted or corrected. However, the East Coast approach would give New Yorkers the right to sue companies directly over privacy violations. On the West Coast, this element of law enforcement is left to the state's office and only applies to businesses that gross more than $25 million annually. New York's act would allow for personal litigation against any company of any size — something that could hold major repercussions for those who do not play by the rules.

Perhaps unsurprisingly, privacy proponents have praised the bill, while tech representatives have all but trashed it. A director for the Internet Association, which represents the likes of Facebook, Google, Amazon and Microsoft, has called the act "unworkable" and questioned whether the legislation actually provides "meaningful control" over personal data.

The reactions mirror those of the Californian law rollout, and one can only predict that similar battles on either side of the debate will continue to play out, while there remains no formal federal position. It begs the question, where is privacy protection headed on a national scale?

"The U.S. needs federal oversight because competing data laws will only result in weaker laws across the board."

OTHER STATES ARE FOLLOWING SUIT

Since the federal government currently has no position on privacy protections, it seems that state-by-state legislature will continue to be the way forward for the time being. Maine and Nevada already have consumer privacy protections signed into law. While both pale in comparison to the protections presented by California and New York, they are a start. The citizens of Maine, under the Act to Protect the Privacy of Online Consumer Information, are protected from broadband providers using, selling, distributing or permitting access to customer personal information for purposes other than providing services. Meanwhile, Nevada's Senate Bill 220 amends the state's existing law to require websites and online services to post privacy notices to users regarding access to their information.

Other states seem to be following similar paths — though none are as strong as the protections put forward by California or New York. Maryland's Online Consumer Protection Act, if passed, would force companies to demand access to user data and disclose when user data is being collected and what user data is being sold.

Texas has decided to revise its provisions relating to security breaches by creating the Texas Privacy Protection Advisory Council. North Dakota, similarly, has chosen to provide a legislative management study of consumer personal data disclosures.

THE PROBLEMS INHERENT IN A STATE-BY-STATE APPROACH

First, differing governmental battlegrounds make for higher susceptibility to corporate lobbying. Lobby groups have already played a big part in the legislature push in California and New York, so one can only imagine smaller, less affluent states being prime targets for big tech lobbyists.

Second, a patchwork of protections legislated at the state level makes for an uneven and confusing legal environment. Different rules in Nebraska from Idaho could translate into privacy that is complex and onerous for any company. Again, this would be to the detriment of smaller companies without the resources nor legalese to operate across differing privacy expectations.

Third, the right to privacy is fundamental for many. Protecting privacy on state lines will only make for uneven rules that are more difficult to enforce. Further, they will simply be more difficult to understand for both consumers and companies. As evidenced by the GDPR, one rule for one region works.

