MARSH & McLENNAN INSIGHTS

MMC Cyber Handbook 2019

Perspectives on Cyber Risk in the Digital Era

MARSH GUY CARPENTER MERCER OLIVER WYMAN

FOREWORD

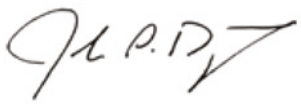
Cyber risk is a critical concern for business leaders. According to the World Economic Forum's 2018 Executive Opinion Survey of more than 12,500 executives, large cyber-attacks are ranked as the #1 risk for doing business virtually across all advanced economies. As companies develop their approach to this dynamic and challenging threat in 2019, there are some emerging trends that they should consider.

First, the growing use of technologies such as artificial intelligence, the Internet of Things, and robotics are broadening the cyber attack surface. While these technologies have significant potential to improve a company's productivity and efficiency, they are often being deployed without full consideration of the degree to which they might increase the firm's cyber exposure. Decisions around the deployment of new technologies need to consider increased cyber risk as an important part of the cost/benefit analysis.

Second, for many businesses, first party risk (not third-party risk) is now the primary cyber consideration. The potential financial loss from the theft of third party information in a cyber attack remains a critical issue. However, as organizations become increasingly dependent on technology for their core business processes, the cyberattack scenarios that create the greatest damage for many businesses are those targeting vulnerabilities within their own digital infrastructure and which can result in significant business disruption or property damage. Cyber risk planning needs to fully address both first party and third-party scenarios.

Third, as the mindset for approaching cyber risk planning, organizations need to internalize that it is not a question of "if" but "when" they will experience a major cyber event. This will rebalance the way companies invest and allocate their cyber risk management resources. While businesses need to continue to put processes and infrastructure in place to detect and deter potential cyber attacks, they also need to invest in processes which help them respond and regenerate after an event takes place. For many organizations, we see re-allocating resources from prevention to response as a constructive direction.

Against the backdrop of these trends, the 2019 edition of the *MMC Cyber handbook* includes our perspectives on major developments, specific industry implications, and strategies to increase resilience. It features articles from business leaders across Marsh & McLennan Companies, as well as experts from Microsoft, CyberCube, Cisco, and FireEye. We hope this handbook will help provide you with some new perspectives on how to increase your cyber resiliency in the face of this ever-expanding threat.



John Drzik

President, Global Risk and Digital
Marsh & McLennan Companies

TABLE OF CONTENTS

TREND WATCH

INDUSTRY DEEP DIVE

TREND WATCH

UNDERESTIMATING VOLATILITY IN THE CYBER INSURANCE MARKET

Ashwin Kashyap
Co-founder and Head of Product & Analytics, CyberCube

Cyber insurance is the fastest growing line of business in modern history, permeating most traditional lines of business with very attractive profit margins. What started as a cover to protect companies against hacking has now extended to cover business interruption, extortion, financial fraud, legal liability and system failure arising from cyberattacks.

But while cyber insurance teams have enjoyed the benefits of higher premiums and resulting profits, the broader market systematically underestimates the volatility of the underlying loss distribution.

DISCOUNTING FORWARD-LOOKING VARIABLES

Traditional approaches toward volatility quantification include the collection and analysis of loss information for decades in a relatively stationary world. For most firms, however, the model for volatility is far from robust due to limited clarity on modeled and non-modeled cyber risks. The volatility estimates are generally predicated upon knowledge derived from the space of known threat actors and known attack vectors along with historical near-misses and actual events. A perspective of this nature suffers from recency bias and has a tendency to provide a false sense of comfort to decision-makers.

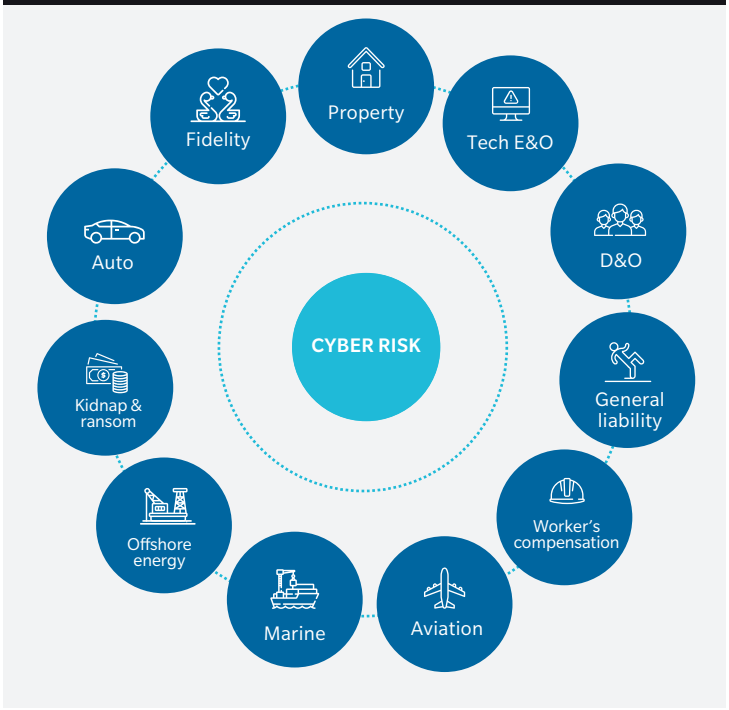
Forward-looking variables have played a relatively limited role in business decisions around pricing, capital allocation and reinsurance risk transfer. What is generally excluded is the space of technology developments, unknown threat vectors, emerging threat actor groups that render existing preventative measures obsolete. The implied volatility in the losses arising from cyberattacks is best estimated through a strong, fundamental understanding of developments in technology and relevant emerging threats.

Some examples have been provided below:

SCALED RANSOMWARE CAMPAIGNS

Ransomware has been successfully used since 2005 for the purposes of relatively small-scale financial gain by threat actor groups. Historically, the scale of a ransomware campaign has been quite minimal, and it is only in the last year that we observed patterns that demonstrated what an untargeted and indiscriminate ransomware campaign could lead to. While most models had considered ransomware as an attack vector, the scale was massively underestimated. The increase in volatility stemming from the dimension of scale within an existing attack pattern like ransomware was not considered in pricing cyber insurance policies.

EXHIBIT 1: CYBER RISK PERMEATES THROUGH THE MAJORITY TRADITIONAL INSURANCE LINES

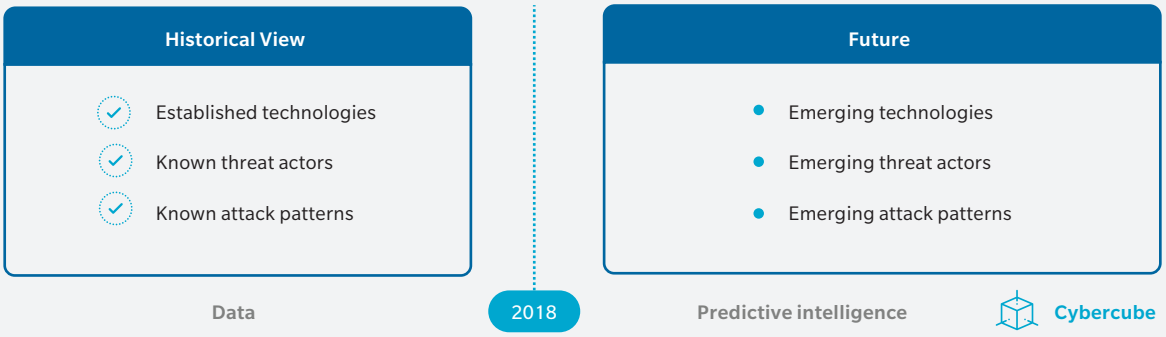


QUANTUM COMPUTING

Another example of a forward-looking technology trend that is not commonplace today is quantum computing.

Let's observe the link between quantum computing and cryptography. The core principle in cryptography is that large prime numbers are relatively easy to generate and multiply. However, factoring a large number generated using this method into two primes is hard using existing computing capabilities. If quantum computing capabilities at scale become available to nation state threat actors, systems that are built and secured using current encryption standards will be vulnerable. Encryption methods that cannot be cracked using quantum computing are lagging in their development in relation to the proliferation of quantum computing capabilities. This poses an existential risk to current encryption standards.

EXHIBIT 2: PREDICTIVE INTELLIGENCE
Leveraging new variables to enhance risk transfer decisions



INTERNET OF THINGS

When day-to-day appliances in a connected world have physical locks being replaced by digital locks and examples of weaponization of household appliances emerge, the exposure profile of insured entities changes quite dramatically. If homeowners' policies extended coverage to include cyber risk, existing pricing and reserving guidelines will not hold. There is evidence in the market that homeowners' policies provide the option of electing to insure cyber risk, but it is unclear whether such systemic exposures are considered for pricing decisions.

MASSIVE UNDERREPORTING OF BREACH INCIDENTS

Insurance products that have offered coverage against data privacy, availability and integrity have seen lower loss ratios and combined ratios when compared to other well-established lines of business across most market participants. One of the reasons for this is that a substantial majority of breached companies decide not to disclose publicly that they have been breached owing to reputational damage, legal liability and increased scrutiny from their customers and the public. An exception to this is when there is a disclosure requirement by law. The true frequency of breaches and the associated volatility has therefore been underestimated in most models that are used today.

This observation has led many insurers to offer cyber coverage at a substantial discount to existing policyholders from other lines of business with the goal of gaining market share. Because of these reasons, pricing levels are determined almost entirely by competitive dynamics as opposed to technical risk associated with the policies.

LACK OF LOSSES FROM LARGE-SCALE CYBER ACCUMULATION EVENTS

There have been several near-misses from an accumulation perspective in the last five years in the cyber insurance market. The absence of a large-scale industry-wide loss until 2017 resulted in the underestimation of volatility with the expectation that security defenses and business continuity plans of companies are equipped to handle business interruption resulting from a cyberattack.

This hypothesis has now been turned around completely. Months of downtime have been observed by companies that were impacted by *NotPetya*, the event that showcased significant accumulation impact with claims being made against property policies. This outcome was

unexpected and was not priced in to the policies that covered this risk, accidentally or otherwise. Such silent exposures exist for many insurers, leading to increased volatility in the risk profile of the carriers running large-scale P&C businesses.

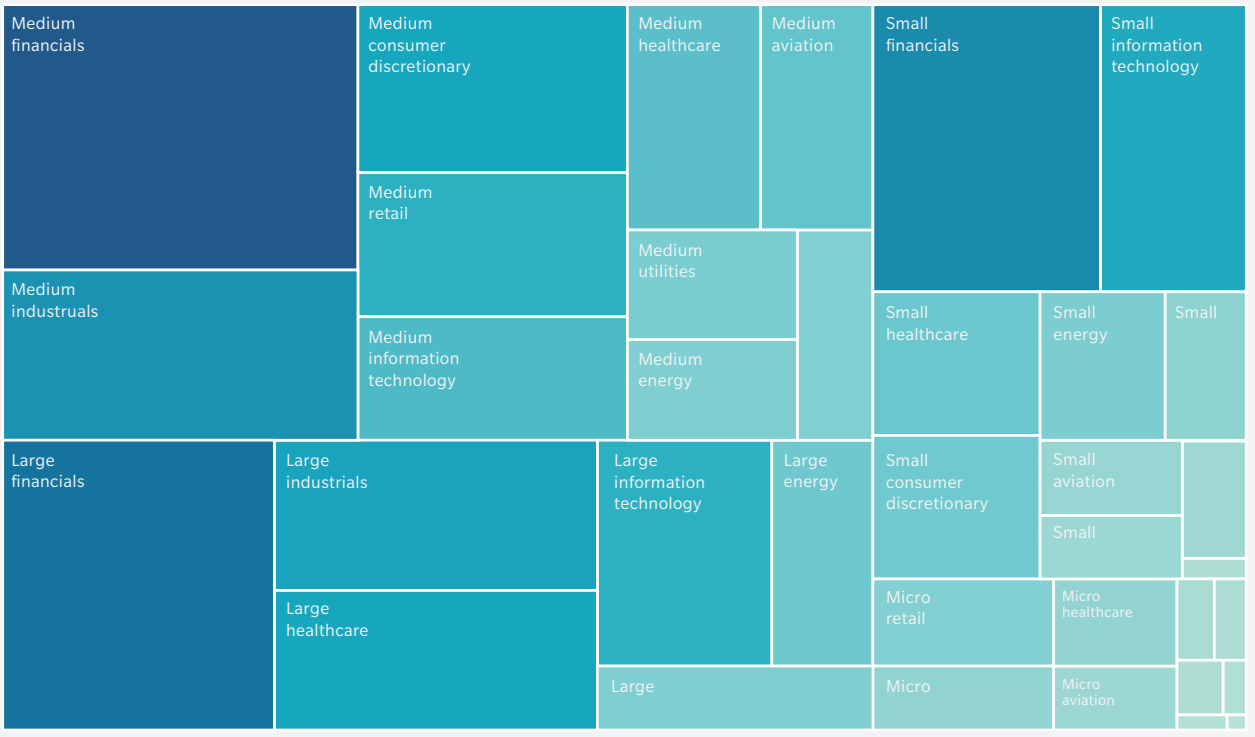
INTRODUCTION OF APPROPRIATE CYBER CATASTROPHE LOADS

We have pockets of emerging intelligence about how pricing and accumulation management needs are impacted as a result of cyber risk embedded within all lines of business.

Insurers have made a move toward determining appropriate cyber catastrophe loads in rating plans. When determining catastrophe loads, not all insured risks are alike and the ability to understand relativities across these risks is paramount to pricing decisions. A large financial services company with hundreds of vendors, hundreds of millions in revenue and thousands of employees has a different risk profile when compared to a small business in professional services with low revenue, few employees and few dependencies.

There is directional consensus in the market that adjusting the volatility estimates to account for forward-looking uncertainties is a necessity. Insurers and reinsurers are using models and technology partnerships to broaden their horizon around this complex risk.

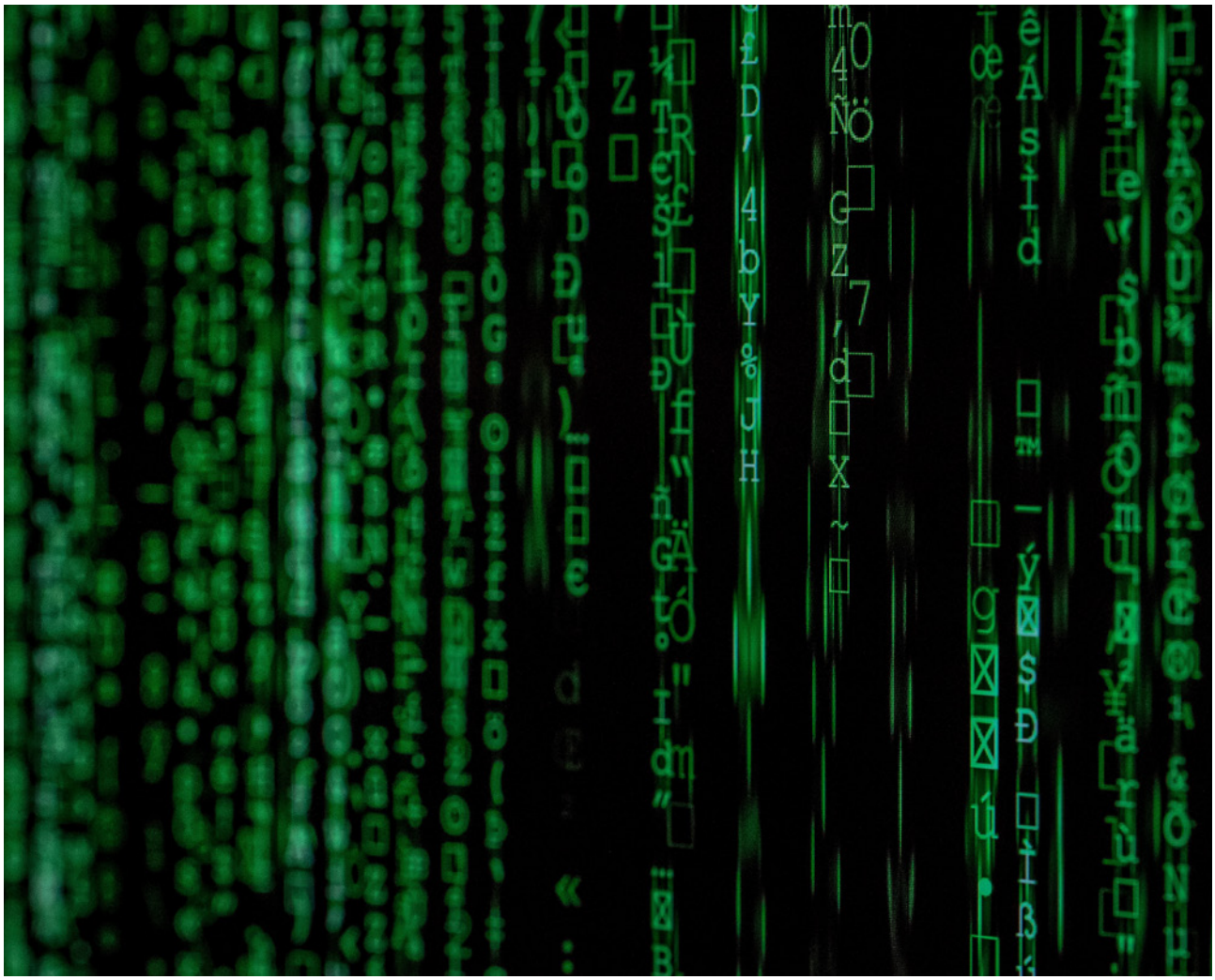
EXHIBIT 3: CYBER RISK RELATIVITY MAP



TREND WATCH

SPECTRE AND MELTDOWN

THE CANARY IN THE COAL MINE FOR DIGITAL INNOVATION?



Paul Mee
Partner and Cyber Lead, Oliver Wyman

Chris DeBrusk
Partner in Finance and Risk and Digital, Oliver Wyman

Numerous press reports this week spotlight *Spectre* and *Meltdown*, two newly discovered cybersecurity flaws. What makes these flaws different from other security "holes" is that they are hardware, not software flaws — and manifest in the microprocessors that run most of the computers and phones in the world. Software security flaws can be virtually patched; hardware flaws often require physical-part replacement, like an automaker's airbag recall.

WHAT ARE SPECTRE AND MELTDOWN?

In general, both the *Spectre* and *Meltdown* flaws allow an attacker to access areas of computer memory that should be inaccessible. Hackers gain access by taking advantage of aspects of microprocessor design that are used to improve performance, including memory read-ahead and out-of-order instruction execution. If a program can access memory that should be walled off, an outsider could potentially access sensitive information. That sensitive information could be passwords or other access information that could open the door to a much larger data breach.

