MARSH & McLENNAN ADVANTAGE

MMC CYBER HANDBOOK 2021

Cyber Resilience Perspectives: Clarity In the Midst of Crisis

MARSH GUY CARPENTER MERCER OLIVER WYMAN

FOREWORD

Cyber attacks are among the most severe and likely risks facing business leaders in advanced economies, according to the latest *Global Risk Report*, published by the World Economic Forum with support from Marsh & McLennan. Further heightening this cyber risk for businesses, the world subsequently experienced an unprecedented level of societal, economic, and geopolitical upheaval brought on, in part, by the COVID-19 public health crisis.

Cyber security will remain an enduring focus and responsibility for businesses for several reasons. First, COVID-19 has forced many businesses into a remote mode of work, presenting an expanded threat surface for cyber-criminals to exploit. A trend which will persist well beyond the current crisis. Second, the pace of technological development continues to rapidly advance. Artificial Intelligence is enhancing both the effectiveness and peril of traditional cyber threats, while other emerging technologies increasingly create unforeseen vulnerabilities in novel ways — deep fakes, voice-based digital assistants, Internet of Things (IoT) devices, and more. Finally, many firms operate in complex supply chains that expose them to third-parties, which may not have the resources to maintain the same level of focus on cyber risk management. This interdependency heightens the challenge of maintaining cyber resilience across the ecosystem.

Given these factors, business leaders recognize that cyber is a risk that must be identified, quantified, and managed — but it is also one that cannot be entirely eliminated. A cohesive cyber strategy is required, one which keeps pace with technological development in an environment of increasing digital seamlessness and data ubiquity, and also, considers the human elements necessary to promote good cyber hygiene — culture, awareness, and technology enablement and support.

In the coming year, the cyber landscape will be more complex than ever before. The *MMC Cyber Handbook 2021* features perspectives from business leaders across Marsh & McLennan, as well as strategic partners who hold some of the most dynamic perspectives about the cyber economy. This handbook explores significant cyber trends, industry-specific implications, emerging regulatory challenges, and strategic considerations.

I hope that you find these perspectives informative.

John Doyle
President and Chief Executive Officer
Marsh

TABLE OF CONTENTS

01. TREND WATCH

Cyber Security for a Remote Workforce 6
Paul Mee, Partner, Digital and Financial Services, Oliver Wyman
Rico Brandenburg, Partner, Financial Services, Risk and Public Policy and Digital, Oliver Wyman

Digital Deception: Is Your Business Ready for Deep Fakes? 10
Stephen Vina, Senior Vice President, Marsh
Steve Bunnell, Former General Counsel, Department of Homeland Security

Prepare to Protect Your Customers' Voices 13
Paul Mee, Partner, Digital and Financial Services, Oliver Wyman
Gokhanedge Ozturk, Partner at Oliver Wyman

Cyber Literacy and Education Index 17

02. INDUSTRY DEEP DIVE

Is Your Company a Risk to Others in the Supply Chain? 19
Joram Borenstein, General Manager, Microsoft's Cyber security Solutions Group

Looking Beyond the Clouds: A US Cyber Insurance Industry Catastrophe Loss Study 23
Siobhan O'Brien, Head of International Cyber Center of Excellence, Guy Carpenter
Erica Davis, Managing Director and Cyber Risk Strategy Leader, Guy Carpenter
Christopher Shafer, Assistant Vice President, Cyber Center of Excellence, Guy Carpenter

Winning the Cyber Risk Challenge: Rapid Digitalization in the Energy/Power Sector Continues to Outpace Cyber Readiness 27
Leslie Chacko, Managing Director, Marsh & McLennan Advantage, Solutions
Wolfram Heidrich, Partner, Risk and Finance Practice, Oliver Wyman
Rachel Lam, Consultant, Oliver Wyman

Cyber Attacks: The increasing Risks for Retail 32
Stephen Picard, Principal, Retail, Oliver Wyman
James Bacos, Global Retail and Consumer Goods Practice Leader and Russia Lead, Oliver Wyman

03. CURRENT AND EMERGING REGULATIONS

Silent Cyber — no longer silent? **34**
Siobhan O'Brien, Head of International Cyber Center of Excellence, Guy Carpenter
Erica Davis, Managing Director and Cyber Risk Strategy Leader, Guy Carpenter

Two Years On, the GDPR Continues to Shape Global Data Privacy Regulation **38**
Marsh

With the Commencement of CCPA Enforcement, Now is the Time to Prepare and Measure its Potential Impact **42**
Allison Pan, Senior Vice President, Emerging Risks, Marsh
Jennifer Lawson, Senior Vice President, Legal and Claims Practice, Marsh

04. STRATEGY

How to Protect Data in an Age of Digital Seamlessness **47**
Paul Mee, Partner, Digital and Financial Services, Oliver Wyman
Rico Brandenburg, Partner, Financial Services, Risk and Public Policy and Digital, Oliver Wyman

Human Resources' Increasing Role in Cyber Risk Management **50**
Brian Warszona, UK Cyber Growth Leader, Marsh

Don't Forget Your Cyber Risk Sentries **54**
Karen Shellenback, Global Products Leader, Analytics and Research, Mercer

Cyber security After COVID-19: 10 Ways To Protect Your Business And Refocus On Resilience **57**
Thomas Fuhrman, Managing Director, Cyber security Advisory, Marsh

01.
TREND WATCH

Paul Mee
Partner, Digital and Financial Services, Oliver Wyman

Rico Brandenburg
Partner, Financial Services, Risk and Public Policy and Digital, Oliver Wyman

This article was first published in *MIT Sloan Management Review* on July 23, 2020

CYBER SECURITY FOR A REMOTE WORKFORCE

Employees are starting to return to offices as countries begin to ease COVID-19-induced lockdowns and lift stay-at-home orders. But as uncertainty related to the pandemic lingers, many organizations are choosing to maintain semi-remote, virtual workplaces over the next 12 to 18 months — and possibly for good. Facebook is allowing employees to work from home permanently, while Canadian e-commerce platform Shopify announced that it is becoming "digital by default."

Organizations have rapidly shifted to semi-remote working arrangements and thus they must be equally speedy in mitigating the cyber risks created by the expanded "attack surfaces" that have accompanied the "work anywhere" operating models.

To take on the new cyber security challenges of this virtual working environment, organizations must understand the changes in their cyber security risk profile and revamp their strategies, training, and exercises to address these changes.

THE NEW CYBER NORMAL

Five key factors drive the cyber security risk implications in this new, likely semi-remote, working environment. Organizations should keep these factors in mind when defining how to adjust their cyber security risk programs.

1. An increasing number of cyber attacks

Since the COVID-19 outbreak began, the number of cyber attacks has soared as hackers have exploited a greater number of weakly protected back doors into corporate systems as well as the human distraction caused by COVID-19-related events. The FBI is receiving 3,000 to 4,000 cyber security complaints daily, up from 1,000 prior to the pandemic. Hackers continue to target key industries such as health care, manufacturing, financial services, and public sector organizations like the World Health Organization. Banks are now fending off nearly three times as many cyber attacks as cyber criminals flood employees' inboxes with COVID-19-related phishing emails, often attaching seemingly innocuous files designed to lure unsuspecting employees into executing malware.

2. Changing attack surfaces

The shift to using new teleworking infrastructure and processes may lead to the undetected exploitation of vulnerabilities in existing remote work technologies. Security agencies in both the United States and the United Kingdom have warned that a growing number of cyber criminals are targeting individuals and organizations with malware. In addition, cyber risks via business partners and third parties are increasing as well. It is hard enough to prepare internally for a semi-remote working environment but even harder to verify the preparedness of vendors ranging from IT service providers to business process outsourcing firms to law firms.

3. Distracted workforces

A vast number of successful cyber attacks are caused by human error, including an estimated 90 percent of such attacks in the UK in 2019. Increasingly preoccupied by greater personal and financial stress at home, employees are more vulnerable to cyber threats and "social engineering" cyber attacks designed to trick them into revealing sensitive information.

4. Unanticipated staff shortages

Workforces are stretched thin as employees (including cyber security professionals) call in sick or take time off to care for dependents, further harming organizational abilities to respond to cyber threats. Furthermore, since mass work from home began during the coronavirus outbreak, self-reported data in the United States shows decreased productivity across industries, with 11 percent of professional and office workers and 17 percent of industrial and manual service workers reporting lower productivity.

5. Multi-stress environment

Security teams are operating in an unprecedented environment in which multiple crises are constantly arising, each demanding significant attention from cyber security and management teams. COVID-19-related challenges will be the baseline for the foreseeable future. Moreover, organizations still have to manage through other crises and stress events, like hurricanes, forest fires, or widespread protests as recently observed in the United States.

ASSESS YOUR CHANGING CYBER SECURITY RISK PROFILE

As organizations transition to the new ways of working, the resulting changes to the company's cyber security risk profiles must be repeatedly assessed and monitored so that they can be actively managed, prioritized, and mitigated.

The list of entry points for attacks as a result of far-flung workplaces keeps growing. Bad actors can openly record sensitive customer information shared with customer service employees taking service calls on their mobile phones at home, instead of in highly secure and monitored call centers. Inadequately tested new technologies and digital products rapidly deployed to meet customer needs during the pandemic, like customer service chatbots and Paycheck Protection Program applications could inadvertently introduce new threats. Remote working operations of interconnected vendors and customers further amplify organizational risk.

Based on this risk assessment, teams of risk management, business, and security personnel should work together to reevaluate cyber security budgets and prioritize investments to improve a company's cyber resilience in line with its risk tolerance.

ADJUST YOUR CYBER STRATEGY

Start with stopgap measures that can be implemented immediately, such as revising existing cyber risk guidelines, requirements, and controls on how employees access data and communicate with a company's network. Rules of behavior analytics need to be adjusted to consider changes to the "normal" behavior of employees, many of whom now work outside standard business hours so that security teams can effectively focus investigations.

Then examine new security tools and requirements for sharing and maintaining private information with vendors. For example, organizations may need to adopt more robust data loss controls, traffic analysis tools, and access restrictions. Ensure that vendors that aren't currently prepared for heightened cyber attack risk commit to developing cyber preparedness plans to safely handle information or interact with your corporate network.

Review changes to boost your technology and security infrastructure today, even if such changes may take years to implement. Some organizations may want to speed up their cloud strategies so that their IT resources can rapidly meet demand spikes from large-scale remote work. Other common improvements include investing in automation and advanced analytics to improve the effectiveness of security processes, introducing greater discipline around cyber-relevant data, rationalizing duplicative monitoring and security tools to manage the cost of exploding data volume, and focusing cyber security teams on the highest-risk areas.

Finally, develop mechanisms to understand how your security program changes reduce cyber security risks after each initiative is rolled out. This is not a one-and-done exercise; organizations need ongoing agility to hit what is a decidedly moving target.

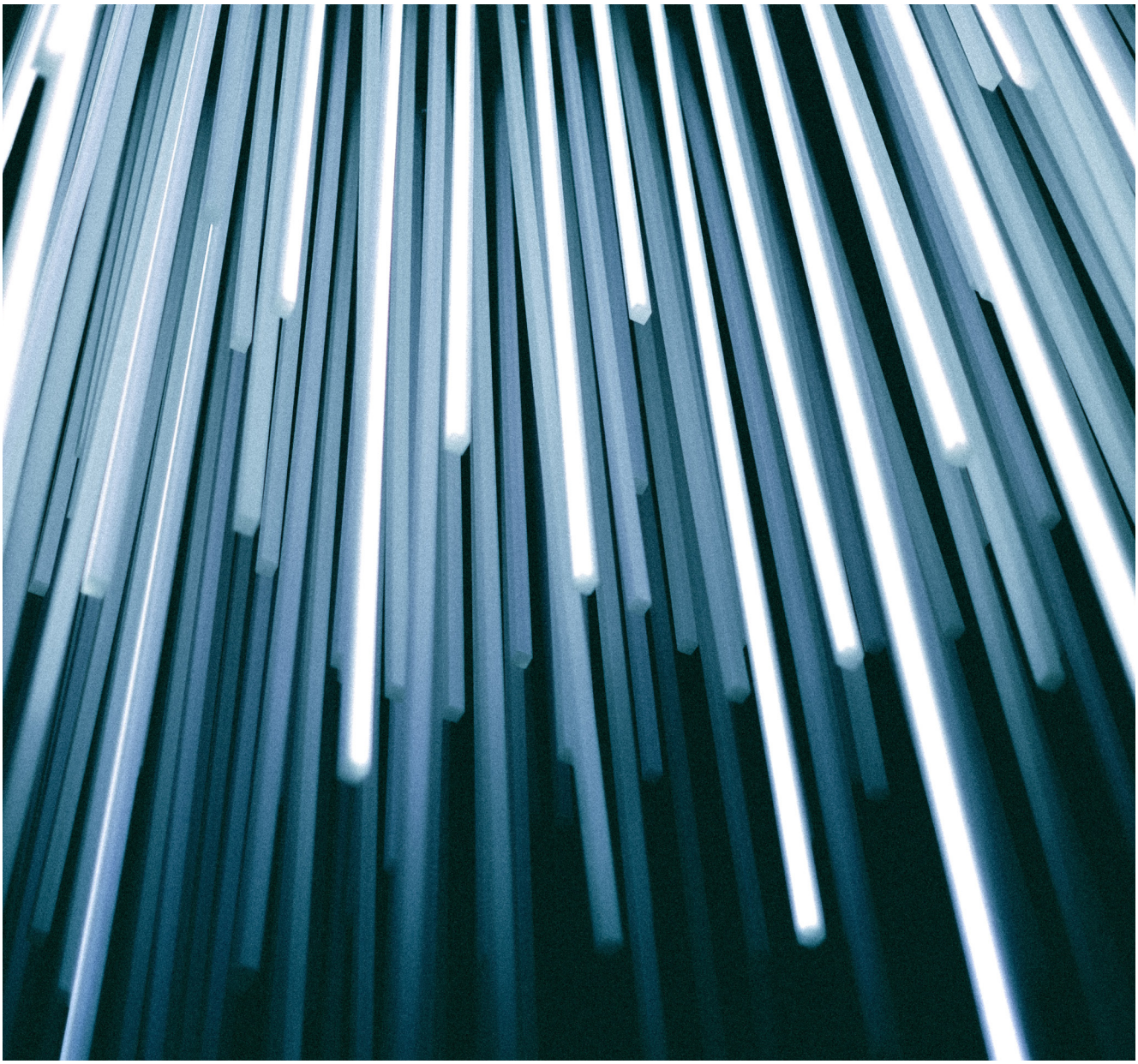
STEP UP CYBER TRAINING AND EXERCISES

Employees need to be informed of new cyber risks and reminded of their role in effectively preventing, detecting, responding to, and recovering from cyber attacks.