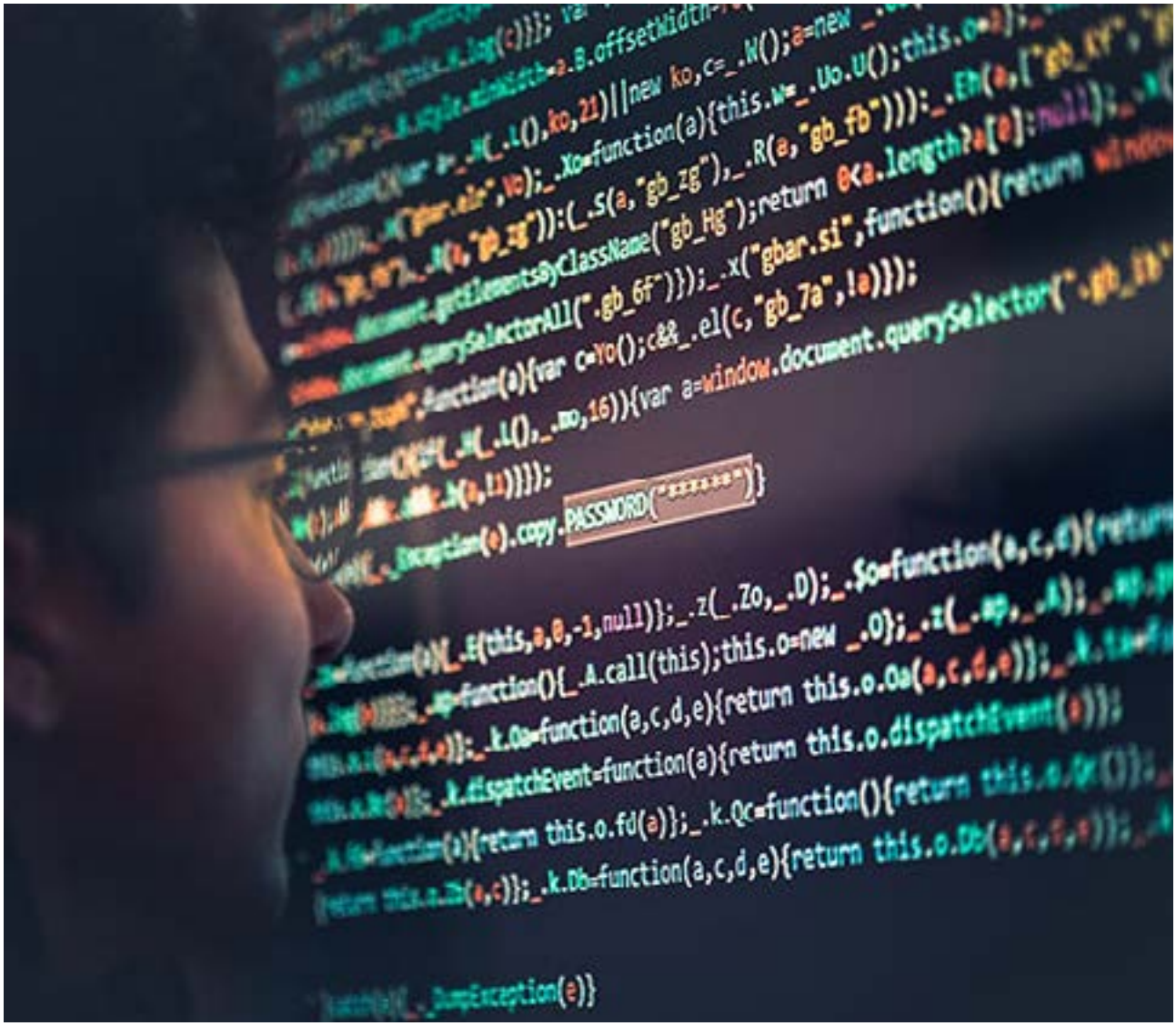
THE NEED FOR FEDERAL OVERSIGHT

The U.S. needs federal oversight on something as important as citizen digital privacy to ensure one standard for many — competing data laws will only result in weaker laws across the board. This is an issue that will only grow in importance as internet-of-things devices continue to take over our homes and our lives in the coming years. These devices, which often use susceptible connections between the server and receiver, have the potential to reveal sensitive details of unsuspecting users. This should be especially concerning when many of these devices have the ability to collect countless data points through microphones, cameras and sensors.

California and New York have created two sets of laws, which, by and large, do protect user privacy. In the absence of federal oversight, both states have acted to ensure the rights of their respective citizens. However, this does not detract from the need for federal action on this issue. Fifty different approaches to privacy will not improve upon one strong, national standard — the future of the nation's citizens depends on it.

CYBER RESILIENCE STRATEGY

CYBER RESILIENCE IS THE FUTURE OF CYBERSECURITY



Jaclyn Yeo
Research Manager,
Marsh & McLennan Insights

Rob van der Ende
VP, Mandiant APJ,
FireEye

In the corporate world, the rise of cyber attacks is far outpacing the level of investment in protection from cyber threats: There has been a 33% increase in the cost of cybercrimes since 2016, but investments in cybersecurity lag behind, having only increased by 10%.

Digital adoption and technological innovation are allowing businesses to reach more people than ever before. However, the wider these digital nets are cast, the more opportunities cyber threat actors have to infiltrate and exploit company systems and data, while businesses and staff often do not have the adequate combination of knowledge and tools to respond to these threats.

A recent report by Marsh & McLennan Insights and FireEye, an intelligence-led security company, addresses the need for organizations to prioritize cyber resilience over traditional cybersecurity and defense approaches.

MOST SECURITY BREACHES COME FROM EMAIL

The most vulnerable part of a company's cybersecurity is its employees. Today, social engineering is recognized as one of the greatest security threats facing organizations, where more than 90% of cyber incidents are a result of 'human-enabled' network compromises.

Cyber threat actors rely on them to click links or open files that release malware into the system. Threat actors also assume false identities in conversation with company employees to collect sensitive data in the process. 93% of cyber breaches are due to phishing and pretexting, with email being the most common entry point at 96%.

According to the report, "more than 90% of cyber incidents are caused by social engineering techniques," which rely on "human interaction to gain trust and manipulate[s] people into breaking standard security practices."

Protection from these incidents can start with everyone at the company, regardless of department. If all staff are educated on how to identify phishing emails and verify supposed company partners, they could be the most effective defense against cyber breaches. However, a study on evidence-based malware cybersecurity training for employees shows that awareness of cyber risks alone is not sufficient to change employee behavior. The study states that another motivating factor for employees to take preventive action is an awareness of their own personal risk that goes along with being involved in a cybersecurity breach or attack.

EXHIBIT 7: CYBER ATTACK VECTORS

96%

Email continues to be the most common vector at 96%

90%

Phishing accounts for more than 90% of successful attacks

Source: Advancing Cyber Risk Management: From Security to Resilience, FireEye and Marsh & McLennan Insights

The other imperative element of a cyber risk strategy, especially in terms of resiliency, is cyber risk insurance.

CYBER INSURANCE OUTPACING ALL OTHER INSURANCE

Due to an expanding market for cyber insurance, premiums are growing "three times faster than the general property-casualty insurance market," according to the report. They are expected to increase at "a compounded annual growth rate of 20.1%, between 2014 and 2020."