Since these flaws have been identified, a patch has been issued for major operating systems that addresses *Meltdown*, although potentially at a fairly material impact to performance. There is not currently a patch for Spectre, but the speculation is that it cannot be fully remediated without physically replacing the processor in every affected computer and server.

There are two primary ways in which an attacker could take advantage of these flaws to get access to confidential or sensitive data. The first would be to run an attack program on a public cloud that attempted to steal information that was simultaneously running on the same physical servers, given that public cloud is a shared, virtual environment. While possible in theory, this sort of attack would be highly speculative, not unlike fishing in the middle of the ocean with no idea of what's below. Plus, the big cloud providers have already patched their infrastructure or added protections to prevent this sort of information leakage.

The second is much more likely. By tricking someone into running malware on a specific machine, likely via a phishing attack, other information running on that same machine could be compromised. That being said, there have been no documented attacks of this type and the operating-system publishers have been rolling out patches and protections to reduce the likelihood of it happening.

How important is this distinction from the perspective of cyber risk and digital innovation? We think it is very important, and likely signals the beginning of a new era in tech design.

HARDWARE ISN'T SAFE ANYMORE (AND REALLY WASN'T EVER SAFE)

People generally think that software is often bug ridden and hackable, but physical hardware is safe. Spectre and Meltdown have highlighted the fallacy in this assumption. What this means from a practical perspective is that the hardware stacks in captive data centers, and on laptops, phones, and consumer devices, need to be treated as potentially compromised (and often un-patchable). Security postures must be adjusted accordingly.

This realization reinforces the notion that the castle approach to cybersecurity is fundamentally flawed, and that companies need to take a layered approach to security that increases control (and, likely, user friction) as assets become more sensitive. At the core of this philosophy is the assumption that you will be hacked and act to limit any damage.

DEVICES ARE THE NEXT THREAT VECTOR

Over the last five years there has been a continuous march to network nearly everything in our daily lives. From smart thermostats, to garage-door openers, to lightbulbs, to kids' toys and even fish tanks — everything is being connected to the local WiFi access point so it can be controlled remotely and upload data into the cloud. On the surface, this is a good thing — smarter devices are easier to use, save us energy, and make sure our fish stay alive.

Unfortunately, all these networked devices also afford hackers millions of new points of attack that are often not effectively hardened. Even worse, device manufacturers rarely put in place the necessary upgrade-and-patch programs to identify and close security holes as they are discovered. Plus, these devices are full of microprocessors and other hardware that can create additional risk.

As the spread of networking and the Internet of Things is likely to continue accelerating, it is absolutely critical that the buyers of devices (both consumers and corporations) demand protection of their data. After all, your fish tank shouldn't let hackers steal all your data.

SECURITY NEEDS TO BE THE FIRST DESIGN CONSTRAINT, NOT THE LAST

Given that hacking is already pervasive and will likely get worse, security must be a focal point, and not an afterthought, in device design — starting at the whiteboard stage. The current practice of doing a cursory security review just before releasing V 1.0, and then quickly patching security issues that are discovered (often after the first hacks), is simply unacceptable in today's cyber environment.

Likewise, the base assumption that adding user friction to improve security is unacceptable also needs to be challenged directly and continually. Users need to be trained to accept some additional complexity in exchange for being protected — and user-experience designers are going to need to get creative in how they natively build security into the user experience.

Spectre and Meldown are likely just the beginning when it comes to hardware-based security holes. Both flaws resulted because engineers compromised security to gain performance, which likely made sense 20 years ago. In today's fully networked, always "on" environment, these types of tradeoffs will just create avenues for hackers to exploit.

TREND WATCH

MACHINE LEARNING AND SECURITY

HOPE OR HYPE?

TK Keanini
Distinguished Engineer,
Cisco

There is a temptation to hail major advances in technology as a cure-all for the challenges facing organizations and society today. The fanfare usually ends in disappointment when the latest superhero technology doesn't live up to its expectations.
Not surprisingly, machine learning, a domain within the broader field of artificial intelligence, has been hailed as the current be-all/end-all answer in cybersecurity. As a result, it is currently at the peak of inflated expectations in Gartner's most recent Hype Cycle for Emerging Technologies.

WHAT MACHINE LEARNING IS... AND ISN'T

Arthur Samuel defined machine learning in 1959 as "the field of study that gives computers the ability to learn without being explicitly programmed." Put another way, machine learning teaches computers to do what people do: learn from experience and get better over time.

An important distinction is that machine learning is a domain within the broader field of artificial intelligence. The two terms are not entirely synonymous, despite often being used interchangeably.

Machine learning primarily consists of three high-level categories:

- **Supervised Learning:** When you know the question you want to ask and have examples of it being asked and answered correctly
- **Unsupervised Learning:** You do not have answers and may not fully know the questions
- **Reinforcement Learning:** Trial and error behavior effective in game scenarios

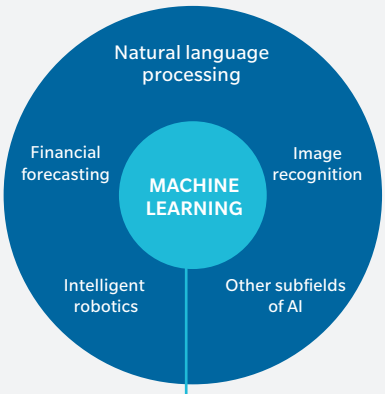
EXHIBIT 4: MACHINE LEARNING: COMMON TERMS

Artificial Intelligence (AI) is a scientific field within Computer Science, focusing on the study of computer systems that can perform tasks and solve problems that require human intelligence

Machine Learning (ML) is a field within AI that focuses on a particular class of algorithms that can learn from data without being explicitly programmed

There are three main ways a machine can learn from data: Supervised, Unsupervised, and Reinforcement Learning

Each category of machine learning is effective in tackling particular kinds of tasks and problems



Supervised machine learning	Unsupervised machine learning	Reinforcement learning
Mapping inputs to labelled outputs	Finding patterns in unlabeled input data	Performing actions to maximize rewards
Commonly used in classification and regression problems such as: • Natural language processing • Image recognition • Financial forecasting	Commonly used in segmentation and clustering problems such as: • Pattern and trend recognition • Customer segmentation • Transaction monitoring	Similar to supervised learning, but reward mechanism in place instead of labeled output: • Board and video games • Robotics

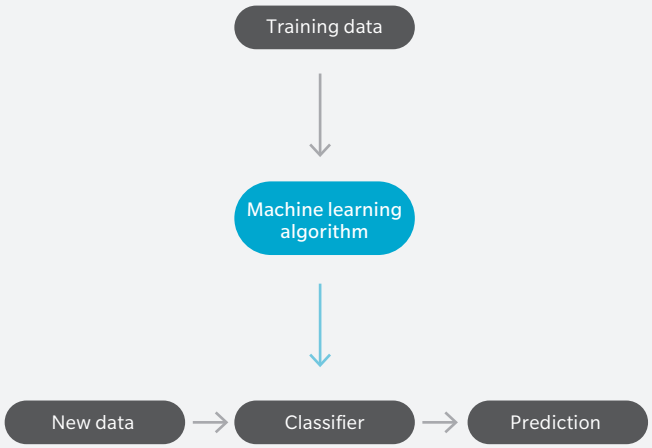
HOW SUPERVISED MACHINE LEARNING WORKS

The details and terms of machine learning can seem intimidating to non-data scientists so let's look at some key terms.

Supervised learning requires training data, sets of correct question and answer pairs, called "ground truth." This training lets the classifiers, the workhorses of machine learning that categorize observations, and the algorithms, the techniques that organize and orient classifiers, to do great work when analyzing new data in the real world.

A common example is facial recognition. Classifiers analyze specific data patterns they are trained to recognize — not actual noses or eyes — to accurately tag a particular face amongst millions of photos.

EXHIBIT 5: MACHINE LEARNING
Key terms



MACHINE LEARNING IN CYBER SECURITY

The cyber threat landscape today forces organizations to constantly track and correlate millions of external and internal data points across a number of endpoints. It simply is not feasible to manage this volume of information on an ongoing basis with a team of people.

Machine learning shines here because it can recognize patterns and predict threats in massive data sets, all at machine speed. By automating the analysis, cyber teams can rapidly detect threats and isolate situations that need deeper human analysis. Machine learning techniques can better protect organizations in a number of ways:

1. Detecting surreptitious attackers on networks: Machine learning can detect behavioral anomalies to find attackers on the inside or logged in with stolen credentials

2. Predicting "bad neighborhoods" online: By learning from internet activity patterns, machine learning can automatically identify attacker infrastructure being staged to launch the next threat

3. Attack detection through novelty and outliers: Machine Learning finds attack patterns humans cannot readily detect, like a new peer relationship on the network with hosts communicating that can't or shouldn't be

4. Find suspicious cloud user behavior: Analytical techniques uncover suspicious user behavior indicative of cloud account compromise to extract data or perform malicious operations

5. Modern malware detection: Machine learning is valuable in detecting polymorphic malware, breaking down threat attributes to better stop new and reengineered polymorphic threats

BEWARE THE PITFALLS

While machine learning offers tremendous promise for cybersecurity, it has its share of shortcomings that need to be acknowledged in order to use it appropriately.

1. Dealing with bad recommendations: If an application using machine learning suggests an incorrect movie recommendation, it is typically ignored. However, if machine learning incorrectly misses a threat or falsely convicts a good file, that could potentially interrupt business operations. Machine learning attempts to account for the real-world cost of mistakes, but it shows how challenging security is for machine learning, so it neither misses threats nor blocks legitimate business

2. Accounting for change: How can machine learning account for changes occurring in the world around it? For example, if it operates in an environment in which two countries are foes, how can it account for a peace treaty struck between the former adversaries? This makes periodic retraining vital so it remains accurate as the world evolves

3. Dealing with "explainability": When machine learning detects something bad, it often explains itself with math logic, instead of relevant security context. For example, say a machine learning system detected an infected device in the finance office. Prior to potentially yanking the CFO off the network, a security practitioner must confirm the relevant security event details of the infection — how the computer was infected, if there is a vulnerable application on the laptop, what file turned malicious etc. to better understand how to respond. Math logic won't help here, but rather the related security event information we note that machine learning doesn't always share. This "explainability" problem is a real challenge

MAKING MACHINE LEARNING WORK FOR YOUR ORGANIZATION

Machine learning is not a panacea for increasing cyber resilience. Rather, it is a helpful, additional security layer to augment other techniques in place. Rather than being used in isolation, it needs to be combined with other cybersecurity techniques from intrusion prevention rules and anti-virus signatures, to whitelists, to sandboxing to behavioral techniques. Specific to machine learning, no one single technique or method will suffice, rather we must call on a pipeline of hundreds of algorithms working together for successful outcomes.

Second, no security approach is effective without a team of humans carrying out threat intelligence research, confirming all is working as it should and addressing changes in context (remember that peace treaty?)

Last but not least, machine learning has many technical measures of success, but not all are helpful for a security professional. For machine learning to be most successful and embraced wholeheartedly, it must generate understandable outputs and generally "show its work" with security context.

TREND WATCH

NOTPETYA WAS NOT CYBER "WAR"

Thomas Reagan
US Cyber Practice Leader, Marsh

Matthew McCabe
Assistant General Counsel
for Cyber Policy, Marsh

This summer marked the anniversary of the most costly cyber-attack in history. *NotPetya* wreaked havoc for some large companies, costing them billions of dollars in lost revenue, damaging computer systems, and requiring significant expense to restore global operations. In its wake, entire industries reassessed their practices for patching, business continuity, supply chain interruption, and more.

In the year since *NotPetya*, we have learned much about the attack, but many details remain elusive. One continuing discussion for the insurance industry, however, is whether *NotPetya* was "warlike" — and more specifically, whether the ubiquitous war exclusion found in cyber insurance policies could have prevented coverage. A recent Wall Street Journal article described this as "a multimillion-dollar question for companies that purchase cyber insurance."

Conflating the war exclusion with a non-physical cyber event like *NotPetya* grows out of two factors: (1) *NotPetya* inflicted substantial economic damage on several companies, and (2) the US and UK governments attributed the *NotPetya* attack to the Russian military. These two factors alone, however, are not enough to escalate this non-physical cyber-attack to the category of war or "hostile and warlike" activity. These terms of art that have been considered by courts, and the resulting decisions, which are now part of the Law of Armed Conflict, make it clear that much more is required to reach the conclusion of "warlike" action.

First: What were the effects of the attack? For a cyber-attack to reach the level of warlike activity, its consequences must go beyond economic losses, even large ones. Years before *NotPetya*, when President Obama was asked to characterize a similar nation-state cyber-attack that inflicted no physical damage but still proved "very costly" for a US company, the president aptly described the incident as "an act of cyber vandalism." His comments were supported by a legal history of armed conflict in which warlike activity always entailed casualties or wreckage. For a cyber-attack to fall within the scope of the war exclusion, there should be a comparable outcome, tantamount to a military use of force.

Second: Who were the victims and where were they located? Did the victims serve a military purpose and did they reside near the actual conflict or "at places far removed from the locale or the subject of any warfare." The most prominent victims of *NotPetya* operated far from any field of conflict and worked at purely civilian tasks like delivering packages, producing pharmaceuticals, and making disinfectants and cookies.

Third: What was the purpose of the attack? *NotPetya* was not a weapon that supported a military use of force. The attack struck just before Constitution Day, when Ukraine celebrates its independence. The resulting chaos caused by *NotPetya* bore greater resemblance to a propaganda effort rather than a military action intended for "coercion or conquest," which the war exclusion was intended to address.

As cyber-attacks continue to grow in severity, insurers and insurance buyers will revisit the issue of whether the war exclusion should apply to a cyber incident. For those instances, reaching the threshold of "warlike" activity will require more than a nation-state acting with malicious intent. As shown by the recent indictments of foreign military intelligence officers for interfering with US elections, most nation-state hacking still falls into the category of criminal activity.

The debate over whether the war exclusion could have applied to *NotPetya* demonstrates that if insurers are going to continue including the war exclusion on cyber insurance policies, the wording should be reformed to make clear the circumstances required to trigger it. Absent that clarification, insurers and insurance buyers must default to the Law of Armed Conflict, including rulings that might be more than a century old, to discern between the categories of criminal activity and warlike actions. As for the latter, all precedent indicates that *NotPetya* simply didn't reach that level.

TREND WATCH

MINING FOR VIRTUAL GOLD

UNDERSTANDING THE THREAT OF CRYPTOJACKING

Stephen Viña
Senior Vice President, Marsh

Paula R. Miller
Senior Vice President, Marsh

Instead of stealing company data or holding it ransom, cyber criminals have mastered a new way to attack businesses. Through cryptojacking, one of the fastest growing types of cyber-attacks globally, criminals can siphon an organization's computing power to mine cryptocurrency, opening the door to new sources of illicit revenue at the company's expense. And your organization may already be a victim and not even know it.

WHAT IS CRYPTOJACKING?

Thousands of cryptocurrencies or "coins" exist today, all with varying purposes. Some, such as Bitcoin and Monero, serve as a digital currency and can retain considerable monetary value. The all-time high for a single Bitcoin, for example, peaked around $20,000 in December 2017; the value fluctuates daily based on availability and currency movement. Creating certain cryptocurrencies, including Bitcoin and Monero, requires the completion of a complex cryptographic puzzle that is recorded on a blockchain, a process known as cryptomining. Performing these calculations can be expensive, requiring considerable processing and electrical power and, in some cases, specialized equipment. For their efforts, miners are rewarded with newly created units of the mined cryptocurrency, providing a potentially lucrative pay day depending on the value and quantity of the coin.

As the value of cryptocurrencies has soared, many organizations have turned to coin mining as a new source of revenue. Some companies have asked online users whether they would allow the mining of cryptocurrency on their computers in exchange for eliminating advertisements. However, a growing number of miners are now simply stealing or "hijacking" the necessary computing power from unsuspecting consumers and businesses. What was once a complicated process has become relatively easy with the advent of in-browser mining scripts that allow scammers to use the computing power of anyone who visits an infected website. Cryptomining malware can also be spread through malicious links, advertisements, email attachments, public Wi-Fi, fake apps, and system backdoors.

Infections have been rampant, affecting nearly 30% of companies monitored by cybersecurity firm Fortinet in the first quarter of 2018, doubling 2017's record numbers. In February 2018, for example, hackers compromised a screen-reading web plugin for the blind, affecting over 4,000 websites worldwide, including the UK's National Health Service.

Some companies represent particularly strong targets for cryptojacking. These include:

- Critical infrastructure companies, which consume significant amounts of power and often have vulnerable industrial control systems
- Companies that rely heavily on cloud services, which present the opportunity for "high-powered mining."

Cryptojacking is also frequently tied to Internet of Things (IoT) devices such as mobile phones, which can allow miners to quickly amass armies of hijacked devices to mine cryptocurrency at scale.

HOW CRYPTOJACKING CAN AFFECT BUSINESSES

The theft of company computing power through cryptojacking can have real financial consequences over time. Accurately capturing the direct costs of cryptojacking, however, may prove difficult, since most victims may not notice an infection or recognize the culprit.

But the threat is real. The performance of an infected computer system could become sluggish due to the complex and continuous operations required to perform mining calculations. Overworking computers could lead to the crashing of necessary functions and, in some cases, the overheating and ultimate failure of central processing units. This may seem like a temporary or isolated nuisance, but spread across a corporate enterprise, it could have disruptive and costly implications for companies. In addition to the potential degradation in service and resulting lost productivity and income, businesses may incur costs for higher energy consumption

or cloud usage. An organization could also iWncur extra expenses to replace hardware sooner or more frequently than planned, and for additional IT support to help address system performance issues.

Companies that transfer cryptomining software to unsuspecting third parties have also become the subject of litigation and regulatory scrutiny. The Federal Trade Commission, for example, recently launched a system for consumers to file complaints if they become victims of cryptojacking and has brought enforcement actions against companies that have hijacked consumers' mobile devices with malware to mine virtual currency.

Of course, if miners are able to compromise a corporate network to steal company computing power, it is possible for the same individuals to access data, install malware, or exploit other vulnerabilities to cause mischief. And, just as announcing any type of major data breach can bring reputational harm, publicly disclosing a cryptojacking event may also damage a company's standing with customers and others.

CAN CYBER INSURANCE HELP?

Cyber insurance policies are designed to cover both direct loss and liability caused by a cyber event. Cyber policies can cover expenses incurred directly by policyholders for IT forensics, recreation or restoration of data assets, data breach response, loss of business income, and reputational damage. Coverage also extends to third-party liability claims for privacy breaches and security failures, such as the transfer of malware to a third party or the unauthorized disclosure of sensitive customer data.

A cryptojacking incident could result in several types of losses that are covered under cyber insurance policies. For example, a cryptojacking incident could disrupt important control systems or a company network, triggering business interruption coverage, or it could result in the loss of sensitive information, triggering data asset recovery coverage. Cyber insurance may also help cover costs for investigations to determine the cause, source, and scope of a cryptojacking event and forensic accounting services for claim preparations. Companies that unwittingly pass cryptojacking malware to third parties may also look to a cyber insurance policy for relief from any related claims for damages.