Design role-based training programs and exercises to raise the awareness at every level of new and changed cyber risks introduced by increased remote working. Training programs should cover new threats, rules for approved device and data use, and processes to report suspected cyber incidents.

Management teams should engage in walk-throughs and simulations for new cyber attack scenarios armed with playbooks that provide clear guidelines for required actions, including when (and to whom) decisions should be escalated. By doing so, teams can identify shortcomings that must be overcome in order to respond effectively to cyber attacks.

Much of the operational shift that has occurred as a result of the pandemic will outlast the immediate crisis and aftermath. To adapt securely, organizations need to understand how their cyber risk profiles have changed and must revamp their strategies, training, and exercises to address threats and minimize risks.



Stephen Vina
Senior Vice President, Marsh

Steve Bunnell
Former General Counsel, Department of Homeland Security

This article was previously published by *Business Insurance*

DIGITAL DECEPTION:

Is your business ready for “deepfakes”?

ABC Shoe Corporation has just completed the most successful quarter in its history. The CEO holds a press conference to announce the good news. Several hours later, an altered video of the CEO at the press conference goes viral on social media, showing him slurring his words and appearing inebriated. ABC Shoe Corporation has become a victim of a “deepfake.”

This story may seem farfetched, but similar incidents have already played out in real life, impacting mostly politicians and celebrities. Businesses too are starting to see deepfakes targeting them. What once took significant skill and time to create can now be done cheaply, quickly, and convincingly, posing a major threat to both public and private sectors.

A "deepfake" is a sophisticated digital forgery of an image, sound, or video. The forgery may be so good that a human is unlikely to detect the manipulation. The goal is to mislead and deceive, making it appear as though a person has said or done something when that is not the case. Supported by advances in artificial intelligence, deepfakes have proliferated across the internet as the technology becomes less expensive and more accessible.

RISKS FOR BUSINESSES

Businesses have always taken great strides to protect the "CIA" triad of information security — confidentiality, integrity, and availability. Data confidentiality has frequently been threatened by massive data breaches involving businesses, while attacks on the availability of data have become a new normal with the proliferation of ransomware attacks.

Attacks on data integrity, however, appear to be a more recent phenomenon. And businesses may not be prepared to respond to this sleeping giant, one that could have devastating impacts.

Nation-states, competing businesses, disgruntled employees, criminals, and anonymous saboteurs may use deepfake technology to disrupt business operations or facilitate fraud. Indeed, news reports surfaced in August 2019 that — for the first time — deepfake audio technology was used to mimic the voice of a CEO to facilitate the fraudulent transfer of funds. This type of misuse introduces a potentially dangerous trend.

Deepfakes can also have a severe impact on a company's reputation. A deepfake posted on social media could easily go viral and spread worldwide within minutes. Companies would have to spend valuable resources identifying, removing, and rebutting such fake content; legal fees and crisis management expenses would likely also stack up. If the deepfake was embedded in internal materials, companies would need to investigate the network intrusion and remediate corrupted systems and data. Though a company might ultimately prove it was the victim of a deepfake, the damage to its reputation will already have been done, potentially resulting in lost revenues.

CURRENT LEGAL REGIME

As with many advances in technology, deepfakes are outpacing the law. While no law directly addresses deepfakes, several criminal and civil laws may be applicable.

Criminal statutes governing fraud, extortion, and cyberstalking, for example, may broadly serve as criminal remedies and deterrents to combat deepfakes. Federal securities law may also apply to a deepfake used to defraud anyone in connection with registered securities. Impersonating a government official through a deepfake could also result in criminal penalties.

Civil remedies provide more flexibility for businesses in holding deepfake perpetrators accountable. Unlike criminal remedies, if a business can prove a general harm, such as defamation, copyright infringement, or a violation of the right of publicity, the business can sue the perpetrator.

Knowing exactly whom to bring actions against and being able to bring perpetrators under the jurisdiction of US laws — particularly if they live abroad — may be difficult. If a deepfake is spread over the internet, however, the victim business will likely only be able to sue the perpetrator of the deepfake. Content platforms, even when hosting fake content, are typically immune from civil liability under US law.

PROTECTING DATA INTEGRITY

Risk managers can take action now to build enterprise resilience and address the potential onslaught of new data integrity threats. Public relations and crisis communication planning — along with identifying properly legal remedies — can be critical to responding to a deepfake and mitigating reputational harm. Cyber risk assessments and strong cyber hygiene can also help thwart attacks that are targeting data on company networks, while robust backup procedures can help restore or verify corrupted information.

For those businesses that fall victim to a deepfake, cyber insurance policies may provide relief for some financial loss.

A data integrity attack on a company network, like other cyber attacks, could result in a security incident that would need to be investigated and remediated. Cyber insurance policies often offer broad cyber event management coverage for the cost of crisis communications and computer forensic specialists responding to an incident. If data has been corrupted, cyber insurance policies may cover the cost to replace, restore, or recreate the data. A cyber policy may also respond to a ransom demand linked to a deepfake on a corporate network.

Cyber policies are also expanding to include coverage for attacks on a company's reputation from adverse publicity after a cyber incident or privacy breach. For example, a cyber policy can cover lost revenues and the costs to hire public relations consultants after a reputational attack. While wordings vary and are often tied to a network intrusion, these coverages continue to evolve and could be helpful to a company that suffers reputational harm from a damaging deepfake.

Crime policies — and, to a lesser extent, cyber policies — could also help companies that have fallen victim to deepfakes recover funds that were transferred to third parties under false pretenses.

Deepfakes are a new type of threat for businesses, and insurers are still assessing potential risks. Whether a cyber policy responds to a deepfake ultimately depends upon the circumstances of the incident and the terms and conditions of the policy. Risk managers should carefully review their policies and work with their insurance advisors and legal counsel to assess potential exposures and coverages for this evolving threat.

Paul Mee
Partner, Digital and Financial Services, Oliver Wyman

Gokhanedge Ozturk
Partner, Oliver Wyman

This article was first published in *MIT Sloan Management Review* on May 05, 2020

PREPARE TO PROTECT YOUR CUSTOMERS' VOICES

The threat of voice-based cybercrime is growing along with the explosion of voice-directed digital assistants, billions of which are already embedded in our mobile phones, computers, cars, and homes. Digital assistants are always listening, creating a significant security risk, especially as millions of people work from home during the pandemic. It's estimated that in the next two years, there will be more virtual digital assistants than people in the world. Nearly two-thirds of businesses plan to use voice assistants for their customer interactions, according to a 2018 survey conducted by Pindrop Security.

Already, the number of cyber attacks on voice-recognition systems is rising as people converse with bots to play music, pay their bills, book reservations at restaurants, and perform other everyday tasks. It now takes less than four seconds of original audio to create a deepfake of someone's voice. Recently, hackers used machine learning software to impersonate a CEO and order subordinates to wire hundreds of thousands of dollars to a fraudulent account.

Much of today's voice fraud, known as "vishing," involves controlling voice assistants by methods such as embedding undetectable audio commands, replaying voice recordings, and modifying fraudsters' voices to match the pitch of their victims' voices. As hackers become better at impersonating people, they will be able to apply deepfakes of voices that will be far harder to detect.

The damage could be catastrophic unless companies take appropriate cyber security precautions. Financial services companies send millions of customers new credit cards after criminals steal information, but they can't send them new voices. Unless voice activation is made secure, the rapid growth of machines that recognize voice commands could grind to a halt, damaging customers' trust in the privacy safeguards of the many companies that use voice systems.

Pindrop's survey found that 80 percent of businesses worldwide considered the security of their voice-directed services to be a concern. So how can managers make their customers' voices safe?

As a first principle, companies should roll out voice-directed services only when they are confident of their ability to mitigate the accompanying cyber security risks. For example, at first, financial companies may want to offer customers only the ability to check basic facts by voice — such as account balances and stock quotes — and have them continue to use manual means or biometrics like the person's face or fingerprint to execute transactions.

As the range of voice-activated services extends and becomes more sophisticated, here are some other measures businesses can take.

STRENGTHEN CUSTOMER AUTHENTICATIONS

Companies should introduce screening protocols for voice-controlled services that are at least as robust as those used for other digital services. Customers should receive alerts if their orders exceed a certain threshold or appear to deviate from their typical purchasing patterns.

Companies can increase awareness of potential scams by distributing checklists to help customers gauge whether a third party's approach or a request for information could be fraudulent. For example, a company could advise customers to hang up if a caller doesn't know their name and relationship to the company, or if the caller's phone number seems suspicious. Recently, scammers have been tricking people into giving away sensitive information when they use voice searches to find customer service numbers. Customers should also be made aware of the extent to which they are insured against fraud whenever a company launches a new voice-directed service.

At the same time, voice-directed services should ask for additional forms of authentication. These could consist of biometrics such as a customer's fingerprint or face. Or they could be qualitative verbal authentications that can't be found in the public domain — personal preferences, for instance, or the relative a customer visited with most often as a child, or both.

Companies will also have to invest in filtering technologies that detect whether a voice is real or synthesized as they become available. Some companies are already trying out technologies that can detect clues that human hearing normally misses, such as the sound of breathing, which may be present in a genuine voice but absent in a synthesized impersonation. Systems are also being designed to block inaudible commands by identifying and canceling ultrasonic signals, which researchers have found can take control of voice-recognition systems.

CONDUCT CYBER EXERCISES

Hackers will continue to develop new methods to exploit the weakest links in systems. Companies offering voice-activated services need to test their security constantly, conducting cyber exercises that identify vulnerabilities to determine ways to plug the gaps. They should also prepare responses to deploy in the event of a successful cyber attack.

As a training exercise, some of a company's cyber security experts could try to exploit a voice assistant's security gaps while others guard against the attackers. Alternatively, companies could engage ethical hackers to conduct surprise attacks on voice-assistant services — either on their own or in collaboration with other businesses or industries. The defense and payment industries already hold cross-industry cyber war games of this kind.

Cyber security teams should simultaneously explore alternate ways of operating should a voice-related cyber crisis arise. Experts should puzzle out in advance how to react to scenarios by considering a series of questions: If withdrawals are suddenly made from a bank using deepfaked customer voices, how should it react? How would it detect an attack in the first place? And what alternatives should be made available in the event of an emergency?

COMMUNICATE ACROSS INDUSTRY

Today, regulations exist for voice-directed services. For example, the California Consumer Privacy Act limits the sale and mining of consumer voice data collected through smart televisions. Europe's General Data Protection Regulation requires companies to report personal data breaches to their relevant local regulatory authority, though it does not currently address voice compromises directly.

Whatever the rules, cyber security officers should maintain regular contact with governments and others in their industries in order to stay ahead of regulations and potential new threats. Voice operations — and the convenience and efficiency they bring — will only spread so long as the companies offering them show that they can safeguard customers' voices.

Companies should establish forums and other methods to share data about voice-assistant breaches so that whole industries can stay ahead of their adversaries. Once voice assistants become a common method for transferring money, new security protocols may also be needed.

THE POTENTIAL OF THE CONVERSATIONAL ECONOMY

If voice-directed services were made secure, they could deliver services that would improve — and possibly transform — consumers' daily lives. People could tell cars to take them to appointments. They could turn to mobile phones to arrange their vacations. One day, they might even ask virtual assistants for financial advice.

But delivering this conversational future will require cyber security to stay ahead of hackers' ability to abuse voice systems. Businesses should prioritize exploring now what it will take to keep their customers' voices safe — and prepare to continue the battle indefinitely.