EXHIBIT 8: ESTIMATED VALUE OF CYBER INSURANCE PREMIUMS WRITTEN GLOBALLY FROM 2014 TO 2020

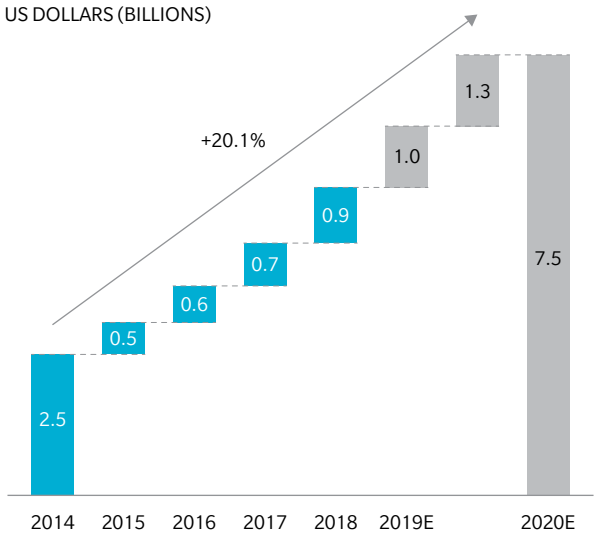
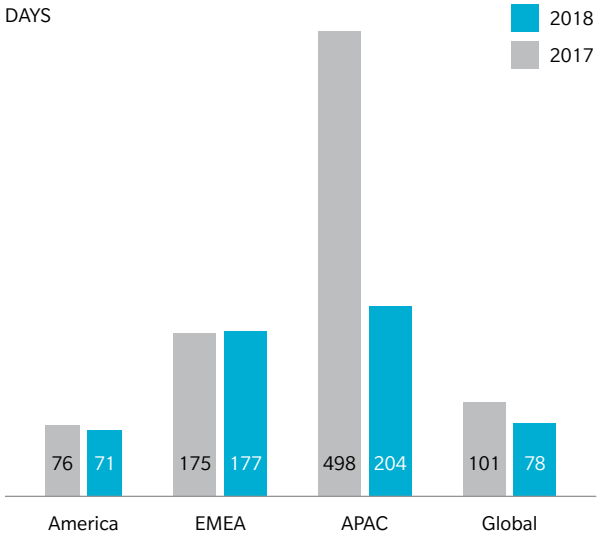
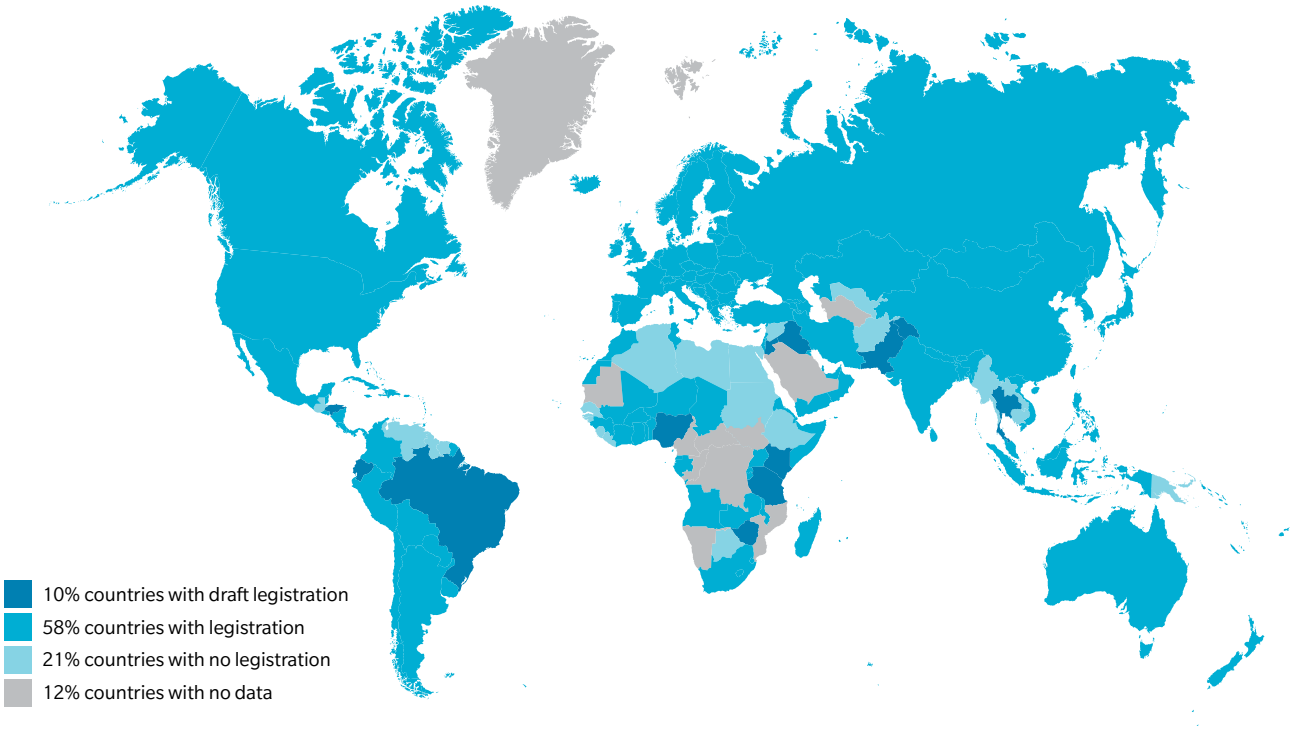


EXHIBIT 9: 2018 MEDIAN DWELL TIMES COMPARISON





Source: Advancing Cyber Risk Management: From Security to Resilience, FireEye and Marsh & McLennan Insights

The high cost of cyber insurance premiums is due in part to having a high risk exposure, but insurers' lack of visibility into company risk profiles also drives up the cost of premiums. Thus, in addition to safeguarding your systems and data, a cybersecurity and resilience strategy — made transparent to the insurer — may lower cyber insurance premiums.

Cyber risk insurance can hasten the response and recover from risk incidents involving anything from data restoration, data breach fines and payment to PR firms for handling post-breach communications. Some insurers will even cover social engineering fraud.