Whether cyber insurance responds will depend upon the specific terms and conditions of a given policy. Businesses should consider carefully reviewing specific coverage provisions to determine whether and how their policies will react to cryptojacking losses. Businesses should also work with their risk advisors to ensure that their cyber policies include specific claim triggers and broad definitions of loss in order to capture all possible scenarios for which an insured would expect to recover loss.

RECOMMENDATIONS

As long as there is big money to be made, cyber actors will likely continue to hijack computer systems to mine cryptocurrency, evolving their methods along the way. Like other cyber attacks, businesses should look to detect and prevent this growing and evolving threat and closely watch for signs of infection.

To further protect your business from cryptojacking, work with your insurance advisor to assess your potential exposures to cryptojacking and determine how your cyber policy may respond. The time to assess your cyber insurance policies for potential coverage is before your organization is attacked.

TREND WATCH

FOLLOW THE MONEY

AN UP-CLOSE LOOK AT THE MASSIVE CREDIT CARD HACKING RING, FIN7

Nick Carr
Senior Manager, FireEye

Barry Vengerik
Technical Director, FireEye

Financial threat actor FIN7 made headlines in August 2018 when a United States District Court indicted three of its members for hacking. The group had carefully targeted its victims, focusing on large-scale theft of payment card data using nation-state-level techniques and a rapid, innovative development cycle. These malicious actors are members of one of the most prolific financial threat groups of this decade, having carefully crafted attacks targeted at more than 100 organizations. FIN7 is referred to by many vendors as "Carbanak Group."

The threat group is characterized by its persistent targeting and large-scale theft of payment card data from victim systems, but FIN7's financial operations went beyond stealing credit information. In some instances, when they encountered but could not obtain payment card data from point-of-sale systems secured with end-to-end encryption or point-to-point encryption, FIN7 pivoted to target finance departments within their victim organizations.

FireEye has followed FIN7 since 2015, noting its move from weaponized Microsoft Office macros to keep from being discovered. FIN7 evolved to using phishing lures with hidden shortcut files to infect targets and compromise them. During campaigns that FireEye associates with FIN7, the group targeted victims within the following sectors in the United States and Europe: Restaurants, hospitality, casinos and gaming, energy, finance, high-tech, software, travel, education, construction, retail, telecommunications, government, and business services.

In April 2017, FIN7 sent spear phishing emails to personnel involved with United States Securities and Exchange Commission (SEC) filings at multiple organizations, targeting individuals who would likely have access to material non-public information that FIN7 actors could use to gain a competitive advantage in stock trading.

With its more recent attacks, FIN7 usually deployed point-of-sale malware within targeted organizations. The group sent spear phishing emails and then called the targets, encouraging them to open malware-laden emails and begin the infection process. The result? Well over $1 billion in losses for the victims.

People who purchased anything at over 3,000 affected locations saw their wallets take a hit. FIN7 digitally stole 15 million credit card numbers, and then sold them on the black market for other criminals to use.

FireEye spoke with Nick Carr and Barry Vengerik, two analysts who have tracked FIN7 for years, about who the group is targeting and how, and what might be next for the massive hacking ring in light of the recent arrests of three of its leaders.

FIN7 really seemed to focus on restaurants, hospitality, and casinos and gaming. Why those industries in particular?

Barry Vengerik: These industries are heavily focused on customer service. With the hotels they targeted earlier on, FIN7 would communicate as if they were attempting to book large corporate events, with ballrooms and multiple rooms. That is enticing lure content for anybody that's in charge of booking at those hotels.

Similarly, for restaurants FIN7 used themes of catering or large orders, but also themes of complaints about the restaurant, like, "The food made me sick," or "I left my bag in your restaurant." FIN7 really attempted to capitalize on the customer service aspect, as well as targeting specific users within the organization whose regular duties are to open unsolicited attachments — which is in direct contrast to the spear phishing advice we usually give customers. The targeted folks at these organizations were not in a position to avoid interacting with these unsolicited attachments.

What types of payloads did FIN7 use to get into the victim environments?

Barry: For the first couple years, the group pretty consistently used a Java Script backdoor we call "half-baked" and added new features to it with each victim. Once they established initial access, we saw an interesting grab bag of secondary payloads, including the famous CARBANAK backdoor. It was a mix of a simpler backdoor on the front end that received a lot of active development, and then they quickly pivoted to a lot of different tools and techniques based on the customer environment.

With such a variety of tools and constant changes, does it make it more difficult to find FIN7 in a customer environment? Can you continue to track them through all those changes?

Nick Carr: The FireEye response is focused on protecting our customers from those initial spear phishing emails. At the same time, we did a tremendous number of incident response engagements into FIN7 intrusions, most often at clients who don't have our products. Simply being able to detect what they look like when they're trying to get into the network isn't good enough — it is about detecting some of those methods that Barry mentioned, blending in and looking like good systems admins. It's pretty interesting.

Some FIN7 members were arrested in August. Did you see any changes in the group after the arrests?

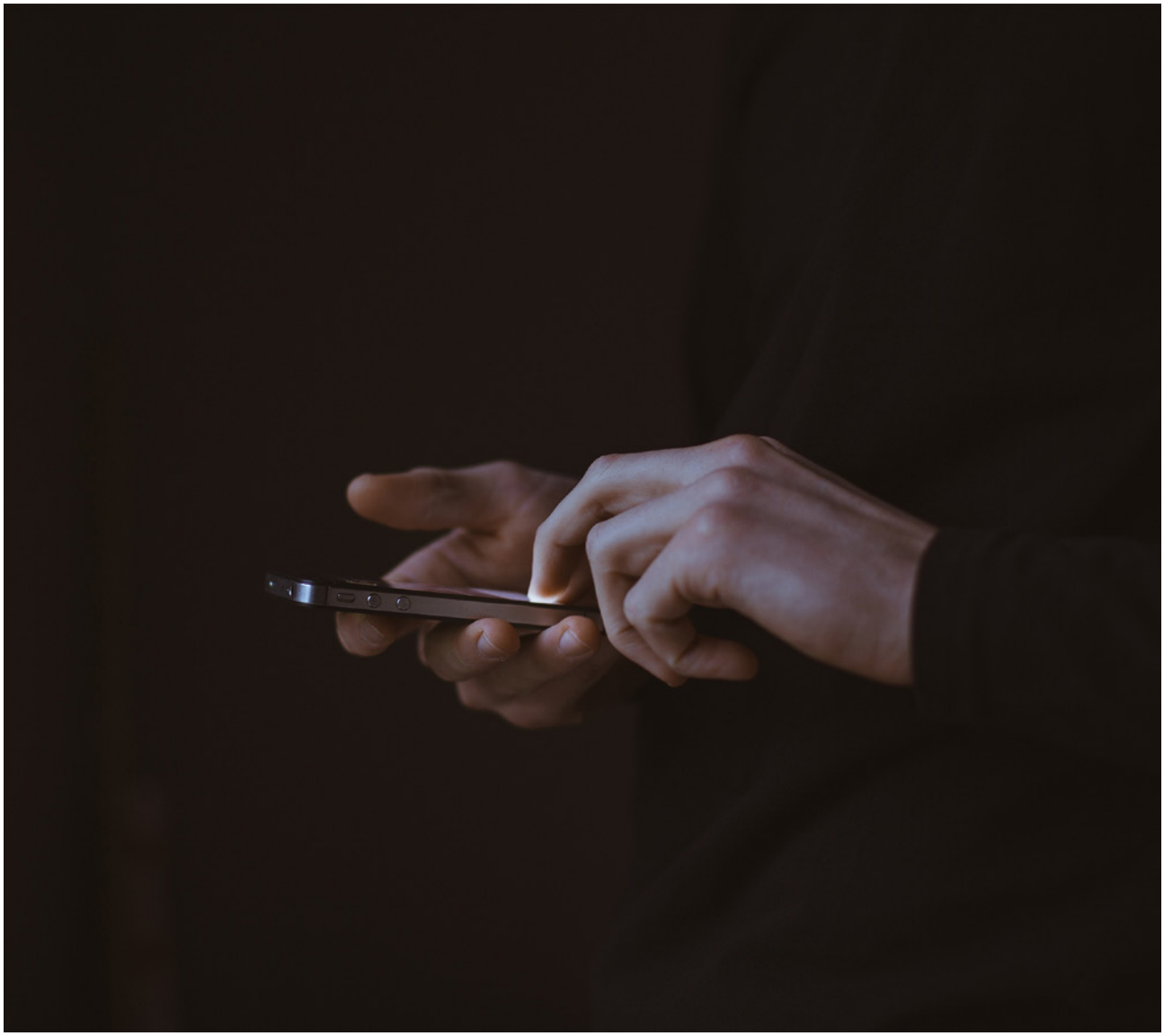
Barry: Starting last summer, we saw a new initial vector backdoor called BATELEUR, targeting pretty much the same victim set. It was a different Java Script backdoor but very similar functionally to the backdoor we had seen from FIN7 in the past. We saw traditional FIN7 half-baked backdoor activity slow down and BATELEUR activity ramp up. So, we've actually got pretty high confidence that this is a newer aspect of FIN7. Given the apparent size of the organization behind this, it can become really difficult to identify what is actually controlled by the same organization, or maybe it's a developer that left and is starting their own gig, or a third party providing infrastructure or malware for this organization.

Do you expect any changes going forward as a result of the indictments against some members of FIN7?

Nick: We see the individuals continuing to operate. As long as there's non-extradition countries where these guys are located, the majority of the activity will continue on.

TREND WATCH

GLOBAL CYBER TERRORISM INCIDENTS ON THE RISE



Jeremy Platt
Managing Director, Guy Carpenter

Emil Metropoulos
Senior Vice President,
Guy Carpenter

The nature of the terrorism threat facing society has changed considerably in the last 20 years. Previously, governments and (re) insurers structured their mitigation strategies and responses to deal with attacks that were large in scale.

Recently, though, we have seen a spate of smaller, less sophisticated, yet no less appalling acts of terrorism across geographies that involve mass casualties and fear-inducing events. And the type of threat will continue to change as new technologies and opportunities reveal themselves to terrorist organizations – cyber terrorism is an example of a newly developing frontier within the peril.

Traditionally, most cyber-attacks have been carried out by criminal organizations, with the majority of incidents failing to register on an enterprise risk scale of businesses that faced significant setbacks. In 2017, this dynamic changed with the *WannaCry* and *NotPetya* incidents. These two attacks affected organizations in more than 150 countries, prompted business interruption and other losses estimated at well over USD 300 million by some companies, brought reputational damage, and resulted in loss of customer data.

In December 2017, the U.S. government took a rare step and attributed the *WannaCry* attack to hackers backed by North Korea. *WannaCry* and *NotPetya* exposed a systemic risk and affected a broad cross-section of businesses without specific targeting, demonstrating the potential for escalation in the threat of cyber terrorism.

Against this backdrop, a few trends are emerging:

The landscape for points of attack is growing. Traditional physical processes carried out by industrial control systems — including critical infrastructure industries such as power utilities, water treatment services, and health and emergency systems — are coming online. Guy Carpenter affiliate Oliver Wyman forecasts that 30 billion connected devices will be in use by 2030, creating more assets susceptible to attack and adding more vulnerabilities to be exploited.

Cyber threats are becoming more advanced. The upsurge of highly skilled hackers, often nation-state supported, is coinciding with the development of more sophisticated tools that are likely seeping into the broader environment through a thriving black market.

The consequences are high. Companies are now deeply dependent on their systems and data, and interference with those assets can materially affect market capitalization and endanger executive leadership, reputations, sales and profits. Failures in cybersecurity have the potential to destabilize an enterprise overnight.

A shift has begun to take place in the nature of cyber incidents; from affecting primarily consumers to having an impact on global political or economic systems as a whole. Examples of this changing trend are the recent headlines covering the banking industry. Large scale cyber-attacks on the banking industry can result in stolen money and personal information entrusted by consumers to these institutions and also, in a worst-case scenario, cause a "run" on the global banking system. Terrorist groups have ambitious goals for cyber-induced attacks. The industrial control systems that support the electricity industry were largely sealed off from external threats. However, the protections that came with the isolation have weakened with the introduction of automated controls managed

through interconnected network systems. As automation grows, so does the opportunity to manipulate an industrial control system through a cyber-attack.

For utilities and other infrastructure facilities, the potential costs of a power grid interruption as a result of a cyber-attack can include:

- Lost revenue;
- Additional expenses to restore operations and to improve cybersecurity defenses;
- Regulatory fines and additional scrutiny; and
- Reputational damage

Such attacks, though rarely made public, are occurring more frequently. The potential perpetrators of acts of cyber terrorism can be separated into five categories: organized crime, hacktivism, non-state terror groups, lone wolves, and nation states. Although the motivations, capabilities and priorities vary among the groups, each can wreak havoc on a global scale; with ever-increasing funding, these attacks can become more catastrophic.

As these factors converge, opportunity could combine with existing motives to inflict catastrophic cyber terrorism losses for businesses. Over time, cyber insurance policies have evolved to cover the failure of technology and the resulting interruption or loss of revenue. Insurers are also increasingly recognizing the interdependence of businesses, especially through technology. Many cyber policies now contain provisions for business interruption and contingent business interruption, including those involving disruption of an organization's supply chain from a data breach.

Business interruption coverage has become a more common coverage component within cyber insurance policies over the last 24 months. Reinsurance solutions in the cyberspace tend to follow the security and privacy coverage offered in the insurance market. Although reinsurance contract wording varies, cyber insurance typically covers network security incidents regardless of the political or ideological beliefs of a non-state actor.

Guy Carpenter's dedicated Cyber Solutions Specialty Practice and Global Cyber Center of Excellence work with professionals around the world to provide risk transfer solutions to help companies quantify potentially catastrophic scenarios and identify the right way to manage, spread and transfer the associated risks. We structure a broad range of tailored reinsurance solutions utilizing our in-house modeling capabilities combined with our investment in third-party models to create our own best-in-class, holistic view of cyber risk for our clients.

INDUSTRY DEEP DIVE

HOW A CYBERATTACK COULD CAUSE THE NEXT FINANCIAL CRISIS

Paul Mee
Partner and Cyber Lead,
Oliver Wyman

Til Schuermann
Partner, Financial Services,
Oliver Wyman

This article first appeared in Harvard Business Review

Ever since the forced bankruptcy of the investment bank Lehman Brothers triggered the financial crisis 10 years ago, regulators, risk managers, and central bankers around the globe have focused on shoring up banks' ability to withstand financial shocks.

But the next crisis might not come from a financial shock at all. The more likely culprit: a cyber attack that causes disruptions to financial services capabilities, especially payments systems, around the world.

Criminals have always sought ways to infiltrate financial technology systems. Now, the financial system faces the added risk of becoming collateral damage in a wider attack oncritical national infrastructure. Such an attack could shake confidence in the global financial services system, causing banks, businesses and consumers to be stymied, confused or panicked, which in turn could have a major negative impact on economic activity.

Cybercrime alone costs nations more than $1 trillion globally, far more than the record $300 billion of damage due to natural disasters in 2017, according to a recent analysis our firm performed. We ranked cyber attacks as the biggest threat facing the business world today — ahead of terrorism, asset bubbles, and other risks.

An attack on a computer processing or communications network could cause $50 billion to $120 billion of economic damage, a loss ranking somewhere between those of hurricanes Sandy and Katrina, according to recent estimates. Yet a much broader and more debilitating attack isn't farfetched. Just last month, the Federal Bureau of Investigation issued a warning to banks about a pending large scale attack known as an ATM "cash-out" strike, in which waves of synchronized fraudulent withdrawals drain bank accounts. In July, meanwhile, it was revealed that hackers working for Russia had easily penetrated the control rooms of US electric utilities and could have caused blackouts.

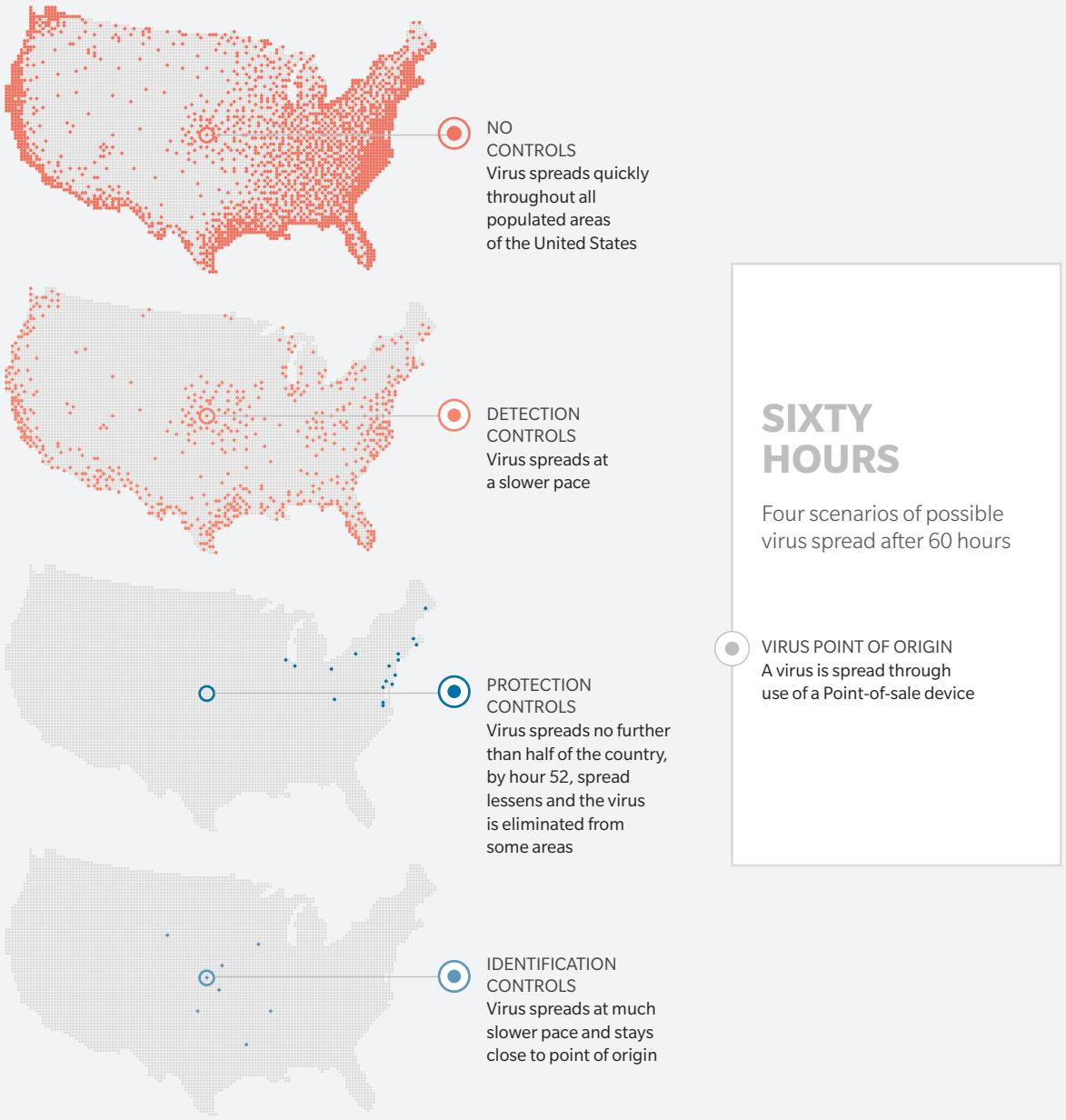
"Cybercrime alone costs nations more than $1 trillion globally, a multiple of the record $300 billion of damage due to natural disasters in 2017, according to a recent analysis our firm performed"

How might a financial crisis triggered by a cyber attack unfold? A likely scenario would be an attack by a rogue nation or terrorist group on financial institutions or major infrastructure. Inside North Korea, for example, the Lazarus Group, also known as Hidden Cobra, routinely looks for ways to compromise banks and exploit crypto currencies. An attack on a bank, investment fund, custodian firm, ATM network, the interbank messaging network known as SWIFT, or the Federal Reserve itself would represent a direct hit on the financial services system.