CYBER LITERACY AND EDUCATION INDEX

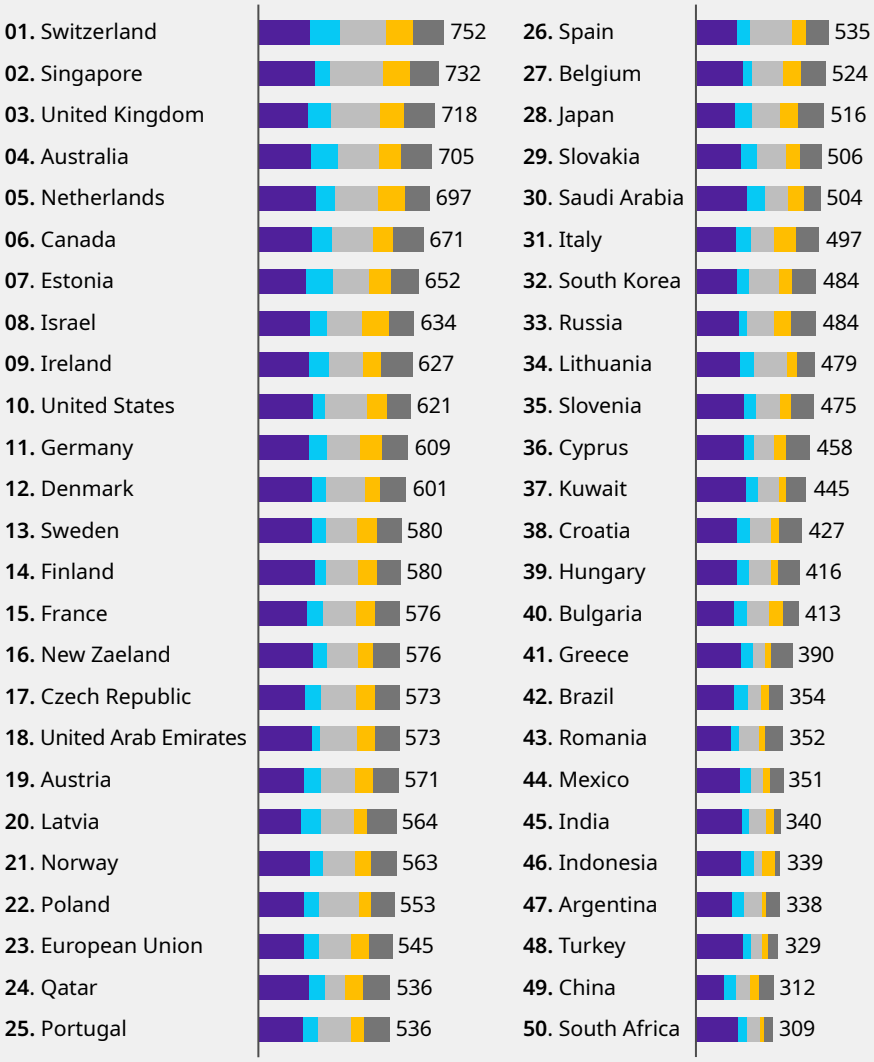
Like financial literacy or health literacy, cyber risk literacy is fundamental knowledge that all individuals should understand. As the world digitizes, governments and businesses increasingly rely on individuals to protect themselves and others in cyberspace.

The Oliver Wyman Forum's Cyber Risk Literacy and Education Index provides a comprehensive framework for measuring literacy at the population-wide level to enable geographies to discover best global practices and focus their attention on areas of need.

The Index measures not only current populations' ability to understand cyber risk but also whether current structures in governments, education systems, and employers have the tools and incentives to train future generations with essential cyber risk knowledge and skills in an inclusive manner.

The first edition of the Index ranks 50 geographies, including the European Union as a population-weighted aggregate of our ranked EU geographies.

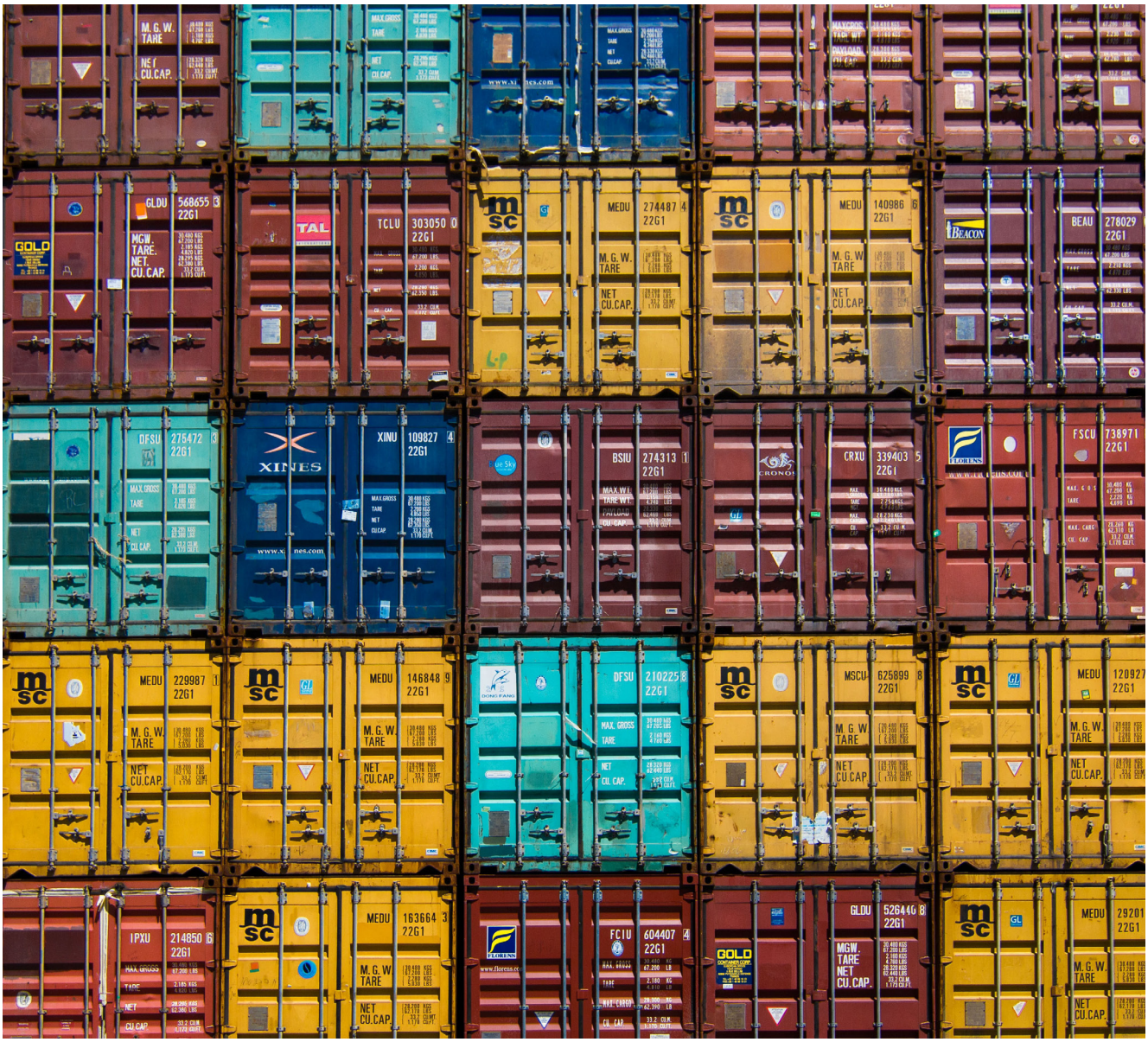
Exhibit 1: Summary of index rankings, weighted driver scores (as of October 2020)



Public motivation	Cyber risk awareness of the population
	Cultural proclivity towards personal/societal cyber-risk reduction
Government policy	Long-term vision and commitment by the government to advance cyber literacy
Education system	Formal education that incorporat es early cyber-risk awareness
	Labor upskilling ability and actions to strengthen cyber-risk consciousness of the national workforce
Labor market	Cyber-risk skills demand from employers
	Demand for innovation-driven skills
Population inclusivity	Technological inclusivity which creates equality in digital access and digital pervasiveness
	Educational inclusivity on cyber security programs available for vulnerable population and non-traditional communities

Source: Oliver Wyman Forum

02. INDUSTRY DEEP DIVE



Joram Borenstein
General Manager,
Microsoft's
Cyber Security
Solutions Group

This article was first published by *BRINK* on December 17, 2019

IS YOUR COMPANY A RISK TO OTHERS IN THE SUPPLY CHAIN?

In the world of global supply chains, trust is becoming an increasingly important commodity.

The concept of "technological social responsibility" — the recognition and acknowledgment by each organization of its cyber security obligations within the supply chain — is now on the agenda for many industry leaders.

Every organization needs to play a role in the integrity and security of its digital supply chains, as a lack of trust can impede business performance and innovation.

"Risk management, supply chain security assurance, safety, regulatory compliance and licensing all require a synergetic approach toward quality assurance and end-to-end discipline, traceability and visibility," according to a report titled *ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies* from the Carnegie Endowment for International Peace.

ARE YOU A RISK TO OTHERS?

Organizations are aware of the risks their supply chain partners may pose to their own cyber posture, but most do not fully appreciate the risk in reverse, according to the 2019 Global Cyber Risk Perception Survey from Marsh and Microsoft. There is a marked discrepancy in many organizations' views of the cyber risks they face from supply chain partners, compared to the level of risk their organization poses to its counterparties.

Thirty-nine percent of organizations perceive risk from their supply chain partners, but only 16 percent perceive risk they present to their supply chain partners. This pattern appears consistently across industry sectors and geographic regions.

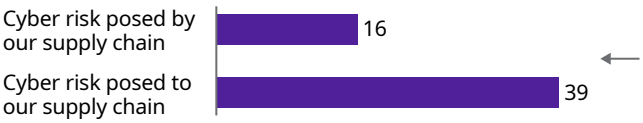
And this gap increased significantly with revenue size, with 61 percent of companies of US five billion revenues or more saying they faced high risks from their supply chain — and only 19 percent saying they posed a risk to it.

Exhibit 1: Perceptions of cyber risks in supply chains

Percentage of perceived risk level

Base: All answering (n=786, 2019)

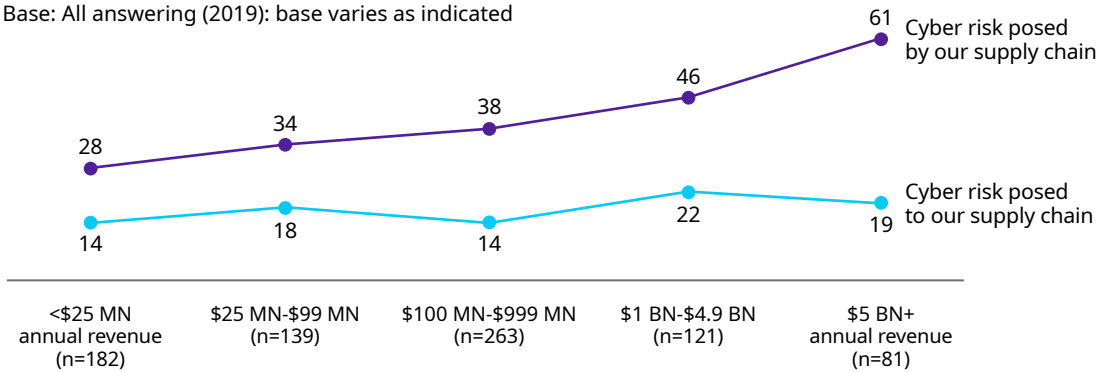
Many organizations are more attuned to the risks they face from their supply chains than the risks they themselves pose.



Q: What level of cyber risk is posed to your organization by its supply chain/ third parties? And the reverse: What level of cyber risk does your organization pose to its supply chain/third parties?

Risk perception gap

Base: All answering (2019): base varies as indicated



Note: Percentage regarding each risk as "somewhat" or "very high"

Source: Marsh Microsoft *2019 Global Cyber Risk Perception Survey*

This is a dangerous perception gap that many organizations, especially large ones, need to address to effectively protect their supply chain ecosystem.

RESPONSIBILITY TO SUPPLIERS

There was also a disparity between the cyber security measures and standards that organizations apply to themselves, versus those they expect from suppliers. On balance, respondents were more likely to set a higher bar for their own organization's cyber risk management measures than they do for their suppliers.

For example, 56 percent of organizations said they expect suppliers in their digital supply chains to implement awareness training for their employees; yet 71 percent said that their organization has implemented such a requirement for itself.

Such disparities could lead organizations to think their suppliers are less prepared to manage cyber risk than they are, thus diminishing the organization's trust in its supply chain.

The disconnect may also be driven by organizations' low confidence in their abilities to prevent or mitigate cyber risks posed by commercial partners. The proportion of organizations stating they are "not at all confident" that they could mitigate cyber threats from supply chain partners ranged from 13 percent to 30 percent, generally twice as high as those who reported being highly confident.

Overall, 43 percent reported "no confidence" in their ability to prevent cyber threats from at least one of their third-party partners.

APPETITE FOR GOVERNMENT'S ROLE DRAWS MIXED VIEWS

In recent years, regulators globally have enacted numerous measures to hold corporations and executives more directly accountable for ensuring effective cyber security and for keeping customers' data safe. Many of these regulations and legal frameworks require a greater degree of transparency from organizations at all levels of their data-handling activities and in their cyber risk management readiness.

The growth in such laws and regulations complement a body of well-established cyber and information security standards from industry authorities, such as the National Institute of Standards and Technology and the International Organization for Standardization.

Only 28 percent of respondent organizations identified government regulations and laws as being "very effective" in improving cyber security.

This held across all major regions, despite considerable variance in local laws and regulations. Highly regulated industries, such as aviation, financial institutions and communications were more likely to see value in government regulation of cyber risk.

NATION-STATE ATTACKS ARE DIFFERENT

The major area of difference in the attitude toward cyber regulation related to cyber attacks by nation-state actors. A majority (54 percent) of respondents said they are highly concerned about the impact of nation-state cyber attacks.

And 55 percent of organizations said there is a need for governments to do more to protect private enterprise from nation-state cyber attacks. This call for action resounds consistently across regions, with the highest positive response among financial institutions and professional services organizations.

These results show that while firms generally prefer a non-prescriptive approach to managing their cyber security and cyber risk affairs, nation-state activity is a clear exception.