Insurance cost is also affected by policy. The World Economic Forum's report on cyber resilience notes that cyber insurance can be voluntary, incentivized or mandated, with financial trade offs for each option. With voluntary insurance, the upfront costs for insurers are lower due to a lack of security controls, but over time, the cost would be too great to maintain; with mandated insurance, companies would pay more up front for a more sustainable cost structure in the long term, accompanied by security controls on the cost of insurance.

A DROP IN DWELL TIMES

Despite the global lag in investing in cybersecurity, there are some encouraging trends, especially in dwell time, which is "the number of days an attacker is present on a victim network, from first evidence of compromise to detection."

In 2018, dwell time decreased by 23 days to 78 globally compared to 2017. Asia-Pacific still has the highest dwell time at 204 days, but since 2017, its dwell time has plummeted to 204 from 498, decreasing by 294 days in one year.

There are other positive trends in data security policy being implemented across the globe, especially following the implementation of the General Data Protection Regulation (GDPR) enforced by the European Union (EU).

Regulators in other parts of the world have also become more transparent about their growing cyber threats and malicious data breaches in response to the GDPR, to more accurately reflect the cyber threat levels in their respective jurisdictions. Sixty-eight percent of countries have either implemented data protection policies or have drafted legislation to do so.

CLOSING THE GAP

The mission in cybersecurity is not necessarily to wholly avoid breaches and attacks, but to know how to respond intelligently and systematically when they happen — because it's likely they will. There are three steps to strengthening cyber resilience: 1) understanding business vulnerabilities, 2) understanding the level of risk that can be absorbed and 3) understanding tools and strategies for cyber threat protection.

In addition to focusing time and investments on strategic reactions, knowledge and tools to cyber breaches and attacks, considering a company's entire staff as the first line of defense can strengthen cyber resilience considerably. The outlook, attitudes, values, moral goals and legacy systems shared within the company will have a direct impact on how cyber threats are perceived and managed. Cybersecurity will involve many different hard skills and technical solutions, but resilience cannot be fully achieved without the right mindset.

With this approach, the global level of investment in cybersecurity may begin to increase at least at the same rate as the climbing costs of cybercrime.

CYBER RESILIENCE STRATEGY

NAVIGATING CYBER RISK QUANTIFICATION THROUGH A SCENARIO-BASED APPROACH

Tanishq Goyal
Engagement Manager,
Oliver Wyman

Jayant Raman
Partner, Finance & Risk Practice,
Oliver Wyman

Despite the increasing importance of cyber risk agenda within organizations, very few have a comprehensive understanding of their cyber risk exposure. It is also challenging to quantify cyber risk exposure with limited historical data available. However, quantification is all about probability and is meant to provide a directional view around the level of risk an organization should be prepared to manage, rather than a definitive answer that provides an accurate measure.

Quantification of cyber risk would help organizations to:

- Uncover various implications from a financial standpoint
- Get clearer understanding of organization's probable cyber exposure and its impact
- Enable informed discussion around transfer of risk through insurance
- Catalyze an increased awareness beyond IT to the rest of the organization
- Inform educated investment in reducing overall cyber exposure

However, many challenges arise in quantifying cyber risk, such as:

- Constantly changing landscape of attack as hackers become more advanced and unpredictable
- Organizations typically lack a formally defined risk appetite that drives business decision and strategy around risk management
- Limited historical data and scarcity of detailed publicly available information on cost of cyber attacks making it difficult to model cyber risk
- Cyber risk management not fully integrated into Enterprise Risk Management, increasing overall barrier and visibility to CXOs. Potential misplaced focus on prioritizing protection of IT assets over business assets

NARRATING REALISTIC SCENARIOS

Quantification becomes challenging in the absence of clarity. Therefore, the more specific we can be in the scenario narratives, the easier it is to guide the conversations on estimation. In order to be able to narrate a scenario that clearly articulates the cause, event and impact towards the organization's operations, a few common pitfalls should be avoided:

- **Boiling the ocean with granular scenarios:** Do not boil the ocean with many different scenarios without priorization and alignment. Instead, agree on the top 3-5 scenarios that align most with your assessment criteria and focus on those
- **Baselining against too many data points:** Narrating scenarios at 2 levels of severity: e.g. Material (1-in-2 years) and Extreme (1-in-30 years), is sufficient
- **Misalignment of narrative and the organization's risk controls:** Reflect your understanding of the organization in your narratives to avoid lengthy debate and a lack of trust in the quantification
- **Falling into the trap of data availability/ unavailability:** There is a fine line between using historical data as a baseline and falling into its trap because of changes in processes and enhancements in security over time, making historical data directionally relevant, at best
- **Enabling potential biases to influence perceptions:** In order to avoid this, be aware of stakeholders' biases and take mitigating actions (e.g. benchmarking information, playing devil's advocate, and engaging relevant subject matter experts)

QUANTIFYING SCENARIOS

Once a specific narrative is in place, relevant stakeholders from different teams and departments need to be engaged to help analyze the scenario response actions and the estimated cost drivers for both material and extreme attacks. Depending on the maturity of the organization's risk appetite and scenario response management, this may require several iterations before arriving at an estimate.

To assist stakeholders from different business units to analyze the scenario response actions and estimated costs, we recommend using the following as a benchmark to kickstart discussions.