Another possibility would be if a so-called hacktivist or "script kiddy" amateur were to use malicious programs to launch a cyber attack without due consideration of the consequences. Such an attack could have a chain reaction, causing damage way beyond the original intent, because rules, battle norms, and principles that are conventional wisdom in most warfare

EXHIBIT 9: HOW A CYBERATTACK SPREADS

How fast cyberattacks will spread depends on what controls are in place to prevent them. Below we explore how far a cyberattack virus could spread in 60 hours under four different scenarios



Source: Oliver Wyman analysis

situations but don't exist in a meaningful way in the digital arena. For example, in 2016 a script kiddie sparked a broad denial-of-service attack impacting Twitter, Spotify, and other well-known internet services as amateurs joined in for mischief purposes.

Whether a major cyber attack is deliberate or somewhat accidental, the damage could be substantial. Most of the ATM networks across North America could freeze. Credit card and other payment systems could fail across entire nations, as happened to the VISA network in the UK in June. Online banking could become inaccessible: no cash, no payments, no reliable information about bank accounts. Banks could lose the ability to transact with one another during a critical period of uncertainty. There could be widespread panic, albeit temporary.

Such an outcome might not cause the sort of long-simmering financial crisis that sparked the Great Recession, because money would likely be restored to banks and payments providers once systems were back online. At the same time, it isn't clear how a central bank, the traditional financial crisis firefighter, could respond to this type of crisis on short notice. After the problem is fixed and the crisis halted, a daunting task of recovery would loom. It would be even more difficult if data were corrupted, manipulated or rendered inaccessible.

How can we prevent such a scenario? Companies must implement systems that enable them to stop the spread of a cyber attack contagion, and to resume operations as rapidly and smoothly as possible. The financial services industry needs to fully agree on, and be prepared to practice, coordinated response and recovery strategies to prevent systemic breakdowns. Regulators in many nations have been working diligently to prepare for and curtail cyber attacks, but they need to look beyond their own borders and introduce regulations, laws, and cooperative frameworks in unison, such as the European Union's Network and Information Security Directive, which is designed to protect an ever-growing list of critical infrastructure from banking and healthcare systems to online marketplaces and cloud services.

Many of these steps are being undertaken to varying degrees. But more needs to be done. An attack that undermines confidence in those very machines could have debilitating consequences on the flow of money between consumers, businesses, and financial institutions around the world.

INDUSTRY DEEP DIVE

AVIATION INDUSTRY MAY BE VULNERABLE TO CYBERATTACK THROUGH ITS GLOBAL SUPPLY CHAIN

Paul Mee
Partner and Cyber Lead,
Oliver Wyman

Brian Prentice
Partner, Aviation,
Oliver Wyman

Published on Forbes.com on April, 2018

In March, the U.S. Department of Homeland Security and the Federal Bureau of Investigation issued a troubling alert: Since the same month two years before, Russian state-sponsored hackers had been infiltrating the nation's electricity grid and various infrastructure industries, including aviation, collecting information on how the networks were organized and what systems' controls they had in place. While no sabotage appears to have been perpetrated, the unsettling question remains — what are the Russians going to do with the data they collected?

While all these industries, especially their biggest players, tend to have extensive cybersecurity in place, it may not be as comprehensive as the nation would hope. In this case, instead of gaining access through the front door, where the alarm system was more robust, these hackers simply went around back and entered through the more vulnerable networks of third-party and supplier operations, relying on myriad techniques including the use of phishing emails infected with malware and the theft of credentials.

Needless to say, the scenario should send chills throughout the aviation and aerospace industries. While major aircraft manufacturers and airlines make obvious targets because of the potential they represent to conspicuously disrupt international commerce, they also rank high on hackers' to-do lists because they maintain global, highly interconnected supply chains that over the past few years have been aggressively digitizing operations. More digitization means more attack surface for hackers. The many links on aviation's and aerospace's supply chain — some big, many small to midsize — all become potential vulnerabilities, given the daunting task of ensuring that all vendors with access insist on the same level of rigor in both their cybersecurity and their employee training.

VULNERABILITIES IN THE SUPPLY CHAIN

The biggest organizations within the industry's fold may have advanced cybersecurity; the same cannot always be said about the vast network of service providers and suppliers, many of which are members of the maintenance, repair, and overhaul (MRO) industry that services the nation's aircraft.

In a 2018 Oliver Wyman survey of the MRO industry, responses revealed potential holes in the bulwark. For instance, while 67 percent of respondents said their company was prepared for a cyberattack, fewer than half were able to say whether they had conducted a cybersecurity review in 2017. Only nine percent of independent MRO providers, 50 percent of airframe, engine, and component manufacturers, and 41 percent of airlines confirmed that they have established security standards for third-party vendors. That leaves potentially many companies without a clear view into the digital security of vendors — almost all of which maintain credentials to log onto their systems.

EXHIBIT 9: WHICH CYBERSECURITY SAFEGUARDS HAS YOUR COMPANY IMPLEMENTED?
% of total respondents who selected each response for each segment

Source: Oliver Wyman analysis

And that lack of knowledge can lead to disaster as many major corporations have discovered over the past five years. In 2013, for instance, hackers used the stolen credentials of a heating, ventilation, and air conditioning vendor to penetrate the network of retail giant Target to steal the data of 70 million customers and information on 40 million payment cards. The cost to Target: close to $300 million.

While cyber criminals in earlier decades seemed motivated by the money that could be made off stolen data, recent breaches seem more intent on creating organizational chaos. In June 2017, hackers – believed by the CIA and UK intelligence to be Russian military – attacked the Ukraine with software that literally wiped out data and disrupted operations in that country's banking system, government ministries, and metro, and at the former Chernobyl nuclear power plant.

A GLOBAL EMERGENCY

From there, the wiper ransomware, named *NotPetya,* infected computer systems around the world, including those of Danish shipping conglomerate Maersk. This led to serious delays at major ports like Rotterdam, Mumbai, and the Port of New York and New Jersey and the temporary shutdown of the largest terminal at the port of Los Angeles. It is attacks like this one that should prompt transportation companies to reassess their level of cyber preparedness.

Globally, hacking has become a growth industry, costing economies around the world more than half a trillion US dollars annually – a sum that has been increasing every year. In some countries, hackers work out of regular offices and get paychecks to spend their workday looking for vulnerabilities in organizations' digital networks, lying in wait for holes to develop through which they can penetrate and steal information or worse. Experts place the number of professional hackers at over 300,000 worldwide. In places like Russia, China, Eastern Europe, and North Korea, hacking has become a growth industry.

To achieve a comprehensive, unified cybersecurity and risk management strategy for the industry, MRO providers should seriously consider taking several actions. First, companies within the industry should conduct independent audits of existing cybersecurity programs. This includes looking at everything from understanding who and what have access to a company's computer network, to whether a real-time detection process and response mechanism have been delineated, to which managers are responsible for each phase of executing cybersecurity protocol, to whether an oversight process exists to ensure procedures are followed and documented.

INDUSTRY STANDARD

The industry as a whole also needs to develop a clear framework for mitigating and managing cyber risks. The National Institute of Standards and Technology (NIST) has developed a set of industry-specific standards and best practices intended to be leveraged in designing such a cybersecurity framework.

Finally, the industry must work across companies to fortify their information technology systems – both infrastructure and upkeep – and create a security-minded culture. While no solution is guaranteed to avert any and all attacks, developing a holistic approach to the risk management of cybersecurity that's shared across the industry – and updating it regularly – may give companies a leg up. Certainly, cyber criminals aren't standing still.

INDUSTRY DEEP DIVE

CAN BLOCKCHAIN HELP REDUCE THE FINANCIAL INDUSTRY'S CYBER RISK?

Erin English
Senior Security Strategist,
Microsoft

Given the increasing frequency of cyberattacks, financial regulators identify cybersecurity as one of the most pressing risks to the financial services industry. Moreover, due to the interconnectedness of the global financial system, a cyberattack at one bank may affect other banks and financial institutions.

These considerations apply with equal force to permissioned blockchains, which rely on ongoing interconnections. As the financial services industry explores the use of permissioned blockchains — which limit access to a particular ledger to certain known or trusted parties in a consortium — to enhance services and operations, industry participants should recognize and take into account a number of cybersecurity capabilities — as well as risks — relating to this technology.

BLOCKCHAIN'S ADVANTAGES...

One of blockchain's benefits is its inherent resiliency in mitigating cyber risks and attacks, particularly those directed at financial institutions. While not immune to all forms of cyber risk, blockchain's unique structure provides cybersecurity capabilities not present in other legacy technologies. The following are some of the technology's advantages in combating cyber risk:

- The distributed architecture of a blockchain increases the resiliency of the overall network from being exposed to compromise from a single access point or point of failure
- Consensus mechanisms — a key feature of blockchains — improve the overall robustness and integrity of shared ledgers, because consensus among network participants is a prerequisite to validating new blocks of data and mitigates the possibility that a hacker or one or more compromised network participants can corrupt or manipulate a particular ledger
- Blockchains also provide participants with enhanced transparency, making it much more difficult to corrupt blockchains through malware or manipulative actions. Moreover, blockchains may contain multiple layers of security — both at the network level and installed at the level of each individual participant
- Finally, blockchains hosted on a cloud platform, such as Microsoft Azure, feature even greater cybersecurity protections due to the platform's access controls and many other protections

... AND RISKS

Despite the many cybersecurity benefits inherent in blockchains, this technology, like any other, remains subject to inherent cybersecurity risks that require thoughtful and proactive risk management. Many of these risks involve a human element, such as maintaining the confidentiality, integrity, and availability of private keys; human coding errors that can introduce cybersecurity risk from off chain applications; unsecure data that can be ingested from external sources; identity-based attacks intended to corrupt a blockchain's consensus mechanism; and advanced threats that can corrupt the decision-making processes of the blockchain.

Therefore, a robust cybersecurity program remains vital to protecting the network and participating organizations from cyber threats, particularly as hackers develop more knowledge about permissioned blockchains and their vulnerabilities.

A number of important structural considerations should be taken into account when constructing cybersecurity programs for blockchains. For instance, records added to a blockchain generally are immutable. This immutability prevents tampering and creates an auditable record, but may require a special programming adjustment to restore a blockchain's integrity if fraudulent or malicious transactions are introduced into the ledger. Additionally, blockchain participants' roles and responsibilities require a thoughtful governance structure to achieve an effective balance of access and security.

NEED FOR AN EFFECTIVE FRAMEWORK

When considering the public policy tools to enhance the security of blockchains, cybersecurity principles and controls from existing laws, regulations, and industry guidance remain critical components to an effective cybersecurity program for blockchain deployments. Indeed, most cloud service providers, particularly those that support the financial services industry, should already have these controls in place.

Microsoft and the Chamber of Digital Commerce recently released a white paper, *Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry,* to deepen the cybersecurity policy dialogue among blockchain technology providers, such as Microsoft, and financial services organizations using blockchain and their regulators.

While it is encouraging for financial institutions that the guidelines and regulations that are familiar for cybersecurity are just as relevant for blockchain, the process of applying those standards will require new multi-stakeholder approaches for industry and government.

NEXT STEPS

Moreover, the effectiveness of these existing rules — which were not designed for blockchain technology specifically — are often broad enough to cover this new technology. With this in mind, we argued that the following recommendations for policymakers and industry participants provide a framework for a smart and coordinated approach to promoting the development of secure blockchain applications through workable cybersecurity standards.

- Apply a Tailored Version of the NIST Cybersecurity framework to permissioned blockchain activities. Financial Services Industry participants should optimize the framework for permissioned blockchains by shifting the focus from organization or enterprise-level cybersecurity to network-level cybersecurity

- Encourage regulator-industry dialogue, including through regulatory sandboxes. For regulators to understand cybersecurity risk in permissioned blockchains, they first must have a detailed understanding of the technologies and how they operate. Industry participants can help provide this understanding by maintaining an open dialogue with regulators regarding permissioned blockchains, their opportunities, and their risks

- Encourage policymakers to acknowledge the unique cybersecurity benefits of blockchain technologies. While blockchain technologies are continuing to evolve for an expanding range of applications and industries, policymakers should be attuned to these technologies' unique benefits, including cybersecurity benefits

- Foster harmonization across cybersecurity standards applied to permissioned blockchains. Convening interagency councils and public-private governing bodies is a helpful step to making sure that cybersecurity guidance applicable to blockchain technology is consistent and does not impede innovation

PROTECTING CUSTOMERS' INFORMATION

The financial services industry stands to benefit tremendously from the growth of blockchain given the technology's many financial services applications. As cyber threats to the industry continue to evolve in complexity and intensity, emerging technologies, such as permissioned blockchains, can contribute to the important goals of reducing cybersecurity risk and adequately protecting consumers' financial information and the integrity of the global financial system.

Permissioned blockchains offer significant cybersecurity capabilities, share some of the same cyber risks that affect other IT systems, and have unique characteristics, all of which merit further consideration and evaluation by governments and industry.

INDUSTRY DEEP DIVE

ASIA'S HEALTH CARE INDUSTRY REELS FROM CYBERATTACKS

Jayant Raman
Partner, Finance and Risk Practice,
Oliver Wyman

Prashansa Daga
Practice Leader of Health & Life Sciences,
Marsh

Kitty Lee
Principal, Health & Life Science Practice,
Oliver Wyman

Health care is one of the sectors most vulnerable to cyberattacks, with more than one in four (27 percent) health care organizations reporting that they have been a victim of a cyberattack in the past 12 months. This is more than financial institutions (20 percent) and nearly twice the incidence in the communications, media and technology sector (14 percent). Despite this, respondents from the health care industry underestimate the likelihood of a cyberattack.

As the potential impacts of cyberattacks are transboundary, no country is completely immune to this phenomenon. Ransomware attacks such as *WannaCry* and *Petya* had a global reach affecting care delivery businesses and insurers in the region. Compared to global counterparts, it takes almost five times longer to detect an intrusion for companies in Asia-Pacific.

PERCEIVED THREATS

Participants in the latest Marsh-Microsoft Global Cyber Risk Perception Survey were asked about their perception of cyber loss scenarios that would have the highest impact.

Business interruption was highlighted as the primary cyber risk concern in health care (69 percent), similar to other industries. In 2017, the *WannaCry* global attack succeeded in temporarily shutting down the IT systems of hospitals globally. In more life-threatening cases, cyberattackers could compromise medical devices, such as health-networked MRI machines, as entry points into unsecured Wi-Fi networks, causing critical medical devices to malfunction.

Breach of customer information is a more daunting scenario in health care (67 percent) than in other industries. A medical record holds powerful data on an individual, and when compromised, it cannot be reissued or suspended, such as in the case of a credit card. Cybercriminals can use, and even manipulate, such data to cause personal distress, damage users' reputation or compromise corporate accounts, or to monetize stolen data.

SEVERE FINANCIAL CONSEQUENCES

The health care industry is most concerned about financially motivated threat actors: 45 percent of health care respondents flagged organized crime or hacktivist groups as their biggest source of concern.

Moreover, cyberattacks are perceived to have more severe financial impacts within the health care industry. More than 70 percent of health

EXHIBIT 6: TOP CYBER LOSS SCENARIOS WITH THE LARGEST PERCEIVED POTENTIAL IMPACT

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

care respondents expect that each cyber breach scenario in the industry could cost more than $1 million, as compared to a cross-industry average of 65 percent who feel the same way. In fact, the average total cost of data breaches in FY2017 was $3.6 million per company across sectors according to Ponemon Institute.

HOLISTIC APPROACH NEEDED

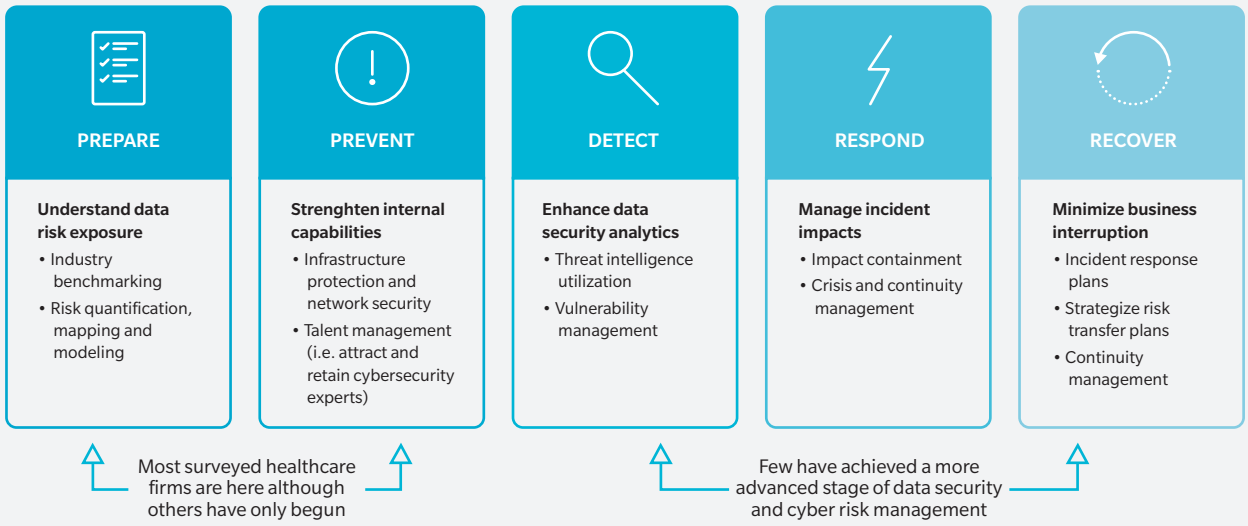
An all-encompassing data and cyber risk strategy is founded upon a thorough assessment of risk, a defined risk appetite and quantification of risk exposure. Then, the risk management strategy drives the right governance, identifies threats and corrective actions, and quantifies the amount of investment necessary to close gaps and vulnerabilities. As part of expectations from management, shareholders, regulators and ratings agencies, industry-specific mechanisms should be designed to safeguard against incidents as well as implement an up-to date, proven cyber incident playbook in case of breaches.