As cyber risks become increasingly complex and challenging, there are encouraging signs in our 2019 Global Cyber Risk Perception Survey that enterprises are, slowly but surely, starting to implement best practices in cyber risk management. Nearly all recognize the magnitude of cyber risk, many are shifting aspects of their approach to match the threat and most are doing a good job in traditional cyber security — protecting the perimeter.

MANAGING SUPPLY CHAIN RISK AS A COLLECTIVE ISSUE

The most savvy organizations are building cyber resilience through comprehensive, balanced cyber risk management strategies, rather than concentrating solely on prevention. These more complex approaches account for the need to build capabilities in understanding, assessing and quantifying cyber risks in the first place, as well as adding the tools and the resources to respond to and recover from cyber incidents when they inevitably occur.

At a practical level, this year's survey points to several best practices that the most cyber-resilient firms employ and that all firms should consider adopting. Notably, this includes managing supply chain risk as a collective issue and recognizing the need for trust and shared security standards across an entire network, including the organization's cyber impact on its partners.

Effective cyber risk management requires a comprehensive approach employing risk assessment, measurement, mitigation, transfer and planning, and the optimal program will depend on each company's unique risk profile and tolerance.

Siobhan O'Brien
Head of International Cyber Center of Excellence, Guy Carpenter

Erica Davis
Managing Director and Cyber Risk Strategy Leader, Guy Carpenter

Christopher Shafer
Assistant Vice President, Cyber Center of Excellence, Guy Carpenter

To learn more, read the full report here

LOOKING BEYOND THE CLOUDS:

A US cyber insurance industry catastrophe loss study

The inexorable spread of the digital economy is fundamentally changing the nature of risk, presenting unique opportunities — and challenges — to the (re)insurance industry. How the industry responds to the rapid pace of technological change is crucial to its long-term relevance and growth.

The constantly evolving nature of cyber risk makes it challenging to definitively quantify, yet it is critical for (re)insurers to understand the impact of severe events to inform strategy and risk tolerance. It is essential to develop a deep understanding of the characteristics of cyber catastrophe events and the financial impact they could have on the standalone cyber insurance market today.

As the (re)insurance industry seeks to reduce protection gaps and drive cyber product adoption, the future growth that results will help develop a robust market better equipped to absorb the potential for large-scale losses.

With that premise in mind, CyberCube Analytics, which offers a software-as-a-service analytics platform for cyber risk aggregation modeling and insurance underwriting, and Guy Carpenter collaborated on an endeavor to help (re)insurers quantify cyber risk. This was done by pooling data resources and analytics capabilities in order to cultivate a view of the potential US cyber industry loss from among a range of cyber catastrophe scenarios. This study aims to contribute to the discussion surrounding the key drivers of catastrophic insured loss within the US cyber insurance market and how these results can be incorporated into portfolio construction, risk retention and transfer strategies and capital allocation.

We focused on the five scenarios that drive the highest loss values. For each, we considered the size of the loss, the single point of failure (SPOF) targeted to execute the attack and the implications of these findings on the insurance market. The five major contributing catastrophe scenarios are:

- Long-lasting outage at a leading cloud service provider (US 14.3 billion loss)
- Large-scale cloud ransomware at a leading cloud services provider (US 11.5 billion loss)
- Widespread data loss from a leading operating system provider (US 23.8 billion loss)
- Widespread theft from major e-mail service provider (US 19.1 billion loss)
- Large-scale data loss from cloud service provider (US 22.2 billion loss)

Insurance companies and the organizations they insure need to be aware of these major catastrophic scenarios, and understand the response plans necessary and potential financial losses in each. Bearing this in mind, the industry must invest in effectively assessing and managing aggregations, educating the business community to drive product adoption, and quantifying cyber risk to promote the purchase of adequate insurance limits.

The following are the five key considerations we highlight for (re)insurers and other stakeholders to help protect profitability and examine capital adequacy of the existing US cyber standalone insurance industry:

- The US industry 1-in-100-year return period produces total annual cyber catastrophe insured losses of US 14.6 billion (this can include one or more events within the same year)
- Both on-premise and cloud service providers face exogenous threats from malicious third parties. Focusing on cloud service providers, the calculated probability of ransomware is four times larger than the probability of other outages
- The top five scenario classes comprise roughly 75 percent of the total average annual loss (AAL)
- The costliest cyber catastrophe scenario is widespread data loss from a leading operating systems provider with potential to generate up to US 23.8 billion of insured loss
- The most likely cyber catastrophe loss scenario is widespread data theft from a major email service provider

GROWING PAINS

According to some estimates, the global market volume for cyber insurance will grow to US eight to nine billion by 2020 — more than twice that of 2017. With many traditional lines of insurance experiencing stagnating growth, cyber is increasingly viewed as having large growth potential for commercial property and casualty (re)insurers.

Despite this growth potential, there are headwinds to overcome as cyber insurance continues to grow and evolve. Increasing competition as new entrants seek to take advantage of the growth potential has created pressure on rates as well as an expansion of available coverage. The exposure data needed by (re)insurers to quantify and price cyber risk appropriately is a moving target as coverage matures and (re)insurers develop a deeper understanding of how to translate cyber security metrics into indicators of loss.

Historically, cyber insurers have seen a series of one-off data breach losses, some of which — the Marriott data breach in 2018, for example, with breach costs estimated at more than US two billion are not fully captured by industry loss performance, since the insurance limit purchased was far less than the expected ultimate economic loss. The largest multi-insured loss arising from a cyber attack is the NotPetya event in 2017, estimated by Property Claim Services (PCS) at more than US three billion. However, due to underinsurance and low product penetration by the affected businesses, most of that loss will likely fall to the non-affirmative insurance market.

There is consistency with the scale of financial impacts as a result of cyber events, regardless of line of business:

- Cybercrime costs are predicted to hit US six trillion annually by 2021. This followed a record year in 2017 of US 600 billion
- The World Economic Forum's 2019 cybercrime estimates put economic losses from cybercrime at US three trillion in 2020
- In the *"Bashe Attack: global infection by contagious malware 2019,"* the global economy is described as underprepared, with 86 percent of the total economic losses uninsured, leaving an estimated insurance gap of US 166 billion"

IDENTIFYING VULNERABILITIES

After analyzing enterprise data for millions of companies worldwide, including:

- Organizational footprint: assessed against factors internal and external to the enterprise, enabling a comprehensive view of key technology dependencies and the "attack surface" available to malicious actors
- Organizational attractiveness: measuring a range of assets and characteristics that could provide a motive for any class of threat actor to target the enterprise
- Cyber vulnerabilities: derived from analysis of internal and external telemetry. This holistic view enables measurement of the relative success rate of cyber attacks
- Cyber security posture: measured against a wide range of indicators that provide insight on the quality of security in place

A few key technology dependencies recur and manifest as potential vectors for a widespread cyber attack on multiple companies across multiple geographies at one time. We call these Single Points of Failure (SPOFs). Key SPOFs that could lead to the costliest losses include: operating systems providers, email service providers, cloud service providers and critical utilities providers.

Many cyber underwriters consider the cloud to be a major SPOF in causing a systemic cyber attack. Adoption of the cloud for business use is certainly increasing dramatically. A LogicMonitor survey in 2018 suggested that 83 percent of companies will be using the cloud by 2020. There is less understanding within the insurance industry of the implications of cloud services. The cloud is not one service, but rather several different types of service — storage, computational power, backup services and so on — and the dependencies on these vary.

However, our study found that major cloud service providers are just one class of SPOF generating catastrophe loss. Other SPOFs that should be considered include operating systems providers, email servers and critical infrastructure providers, because these also serve as points of aggregation, thus enabling a systemic loss in the event of cyber security failure.

We strongly believe that taking a robust, modeled and forward-looking view of cyber catastrophe risk can help enable the cyber insurance market to grow sustainably. Ultimately, sustainable growth will better position insurers to bridge the protection gap for businesses and form lasting partnerships as part of robust cyber security frameworks.

Leslie Chacko
Managing Director,
Marsh & McLennan
Advantage, Solutions

Wolfram Heidrich
Partner, Risk and
Finance Practice,
Oliver Wyman

Rachel Lam
Consultant,
Oliver Wyman

WINNING THE CYBER RISK CHALLENGE:

Rapid digitalization in the energy/power sector continues to outpace cyber readiness

The Energy/Power (E/P) sector's speed of digitalization is outpacing its building of cyber defense capabilities and adaptation of overall risk management strategies. Marsh & McLennan Advantage Insights analyzes the *Marsh Microsoft 2019 Global Cyber Risk Perception Survey* to explore the latest cyber trends in the transitioning E/P landscape and propose strategies to proactively measure and manage cyber risks.

A SHIFTING PLAYING FIELD

Many organizations in the E/P sector are now facing two overarching challenges that are shifting the threat landscape.

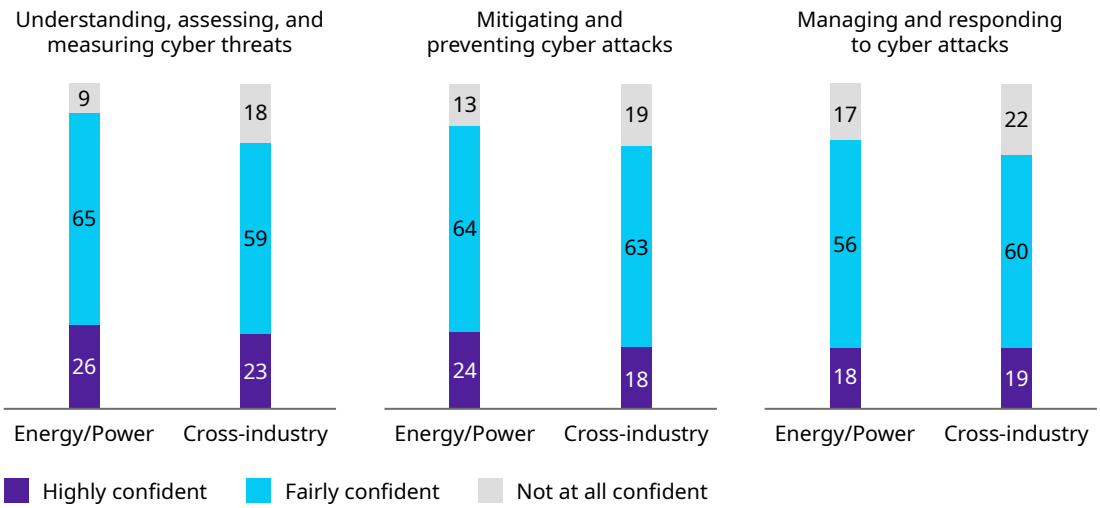
Internal Challenge: Digitalization in the sector is outpacing its cyber defense capabilities

While digital transformation is positively reshaping the sector by reducing operational costs, improving profitability, and enabling faster and more effective decision-making; it also introduces a new set of risks to be managed, such as weaker security baselines and the use of potentially insecure data storage systems and data communication.

While cloud computing is perceived to have the greatest business benefit by respondents (65 percent) in the sector, the perceived level of cyber risk associated with it among respondents is higher than for most other technologies (26 percent), due to potential weaknesses in program interfaces and outside access to data.

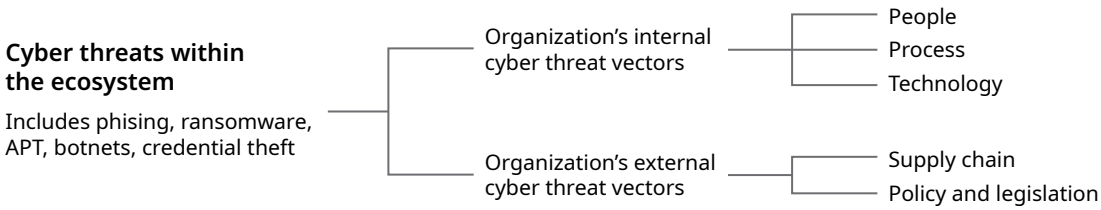
While the sector is aware of the risks, there are concerns that it is not adequately equipped to deal with cyber threats — or perhaps overconfident in its ability to do so. When compared to the cross-industry average, respondents from the E/P sector are more confident in understanding and mitigating cyber risks but are just as insecure when it comes to recovering from cyber incidents.

Exhibit 1: Percentage of perceived confidence among energy/power organizations in:



Source: Marsh Microsoft *2019 Global Cyber Risk Perception Survey*

Exhibit 2: Cyber threats attributable to internal and external threat vectors



External Challenge: E/P organizations are increasingly targeted by sophisticated cyber attackers

Both publicly and privately-owned E/P organizations have become prime targets for criminals and hostile governments. In many cases, the ability to disrupt enemies by bringing down the systems on which they depend has become a more central part of their strategy than conventional warfare. As such:

- 60 percent of respondents are highly concerned about the potential harm that a nation-state cyber attack could have on their business
- 53 percent agree that governments need to do more to help protect E/P organizations against nation-state cyber attacks

BETTER ORGANIZED "OPPONENTS"

Taking a closer look at the external challenge, the E/P sector faces increasing exposure to sophisticated cyber adversaries that can disrupt the sector more easily than events such as earthquakes, physical attacks, and operational errors.

Within their respective ecosystems, organizations need to focus on several internal and external cyber threat vectors to understand their overall cyber exposure.

Internal cyber threat vectors remain the most urgent yet understated sources of cyber risk for any organization and industry. Yet, the sector has some way to go in ensuring that cyber risk management is truly "risk-driven", integrated as a top-down organization-wide shared responsibility. 90 percent of E/P survey respondents indicated that cyber risk responsibility sits mainly within IT, and only 48 percent indicated that the responsibility sits mainly with their risk management team.