DATA FROM PREVIOUS SCENARIOS (CYBER OR NON-CYBER) WITHIN THE ORGANIZATION

- To extrapolate costs incurred in marketing campaigns, hiring of legal counsel, system enhancements, public relations (PR), etc.
- To identify scale and volume of impact based on the number of impacted customers, number of vendors, number of transactions, backup restoration, service-level agreement (SLA), etc.

CYBER ATTACKS ON OTHER ORGANIZATIONS

- To determine a potential scenario response plan in brand-building, system enhancement cost, PR and notification, etc.
- To ensure estimates are reflective of the current external threat landscape

While benchmark figures can be used to steer stakeholder conversations in the right direction, it is critical that these figures are not applied as-is. This is because some of the data may be masked by underlying lack of disclosures, as benchmarks from different organizations may not reflect the same level of security controls, governance, and processes with others and organization's data from past scenarios may no longer be reflective of its current risk profile.

The development of these narratives and estimates would require stakeholders to conceptualize the possibilities. Therefore, ensuring that stakeholders internalize and are comfortable with this concept would be the greatest success factor in quantifying cyber risk.

THE SO-WHAT OF MODELING CYBER EXPOSURE

Individual scenarios give us the loss exposure for individual scenarios – which can be correlated to one another – arriving at a single Value-at-Risk (VaR) number.[3] This single VaR number can be useful as a measure of probable cyber risk exposure for the organization. However, the approach for deriving the VaR number is considered to be quite theoretical and there are several assumptions made to derive the final VaR number – making it much less tangible than loss exposure for individual scenarios. As a result, most organizations focus on quantification exercise for the benefit of understanding the exposure in specific cyber scenarios. With the information of individual loss exposures in hand, the organization can make an informed decision around the level of "protection" confidence that the organization would desire and the resulting strategic risk decisions to help reduce exposure. Possible decision-making insights include:

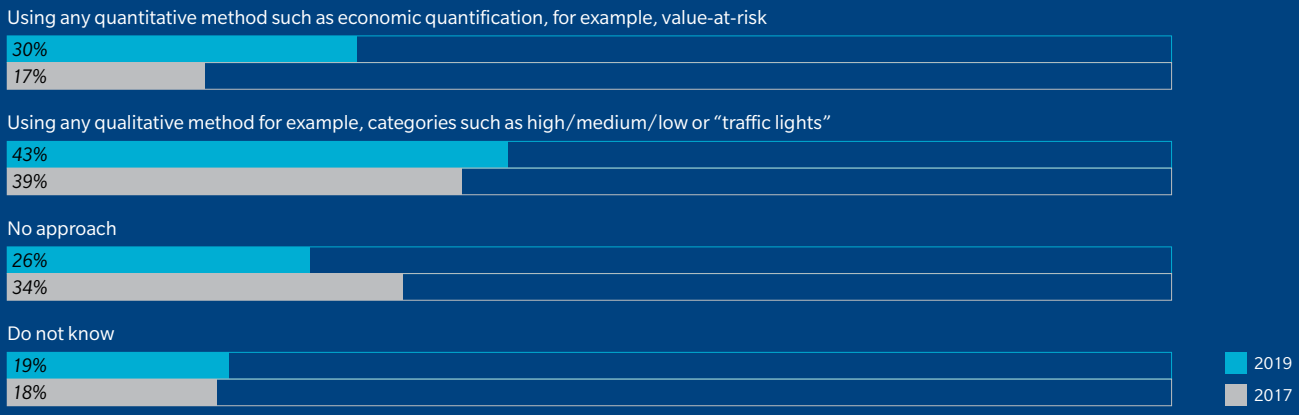
- **Strategy for cyber insurance:** The process of cyber risk quantification can help organizations identify the most significant areas of exposure and the amount of protection required to help define a thorough strategy for the protection.
- **Prioritization of cybersecurity investments:** Using the quantification approach and estimating impact on loss exposures to drive prioritization is a transparent way of prioritizing budget for all stakeholders.
- **Ongoing monitoring of cyber readiness:** Ongoing monitoring of the loss exposure number can give senior management and the Board insights into the cyber readiness of the organization and help identify areas requiring further attention

As high-profile cyber incidents impacting well-known names across different industries are increasingly making headlines, cyber risk is not solely an IT-related issue. By quantifying cyber risk, we open informed discussions throughout the organization – on how and what the organization can do to increase its cyber resilience and build capabilities. Ultimately, this will help the organization realize that the fight to protect against cyber attacks is not an IT or Risk function responsibility, but one for the whole organization.

3 Value-at-Risk (VaR) is a measure of potential risk. In the context of cyber risk, VaR indicates potential loss that could be incurred in the event of an actual cyber attack