PREPARE AND PREVENT

A strong internal risk diagnostic, as a start, is required to assess a company's cyber risks vis à-vis industry peers. Forty percent of health care organizations still haven't conducted a cybersecurity gap assessment in the past two years, and there is room for improvement in understanding and managing their overall risk exposure. Health care organizations need to identify, define and map specific cyber threats and scenarios to their tangible and intangible assets. Such tailored practices need to become a standard operating procedure across the health care industry.

An educated workforce and a cyber-secure culture is imperative to combat increasingly complex and frequent cyberattacks. Many successful and attempted cyber incidents in health care organizations have been attributed to human error. The need to shift from an IT-driven cyber protection strategy to a mature risk-management discipline requires

EXHIBIT 7: FIVE KEY FUNCTIONS OF THE CYBERSECURITY FRAMEWORK AND RECOMMENDED ACTIONS



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

a bottom up approach, such as creating a more cyber-savvy workforce and strengthening a workplace culture of cybersecurity.

Strengthening network security should be a priority given the proliferation of the Internet of Things and mobile devices with access to corporate networks. Health care organizations should emphasize proven cybersecurity hygiene practices — which are missing for half of the health care industry at present. Respondents to the survey admit to not having hardware encryption (47 percent) and multifactor authentication for corporate networks (50 percent). Only half of the health care respondents improved vulnerability and patch management in the past year.

DETECT AND RESPOND

IT departments are the primary owners and decision-makers for cyber risk management across the health care sector globally. Often, cyber risks appear as an add-on, not part of a holistic risk-management assessment. In taking a more proactive approach to enhance cybersecurity, organizations are encouraged to better understand the return on risk, through quantification, and to build in-house capabilities across multiple interconnected functional areas aligned with their cyber strategy. A management-led approach to set out cyber risk appetite is a first step to recognizing that cyber is a firmwide risk.

Underpinning advanced data resilience frameworks is a strong detection mechanism and holistic incident response plan. Almost two-thirds of health care organizations have not developed a cyber incident response plan.

Most alarmingly, 37 percent of respondents are not sure of the reasons behind the lack of a cyber response plan, while only 22 percent are confident that their organization's cybersecurity and firewalls are adequate.

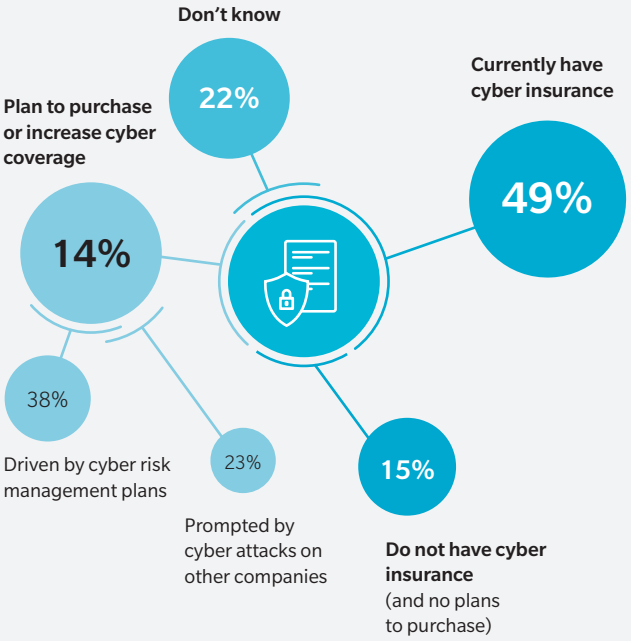
RECOVER

Key risks that health care organizations face today include patient data exposure, shared system data exposure and employee exposure. Recognizing that cyber risks cannot be eliminated, health care organizations are beginning to look to insurance or cyber risk transfer programs as a way to shift the risks as a solution for balance sheet protection and for contractual evidence and compliance. Prompted by the wave of high-profile attacks and new data protection rules, annual gross written cyber insurance premiums have grown by 34 percent per annum over the past seven years. The European Union Agency for Network and Information Security has also found a positive correlation between cyber insurance takeup and the level of preparedness — and health care organizations are only beginning to recognize this.

While less than half of the health care respondents' organizations (49 percent) have cyber insurance coverage, the number is comfortably more than the cross-industry average of 34 percent, but marginally behind financial institutions (52 percent).

The lack of internal agreement on the need for cyber insurance and insufficient budgets and resources are also major impediments (with 22 percent of respondents citing them as reasons) in cyber insurance penetration in the

EXHIBIT 8: HEALTH CARE ORGANIZATIONS' STATUS OF CYBER INSURANCE



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

health care industry. These numbers further support the observation that budgeting in health care organizations is misaligned and technology modernization should be prioritized.

THE HEALTH CARE INDUSTRY NEEDS TO DO MORE

While businesses in key Asia-Pacific markets such as China, Singapore, Hong Kong, Australia, and South Korea are stepping up and improving their cyber insurance coverage in the health care industry, it must be recognized that cyber insurance is not a silver bullet and must be augmented with robust risk strategy and ongoing management.

The health care industry has been taking more actions on average than other industries in the past 12-24 months to prevent and prepare for cyberattacks. For example, 60 percent of health care respondents — as opposed to 51 percent of respondents across industries — indicated that they are assessing the cybersecurity gap to uncover what more needs to be done to protect themselves against future threats. Still, most health care organizations continue to focus more on prevention or preparedness and not sufficiently on detection and response.

INDUSTRY DEEP DIVE

CYBER IN CMT

PROTECTING THEMSELVES AND THEIR CUSTOMERS

Tom Quigley
Communications, Media & Technology, Practice Leader, Marsh

Saahil Malik
Principal, Communications, Media & Technology, Oliver Wyman

As a major enabler of rapid digitalization, the Communications, Media and Technology (CMT) industry, including the Telecommunications sector, is exposed to a broad set of cybersecurity threats. According to the latest Marsh Microsoft Global Cyber Risk Perception Survey, 13.5 percent of the CMT companies reported that they have been a victim of cyberattacks in the past 12 months. Institutions in this space possess critical infrastructure and often act as conduits for critical information and transaction flows — for themselves and for other sectors.

Furthermore, technology evolution (such as increasing Cloud adoption and Artificial Intelligence implementation) is outpacing the ability of CMT companies to manage, respond to and recover from cyberattacks. In some cases, business models are evolving faster than companies' corresponding technical and cybersecurity capabilities. Even though CMT companies were found to be more confident of understanding and mitigating cyber risks than other industries on average, when it comes to recovering from cyber incidents, the CMT industry was just as insecure as others.

Accordingly, it is imperative for this sector to understand the threats, the sources and the impact, and develop a holistic approach towards cyber to future proof its underlying infrastructure, operations and ultimately customer information.

PERCEIVED THREATS

Participants in the latest Marsh Microsoft Global Cyber Risk Perception Survey provided insights on their perceptions of cyber loss scenarios that would have the highest impact. Respondents highlighted business interruption and reputational damage as the top two loss scenarios with the most significant impact.

Business interruption was highlighted as the greatest cyber risk in the CMT industry (77 percent), similar to other industries.

EXHIBIT 9: TOP CYBER LOSS SCENARIOS WITH THE LARGEST PERCEIVED POTENTIAL IMPACT

Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

Communications service providers usually have tight service level agreements and are expected to supply high performance and uninterrupted levels of service to meet customer demands. Accordingly, compromised connectivity or a "failure to perform" could lead to grave disruption, ripple effects and severe loss events.

Along with business interruption, reputational damage was perceived to be extremely harmful to the long-term health of the CMT industry (77 percent, significantly higher than the cross-industry average of 59 percent). For the CMT industry, and particularly in the telecommunications sector, customers, investors and government are likely to evaluate the track record of potential providers as they become more conscious of security.

MULTIDIMENSIONAL THREAT SOURCES AND IMPACTS

The increasingly complex business models of CMT companies, along with the potential for cyber events to impact on the customers they serve, underscore the CMT industry's vulnerability to the human threat factor. Companies in the CMT industry flagged out financially-motivated threat actors (33 percent), and human error and "Rogue" employees (34 percent in total), as their biggest threat concerns. These are difficult to predict and anticipate — and stem from a range of factors, including but not limited to, the prospect of financial gains and coercion, deliberate data manipulation or mere carelessness.

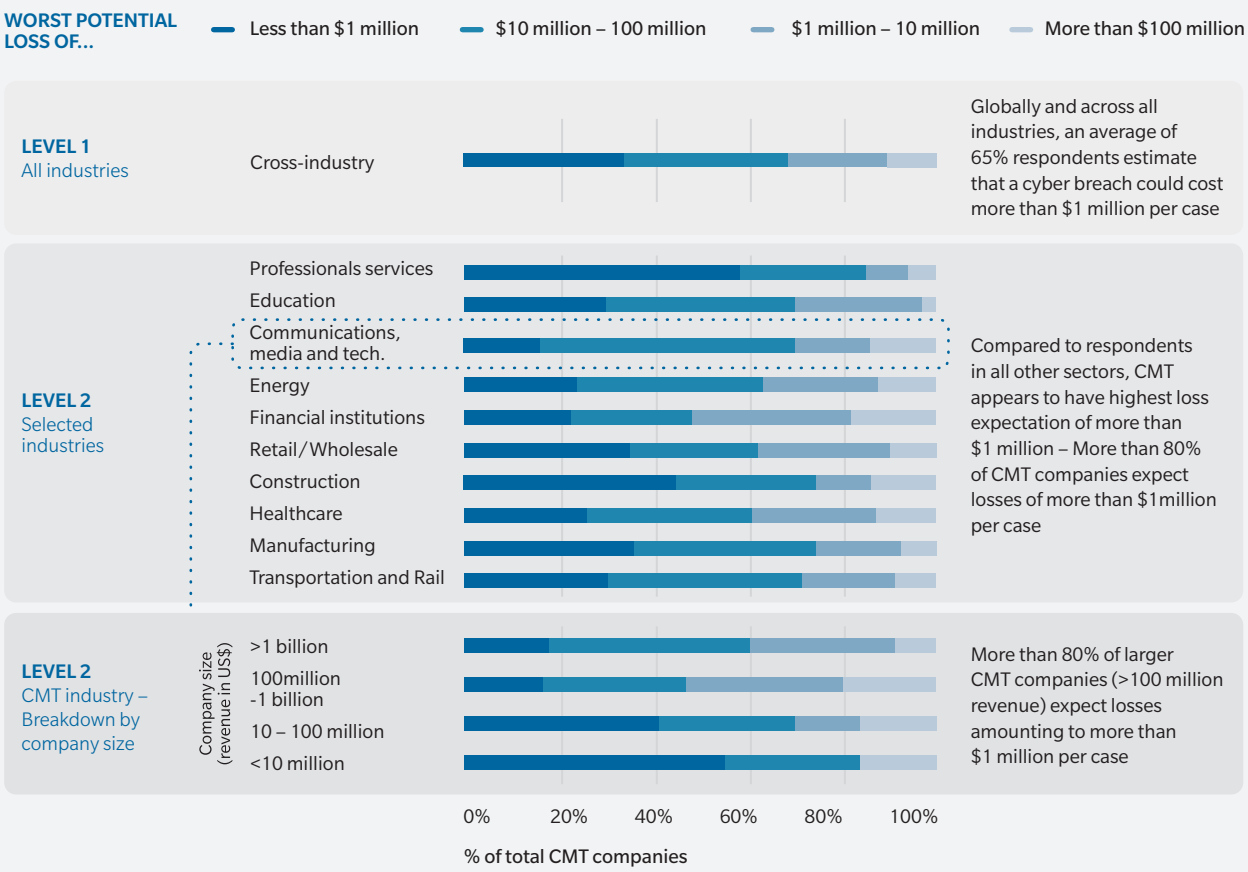
Consequently, the perceived financial impact of a cyber breach for the CMT industry was one of the highest amongst industries. More than 80 percent of the CMT companies expected direct losses of more than $1 million per incident, as compared to healthcare (75 percent), energy (76 percent) and financial institutions (77 percent).

HEIGHTENED REGULATIONS

The risk of regulatory change has increased significantly and the growing attention on regulatory issues, such as cross-border access to data and the repeal of net neutrality in the United States, reflect the growing responsibility placed on telecommunications companies by regulators. Companies in certain jurisdictions are legally required to notify data breaches to their customers and can no longer sweep them under the carpet, while others must now play a greater self-regulatory role in the treatment of data transmissions. For instance, the Electronic Communications Code enacted by the European Commission has outlined new regulatory objectives for the telecommunications sector. It supports the EU's Digital Single Market agenda and significant investment will be required to efficiently comply with multiple, and sometimes conflicting regulations.

The GSM Association (an originally-European trade body that represents the interests of mobile network operators worldwide) has started to work on a cross-industry framework for cyber risk management. Market-specific regulations such as the EU General Data Protection Regulation, China Cybersecurity Law, Singapore Cybersecurity Act, California Consumer Privacy Act and the proposed E-Privacy Regulation will continue to make waves; and regulations around standards and compliance targets, for example, can further complicate the risk-laden operating environment.

EXHIBIT 10: ESTIMATED FINANCIAL IMPACT OF EACH CYBER INCIDENT CASE FROM A TOP-DOWN ANALYSIS



Source: Marsh Microsoft Global Risk Perception Survey 2017

ADVANCING CYBER RESILIENCE IN CMT

A number of companies in this sector have already embarked on various strategic initiatives to improve cybersecurity. For example, in the case of telecom operators, the initiatives range from use of Artificial Intelligence/ Machine Learning technologies, procurement of cybersecurity insurance, focus on internal governance (via appointment of CISOs) and external collaborations around best practice sharing, among others.

As part of expectations from management, shareholders, regulators, and ratings agencies, industry-specific mechanisms should be designed to safeguard against incidents as well as implement an up-to-date proven cyber

incident playbook in case of breaches. Most CMT companies are still putting more emphasis on prevention or preparedness, and do not focus sufficiently on detection and response. Only slightly more than a third of the CMT respondents reported to have a cyber incident response plan in place (39 percent) or have invested in improving cyber event detection (37 percent).

An all-encompassing data and cyber risk strategy is founded upon a thorough assessment of risk, a defined risk appetite and quantification of risk exposure. This risk management strategy should then drive the right governance, identifies threats and corrective actions, and quantifies the amount of investment necessary to close gaps and vulnerabilities.

1. A strong internal risk diagnostic, as a start, is required to assess a company's cyber risks vis-à-vis industry peers. According to the Marsh Microsoft Global Cyber Risk Perception Survey, 42 percent of CMT companies had not conducted a cybersecurity gap assessment in the past two years. CMT companies need to identify, define and map the specific cyber threats to their tangible and intangible assets.

2. Educate workforce and build a cyber-secure culture to combat increasingly complex and frequent cyberattacks. In 2017 alone, for instance, human error was found to increase cloud-related cyberattacks by 424 percent globally, and inadvertent activity such as misconfigured cloud infrastructure was responsible for almost three out of four compromised records. Given the volume and velocity of data within the CMT industry, training of all employees and not just cyber specialists around the handling of customer data and policies associated with sensitive data security is key.

3. Expansion of the cybersecurity program should be a priority given the proliferation of the Internet of Things (IoT), mobile devices with access to corporate networks, and increasing digitalization of physical networks in the CMT industry. Companies should emphasize proven cybersecurity hygiene practices which were missing for half of the CMT companies at present. CMT respondents admitted to not having hardware encryption (42 percent) and multi-factor authentication for corporate networks (44 percent).

4. Embed cyber in enterprise risk management plans. IT departments were perceived as the primary owners and decision-makers for cyber risk management across the CMT industry globally. Companies are encouraged to better understand the return on risk, through quantification, and to build in-house capabilities across multiple interconnected functional areas aligned with their cyber strategy. Moving towards a more "risk-driven" perception will mean making cyber risk management a top-down company-wide responsibility that distributes across departments.

5. Underpinning advanced data resilience frameworks is a strong detection mechanism. Almost two-thirds of CMT companies had not developed a cyber incident response plan yet. Most alarmingly, 32 percent of CMT respondents claimed that their companies lack the expertise to develop one, while only 33 percent were confident that their companies' cybersecurity and firewalls are adequate.