With regards to process, the sector has taken a more proactive approach on cyber risk compared to other industries, though these actions are still largely centered on basic preparation and prevention. Out of the E/P organizations surveyed:

- 91 percent of have made improvements in hardware security
- 84 percent in data protection capabilities
- 77 percent implemented awareness training
- 71 percent strengthened their cyber security policies and procedures

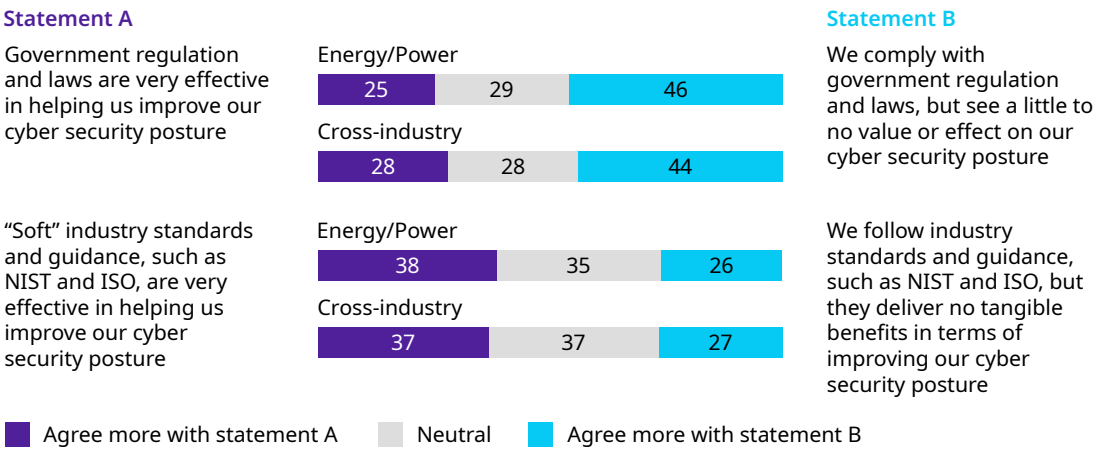
From a technology standpoint, the evaluation of cyber risks should be an end-to-end process with the understanding that cyber risk is a systemic business risk. Currently, a majority of the organizations assess their cyber risks during the initial phase of the project. Almost two-thirds of companies across all industries do so during the testing phase, and almost half of the E/P respondents (47 percent) note that their organizations also do so during the onboarding/implementation stage.

External cyber threat vectors stem from the growing supply chain, including trusted partners, and the evolving regulatory landscape that is seeking more accountability.

Supply chain risk is growing exponentially. As infrastructure rapidly modernizes, and pressure mounts to move operations to the cloud, players become more reliant on and integrated into third-party operations. More and more systems are increasingly interconnected, with interdependencies across the supply chain, and this interconnectivity will only continue to increase.

This raises the stakes for all organizations in the supply chain to maintain cyber resilience, as they now operate in ecosystems that are exposed to weaknesses in other companies, which may not have the same focus on cyber risk management.

Exhibit 3: Across industries, organizations' perspectives on the value of regulations and standards



Note: Percentage of organizations agreeing with each of the statements (presented to respondents as a trade-off)
Source: Marsh Microsoft *2019 Global Cyber Risk Perception Survey*; Marsh & McLennan advantage insights analysis

According to 38 percent of E/P sector respondents, partners in the interconnected supply chains of the E/P sector faced a bigger threat from cyber risks than perceived by their own organizations.

From a policy and legislative perspective there has been a significant increase in the regulation of data privacy and cyber security globally and across all industries, with a primary focus on data protection and supply chain security.

Regulation and cyber threats were highlighted as the topmost concerns in the E/P sector. In terms of what type of standards works (or not) for the E/P sector, there are mixed perceptions on the effectiveness of "hard" government regulations and laws in helping organizations improve their cyber security posture across all industries.

HOW TO WIN

With the embrace of transformative technologies and a long-term move towards cleaner energy sources, most players in the E/P sector have already shifted from mechanical and centralized assets to new operational-plus-digitalized systems that will increasingly expose each player in the ecosystem to cyber risks.

In order to win this digital-cyber challenge, organizations need to advance their cyber resilience by pursuing a range of cyber strategies and building up a portfolio of cyber capabilities. The focus should be equally placed on both cyber risk management as well as innovating with technologies. It will be prudent for organizations to consider embedding cyber throughout their digitalization journey, or risk favoring one at the expense of the other.

CYBER ATTACKS — THE INCREASING RISKS FOR RETAIL

Stephen Picard
Principal, Retail,
Oliver Wyman

James Bacos
Global Retail and
Consumer Goods Practice
Leader and Russia Lead,
Oliver Wyman

Read the full article here

Compared to other industries, retail is more vulnerable to cyber attacks due to the nature of its online traffic and the design of its e-commerce websites. As retail increasingly shifts to a digital environment — particularly as COVID-19 accelerates online purchasing — it is more important than ever for retailers to invest adequately in cyber security safeguards.

How are retailers being attacked?

Mobile in-store payments

Attackers obtain access to customers' log-in credentials for in-store payment apps. This is seen as lower risk, as items are received immediately

Buy online, pick up in store

This purchasing method is attractive to scammers as the turnaround time between online purchase and in-store pick-up is relatively quick

Add new payment

Attackers upload stolen credit card information into existing accounts to leverage on good purchasing history, increasing the likelihood of their fraudulent transactions being approved

Return without receipt

Hackers hijack an account and purchase items online, then return the items in-store without the receipt

Steps retailers can take to mitigate cyber risk

Embrace secure payment processes

Unlike traditional credit card payments, mobile wallets utilize tokenization, which allows payments to be processed without exposing actual account details that could potentially be compromised. Additionally, retailers need to keep up with industry payment standards such as PCI DSS, to ensures all parties involved in accepting, processing, storing, or transmitting credit card information maintain a secure environment

Train your employees and verify their activities

Cyber security training programs need to educate employees on best practices, such as the importance of using virtual private networks (VPNs) when working remotely, how to identify phishing scams, using strong password protection, enabling firewall protection, and more. Companies should also vigilantly monitor data flow and usage within the enterprise

Examine vendors' cyber security preparedness

Companies must proactively examine their suppliers' cyber security capabilities and maintain an up-to-date blueprint on how to prevent security breaches from compromised vendors

Stress test the system

Companies should regularly try to "hack" their own systems to better understand their cyber security weaknesses and institute proper improvement measures ahead of real attacks

Confirm rapid-response capabilities

Executives should know what they need to communicate to a broad range of stakeholders — regulators, employees, customers, counterparties, and investors — to get their company back up and running quickly after a cyber attack. Insurance arrangements should also be updated to mitigate the financial impact of future cyber attacks

Re-examine service outages

Glitches are often a sign of hackers testing their target's cyber defense systems. If a system has experienced an unusual glitch that was initially attributed to technical faults, it should be reexamined to unearth potential hacker activities

Source: *Cyber Attacks — The Increasing Risk For Retail by Stephen Picard and James Bacos*

03. CURRENT AND EMERGING REGULATIONS

Siobhan O'Brien
Head of International Cyber Center of Excellence, Guy Carpenter

Erica Davis
Managing Director and Cyber Risk Strategy Leader, Guy Carpenter

SILENT CYBER — NO LONGER SILENT?

Silent (or non-affirmative) cyber refers to cyber-related exposure within many all-risk general insurance products. If no explicit cyber exclusion applies, coverage for losses caused by cyber perils may apply. This underlying exposure's potential for aggregated loss is currently one of the major issues being considered by the re/insurance industry.

BACKGROUND

The 2017 NotPetya and WannaCry cyber events demonstrated the very real existence of cyber exposure, with economic losses exceeding US eight billion and insured losses estimated at US 3.6 billion on both affirmative and non-affirmative (silent) covers globally.

In 2016, the UK Prudential Regulatory Authority (PRA) carried out a thematic review involving a range of stakeholders including insurance and reinsurance firms, re/insurance intermediaries, consultancies, catastrophe modeling vendors, cyber security and technology firms, and regulators. The results of that review were an expression of concerns about the materiality of silent cyber as a risk to re/insurance companies and a recommendation that firms needed to identify clear ways of managing "silent" cyber risk, set clear appetites and strategies that would be owned by boards and invest in cyber expertise. Subsequently in 2017, the PRA issued their Supervisory Statement SS4/17 setting out their expectations of firms regarding cyber insurance underwriting risk.

In January 2019, all UK-regulated insurers received a further letter from the PRA confirming that they "should have action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover."

In July 2019, Lloyd's issued its Market Bulletin Y5258, and updated this in January 2020 with the follow up Market Bulletin Y5277.

The update required all syndicates to provide clarity on the cyber exposure in all their policies, giving clients contract certainty and a clear understanding of the coverage provided by their policies. This requirement was introduced to ensure that cyber risks and accumulations are understood by all relevant stakeholders, from the boards of directors to junior underwriters, pricing and capital actuaries and exposure analysts.

This approach, which will be phased in over the course of 2020 and 2021, is particularly focused on driving the eradication of silent cyber from traditional lines of insurance by encouraging insurers to identify the exposure and either clearly exclude or affirmatively include it. Insurers should appropriately quantify the risks on an expected basis for pricing and assess the potential for attritional and extreme events. Subsequently, they can reduce the likelihood of silent cyber claims accumulation by identifying classes of business and policy types that are particularly vulnerable to residual silent cyber loss leakage and developing approaches to pricing and capital setting for such cyber risks.

Globally, we have seen regulators issue similar statements on managing silent cyber risks, including the European Insurance and Occupational Pensions Authority and the National Association of Insurance Commissioners in the United States issuing their guidelines to help firms manage this risk.

SAFEGUARDING THE SUSTAINABILITY OF THE INSURANCE MARKET

The goals of Lloyd's and global regulators are to safeguard the sustainability of the insurance market, provide contract certainty for clients and drive innovation of new cyber products to fill the evolving needs of clients.

One of the challenges in achieving the changes necessary lies in the fact that there is no globally agreed upon definition of what constitutes "cyber." Across various classes of insurance, the differences become apparent as some clauses refer to "cyber events" while others refer to the use of "software." Certain clauses deal only with malicious cyber events, some refer to "systemic" risk and others impose conditions related to an insurer's ability to demonstrate the adequacy of their cyber security. This anticipated lack of consistency presents considerable challenges, though underwriters are actively taking steps to address the issue. Approaches underwriters are taking include:

Exhibit 1: Cyber risk approaches adopted by underwriters

Affirmation	Positively affirm where cyber exposure exists in the policy
Affirmation but with sub-limits of the cover available	Positively affirm where cyber exposure exists in the policy and cover will then be provided with a sub-limit to that element of cover
Exclude all exposure	Exclude on an absolute basis any loss from cyber exposure. Typically, these cyber exposures will be defined
Exclude, but write back in specific areas of cover	Exclude on an absolute basis any loss from cyber exposure, but provide specific write-back for a list of perils according to appetite

Source: Guy Carpenter

RELIANCE ON INFORMATION TECHNOLOGY

As companies depend more on technology to conduct business, they are also increasingly subject to technology's unique vulnerabilities. These are wide-ranging and can include system or supply chain disruption or failures, distributed denial of service, hacking and ransomware attacks that may result in increased costs and lost revenue. The timing and severity of these issues can be difficult to predict, and companies increasingly look to their insurance policies to cover business interruptions stemming from these events. Businesses would traditionally have relied on their property policies for this coverage; however, property insurers have been reluctant to address this financial, non-physical loss and have been pushing their clients to purchase cyber-specific policies for these risks by excluding this coverage under their property policies.

SILENT CYBER CASE LAW DEVELOPMENT

Recently there have been many high-profile legal cases where coverage has been denied by insurance providers. Media coverage has criticized insurers for not paying cyber claims, compounding the impression that cyber policies do not pay. However, none of these cases involves a cyber policy denying cover, but clients seeking "silent cyber" coverage under traditional policies.

Case law involving silent cyber claims has the potential to expand re/insurer exposures significantly. In a recent Maryland federal court case, National Ink and Stitch, LLC (the insured) sued its insurance provider (State Auto Property and Casualty Insurance Company) over their decision to deny its property damage claim following a ransomware attack. State Auto argued that because National Ink only lost data, "an intangible asset," and the computers National Ink was seeking to replace were not inoperable, the cyber attack damage did not meet the criteria of a "direct physical loss."

However, the court ruled in favor of the insured, noting that the policy in question expressly lists data as an example of covered property, and contains the phrase "including software" in its heading describing covered property. Though National Ink's computers still functioned after the attack, the Judge found that the overall damage to the efficiency of the computer system also constituted physical loss or damage.

Despite this, it is important to clarify that Maryland courts "have not expressly decided whether data or software can be susceptible to physical loss or damage."

With the increasing prevalence of ransomware and coverage being sought under non-cyber policies, we will undoubtedly see a rise in legal disputes around coverage and further clarification of intent of coverage under these policies in the future.

WHAT DOES THE FUTURE HOLD?

To mitigate of the potentially catastrophic impact of silent cyber within non-cyber lines of business, re/insurers require an effective means of qualifying and quantifying the risk of silent cyber across their whole portfolios.

Regulators and re/insurers will all continue to clarify their respective intentions and appetites for cyber in standalone policies and inclusion of cyber in traditional lines. This should give clients greater clarity of the intent of coverage under their insurance contracts, though there will be some tough negotiations in situations where clients believe they are potentially losing coverage.