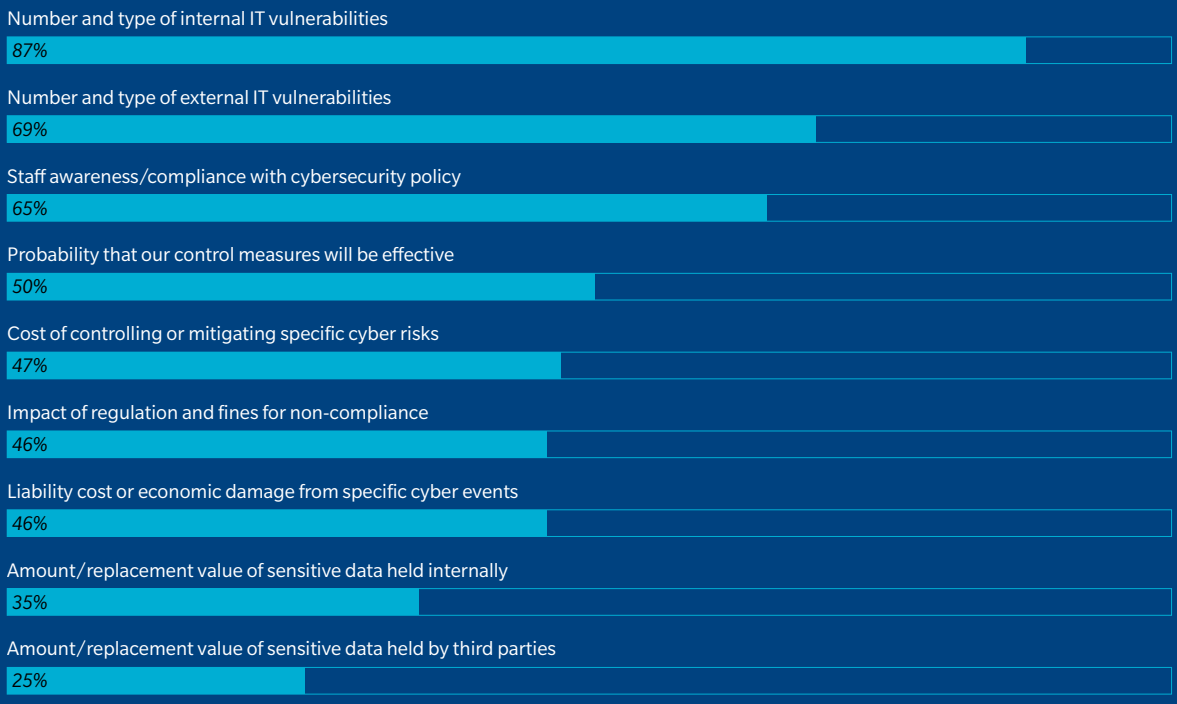
Quantitative measurement of cyber risk exposure has increased substantially since 2017, but remains low overall.[1]

Q: In general, how does your organization measure or express its cyber risk exposure?



Risk assessment methods focus on counting technical vulnerabilities, but fail to adequately consider economic aspects of cyber exposure.[2]

Q: Which of the following does your organization consider in its cyber risks assessment/measurement?