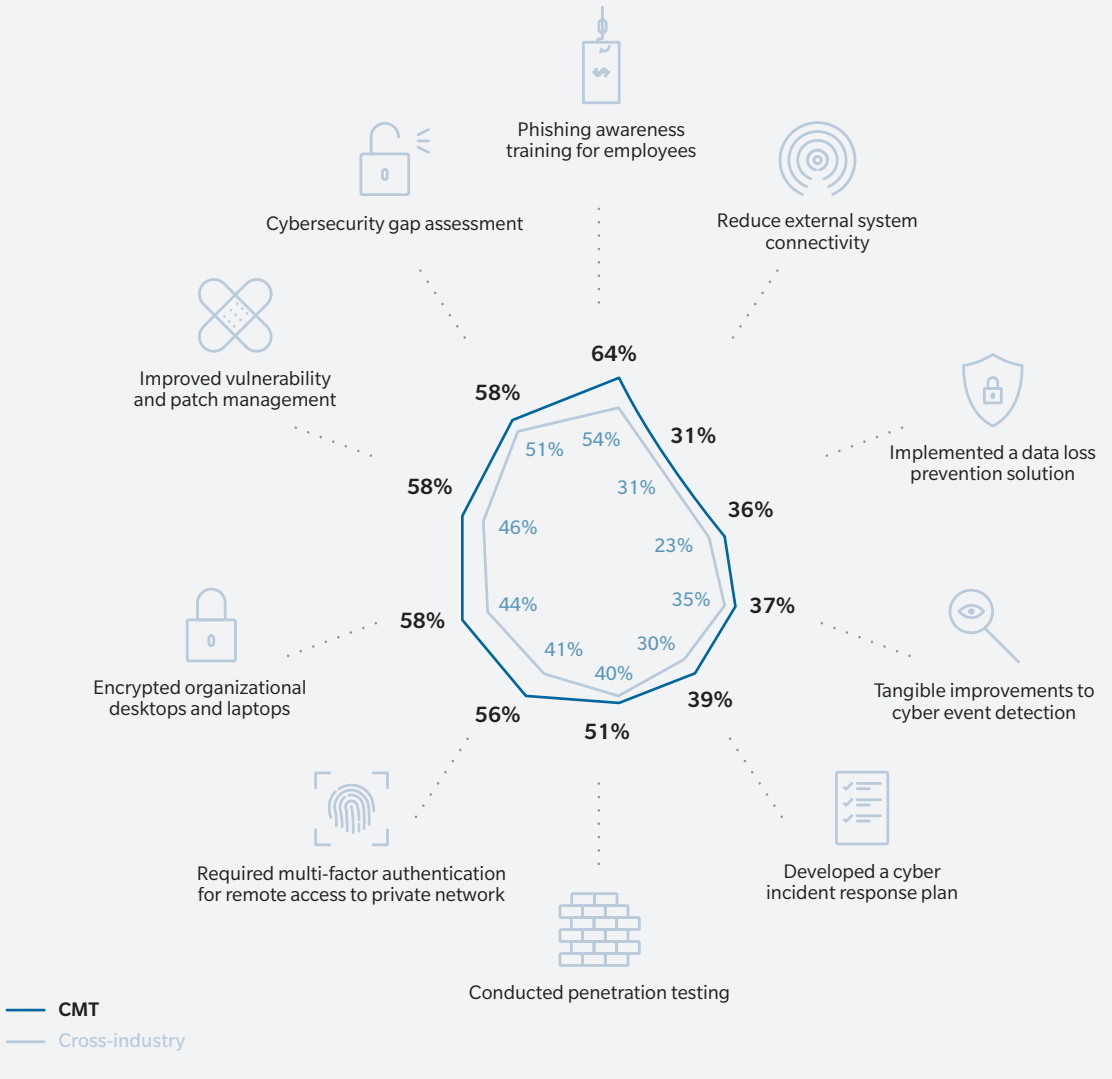
6. Explore a comprehensive set of risk transfer solutions. Given the complexity of cyber risks for CMT companies, only a portion purchase stand-alone cyber insurance. Historically, most of them have been required to purchase Technology Errors and Omissions (Tech E&O)

policies which contain some amount of cyber coverages. However, as the severity of cyber events increases, and as they seek to protect massive research and development (R&D) investments, CMT companies are looking at a range of risk transfer solutions. From adding more stand-alone cyber insurance, to exploring more complex solutions such as integrated risk, alternative risk capital, parametric risk solutions, and captives, there is a recognition that despite their best efforts, there will be loss events to finance.

CALL TO ACTION

In the high-speed race for technology leadership and related uncertainties, companies need to carefully consider the overall approach to security to secure the right balance between security and flexible of use. Only with a stronger position in cyber risk management, with cyber embedded into their business cases, CMT companies can potentially differentiate themselves and bring greater value to their customers and clients.

EXHIBIT 11: ESTIMATED FINANCIAL IMPACT OF EACH CYBER INCIDENT CASE FROM A TOP-DOWN ANALYSIS



INDUSTRY DEEP DIVE

CYBER RISK IN ASIA

RAMIFICATIONS FOR REAL ESTATE AND HOSPITALITY

Jaclyn Yeo
Research Manager,
Marsh & McLennan Insights

Meghna Basu
Research Analyst,
Marsh & McLennan Insights

Globally, the real estate and hospitality (RE&H) sector is the fourth most frequently targeted industry, accounting for almost 11 percent of data breaches in 2016-2017. The RE&H sector is susceptible to cyber-attacks and is a convenient target for perpetrators as they sit on vast treasure troves of financial assets, personal identifiable information (PII), external credit scores, and internal intellectual property (IP) data.

With the onset of the Fourth Industrial Revolution (4IR), confidential information of both companies and end users is also becoming more exposed to criminal activity as the RE&H sector is becoming more connected to the internet than ever. It is crucial for firms to note how their technology adoption is broadening their surface of attack, and for risk managers to identify vulnerable access points that can be exploited by cyber criminals.

INCREASING VULNERABLE ENTRY POINTS

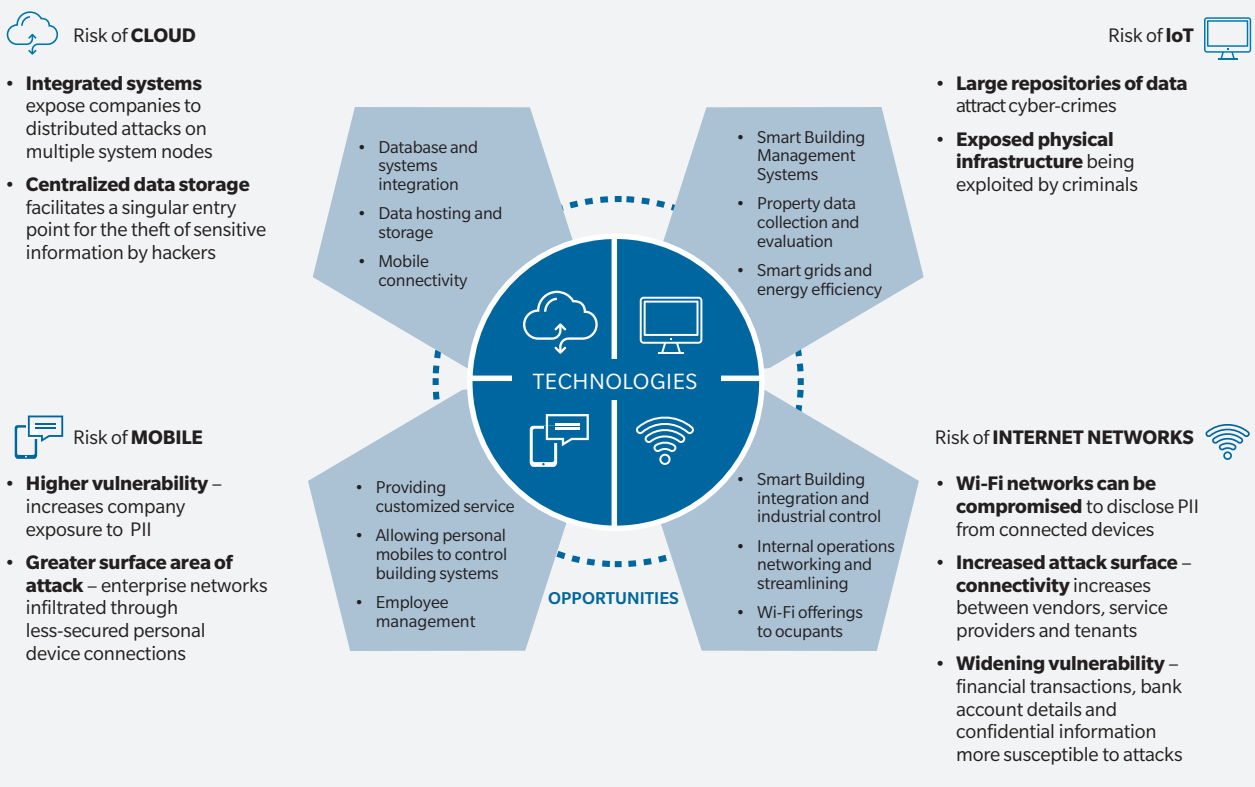
Complications in terms of additional security may also be created without the companies knowing. For example, economic development and urbanization across Asia spurred by various smart city initiatives rapidly create additional data and connect that data to the built environment. Likewise, RE&H firms in the region will be increasingly developing, selling, and using buildings that are amassing vast amounts of sensitive and personal Big Data. These buildings centralize the collection of data across clients, vendors, and businesses, making them prime targets for attack. As a result, increase in connectivity between the RE&H sectors and the built environment adds to the burden on firms to strengthen their cybersecurity measures and ensure adequate client-data protection.

Growing adoption of emerging technologies enable both the amassing and transmitting of Big Data and financial information, both of which pose prime targets for cyber-attacks. Eventually, this will lead to an exponential increase in the number of endpoints for potential attacks.

IN THE SPOTLIGHT

Despite the increasingly innovative techniques used in cyber-attacks, many attackers are still making use of traditional tactics to gain access. They are also targeting executives and other frontline employees to trick them into activating malicious software codes that provide easy access into an organization's network system. The following examples illustrate some old-school techniques used by cyber-attackers.

EXHIBIT 12: RISKS AND OPPORTUNITIES IN ADOPTING EMERGING TECHNOLOGIES IN THE RE&H SECTOR



Source: APRC analysis

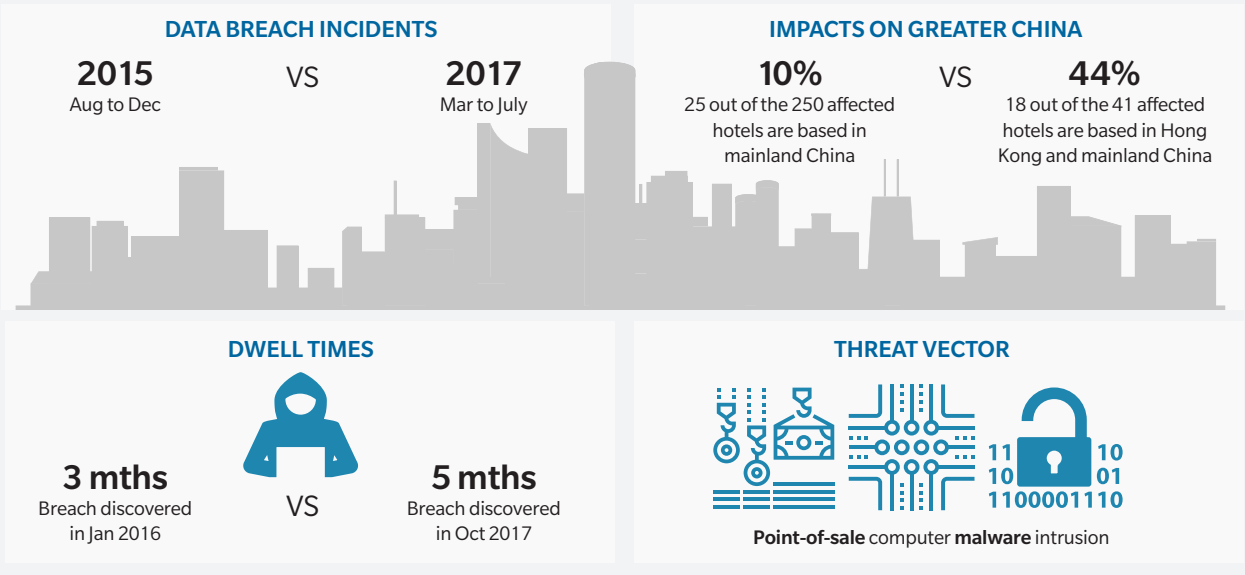
Example 1: A Perth-based real estate agency faced near-theft in September 2016, when there was an unauthorized withdrawal request of A$500,000 (~US$384,000) from the agency's trust account. The cyber criminals had managed to install malware onto the firm's computer systems, which was believed to have infiltrated the system when staff members unknowingly clicked on malicious website links from phishing emails. Once installed, the malware allowed the criminals to record keystrokes and identify the firm's bank login details.

Fortunately, as part of the real estate agency's best practice to reconcile trust accounts daily, the unauthorized withdrawal was discovered in time by a staff member, and the relevant bank retracted the fund transfer before the funds reached the criminals.17 Besides enhancing training programs to raise cybersecurity awareness and educating employees to recognize malicious phishing emails, the real estate firm subsequently introduced a more secure network connection to its bank, which included anti-malware software, and multi-party and multifactor authentication features.

Example 2: A reputable hotel chain suffered two data breaches in 2015 and in 2017 when its cybersecurity systems were compromised, leaking PII and Payment Card Industry information (PCI) of their customers worldwide. While they suffered a considerable hit in 2015 as well, the impact on China and Hong Kong in the 2017 breach was significantly greater, illustrating that cyber threats are on the rise in Asia and impacting the region more than earlier. Both cyber intrusions were caused by malware that infected the hotel chain's payment processing systems, exposing PCI, such as cardholder names, card numbers, expiry dates and internal verification codes—all of which were obtained from credit cards manually entered or swiped at the front desks.

The POS malware breach was caused by an insertion of malicious software code from a third party onto several hotel IT systems via the POS computer. For both incidents, the company did not disclose how many customers were potentially affected and it did not know exactly whose details may have been compromised.

EXHIBIT 13: SUMMARY STATISTICS OF THE HOTEL CHAIN HACK



Source: APRC analysis; dataset from Marsh Hong Kong and Marsh/Microsoft cyber surveys

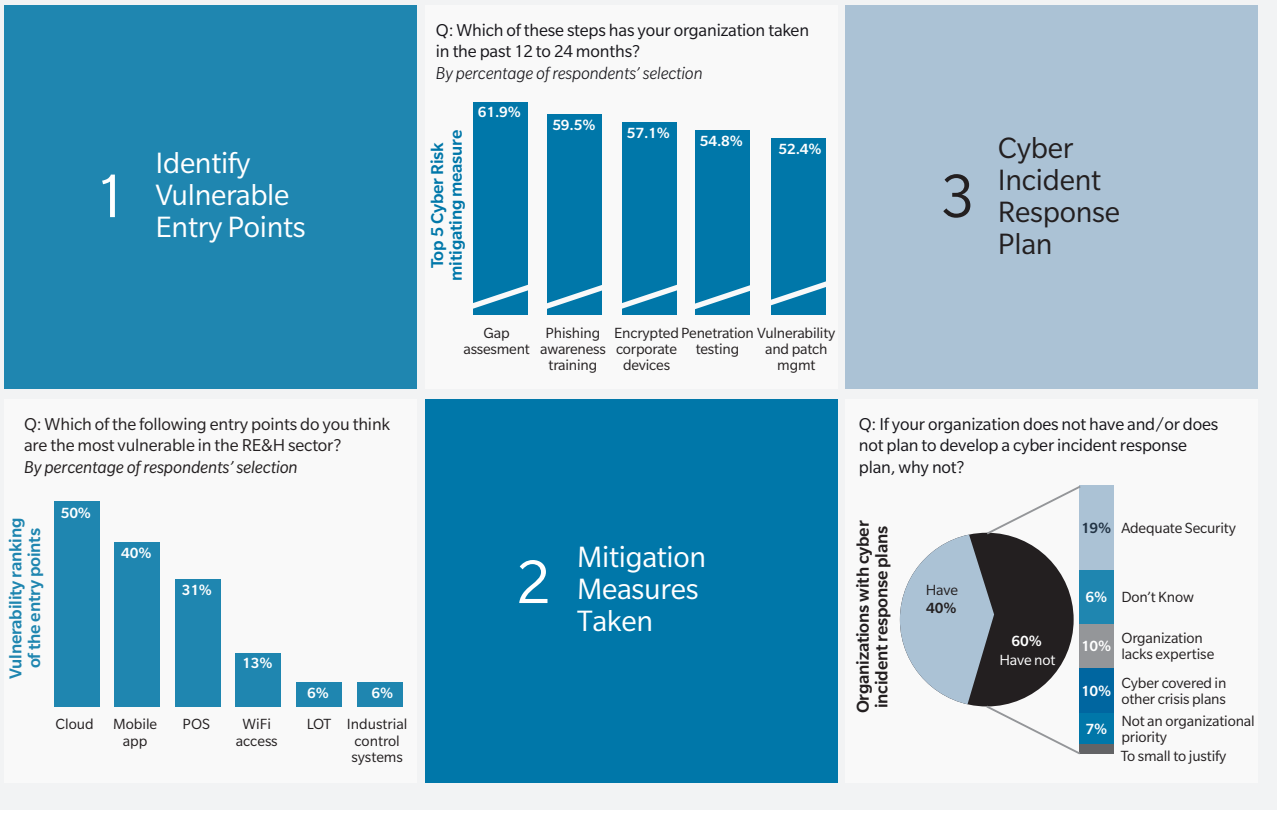
LARGELY UNDER-PREPARED

According to the latest Marsh Microsoft Global Cyber Risk Perception Survey and Marsh Hong Kong Cyber Risk Survey, the lack of cyber preparedness by the RE&H sector may be attributed to the following:

- A widening perception-reality gap
- Insufficient defense against the expanding attack surface
- Indifference towards purchasing cyber insurance

There is wide chasm between how prepared firms think they are for an attack, and how protected they actually are. For example, a large majority (65 percent) of respondents from the RE&H sector in Asia ranked cyber threat as a top-five corporate risk concern; but 85 percent of the surveyed RE&H respondents in Hong Kong spend less than 10 percent of their annual budget on cybersecurity. Furthermore, firms in the RE&H sector appear mostly confident (88 percent) that they understand their cyber risk exposure, but 48 percent are either unaware of or do not have any methods to measure their cyber risk exposure.

EXHIBIT 14: ECYBER DEFENSE STRATEGIES UTILIZED BY THE RE&H SECTOR



Survey respondents also assumed that their internal cybersecurity frameworks were sufficient to prevent cyber-attacks from happening. Six out of 10 RE&H companies do not have and do not plan to develop a cyber incident response plan, despite one in five having responded that they had experienced a cyber-attack in the past 12 months alone. Despite a high chance of being attacked, most of the firms have not prepared to respond to an attack.

Despite being able to identify key entry points and having put in place some form of cybersecurity measures to protect against cyberattacks, the awareness is not matched with adequate level of defense. Sixty percent of organizations surveyed are without proper incident response plans; 10 percent cited the lack of expertise as one reason for not having an incident response plan, while another 10 percent suggested that cyber incidents are covered in other crisis plans and thus need not to be singled out as a standalone plan for incident response.

Huge economic losses are highly likely to occur due to business interruption as critical functions, data protection, and loss prevention backup solutions may cease operations in the event of a cyber-attack. Without proper crisis management and stakeholder engagement, normal business operations will further be delayed as organizations scramble to carry out post-incident forensic investigations and notify affected individuals.

There is also room for improvement in recognizing the significance of cyber insurance in RE&H sector. 31 percent indicated that they have plans to purchase or increase cyber insurance over the next 12 months, primarily driven by internal cyber risk management plans, or prompted by successful cyber-attacks on other companies. In contrast, one in 10 RE&H companies do not have and do not intend to purchase cyber insurance coverage, citing limitations in coverage, cost considerations or the belief that cyber risk was adequately covered in other policies as key reasons.

It is unsurprising that regulatory factors such as legislations or rating agency standards have negligible impact on the decision to purchase insurance in Asia-Pacific, since legislation and enforcement are currently struggling to keep pace in this region. With the EU's General Data Protection Regulation (GDPR) in place, cybersecurity laws and mandatory data breach disclosures across the region is rising. Further, regardless of location, any organization holding on to the personal data of any EU citizen will be affected by the GDPR. As such, cyber insurance adoption rates across sectors in Asia may increase with corporates using the GDPR compliance process to strengthen their key cyber risk practices.

GETTING CYBER-READY

Organizations in the RE&H sector in Asia are more susceptible to cyber-attacks now than ever before. Despite the real estate sector traditionally regarding itself as an unattractive target for hackers, key trends in the region suggest that the real estate, as well as the hospitality sector, are increasingly exposed to cyber vulnerabilities.