TWO YEARS ON, GENERAL DATA PROTECTION REGULATION (GDPR) CONTINUES TO SHAPE GLOBAL DATA PRIVACY REGULATION

When introduced in 2018, the GDPR was a ground-breaking data privacy law, marking a global shift towards more aggressive data privacy laws and enforcement. The scheduled two-year evaluation report by the European Commission (EC), published June 24, 2020, heralds the GDPR's success in strengthening individuals' rights to personal data protection. It also finds that the GDPR is proving flexible to support digital solutions in unforeseen circumstances, such as the development of tracing apps during the COVID-19 pandemic.

The evaluation notes the existence of "inconsistencies" between guidelines provided by the European Data Protection Board (EDPB) and at the national level, and emphasizes the need for Member States to "allocate sufficient human, financial and technical resources to national data protection authorities" so that they can effectively perform their work and ensure that national guidelines are fully consistent with those issued by the EDPB.

It also recognizes the challenges the GDPR may present for small and medium sized enterprises (SMEs), and calls for "intensified and widespread" provision of tools and initiatives by data protection authorities to help support SME compliance efforts.

The impact of the GDPR can be seen in cyber insurance claims. There has been an uptick in data privacy losses in Europe, based on Marsh clients' experience, but business interruption incidents like ransomware attacks continue to account for the lion's share of large cyber event losses in Europe. Still, data breaches, while generally resulting in lower losses than other cyber events such as business interruption, require more work by organizations to prepare for and respond to under GDPR requirements.

SPURRING GLOBAL REGULATIONS

Even as interpretation and enforcement of the GDPR continues to evolve, it has put data privacy squarely on the global map. For many countries, GDPR has served as a catalyst and a reference point for drafting new data privacy laws, overhauling existing laws. While there are variations, these data protection laws follow common themes — increased privacy rights for consumers, new and/or stricter obligations for businesses, and greater powers for regulators.

The following is a non-exhaustive summary of notable developments in several countries:

US/California

While there is no overarching federal data privacy law in the US, individual states are beefing up their laws. One of the most significant data privacy laws passed after GDPR implementation is the California Consumer Privacy Act (CCPA). The CCPA became effective on January 1 and enforced as of July 1, 2020 and enacts some of the broadest privacy protections in the US. Much like the GDPR, the CCPA introduces new privacy rights for consumers, with significant financial implications for non-compliance and the risk of legal private right of action in the event of a data breach. Other states are expected to eventually adopt similar laws.

Canada

Last year the government published its landmark Digital Charter, which kickstarted the process of modernizing the country's main data privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA). Current proposals could significantly broaden the scope of federal privacy law in Canada by potentially imposing severe monetary penalties, new statutory rights and giving far greater enforcement powers and resources to regulators.

Brazil

Brazil was one of the first countries to closely emulate the EU's GDPR when it passed Lei Geral de Proteção de Dados (LGPD), its first comprehensive data protection regulation. This will establish a new National Data Protection Authority, create fundamental rights for individuals, and require businesses

to report data breaches. Like the GDPR, the LGPD is extra-territorial in its reach, as it applies to any business processing the personal data of Brazilians, regardless of where the organization is located.

Australia

Australia introduced tough data breach notification requirements in 2018. The latest proposals would establish more stringent laws regarding organizations' use of data. The ongoing review of the 1988 Privacy Act will consider strengthening consumer rights by broadening the definition of personal information and introducing concepts such as consent and the right to be forgotten.

New Zealand

New Zealand's long-awaited Privacy Bill was passed through Parliament in late June and is due to be implemented on December 1, 2020. Among the key reforms is the introduction of mandatory notification of harmful privacy breaches to increase transparency. This means that if organizations have a privacy breach that poses a risk of serious harm, they are required by law to notify the Privacy Commissioner and affected parties.

India

India introduced its first-ever comprehensive data privacy law, the Personal Data Protection Bill, in 2018. The bill, yet to pass, is based largely on the GDPR and contains many similar concepts, including breach notification requirements, rights for data subjects, and an extra-territorial scope. It also envisages the creation of a new regulator, the Data Protection Authority of India, with substantial enforcement powers.

Singapore

Key proposed amendments to the Singapore Personal Data Protection Act (PDPA) include the increment of financial penalties and enhanced enforcement powers. Currently, organizations in breach of the PDPA are liable for financial penalties of up to one Singaporean million dollars. The draft bill outlines a maximum financial penalty of the greater of 10 percent of an organization's annual turnover or one Singaporean million dollars. Proposed changes include a mandatory notification regime which requires organizations to notify regulators and the affected individuals of data breaches within a specified timeline.

Thailand

Thailand's Personal Data Protection Act (PDPA) was published on May 27, 2019, with most but the government has temporarily postponed its application due to COVID-19. The PDPA, which has extra-territorial jurisdiction, includes provisions on collecting, consent, use, and disclosure of personal data; rights of data subjects; liabilities; and penalties. This legislation allows for criminal penalties — including up to one year imprisonment — and civil liabilities, including punitive damages of up to twice the value of the actual damage.

China

There is no single comprehensive law on data privacy in China. Data privacy and regulation is covered under a number of sector specific, consumer, and cyber security laws and regulations regarding data handling practices, supplemented by a number of non-binding national standards. However, in December 2019, Chinese authorities announced that the enactment of new Personal Data Protection Law and a new Data Security Law would be a matter of priority in 2020. It is expected that the legislation will consolidate existing data protection principles in China.

Vietnam

In December 2019, Vietnam published a draft Decree on Personal Data Protection, future versions of which are expected to include elaboration on the rights of data subjects, measures to protect personal data and the establishment of competent authorities responsible for personal information protection. Foreign and domestic online service providers are already required to store the personal data of citizens in Vietnam. Offshore service providers are required to open representative offices in Vietnam to meet the data localization laws and comply with cyber security laws.

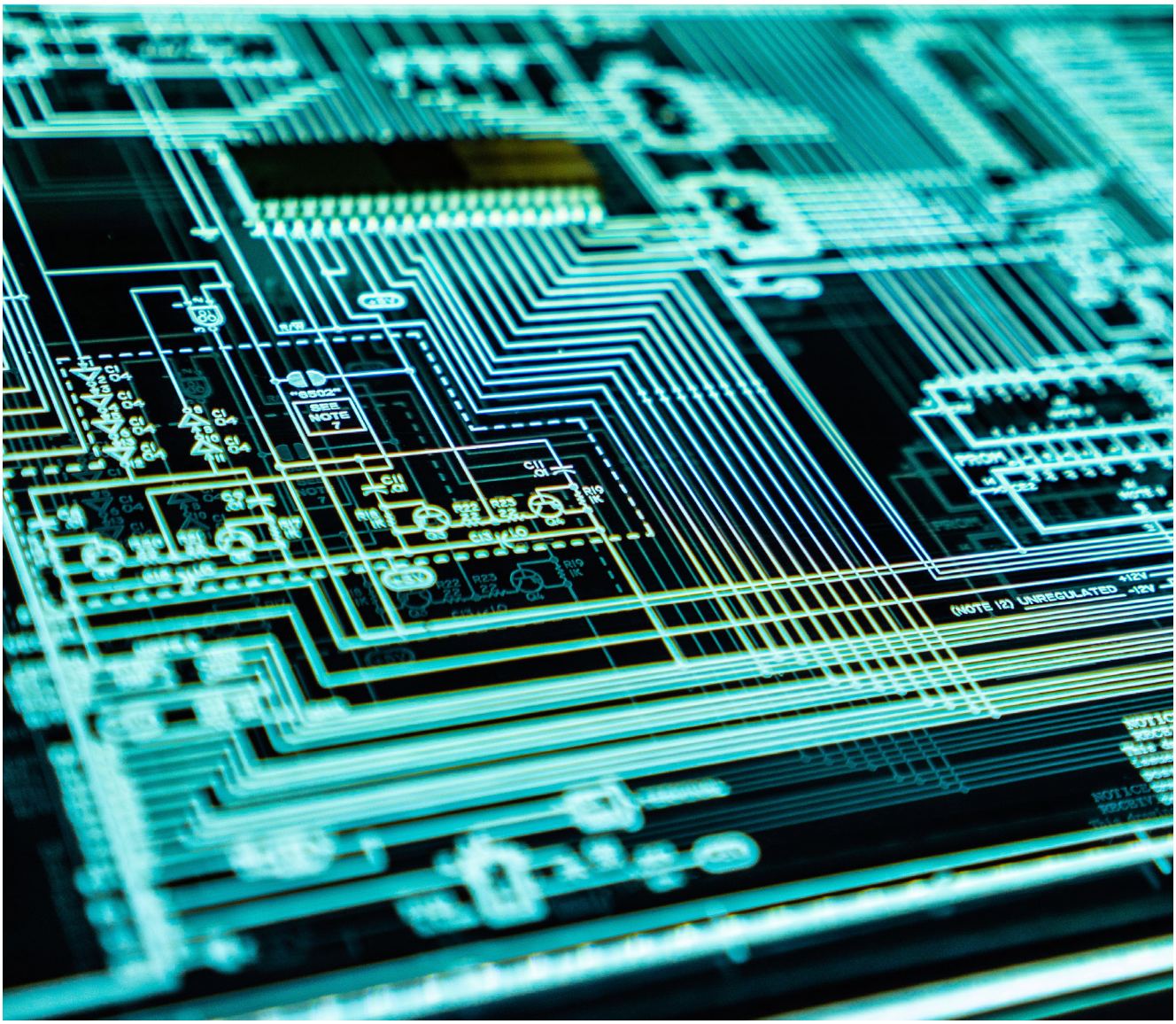
South Korea

South Korea's Personal Information Protection Act (PIPA) imposes strict security requirements on organizations that hold or process personal data, and places tight limits on the sharing and use of such data. In January 2020, the government amended PIPA to clarify the concept of personal data and strengthened the regulator's powers. The country is in the process of rolling out the Cyber Liability Insurance Regulation, which requires companies operating in certain sectors — including financial institutions and information communication service providers — to carry cyber liability insurance or alternative means to compensate damages.

MONITORING AND PREPARING FOR MORE REGULATION

In this fast-evolving regulatory landscape, organizations must stay informed, continually assess which regulations they are subject to, and implement compliance action plans that include an assessment of related enterprise risk. Doing so for new regulations may be a lighter lift for those organizations that have already performed this exercise for GDPR or other regulations. Even companies that are not presently subject to new regulations should assess their data collection practices as there is a strong likelihood that more nations will soon pass their own legislation.

Risk professionals should consult their advisors and insurance brokers about adopting insurance policy terms and conditions to address their organizations' widening exposures. Companies should review applicable insurance wordings, with a focus on the potential insurability of fines, penalties, and financial liabilities.



Allison Pan
Senior Vice President, Emerging Risks, Marsh

Jennifer Lawson
Senior Vice President, Legal and Claims Practice, Marsh

WITH THE COMMENCEMENT OF CCPA ENFORCEMENT, NOW IS THE TIME TO PREPARE AND MEASURE ITS POTENTIAL IMPACT

In July 2020, The California Attorney General's Office began enforcing the privacy protections enacted in the California Consumer Privacy Act (CCPA), a first-of-its-kind law for the US. Businesses — many of which were focusing on the COVID-19 pandemic — had called on California's attorney general to delay enforcement, citing limited resources because of the pandemic and uncertainty about the law's final regulations.

However, CCPA enforcement commenced as planned on July 1. Therefore, organizations — including those not based in California but with customers in the state — must prepare for what could be significant financial implications, including potentially severe penalties for noncompliance. Risk professionals and others must quantify their organizations' exposure to the CCPA and other privacy regulations to articulate potential losses and manage financial risks.

While quantifying all risks in financial terms should be a priority, calculating even approximate financial exposures from the CCPA is bound to be complicated due to lack of historical data. Still, companies can assess their potential exposure by taking the following three actions.

01. BUILD OR REINFORCE A "PRIVACY BY DESIGN" PROGRAM

Similar to preparing for compliance with any privacy regime, the first step in CCPA preparation requires a company to confer with its legal and privacy counsel to consider a "privacy by design" approach to data collection, management, and retention. Such an approach would incorporate privacy into technology and systems by default. By integrating this approach into broader cyber security and information security programs and controls, you can establish a baseline culture of privacy readiness.

There is no one-size-fits-all approach; companies should tailor their privacy programs to their unique data needs and business models. At a minimum, a privacy program should account for information flows, existing data inventory and future data collection, and data retention. It should also incorporate appropriate policies and procedures for purpose-driven data retention.

For example, a data inventory can reveal all data assets held by a company that fall within the CCPA's purview. A comprehensive data inventory is also useful in setting the foundation for compliance with future regulatory regimes in other states.

Data inventories often exclude the information flow and data shared with third parties and vendors. As part of their inventory process, companies should consider re-examining their data sharing practices, contractual relationships, and obligations that either they or their vendors have with regards to data.

By challenging and assessing current data practices, a by-design approach can help companies to shift their privacy culture away from a compliance checklist and instead move toward a holistic understanding of data. This deeper understanding lays the groundwork for a more accurate assessment of regulatory risk, one that takes into consideration not just the CCPA but also other potential future regulations that may address the growing concern over corporate monetization of private information.

02. CALCULATE MAXIMUM PENALTIES

The CCPA includes two distinct categories of financial losses that could result from noncompliance: private right of action damages, either individually or as part of a class action, and regulatory fines and penalties. As organizations quantify the potential financial impact of the CCPA, they must consider both possibilities.

For comparison, the EU's General Data Protection Regulation (GDPR) — a landmark privacy regulation enacted in 2018 — also has a private right of action provision. However, some suspect that the risk may be greater under the CCPA because of the

litigation environment in California. While consumer class actions resulting in large settlements or judgments are commonplace in the US, European jurisdictions do not generally provide US-style class-action rights. Companies should confer with their legal counsel in assessing the likelihood and severity of this risk.