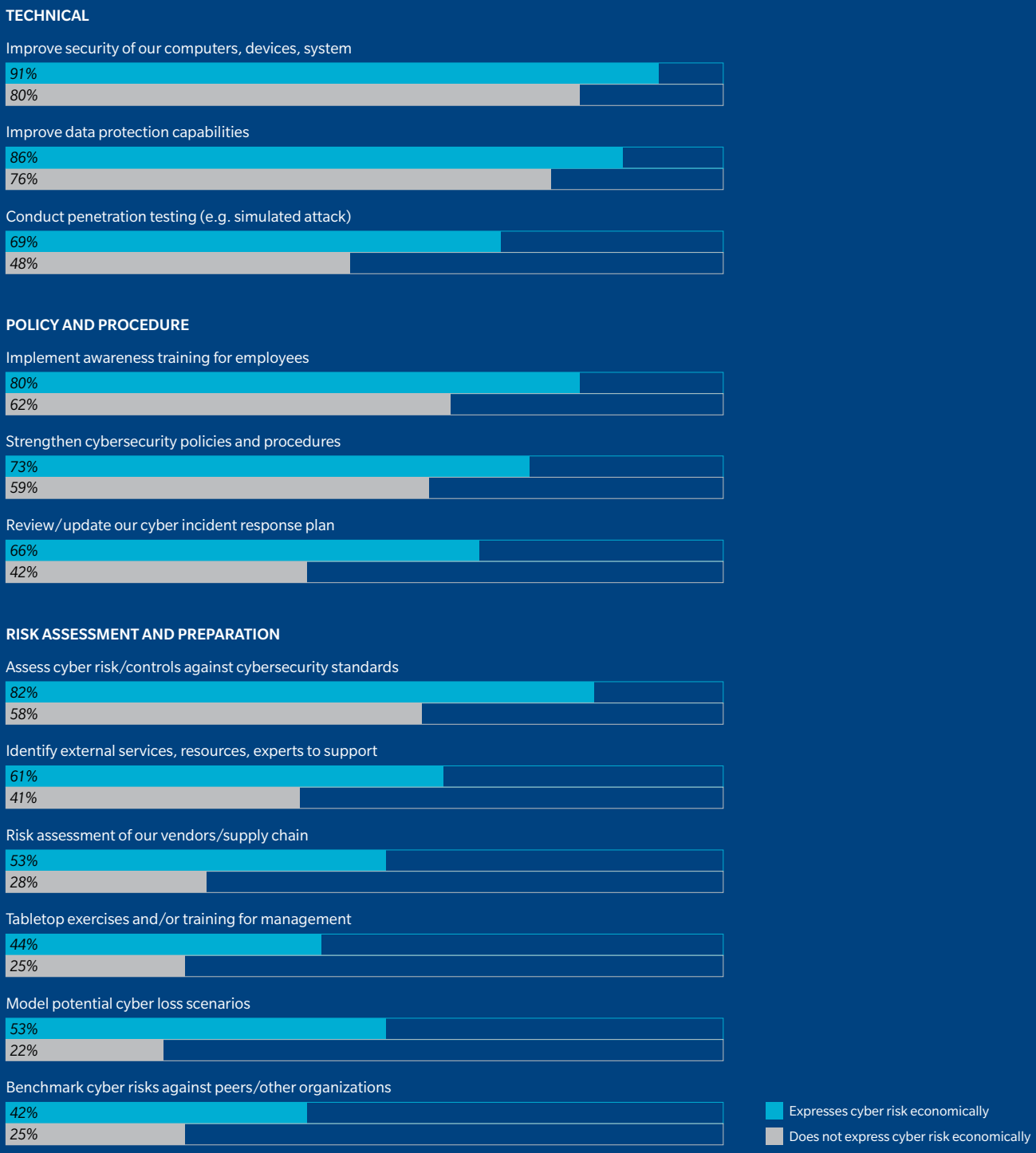


1. Base: all answering; n=1,303 (2019); n=1,312 (2017)
2. Base: Those with some form of cyber risk assessment method: n=660 (2019)

Source: Marsh Microsoft Global Cyber Risk Perception Survey 2019, Marsh & McLennan Insights analysis

Companies conducting economic quantification of cyber risk are more likely to balance technical and non-technical actions.

Q: Please indicate whether your organization has taken the specific actions listed below within the past 12 to 24 months.



1. Base: all answering; n=1,118 (2019)

Source: Marsh Microsoft Global Cyber Risk Perception Survey 2019, Marsh & McLennan Insights analysis

BUILDING CYBER RESILIENT CULTURE

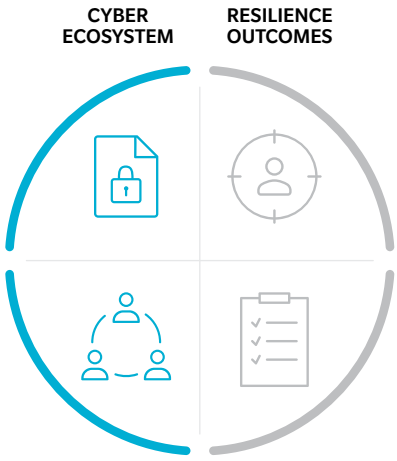
AN ORGANIZATION-WIDE JOURNEY AGAINST EVER-EVOLVING CYBER THREATS

Wolfram Hedrich
Executive Director,
Marsh & McLennan Insights

Rachel Lam
Research Analyst,
Marsh & McLennan Insights

In the face of an evolving cyber risk landscape, what does it take to protect businesses against cyber threats? While many companies implement the right risk assessment frameworks to identify threats early, or employ anti-virus software and encryption solutions, they often forget to ask themselves: "How much do our own staff care about cyber threats in their day-to-day roles"?

EXHIBIT 10: FOUR ASPECTS OF CYBER RESILIENT CULTURE



This is a critical missing part of the puzzle because data breaches are often not the result of a powerful hack or malware attacks on data servers, but employee negligence. A breach could simply result from a single employee forgetting to lock his or her laptop, allowing someone to steal his or her credentials and gain access to confidential data. In fact, of the five billion records stolen or compromised in 2018, such negligence accounted for more than two billion.

This brings into focus the importance of building a cyber resilient culture to protect an organization.

CYBER RESILIENT CULTURE VS. OTHER CYBER MEASURES

Responding to the increasingly digitalized business operations and the prevalence of cyber-attacks in news, organizations are rushing to build their cyber defences through comprehensive cyber risk strategies, including suitable operating models, dedicated cyber Risk Appetite Statements, automated cyber risk dashboards, tightening security controls, quantified cyber value-at-risk measures, and building strong cyber resilient culture.

This leads to the classic debate of how to balance the "hard" and "soft" aspects of cybersecurity, which often leads to following common pitfalls:

1. **"Let's de-prioritize culture for something more concrete":** Many executives typically place greater focus on cybersecurity mechanisms, often as add-ons or "quick-wins", before realizing that the number of security tools an organization has does not guarantee the safety of the business.

2. **"Our defence against insider threats is already good enough, what we need is protection against external attacks":** Almost three in four companies believe they are prepared enough to mitigate internal staff threats, despite more than 50 percent having confirmed cyber incidents due to staff actions in the past 12 months.

3. **"Cyber-attacks always involve sophisticated, technical approaches":** The Boards of too many companies still pick up most of their information about cyber events from media, which brings into focus sophisticated forms of attacks, such as ransomware and malware, but overlooks something as simple as employee negligence or malice.

BUILDING CYBER RESILIENT CULTURE

A strong cyber resilient culture is one where all staff behave in a way that protects the organization against cyber threats. This requires a fully coordinated approach across four dimensions (see Exhibit 10).

On the left side, there is a **cyber ecosystem** that establishes frameworks, policies, and processes, combined with people-oriented measures, as the necessary reinforcing structures to drive adoption. On the right side, there is a set of **resilience outcomes** which ensure that the resulting behavioral changes and stakeholders' mindset is moving towards the right direction.

While all the four illustrated aspects are necessary to achieve true cyber resilience, identifying **desired behavioral changes** is most crucial to drive the overall direction of the culture-building journey.

A **defined set of desired behavioral** changes informs what frameworks, policies, and processes are required to lay down the standard for what is considered as an undesirable behavior or a breach of a desired behavior. Training, incentives, coaching, communications and the like can then be rolled out to ensure adequate adoption and compliance to this agreed standard. Finally, closing the loop, a "pulse" check provides insights on the progress made, and gathers feedback that can be used to make improvements where needed.