REGULATIONS

GENERAL DATA PROTECTION REGULATION (GDPR)

THE DOOR TO THE FUTURE?

Kaijia Gu
Partner, Pricing, Sales & Marketing,
Oliver Wyman

On May 25, 2018, we cross the long-awaited threshold of the General Data Protection Regulation (GDPR) as new legislation comes into force across Europe. For organizations, this will be a radical shake-up across the region of how they approach data privacy — with sizeable financial and reputational consequences. But outside of compliance, other forces are at play.

Until now, GDPR discussions have largely focused on compliance requirements. Being a risk conscious sector, most large insurers and wider financial services firms have been diligently carrying out GDPR readiness programs, ensuring that all the compliance "boxes" have been firmly ticked. For some, GDPR is just a hugely expensive compliance exercise. Yet, treating GDPR as merely a governance issue would not only miss potentially significant strategic opportunities but also pose a threat, should someone else get there better and faster. Oliver Wyman believes that smart companies will leverage this opportunity to open the door to a future where new and disruptive business models can address and solve complex consumer challenges, and provide enhanced value to customers.

LEVELED PLAYING FIELD

GDPR gives the ownership and control of data usage back to customers. Therefore, large companies that today capture and use consumer data can no longer claim this data as their own asset. Crucially, at a customer's request, organizations need to allow data to be transferred to any third party. This will no doubt lead to a dramatic leveling of the playing field between incumbents and new entrants. Post-GDPR, large incumbents will no longer have a monopoly on consumer data, and will need to defend their market positions with different competitive advantages. On the other hand, this is great news to new entrants, especially to ambitious and nimble InsurTech startups, for whom in the past data was difficult and expensive to acquire.

Take the example of policy renewals. For many years, insurers have relied on lengthy quotation forms and clunky comparison processes to deter customers from taking their business elsewhere. But what if filling in cumbersome questionnaires could be circumvented with one click? Post-GDPR, one significant game changer will be the "one-click-quote," so long as customers give their consent to porting their data from elsewhere. This easy lifting of personal data from an existing supplier poses the major threat of increased attrition levels, and massive profit erosion.

TRUST AND REWARD

With data no longer being "walled in" by incumbents, organizations will need to apply fresh thinking to how they differentiate themselves and thus seize a competitive advantage. For increasingly discerning customers, smooth customer experience will be regarded as merely the base line.

Two notable additional factors will be on the minds of insurance customers of the future.

1. "IS MY DATA SAFE?"

High-profile data breaches, increased fraud, questionable social media usage, and headlines claiming wide-scale political manipulation have raised the notion of data safety in the public's collective conscience. Oliver Wyman's Britain's Digital DNA survey established that the biggest fear consumers have about the digital world is the loss of privacy. Over half of the consumers surveyed were worried about sharing personal information online. In future, consumers will be demanding greater transparency in data usage; GDPR makes it mandatory for companies to provide that.

2. "AM I GETTING VALUE FROM SHARING MY DATA?"

Given the explicit consents required to use and share consumer data, consumers will increasingly realize that their data holds a lot of worth. Thus, they will be looking to get more value from sharing their data, be it exceptional service and experiences, personalized products and offers, or discounted products and services. These incentives will become the new currency in exchange for keeping or passing on personal information.

The above points reinforce the need for insurance business leaders to adopt a customer centric strategy that focuses on value, from both a trust and a commercial perspective. Here we list some of the likely compelling value propositions of new business designs and the "score board" of incumbents and new entrants based on their fundamental business "DNA".

NO-REGRET MOVES FOR INCUMBENTS

Strategically speaking, it appears that GDPR brings more threats than opportunities for incumbents by leveling the playing field. However, in the ever-changing and increasingly dynamic insurance ecosystem, the boundary between incumbents and start-ups is quite fluid and there are some enduring benefits to incumbency. Incumbents typically have amassed a large customer base over time and built a trustworthy brand. Many have established a deep understanding of consumer behavior and needs. The key question is whether they become aware of the strategic implications and decide to move out of their comfort zone, adopting a nimble and agile approach in developing business models. Incumbents will also need a major rethink in their assets, capabilities, capital, and talent.

Whether offensive or defensive, we see several "no-regret moves" for large incumbents as the GDPR door opens.

STRATEGIC MAPPING

Incumbents should ask themselves "What will I want to be known for in the next five years, or even 10 years?" They should analyze where the industry is heading on a macro level and align their strategy with a future-focused value chain. While this is critical with or without GDPR, the impending regulation provided a good trigger for companies to embark on this journey — even if they haven't yet started.

DATA ASSET EVALUATION

Future success for incumbents may depend on how well they understand which data assets they require when building the business of the future. Likewise, they will need to comprehend how to protect those data assets they already possess (so that consumers don't ask for their data to be erased), and obtain those that they don't yet have.

AGILITY

The life cycle for new business models is accelerating at a rapid pace in our current era. The old approach of spending years and devoting an army of people to build a "perfect" model does not work anymore. Agile development, software development and operations (DevOps) environments, cloud-based technology, and customer centricity will be essential ingredients to craft new business models.

COMMERCIAL EXCELLENCE

This might seem counterintuitive but, given the margins already competed away, an incumbent successful in reinventing its business model requires potentially significant investment. The ability to optimize the existing business to generate cash and headroom to fund the new business is crucial for most incumbents.

A FINAL WORD

Insurance is a complex business and, from May 25 onwards, the industry will experience considerable transformation. Inertia will make this process gradual rather than overnight. For those who choose to not look ahead and content themselves with simply complying with GDPR, however, the risks of being left behind are very real. It is likely that they will eventually be sidelined by bold contenders — incumbents and new entrants alike — which are willing enough to embrace change and are ready to build exactly the type of business they want. Opportunity is knocking at the door — we are curious to see who's answering.

REGULATIONS

AMID REGULATORY SCRUTINY

FINANCIAL INSTITUTIONS MUST MONITOR THIRD-PARTY CYBER RISK

Alex deLaricheliere
Managing Director – US Banking & Capital Markets, Marsh

Cybersecurity ranks among the top concerns for banks, insurers, and other financial institutions, which can represent prime targets for cyber-attackers and be vulnerable to potential disruptions because of their often-complex technology systems and the valuable financial assets and rich customer data they can hold. As awareness of cyber risks has grown, many financial institutions have developed robust internal capabilities to deter cyber-attacks and prevent technology interruptions. But perhaps equally important — for both organization and regulators — are your vendors' cyber risk management practices.

PROBING THIRD-PARTY CYBER RISK

Since the financial crisis of the late 2000s, the Federal Reserve, Securities and Exchange Commission, Office of the Comptroller of the Currency, and other regulators have heavily scrutinized the risk management practices of financial institutions. One of their biggest areas of focus has been technology risk.

Recently, both the industry and regulators have honed in on the risks presented by vendors. Many large financial insti tutions have developed vendor management offices with the express mission of policing and overseeing their companies' slate of suppliers and other third parties they work with. While regulators seem to appreciate this approach to risk management, they have not let up. Instead, they are now probing deeper, looking at second- and third-tier vendors — the ones that financial institutions' vendors rely on themselves.

For financial institutions, those vendors represent potential cyber risk vulnerabilities that could cost millions. Vendors that hold or process data could become victims of hacking attacks themselves or provide an entryway for attacks on financial institutions' corporate networks. Technology interruptions at vendors can also disrupt financial institutions' operations.

EXAMINING YOUR VALUE CHAIN

Just as companies that produce or sell physical products often regularly audit their supply chains to assess vulnerabilities to natural hazards and other physical risks, financial institutions should assess their value chains, seeking to gain insight into the cyber risk mitigation practices of their first-, second-, and third-tier suppliers.

Your organization may already have this insight. If not, you should:

- Assess existing third-party management processes and data needs, identifying all supplier and third-party relationships and scrutinizing contractual language related to data security
- Develop a risk management framework that includes exposure to each supplier and the risk of breach or business interruption and recommended actions
- Continuously monitor your vendor network's security posture, identifying those companies that present risks to be more closely examined
- Establish a protocol for action that allows you to systematize management of your third-party risk

It's also important to quantify your cyber risk, including third-party exposures. A scenario-based analysis of your cyber risk can help you estimate the likelihood and potential severity of a cyber event involving a vendor — something of great interest to financial regulators. Scenario modeling can also help you identify and evaluate potential risk mitigation and insurance options.

You might already have an effective cybersecurity program in place within your organization, but that might not be the case with your vendors — or the vendors they rely on. Take these steps to better understand and manage your third-party cyber risk.

GUARDING THE PUBLIC SECTOR

SEVEN WAYS STATE GOVERNMENTS CAN BOOST THEIR CYBERSECURITY

Ryan Harkins
Director of State Affairs & Public Policy, Microsoft's U.S. Government Affairs

Erin English
Senior Security Strategist, Microsoft

Hackers are increasingly targeting state governments for their administrative capabilities. How should the public sector guard against such threats?

Across the United States, state and local governments are making significant investments in information technology so that they can take advantage of the same efficiencies that are powering the private sector's charge towards the Fourth Industrial Revolution. This is creating fresh opportunities, but also new risks. US state governments have been targeted at an alarming rate by adversaries that are increasingly sophisticated and driven by broader motives. Consequently, state governments find themselves on the frontlines because of the role they play in the delivery of essential services or their administration of industry and commerce. Indeed, state agencies may hold vulnerable troves of personal data, making them desirable targets for cyber attackers. Perhaps the most concerning threat comes from nation-state attackers who are eager to exploit state government networks.

Naturally, state policymakers are anxious to find ways to protect their systems. They face challenges as they adopt new technologies, grapple with limited budgets, and push to keep pace with rising threats, all the while providing critical services for their constituents. To address these challenges, states must think holistically and adopt comprehensive, risk-based cybersecurity strategies, rather than simply responding to the most recent cybersecurity incident or headline. This requires taking the long view and instilling best practices that are flexible and capable of adapting to an evolving threat landscape.

In July 2018, Microsoft detailed seven best practices that every state should implement to protect its government and constituents from cybersecurity threats. These principles are based upon Microsoft's expertise and experience in combating threats in cyberspace globally.

1. GROUND CYBERSECURITY POLICY IN ESTABLISHED GUIDELINES AND STANDARDS

State governments should adopt federal frameworks (such as the NIST Cybersecurity Framework) to help lay the groundwork for strong, effective state cybersecurity policy. The framework provides a high-level, strategic view of the lifecycle of cybersecurity risk to help states better understand their cybersecurity risk, and it enables them to apply the principles and best practices of managing risk to improve the security and resilience of critical infrastructure and services.

2. ESTABLISH AN ONGOING CYBERSECURITY ADVISORY COUNCIL WITH INDUSTRY AND ACADEMIA

In many states, most cybersecurity expertise lies across industry sectors and academic disciplines, and many of these experts would likely be eager to contribute to state cybersecurity policy. Each state should utilize these assets and create a cybersecurity advisory council. These councils can bring together industry experts, academics, and public sector leaders to develop cybersecurity strategies for state governments and help respond to ongoing threats.

3. CREATE A CULTURE OF CYBERSECURITY

In many cases, the weakest point of security for an organization, including state governments, is its personnel. Reversing this phenomenon requires empowering employees with the skills they need to stay ahead of and be prepared to protect against increasingly sophisticated threats. However, only eighteen states today require cybersecurity training for all of their employees. We believe it is essential to develop a knowledgeable, cyber-literate workforce to reduce cyber risks to the state. To create a

culture of cybersecurity and reduce the risks from cyberattacks, state governments should implement a robust cybersecurity training program for all state employees.

4. LEVERAGE NEW RESOURCES TO ENHANCE ELECTION INTEGRITY

Since 2016, new resources designed to enhance the integrity of elections have been made available to states. Among them are federal funding for securing elections, free election security programs coordinated by the Department of Homeland Security (DHS), technologies to help protect political campaigns (e.g.,Microsoft AccountGuard) and support robust post-election audits (such as risk-limiting audits, or RLAs), and new election security best practice guidebooks.

5. INTEGRATE CYBER RESILIENCE INTO EVERY STEP OF STRATEGIC PLANNING

As state governments develop and implement strategies to protect their IT assets and data from cybersecurity threats and other disasters, they must also focus on making these services data resilient. In other words, ensuring state networks can adapt, recover, and continue to operate if and when an attack happens. Embracing cyber resilience can not only help to ensure that states are more secure; it can create opportunities for states to build comprehensive, long-term strategies that set them on a path toward digital transformation. Moreover, it can promote a culture of innovation, generate new avenues for investment, and contribute to a vibrant and economically competitive state.

6. CONSIDER CYBER INSURANCE TO HELP PROTECT STATE ASSETS

Cyber insurance can help states complement their cyber risk management process by providing financial protection against risks that cannot be fully mitigated. The benefits of cyber insurance are not just financial — cyber insurance is, of course, no substitute for a robust cybersecurity strategy and practice. To qualify, insurance companies typically require that states meet a certain set of cybersecurity standards such as regularly training staff, encrypting sensitive data, and keeping servers up to date. It therefore forces state governments to implement strong cybersecurity practices, increasing the overall health of their technology systems and protection of their data.

7. STRONG PROCUREMENT POLICIES AND COMPLIANCE ARE ESSENTIAL

As data being created and stored by states has increased, so too have states' legal and regulatory obligations. It has become increasingly important that states examine their compliance and procurement policies, and ensure that their vendors can demonstrate that they will enable compliance through their tools and services.

ADVANCING STATE GOVERNMENT CYBER RESILIENCE

Policymakers today must continuously make thoughtful, multidisciplinary decisions to respond to the challenges of their growing populations, increased interconnectivity, changing expectations of government services, and the uncertainties of security in cyberspace. Implementing cybersecurity and policy frameworks to better protect state governments can help meet those challenges while enabling state employees to better protect their systems. Following the recommendations and strategic approach laid out in these seven principles can help states innovate, advance their security goals, and better protect their information technology systems and their citizens.

CYBER RESILIENCE STRATEGY

WHEN THE GOING GETS TOUGH, THE TOUGH GET GOING

OVERCOMING THE CYBER RISK APPETITE CHALLENGE

Michael Duane
Partner, Finance & Risk Management,
Oliver Wyman

Rico Brandenburg
Partner, Risk & Public Policy,
Oliver Wyman

Matthew Gruber
Engagement Manager,
Oliver Wyman

The scale of recent attacks and resulting media attention, supervisory pressures to upgrade cyber risk management, and the pace of technology innovation to keep up with are increasing rapidly. These factors are compelling financial institutions to have a clear understanding of the cyber risks they face, and to determine the level of cyber risk the institution is willing to accept.

An effective, measurable, and actionable cyber risk appetite (the set of statements and metrics that articulate the views of the Board of Directors and senior management about the scope and level of cyber risk the institution is willing to accept) provides institutions with a risk management capability to set and communicate strategic boundaries for cyber risk-taking across the institution.

In our experience, the journey of developing a cyber risk appetite is as important as the cyber risk appetite itself. Therefore, it is essential to engage senior management and the Board of Directors using a structured design approach that combines creating awareness and getting input. In so doing, it becomes clear why zero appetite is just not realistic.

CYBER RISK APPETITE: A STRATEGIC TOOL TO MANAGE THE RAPIDLY GROWING EXPOSURE

As the scale and frequency of publicly reported cyber events — not to mention non-public events and near misses — continue to rise, cyber risk is becoming an ever more prominent topic for senior stakeholders across major financial institutions and their supervisors. In response, both internal and external stakeholders are expecting institutions to develop an effective, measurable, and actionable cyber risk appetite and to embed it into the institution's decision-making processes and governance (e.g. IT spend).

A well-designed cyber risk appetite is a powerful risk management tool for an institution. It provides senior stakeholders (especially those not buried in day-to-day operations, like the Board of Directors and supervisors) with a crisp articulation of the level and type of acceptable cyber risks for the institution, putting cyber risk on par with other, more familiar risks like credit risk, market risk, and operational risk. As a result, an institution's cyber risk appetite can be leveraged as an anchor point to prioritize cybersecurity investments, both within cyber risk and across other risk types, to align the institution's cyber posture to its risk appetite. When cascaded through the institution, cyber risk appetite becomes a powerful communication tool that enables cyber risk to be more tangible across business and support functions, raising awareness for cyber risk and for the need to manage it at every organizational level.

DEFINING AN EFFECTIVE CYBER RISK APPETITE IS HARD

Crafting an effective cyber risk appetite is not a trivial undertaking, and getting it right is hard (despite a common belief that it's not too difficult to "write down a few statements that characterize the institution's risk-taking capacity"). But the consequences of a poorly articulated cyber risk appetite can be significant. A cyber risk appetite is more than just words and metrics. Appropriately adopted by and communicated throughout an institution, it can have tangible impact on business activity and behavior. Poorly articulated statements can cause confusion and may cause employees to take unproductive or potentially harmful actions.

BUT, IT'S IMPORTANT TO GET IT RIGHT

Given the importance of a cyber risk appetite, the challenges in defining it meaningfully, and the consequences if institutions get it wrong, employing a structured approach is critical, starting with a commonly agreed-upon set of design principles.

An effective, measurable, and actionable cyber risk appetite starts with the material cyber risk themes identified through a cyber risk identification and assessment process. A particular theme (or group of themes) is then linked to a statement that is subsequently cascaded to the different elements of the attack surface (i.e., workers, IT architecture, third-parties, customers). At that level, the statement is generally concrete enough to link metrics and thresholds designed to measure compliance with the statement. Metrics are aggregated and rolled up to the Board level using appropriate aggregation approaches (e.g., worst-off). Using this approach allows institutions to derive risk appetite statements and metrics that can be effectively translated into business decision processes to ensure that risk appetite is embedded in the institution.

Linking relevant quantitative metrics to well-designed qualitative statements is important to measure the level of compliance of the institution with the risk appetite statement. Often more than one indicator is needed to adequately reflect a given risk appetite statement. The metrics selection process should ensure that (a) the metrics have a clear link to the statement, (b) data required to measure the metrics are available or can be collected in a timely fashion, (c) the metrics are measuring risk (rather than pure performance) and the design of the metrics is forward looking where possible, and (d) the metrics are simple and easy to interpret for an audience less familiar with the topic.

Changes in the external environment, the internal preparedness, or the business model can significantly impact the threshold for cyber risk metrics. Therefore, thresholds should be reviewed and refreshed at least annually, or more frequently in case of metrics that are impacted significantly by changes in external or internal factors.

But measuring alignment to the cyber risk appetite is not enough. To embed cyber risk appetite within the institution, it is important to link tangible actions to cyber risk appetite threshold breaches. Actions should include a root cause analysis and a remediation plan to address the underlying problem that is discussed with senior management and the Board of Directors. The discussion in senior management and Board of Directors committees creates awareness, and ensures that remediation plans address structural issues and that management has the relevant resources to address the problem.