Organizations can start to calculate potential damages from a private right of action by measuring CCPA exposures based on the letter of the law. For example, since a private right of action can lead to statutory damages of up to US 750 dollars per incident, per consumer, an organization handling data of 200,000 California consumers could see damages of US 150 million for a single privacy violation incident.

Other consumer protection laws in California also provide useful insight. By analyzing litigation arising from other statutes that allow for a private right of action in California and their frequency and severity, businesses can better estimate their potential exposure under the CCPA.

03. EXAMINE EXPOSURE TO CYBER SECURITY EVENTS

The likelihood of an enforcement action or lawsuit under the CCPA closely aligns with the likelihood of a data or technology breach. Thus, in order to calculate the financial exposure arising from the CCPA, you should consider quantifying your overall cyber risk.

Cyber risk quantification starts with basic math: What assets or records do you have, and what would be the first- and third-party costs you would incur if these were lost, stolen, or jeopardized? What types of events are you most susceptible to given your specific threat environment and internal practices? And what areas of your business and data are vulnerable to disruption or damage?

Quantification can also include an honest assessment of an organization's cyber security posture: What controls and security measures do you have in place, and how effective would they be in preventing a breach or cyber-attack? Additionally, it is a good practice to analyze your cyber event history.

Breach modeling can also include a range of potential cyber event scenarios tailored to your specific organization, rather than industry generalizations. It should consider the potential financial impact of events of different severities and frequencies — for example, what would be the cost of a one-in-two-years event? What about the cost of a one-in-100-years event?

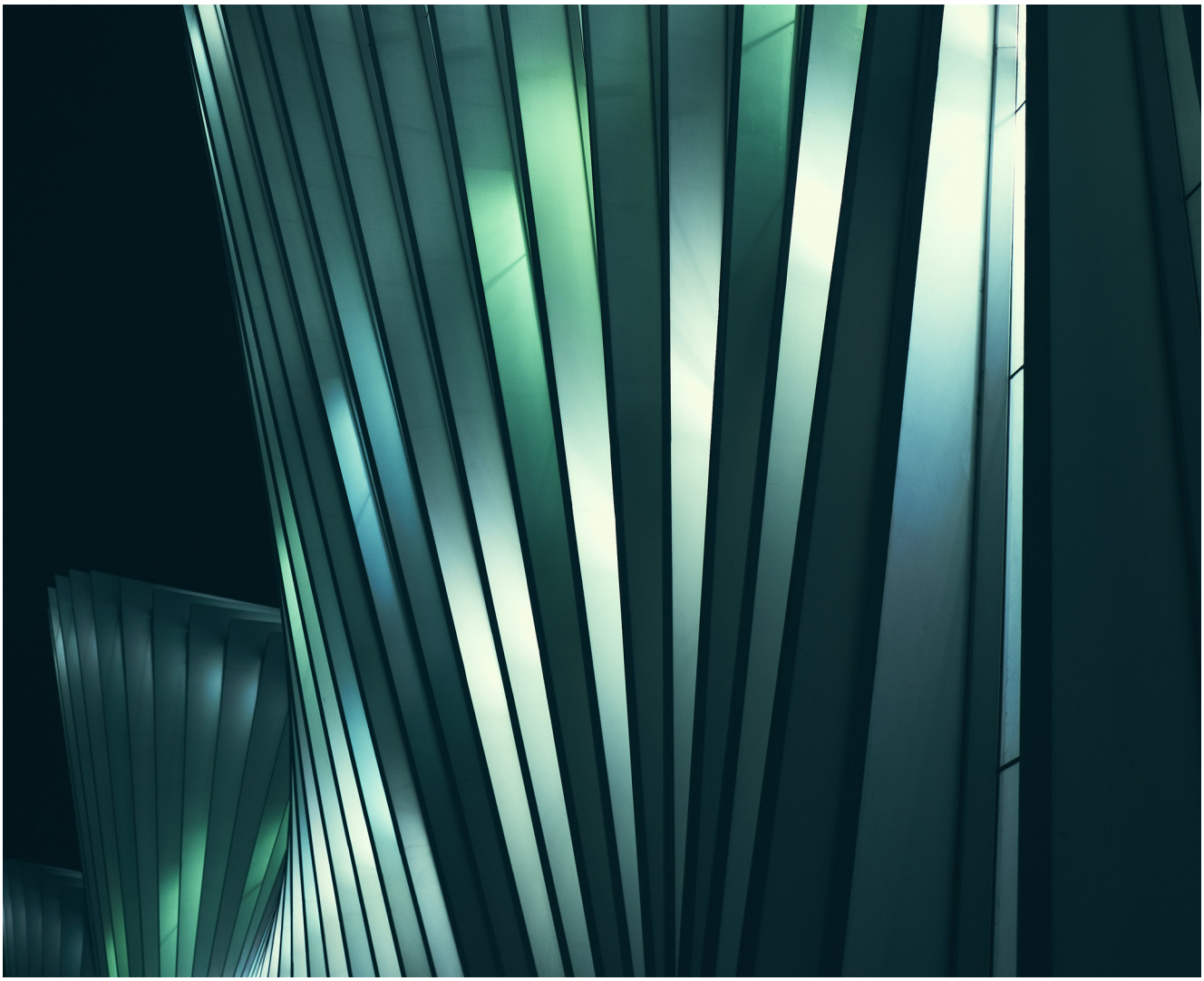
Once you have a clear view of the potential cost of your cyber exposures in general, you can layer on the further risk exposures presented by the CCPA, GDPR, or potential future regulations. The specific metrics and components of risk quantification will be different for every organization, but all companies should consider engaging in it — especially those subject to the CCPA or other privacy regulations.

Determining your exposures to cyber risk in general and privacy regulations specifically can help you make appropriate, data-driven investments and to prioritize technology, risk transfer, and other cyber risk management practices. However, given the fast-evolving cyber threat and privacy regulation

landscapes, that measurement should not be a one-time exercise. Instead, cyber risk assessment should be a continuous and frequent practice that incorporates changes in your own cyber security efforts as well as the external environment.

Finally, it's imperative to remain aware of changes in privacy regulation that could affect your organization, and be proactive in learning what consumer data protections are required by law. Focus on the reason behind the regulations and factors driving their implementation, including consumers' growing desire for privacy protections, and increasing expectations by consumers, regulators, and others for increased corporate accountability and responsible privacy stewardship. Organizations that understand the principles behind privacy regulations, conduct a thorough assessment of their exposures, and adapt their data practices and culture will position themselves ahead of the curve of new privacy regulations rather than constantly playing catchup to comply with new regulations.

04.
STRATEGY



Paul Mee
Partner, Digital and Financial Services, Oliver Wyman

Rico Brandenburg
Partner, Financial Services, Risk and Public Policy and Digital, Oliver Wyman

This article was first published by *BRINK* on November 5, 2019

HOW TO PROTECT DATA IN AN AGE OF DIGITAL SEAMLESSNESS

Think of how you currently book a vacation: the many steps you have to go through, the different companies you have to interact with and the time it takes. Now, imagine booking your annual vacation simply by clicking a "same as last year" button.

Your flights are booked, ground transportation scheduled, accommodation arranged with your particular requirements, insurance purchased, and gym membership paused for the two weeks you'll be away.

DIGITAL SEAMLESSNESS

This is called "digital seamlessness" — the integration of technologies to reduce user effort and hassle. It is the opposite of user friction. The above scenario is not far-fetched.

The trend toward digital seamlessness is accelerating; industries from finance to health care are increasingly using seamless technologies to make it easier for consumers to use their products and services. More than four billion people now own a smartphone, with many using them to buy groceries, manage finances, book travel, arrange deliveries or receive health care.

But the systems that enable these popular services also face a significant risk — large-scale cyber attacks that could expose valuable nonpublic information or, even worse, disrupt entire industries.

GREATER CONVENIENCE BRINGS GREATER RISK

The trend toward digital seamlessness is increasing cyber risk in several key ways. First, attractiveness of the target. The highly valuable data, such as personal and financial information, stored and produced by seamless technology, makes an attractive target for hackers and cybercriminals, who are motivated by financial gain.

Second, volume of data. As users disclose more personal information, for example, their geolocation, in exchange for a more seamless experience, companies collect and store this data in bulk. These massive stockpiles of information are especially appealing to cybercriminals, because a single hack could get them access to far more valuable data.

Third, concentration of risk. Take our travel example. If someone's phone was compromised, the loss could be significant. From one device, criminals could gather the consumer's personal and financial information and use that to charge up credit cards and drain bank accounts. Or even worse, access the biometric data used to secure the booking or your medical history via your travel insurance company. Credit cards can be replaced, but fingerprints cannot.

Fourth, increased attack surface. An attack surface is a connection point between different parts of apps or systems that need to communicate with each other. The same technology that enables consumers to seamlessly use their smartphones to deliver dinner or to reserve tickets creates additional attack surfaces — or connection points — that hackers can target. The more connection points, the more vulnerable a system.

To illustrate these dangers, consider the 2018 case of a major hotel data breach, which exposed more than 500 million customer records. In a pre-seamlessness universe, this may have been limited to a customer's stay and check-in information. Instead, details on the company's customer loyalty program, which makes it easier for consumers to book and use the hotel chain, were also breached, and cybercriminals accessed passport numbers and other information. These records could enable large-scale identity fraud with significant impact on consumers.

PRACTICE GOOD DIGITAL HYGIENE

The good news is that there are a number of measures that businesses can take to mitigate the additional risks introduced with digital seamlessness, without compromising user experience.

Support (and benefit from) the growing awareness of cyber risk in consumers and employees. Companies are spending more time and money to educate staff and even

their customers to avoid some of the most common and costly mistakes. Many cyber attacks could be prevented if people followed basic cyber hygiene, such as not trusting unknown sources with personal information and being circumspect regarding websites that appear real, but are not.

Most retail banks no longer ask customers to share personal information or to transfer money by email and phone, and many also use multifactor authentication via a phone or physical card reader. Customers also should not use the same login password for multiple online services.

These simple techniques would help prevent the majority of breaches. For example, a cloud storage company suffered a breach in 2012 that exposed 68 million records after an employee used the same credentials on work and personal accounts.

OPERATE ON THE 'NOT IF BUT WHEN' PRINCIPLE

Strive for "security by design" — focusing on building in system security from the outset. In an interconnected, seamless world, system elements have multiple complex interdependencies. These should be mapped out fully during the design process to eliminate security blind spots and mitigate exposure to penetration and disruption.

As a guiding philosophy, businesses should operate on the "not if, but when" assumption that defenses will be breached at some point. This puts the focus on timely detection and response, rather than purely on prevention. There is more work to do on this front, but progress is being made: In 2018, the global average dwell time (spent by attackers inside networks before detection) decreased by around 25 percent to 78 days, thanks in part to smarter and more rigorous monitoring of network activity.

KNOW YOUR PARTNERS

Perform thorough due diligence when integrating with third-party services to create a seamless experience. Companies may rely on an extended supply chain to offer a convenient service, but they should carefully evaluate both their upstream and downstream dependencies, along with any cyber risk this may introduce. Many organizations have recently improved their third-party risk management capability, limiting access to critical internal infrastructure, and establishing robust monitoring and visibility, such as through consolidated management dashboards.

VIEW DATA AS A LIABILITY

View data as a liability, weighing the benefits of collecting incremental consumer data that may enable them to marginally improve or tailor a product against the cost of a potential breach. At the end of the day, while consumers seek ease, they also value privacy. No one wants to have their identity stolen when they book a vacation.

The benefits of digital seamless are significant and exciting, but to quote a certain superhero, "with great power comes great responsibility." As digital seamlessness becomes more and more a part of our day-to-day lives, it is essential to have consistently strong cyber resilience across this fast-changing ecosystem.

Brian Warszona
UK Cyber Growth Leader, Marsh

HUMAN RESOURCES' INCREASING ROLE IN CYBER RISK MANAGEMENT

The human resources (HR) function has become integral to organizational cyber risk management in recent years. Along with information security/information technology (InfoSec/IT), HR is increasingly called upon to help determine and enforce employee data permissions, train and enforce cyber security policies and procedures, and help respond to cyber events involving employees.

HR's increased involvement is due to a convergence of factors, including: a more active regulatory environment, the pervasive use of technology and devices in employees' work, and recognition of the importance of a strong organizational cyber security culture.

Employees' data and security practices are critical determinants of an organization's overall cyber security. Almost two thirds (62 percent) of executives say the greatest threat to their organization's cyber security is employees' failure to comply with data security rules, not hackers or vendors, according to Mercer's 2020 Global Talent Trends Study.

Yet HR is not typically a primary owner or driver of cyber risk management, as found in Marsh and Microsoft's 2019 Global Cyber Risk Perception Survey. The great majority (88 percent) of companies continue to delegate cyber risk first and foremost to InfoSec/IT, followed by the C-suite, risk management, legal, and finance.

This needs to change. A strong partnership between InfoSec/IT and HR is essential for managing data and technology risk, particularly in a remote-working environment. Below we explore four key areas where the evolving regulatory and cyber risk landscapes are changing HR's role.

REGULATORY COMPLIANCE

Many regions around the globe and US states are implementing privacy regulations that set strict guidelines for how organizations collect and use consumer data. These include the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act, Illinois' Biometric Information Privacy Act, and the NYSDFS Part 500, among numerous others.

Many of these regulations carry heavy fines, penalties, and the potential for lawsuits, not just for data breaches, but also for improper handling of consumer data. Business leaders recognize the growing risk — ranking regulation/legislation the fourth top risk in our *2019 Global Cyber Risk Perception Survey*.