For example, one commonly desired behavior for employees is to not fall for phishing messages. To truly drive this behavior change, the following needs to be implemented. Control measures can range from automated flagging of suspicious emails to removing email access of staff who do not need one. In addition, a periodic phishing test can be conducted to measure staff's awareness on phishing emails. To make the phishing test truly effective, people-oriented measures such as training, townhall sessions with team leads for them to educate their teams, and ultimately, linking performance in phishing tests to employees' key performance indicators (KPIs), need to be taken. A "pulse-check" survey to understand staff comfort level with phishing emails and the challenges faced during phishing drills, or even any possible additional support that can help strengthen cyber resilient culture.

HOW TO MEASURE PROGRESS?

Strengthening cyber resilience is a long journey, and it is important to measure progress so as to ensure it is going in the right direction and has sufficient impact. This requires a set of measurement metrics — see Exhibit 11 — that collectively track progress across all four pillars of the cyber-resilient culture.

THE RIGHT ROUTE AND PACE

Building a cyber resilient culture is a long-term endeavor. As in any cultural change, it is important that organizations follow the right path, at the right pace. This entails the use of nudges and interventions at different points, as required.

In designing nudges and interventions, we recommend drawing from techniques that rely upon insights around how professionals learn new behaviors and establish new neural networks. We have found that the most effective tools apply some of the latest thinking from research in neural science, neuro-linguistic programming techniques and behavioral change. Many of these activities nudge behaviors by influencing them at both a conscious level (where many programmes focus) and a subconscious level (where most behavioral change occurs).

In addition to role modeling behaviors, both formal and informal communication supports the change, and helps use authority bias and group dynamics to precipitate changes in behavioral habits. In addition to normal corporate change communications, targeted — and at times provocative — communications can be used to help nudge people and get them thinking about the change in their day-to-day working environment.

EXHIBIT 11: ILLUSTRATIVE SET OF METRICS

PILLAR	METRICS' DETAILS	EXAMPLES
 **Framework, policies, processes**	To measure the effectiveness of frameworks, policies and processes in setting up a cyber resilient culture by measuring residual risk, breaches, exceptions, etc.	• Number of business partners onboarded without cybersecurity checks • % of staff with approved exceptions to allow usage of USB sticks • Number of systems with high residual risk
 **People-related measures**	To evaluate the effectiveness of people-related initiatives in strengthening cyber resilient culture by measuring how comprehensive they are	• % of staff with cyber-related KPIs (for example, individual performance in phishing drills) integrated in their roles • % of staff participating in one or more cyber awareness campaigns in the year • % of staff with access to cyber trainings adequate for their day-to-day roles
 **Desired behavioural changes**	To measure change in staff behaviors through objective and quantitative means	• % of staff who installed security patches only at the point of "forced install" • % of critical new threats identified not resolved within two days • % of staff who completed cyber training within one month of launch
 **"Pulse" check**	To measure the organization's pulse towards change that is being created. These metrics measure the mindset shift of the organization towards the cyber change program	• Employee awareness score on their capabilities to protect the organization • Employee awareness score on organization's focus to protect itself, its customers and staff • Employee awareness score on organization's capabilities to protect itself

Ultimately, the goal is to have all stakeholders intuitively demonstrate desirable cyber resilient practices whenever and wherever they are.

A LASTING FIGHT

Organizations must realize that becoming secure is as much about building a cyber resilient culture as it is about implementing cybersecurity frameworks. This has been amply demonstrated by recent cyber incidents globally.

Building a cyber resilient culture requires strong senior management attention and investment. Most importantly, it requires an awareness that building greater cyber resilience is a long-term commitment.

CONTACT

For further information and other inquiries, please contact us at the below.

Tom Reagan

US Cyber Practice Leader,
Marsh

Thomas.Reagan@marsh.com

Jeremy Platt

Cyber Specialty Solutions Practice Leader,
Guy Carpenter

Jeremy.S.Platt@guycarp.com

Kevin Richards

Global Head of Cyber Risk Consulting,
Marsh

Kevin.Richards@marsh.com

Paul Mee

Partner and Cyber Lead,
Oliver Wyman

Paul.Mee@oliverwyman.com

Victoria Shirazi

Associate Director, Cyber Resilience,
Marsh & McLennan Solutions

Victoria.Shirazi@mmc.com

EDITORS

Leslie Chacko

Managing Director, Digital Insights & Solutions
Marsh & McLennan Companies

Lily Phan

Research Manager,
Marsh & McLennan Insights

ABOUT MARSH & MCLENNAN ADVANTAGE INSIGHTS

Marsh & McLennan Advantage Insights uses the unique expertise of our firm and its networks to identify breakthrough perspectives and solutions to society's most complex challenges. Marsh & McLennan Insights plays a critical role in delivering the Marsh & McLennan Advantage – Marsh & McLennan's unique approach to harnessing the collective strength of our businesses to help clients address their greatest risk, strategy and people challenges.

ABOUT MARSH & MCLENNAN COMPANIES

Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's 76,000 colleagues advise clients in over 130 countries. With annualized revenue approaching $17 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. Marsh advises individual and commercial clients of all sizes on insurance broking and innovative risk management solutions. Guy Carpenter develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. Mercer delivers advice and technology-driven solutions that help organizations meet the health, wealth and career needs of a changing workforce. Oliver Wyman serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit mmc.com, follow us on LinkedIn and Twitter @mmc_global or subscribe to BRINK.