Responsibility for navigating privacy regulatory compliance is increasingly shifting toward HR in conjunction with InfoSec/IT.

HR has traditionally led training on safeguarding sensitive data and the secure use of devices and technologies as part of the onboarding process. Now HR is also often tasked with conducting privacy regulation training, in conjunction with IT, for employees and for third-party vendors engaging with the organization's data.

Determining internal accountability for errors and misdeeds usually falls under the remit of IT, compliance/legal, and third-party investigators. But given its role in managing employee compliance with organizational policies, HR logically is best positioned to provide guidance on the appropriate punitive or remedial actions for data handling misconduct or errors, as defined by the company's policies.

For this reason, IT, HR, and the C-suite need to be aligned in creating and implementing a robust data incident response plan, particularly for handling events involving employees. This can be aided by agreeing how their respective roles overlap in setting and enforcing data practices and policies, and how the organization will respond to any regulatory data violation.

EMPLOYEE DATA CONTROLS AND ACCESS

Determining appropriate standards for access and controls around sensitive data is a key part of a sound cyber risk management strategy. Here again HR is well-positioned to help determine which employee and corporate data is most critical, who in the organization needs access to it, and how to control this access. Often this is defined when an employee is hired and on-boarded.

The end of an employee's tenure at a company is also a pivotal moment when HR can play a vital role in supporting sound cyber security practices, with advice from the IT team. Several malicious insider cases have occurred after employment was terminated, regardless of whether by mutual decision or not. HR and IT need to be in sync around the termination process (and mutually agreed departures) so that data access rights are halted as soon as appropriate, usually upon or no more than 24 hours post departure.

DATA DISCLOSURES

HR also has an important role to play in helping to manage data disclosures and breaches. Whether accidental or malicious, such events can result in significant financial damage, legal action, reputational harm, and loss of consumer trust.

Information disclosures may extend to employees exchanging sensitive information within the office, or remotely around a "virtual water cooler," such as social media.

In the event of accidental disclosure or a former employee requesting the deletion of their information, best practices call for the incident response plan to define which department would field the breach or deletion notification, which would respond, and what the appropriate response would be. HR is often first to receive such a request from a former employee and their communication and direction with other functions is key to handling it appropriately.

Within most cyber incident response plans, assessing accountability for disclosure events is usually the primary remit of IT, in conjunction with third-party investigators. Again, however, given its role in helping establish and enforce compliance with company policies overall, HR is well placed to provide guidance on appropriate remedial or punitive actions.

Whether the disclosure or breach is accidental or malicious, HR policies governing the treatment of sensitive data and employees' social media activities — where those "virtual water cooler" discussions take place — are critical.

CYBER SECURITY CULTURE

HR is usually the first (and last) point of contact for employees, and therefore plays an important role in creating and maintaining a robust cyber security culture.

Although IT traditionally created cyber security training sessions, HR's involvement has increased as the importance of such training for employees has become better understood. Information provided to new employees about how to practice good cyber security hygiene in their daily tasks, can greatly affect their confidence if or when confronted by a scenario requiring them to mitigate a cyber risk.

Training should include guidance for recognizing and handling common scenarios, such as phishing and password security. It should also include how to handle the

organization's digital transformation and implementation of new technology, as well as best practices for bring-your-own-device, remote access, business continuity, incident response and recovery, and use of devices.

The COVID-19 environment makes training and policy compliance even more critical, given that work-from-home cyber security protocols and practices may not be as robust as normal office conditions.

A strong cyber security culture must also include consequences for non-compliant behavior. HR and IT need to collaborate to communicate the ramifications for not following best practice safety procedures, or not completing training — for which more employees are being penalized in their performance reviews and even compensation.

A robust cyber security culture starts from the top of the organization and involves continuous communication and training for leaders across all key functions. Table-top exercises — simulated cyber events that test a company's response — are highly useful for aligning the actions and priorities of IT, PR, risk management, C-suite, board members, and legal/compliance.

True enterprise cyber risk management programs include HR in these response testing exercises. Besides HR's important role in cyber risk management planning, its inclusion in event response planning can help align the contemplated treatment of employees with applicable employment regulations and laws and help mitigate the risk of potential litigation.

Karen Shellenback
Global Products Leader, Analytics and Research, Mercer

DON'T FORGET YOUR CYBER RISK SENTRIES

The exponential surge in the numbers of employees working from home (WFH) during the COVID-19 pandemic is increasing organizational cyber risk in terms of overall number of potential threats and the potential impact of those threats.

Every home device or wireless connection is a potential cyber risk entry point, yet for many employers maintaining business continuity through secure work from home (WFH) networks is more important than ever.

Not only has the number of risk vectors increased but unpredictability is creating some chaos in terms of normal. IT processes and situational decision making among both WFH employees and cyber risk staff — potentially leading to exposed loopholes. The tsunami of rapid response required of businesses to distribute their all workers, with less than five day's notice, has opened potential holes in the firewall for many organizations — holes that nefarious entities are continuously trying to exploit.

The situation is of course, exacerbated by the sheer number of at-home workers but also the stressors placed on IT and cyber risk staff to supply and support new remote modes of working. Cyber and IT staff in normal operating environments are under tremendous stress — their jobs often require monotonous technical work and dedicated attention spans. Under these new conditions, IT and cyber teams are operating on over-drive.

The unprecedented "stay home, work safe" situation has created further strains on over-stretched cyber risk and IT staff that can lead to more compromised risk and security breaches. Malicious actors are aware of and taking advantage of situational weak points.

PANDEMIC-RELATED CYBER CHALLENGES:

Normal security protocols and cyber hygiene practices are set aside. Immediate WFH measures can create situations in favor of rapid response setting aside security protocols. New hardware and software systems in these environments may have been deployed with reduced security. Most organizations did not pre-plan, run pandemic contingency scenarios, and stretch-test their technology and protocols for the sheer breadth and depth of the current situation.

Use of personal devices for work/business. While the good news is only three percent of corporate executives report that their organizations reduced security requirements for universal WFH, it seems that in one-quarter of organizations across the globe, IT and procurement could not handle the extra load in terms of buying or renting new laptops and therefore have allowed employees to use their personal technology at home for work. (Mercer COVID-19 survey live results.) This creates a potentially risky security challenge.

Overworked staff due to increased IT tickets/caseload. In addition, the IT team is tasked with immediate tech support resolutions for the hundreds or thousands of staff now using new systems and processes remotely. While everyone is adjusting to new modes of working, the workload for IT and cyber risk teams just became infinitely harder to manage. In this environment, shortcuts executed by overworked and tired IT/cyber risk staff is a concern.

Absences due to sickness or stress. Not only are IT and cyber staff responsible for getting potentially thousands of workers set up to work from home on new laptops and possibly new collaboration tools, but they must execute this work on top of normal cyber and IT responsibilities. A further challenge is absence due to stress and potential sickness of IT/cyber team members. "Organizations should prepare for temporary or permanent loss of key cyber staff and leadership, the evacuation of a Security Operations Center, or a serious attack where only a portion of staff are able to work."

Financial setbacks may lead to reduced cyber budgets. Everyone is squeezed and budgets are tight or gone. Corporate financial setbacks can negatively affect cyber risk

staffing and the prioritization of new effective technologies needed to mitigate the ever-changing risk environment.

Support from third party vendors may be reduced or impacted. Furthermore, third party vendors who supply technology and other SaaS services are also experiencing similar stress among their IT/cyber, customer service, and relationship management teams. Resolution of issues may take longer, patches may not be deployed, and again, some minor security protocols may be ignored in favor of the fastest, most expedited solution. Leadership needs to address these potential liabilities with all vendors.

If an attack occurs, incident response may be impacted. On top of all the above challenges, the impending danger of an imminent attack weighs heavily on the team. Companies are especially vulnerable given that it may take extra time to recognize an attack and/or respond in an optimal timeframe (compared to normal circumstances). Delays in response time creates exponential brand damage and financial loss.

COVID-19 RECOMMENDED CYBER RISK AND IT STAFFING TASKS:

Your cyber analyst and tech team are on the front lines mitigating the myriad of challenges. During the pandemic, the following are extra cyber risk protocols recommended for a widespread WFH business environment:

- Implement VPN (virtual personal networks) and MFA (multi-factor authentication) for all remote systems on distributed networks
- Include threats from insiders in risk assessments, especially those with WFH set-ups
- Ensure you have the people, processes, products (technology) to detect and respond to threats and risk across the full remote network
- Ensure remote access systems are fully configured, updated, and patched. Maintain the same overall security landscape for WFH networks as the traditional onsite configuration
- Run phishing campaigns to assess the current security landscape and uptake on the remote network
- Use endpoint detection and response (EDR) software to quarantine systems remotely if there is a breach
- Craft a secure remote access plan for privileged users. Track the access and use of highly sensitive/confidential accounts
- Ensure that the system access provided to employees is the minimum required for each role and function. Monitor access in the event of changes in jobs and locations
- Deactivate sensitive system access following employee termination and after employee role changes
- Use automated auditing software to track employee activity, establishing a baseline of “normal” activity against which unusual attempts at computer or file access can be measured. Monitor and audit employee network activities and suspicious behavior (logging on at odd hours, impossible locations, significantly increased export of reports from internal systems, regular access of unauthorized cloud storage sites, and no collaboration on this workload with others, etc.)
- Use data analytics software to scan email and social media posts to flag “disgruntled” employees. Look for potential malfeasance among “at-risk” employees and discuss scenario planning to address “at-risk” or “on-notice” employees with HR. The equipment of terminated employees may not be returned after termination — focus on terminating access to networks and systems.

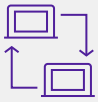
CYBER SECURITY AFTER COVID-19:

10 ways to protect your business and refocus on resilience

Thomas Fuhrman
Managing Director,
Cyber security
Advisory, Marsh

Read the full article here

Organizations need to de-risk and adapt to the "new normal." This requires a thorough evaluation of coronavirus-driven IT and cyber security changes, some of which were rapidly put in place during the response phase of the pandemic. Listed below are actionable ways in which enterprises can enhance their cyber security capabilities in 10 different cyber-related areas that require attention.



Teleworking solutions

Establish VPN capacity through the deployment of Internet Protocol Security (IPsec)-based VPN clients or other secure connectivity solutions to employee workstations

Supply chain and third-party management

Conduct cyber security audits and establish ongoing requirements for all third parties with authorized access to company networks, systems, or data

BYOD policy

Implement a company-issued mobile device management and BYOD policy, examine or reshape it and properly document any measures implemented during the pandemic

Cyber attack financial protection and recovery

Review existing insurance coverage and be aware of potential changes in terms and conditions at renewal as insurers assess losses and changes in claim patterns post-pandemic

Cloud services

Use a cloud access security broker (an on-premises or cloud-based software that monitors cloud activity and enforces security policies). This can help detect and monitor cloud usage within the enterprise, enforce related cybersecurity policies, alert administrators of anomalous data flow and guard against malware

External perimeter protection

Implement remote endpoint isolation and forensic capabilities that meet forensic chain-of-custody requirements and identify unauthorized activity

Secure collaboration tools

Move beyond conventional productivity tools and explore emerging capabilities such as augmented/ virtual reality and chatbots to enhance operations

Cybersecurity policy

Conduct risk assessments and identify enforcement mechanisms, such as multi-factor authentication, single sign-on, and automatic logout from unattended devices

Cyber operations

Disable split tunneling for VPN profiles to prevent remote employees from accessing the internet directly from their personal laptops while also accessing corporate information systems

Cyber incident breach response (CIBR) plan

Coordinate and cross-reference CIBR plans with disaster recovery, business continuity, and enterprise crisis management plans to create comprehensive crisis planning document sets

Source: *Cyber security after COVID-19 — 10 ways to protect your business and refocus on resilience by Thomas Fuhrman*

CONTACTS

Cyber Risk Leaders

Paul Mee
Partner, Digital and Financial Services and Cyber Platform Lead
Oliver Wyman
paul.mee@oliverwyman.com

Thomas Reagan
Leader, Cyber Practice, Financial and Professional Products (FINPRO) Specialty Practice
Marsh
thomas.reagan@marsh.com

Corrado Zana
Head, International Cyber Risk consulting
Marsh
corrado.zana@marsh.com

Siobhan O'Brien
Head of International Cyber Center of Excellence
Guy Carpenter
siobhan.obrien@guycarp.com

Reid Sawyer
Head, US Cyber Risk Consulting
Marsh
reid.sawyer@marsh.com

Sarah Stephens
Head of Cyber, International
Marsh
sarah.stephens@marsh.com

Erica Davis
Managing Director and Cyber Risk Strategy Leader
Guy Carpenter
erica.davis@guycarp.com

Editors

Leslie Chacko
Managing Director
Marsh & McLennan Advantage, Solutions
leslie.chacko@oliverwyman.com

Ben Hoster
Managing Director
Marsh & McLennan Advantage, Insights
ben.hoster@oliverwyman.com

Victoria Shirazi
Associate Director, Global Corporate Strategy
Marsh & McLennan Advantage, Solutions
victoria.shirazi@mmc.com

Lily Phan
Research Manager
Marsh & McLennan Advantage, Insights
lily.phan@oliverwyman.com

Toshin Sequeira
Research Analyst
Marsh & McLennan Advantage, Insights
toshin.sequeira@oliverwyman.com

ABOUT MARSH & MCLENNAN COMPANIES (MMC)

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 annual revenue of $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 redefine the world of work, reshape retirement and investment outcomes, and unlock health and wellbeing for 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.