KEY STEPS FOR CRAFTING AN EFFECTIVE CYBER RISK APPETITE

Designing an effective cyber risk appetite for an institution starts at the Board of Directors level. Once the Board-level cyber risk appetite is established, the statements and metrics can be cascaded to lower levels of the institution. Starting from the Board of Directors, we recommend using a structured approach to designing an institution's cyber risk appetite framework.

Designing an effective cyber risk appetite is crucial for any institution that has exposure to the internet. Although it can be a daunting task, getting it right can deliver real value for the institution. A well-designed cyber risk appetite (including statements and metrics) serves as a powerful tool for prioritizing cybersecurity investment, making sound cyber risk management decisions, and creating awareness for cyber risk across the institution.

PREPARING FOR A CYBER ATTACK

James Cummings
Senior Advisor, Cyber Risk,
Oliver Wyman

Paul Mee
Partner and Cyber Lead,
Oliver Wyman

"Tabletop" exercises help develop "muscle memory" to defend against internal and external system breaches.

Cybersecurity in many organizations has over the last few years been exposed as kind of a Swiss cheese solution, as cyber criminals have found vulnerable entry points to pull off major hacks costing companies hundreds of millions of dollars. In countless cases, companies have failed to erect strong defenses, or failed to recognize and quickly react to an attack. Clearly, cybersecurity needs to be elevated to the top levels of risk-mitigation strategy, alongside currency risk, natural disaster, and terrorist attacks.

In our view, cyber "tabletop" exercises can be enormously valuable for many companies, especially those with huge daily revenues and/or thousands of transactions. Tabletop exercises can start with straightforward scenarios and proceed to more sophisticated simulations with complicating factors. A given exercise is structured to simulate a real attack, with the various stakeholders — C-suite executives, heads of business units, or both — responding with potential actions and reactions, as well as their assumptions and expectations behind those actions.

A prepared moderator and team facilitate moves, putting defenders inside the mind of a hacker/criminal. The moderator applies complicating factors such as misinformation, distractions, extreme weather events, or timing. A team of analysts observes the simulation and upon its conclusion facilitates a "hot wash" — distilling the shortcomings, failures, and gaps, and translates them into a set of practical recommendations.

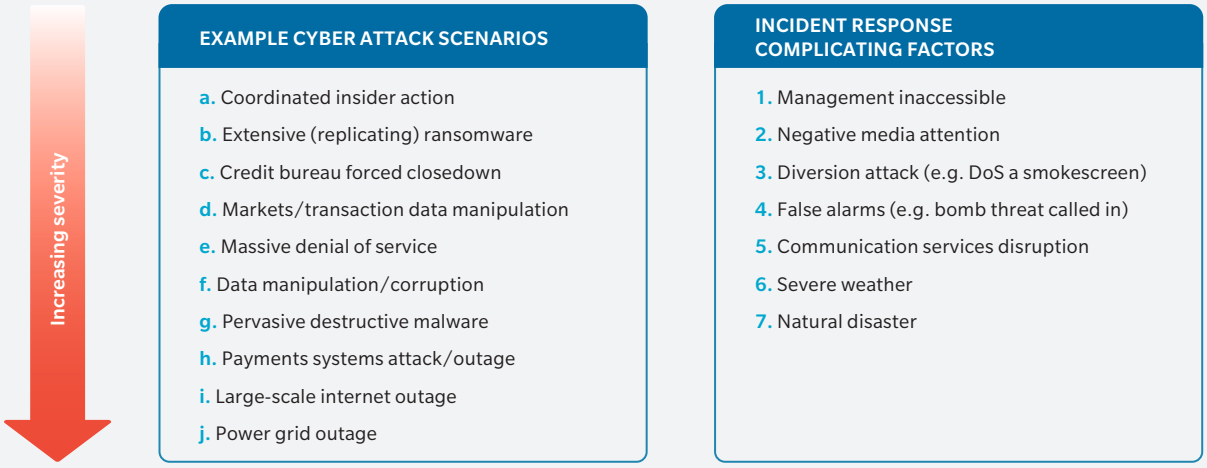
ROADMAP FOR A TABLETOP CYBER EXERCISE

A company should review its particular threat landscape and outlook, with the broad goals of identifying gaps in cyber resilience and optimizing response governance (who calls whom when?). Based on the threat landscape recent attacks, especially to peer organizations — you can customize the exercise with cyber-related risks specific to your organization's ecosystem. From the outset, it's essential to define what a given organization or community wants to learn from a cyber tabletop exercise.

EXHIBIT 15: DEFINE LEARNING OBJECTIVES

1. What is the full scope of parties that should be involved throughout a major cyber incident?
2. What relationships with government and other agencies, and law enforcement, need to be in place?
3. What leadership arrangements are needed and how does this vary by incident type/severity?
   For example, when would the mayor's office lead the response?
4. Where do governance arrangements and decision rights need to be better defined?
5. How will key decisions be made, communicated and acted on, regarding:
   - Determination of incident severity
   - Containment
   - Systems shutdown
   - Public, media, and supervisory messaging
   - Declaring an 'all clear'
6. What coordinated recovery and remediation related decisions do we need to be prepared to make?
7. What remediation plans, operating arrangements and resources would be needed following a major cyber incident?
8. What is the full scope of parties needing to be involved in recovering from a major cyber incident?

EXHIBIT 16: CYBER-ATTACK SCENARIOS



SCENARIOS

Drawing on case studies of recent major cyber events, you can select scenarios based on the real-risk probability to your organization. The basic scenarios can be drawn up with varying degrees of severity, idiosyncrasies, and surprises, depending on your current level of preparedness or sophistication.

The standard process is to start with a basic, linear path, such as Coordinated Insider Action or Denial of Service (DoS), with which most stakeholders are familiar. The second, more dynamic path, adds more serious attack scenarios, such as Data Manipulation, Pervasive Destructive Malware, or Severe Internet/ Power Grid Outage. The third path builds on the previous but adds complicating factors — such as a Smokescreen Attack, Negative Media Response, Severe Weather, or Terrorist Attack (see Figure Exhibit 16 "Cyber-Attack Scenarios").

CYBER EXERCISE

The length, timing, and setting of the actual tabletop exercise is to a large extent determined by the objectives — and the availability of executive or key stakeholders. Full attendance is not totally necessary, but helpful. Ideally, the exercise is a one or two-day offsite to enhance the active engagement of responsible senior managers and executives. Cyber experts and technicians are also in attendance as a reality check and to challenge assumptions or proposed actions.

Conduct cyber exercises across agreed scenarios:

- Linear path #1 — fairly basic *(~60 minutes)*
- Linear path #2 — more complex *(~90 minutes)*
- Dynamic path — complicating factors *(90 to 120 minutes)*

Responses include determining incident severity, containment, systems shut down, and media communications. Once an attack is detected, the immediate question is whether or not to shut down all systems, just a segment, or none at all. Do you try to contain the visible attack, or do you heighten defenses all around to protect against a wider attack? Part of the calculation is a function of determining whether you are dealing with a 14-year old hacker or a nation state.

The nitty-gritty of this cyber exercise is mapping out who does what, and when. Who makes the call? How is it then executed? If key actors are offsite, can remote action be easily taken? When do you alert the media or local law enforcement? What's the "call tree" — and are there redundancies built in in case a key player cannot be reached? Part of designing a call tree, in addition to basic contract information, is drawing a map of decision rights — who has the authority in a given organization/unit or geography? And are there redundancies if a given person is unavailable?

As to the end game, who gives the "all clear" signal that the attack is over and business systems can be restored? In all cases, timing is important — how do weekends, holidays, or vacations affect response? Is there a backup team, and is it up to speed?

"HOT WASH" DEBRIEF

The "hot wash" post-mortem is a key element of the overall exercise. The proposed responses and identification of call trees needs to be fully analyzed and refined. Were the right people making decisions? Where are the key gaps, what issues rise to the fore, is the governance set for attacks, what's the internal and external communication plan?

Rehash the analyst's notes to determine if there really was a prepared plan in place, or whether people were making things up on the fly. In the latter case, it's clear that a book of procedures needs to be drafted. Determine if law enforcement should have been called — or called earlier. When Sony Pictures was hacked in 2014 — possibly by North Korea — it waited a week before calling in law enforcement. In retrospect, it appears that immediate notification would have made the event much less painful for Sony. Even if you decide not to call law enforcement, it's clearly good to make that a conscious decision and not an oversight.

This "hot-wash" exercise naturally leads to a set of recommendations for individuals, the collective group of key stakeholders, and outside pillars such as law enforcement and the media. Develop a long list of observations, gaps and primary concerns, then distill into recommendations. Produce a briefing pack and socialize the findings.

RINSE AND REPEAT

Setting up the first tabletop exercise is typically a multi-week exercise. Subsequent exercises can be organized much more quickly. The set-up includes interviewing key participants to set objectives and assess availability. Once a time and place is agreed on, the core team (moderator and analysts) should run a dress rehearsal.

Running such an exercise is not a one-time event. Given the increasing sophistication of cybercriminals, and the ever-expanding, cloud-based infrastructure, there are always new vulnerabilities to protect against. Ideally, such tabletop exercises are a quarterly or biannual event. Many organizations now run quarterly exercises in different areas of the organization — finance, risk, lines of business. A regular cadence of exercises will develop an organization's "muscle memory" to react and justify the spend to improve defenses. Just as when painting the Golden Gate bridge, when you have run through all parts of the organization, you start over again. You're running a race without a finish line.

FINDING THE ELUSIVE CYBER LOSS CURVE CAN PAY BIG DIVIDENDS FOR FINANCIAL INSTITUTIONS

Kevin Richards
Global Head of Cyber Risk Consulting, Marsh

Thomas Fuhrman
Managing Director – Cybersecurity Advisory, Marsh

Alex deLaricheliere
Managing Director – US Banking & Capital Markets, Marsh

What is the likelihood that your organization will experience a material cyber event in the next 12 months? Is the risk greater than 50%? Less than 25%? These questions are ever-present on the minds of risk managers, who long for at least a practical — if not precise — answer.

Cyber risks are among the most serious perils facing the financial industry. Cybercrime is not only increasing in frequency, but also in magnitude, costing the world an estimated $600 billion, or 0.8% of global GDP, according to a recent report published by McAfee and the Center for Strategic and International Studies. But while financial institutions have become practiced at estimating most operational risks and using this data to develop risk capital strategies, they often perceive roadblocks to extending these methods to cyber.

AN INFORMATION CHASM

One major problem revolves around the lack of data. Unlike other risks, there is limited historical data about cybercrime, mainly because it is a relatively new risk area but also due to its constantly changing form. Cyber risk management has not yet been "reduced to practice" on a wide scale.

Traditionally, financial entities have used qualitative frameworks — red, yellow, green, or high, medium, low — to characterize cyber threats, a system also commonly used in other industries. This approach can be quite useful, but it is no longer sufficient for the financial sector, which has been feeling a growing need to put numbers to cyber risk, calculating both severity and likelihood. A more quantitative methodology is needed both to improve a company's protection and to comply with increasingly stringent regulations, including the Basel II framework and standards imposed by national regulators.

While this can be a complex endeavor, a starting point is to consider scenario analysis. This approach enables point estimates of the financial cost — the severity — of cyber events with good accuracy. Significantly more difficult is determining the likelihood of an event. Having credible quantitative estimates for both severity and likelihood will allow risk managers to answer the fundamental question: "What is the likelihood that our organization will experience a cyber event causing a loss of greater than, say, $100 million in the next 12 months?" Most often, it is the likelihood question that derails many attempts at quantifying cyber risk, due to the unpredictable nature of a human-initiated threat. However, despite the limitations, financial risk professionals should enter this challenge holding to the adage that every risk can be modeled.

In recent years, driven by the Basel Committee on Banking Supervision's standards and guidelines, banking regulators both in the US and globally have emphasized the need for financial institutions to have adequate capital reserves by modeling a wide range of risks. Further, financial companies in the US are required to carry out stress tests on their balance sheets, looking at a number of high impact-low likelihood scenarios, including cyber events. And US bank examiners regularly carry out cybersecurity assessments of all banks.

In 2016, the Federal Reserve, the Comptroller of the Currency, and the Federal Deposit Insurance Corporation issued an Advance Notice of Proposed Rule Making (ANPR) declaring their intention to establish more stringent standards on systematically important institutions. Among other proposals, the ANPR asserted its aspiration to develop "consistent, repeatable methodology" to measure cyber risk. Its call for submissions for potential methodologies to quantify inherent and residual cyber risk underlines the necessity that the financial industry applies such procedures to meticulously measure cyber risk.

Beyond the regulatory push, there is high recognition within the industry that financial institutions must embark on robust efforts to identify and estimate cyber risk and protect their operations and customers from the disruptive and potentially costly repercussions of cyber-attacks.

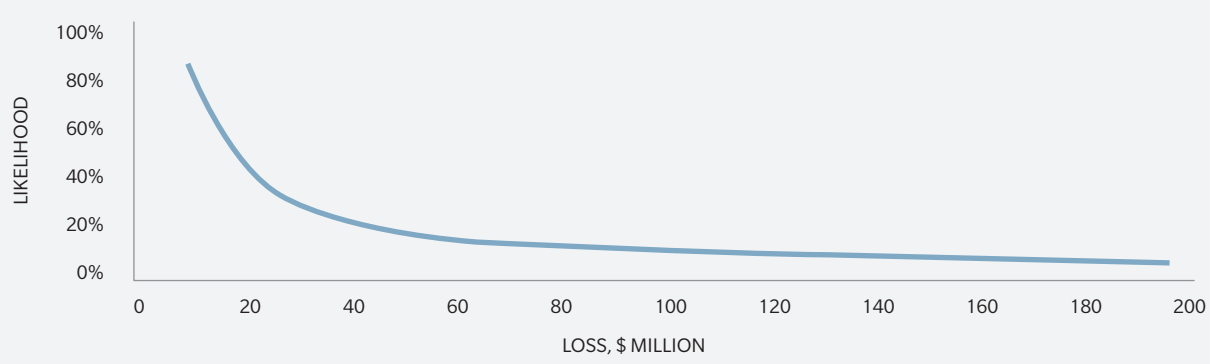
CALCULATING THE LOSS CURVE

When dealing with improbable events, likelihood and impact are inextricably linked; this is the case in every risk area. Generally, the relationship between the two can be expressed through a non-linear loss distribution curve (see Exhibit 17), which describes a situation where higher cost is associated with lower likelihood. Very costly events are rare; less costly events are more common. Where sufficient historical data is available, it can usually be described with this type of characteristic curve. If a loss curve can be represented mathematically with a fair degree of confidence, it can open up tremendous opportunities for managing the risk it represents. It helps risk professionals calculate risk appetite and risk tolerance within their organizations, and to get a good understanding of the risks associated with events in the "tail" (the right side) of the curve. No model is perfect, but a data-driven estimate of the loss curve can enable business leaders to better understand the risks of cyber and take action to manage them. The loss curve has, in fact, been used as a backdrop for modeling operational risks for some time. But what about cyber? Cyber itself is, after all, an operational risk. Does the long-established loss curve idea apply to cyber? Certainly, the traditional loss curve has intuitive appeal when we think about cyber risk. It would seem that a loss of, say, $150 million due to a cyber-attack is at least somewhat less likely than a loss of $50 million. While there is no certainty that cyber risks can be described effectively with the traditional loss curve — could hackers cause more expensive tail events to become more likely than less costly events? — it is an attractive modeling approach to start with.

DEVELOPING A CYBER-SPECIFIC LOSS CURVE

Cyber is presently one of the most challenging among operational risks and it may be a long time, if ever, before there is sufficient historical data to develop an organization's cyber-specific loss curve with certainty. But scenario analysis can help. Risk professionals are already familiar

EXHIBIT 17: REPRESENTATIVE LOSS CURVE



with scenario modeling to sketch out the loss curve for operational risks. This approach can also work in cyber. A few simple rules apply to scenario development: focus on tail risks; aim for events that are unlikely but plausible; and ensure the events are organization- and system-specific with enough detail to analyze losses accurately. Once there are enough estimates for impact and likelihood, even with large confidence intervals, "pseudo-data points" can be plotted, and the loss curve starts taking shape.

The pseudo-data of scenario estimates can be combined with the actual data of real-world events, when these are available (see Exhibit 18). Through reasonable curve-fitting based on an assumed distribution — such as the log-normal, Poisson, or other — a financial institution can develop an approximation of the elusive loss curve for cyber.

This type of analysis ties likelihood and severity together in a mathematical formula, offering insight for risk managers and other key figures into the risk that cyber poses to their organizations. Ultimately, finding the loss curve in cyber can pay big dividends. Financial institutions can use this type of modeling as an aid to developing a meaningful capital risk framework for cyber that can not only address regulatory requirements but also raise the organization's game in cyber risk management.

WHAT CYBER-ATTACK SCENARIOS SHOULD FINANCIAL INSTITUTIONS CONSIDER?

1. Interruption or disruption of core banking platforms: Identify the different areas that could be affected, and whether there could be alternative work practices that can be used during a down period.

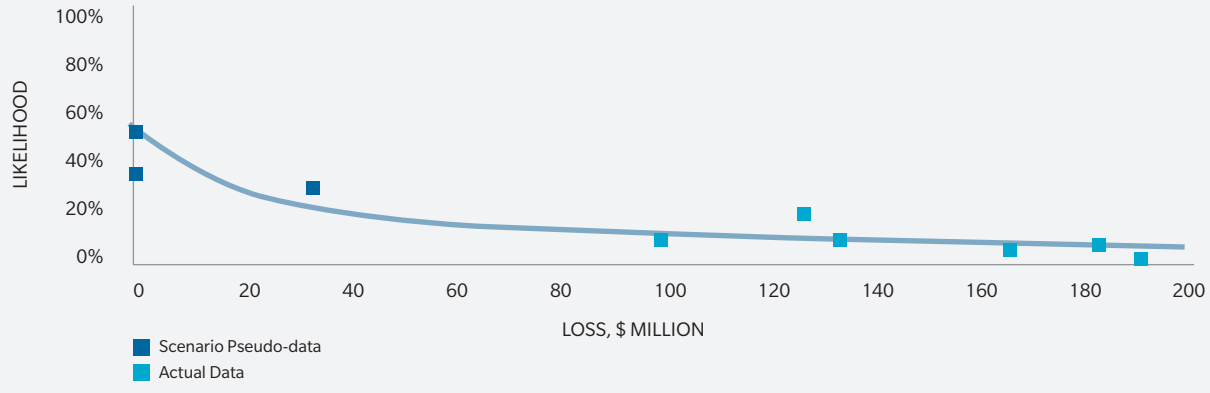
2. Corruption of databases: Consider whether you need to have physical copies to continue operations in case of a cyber-attack.

3. Corruption of back office systems: Determine the cost of such an interruption and create a robust backup plan.

4. Interruption of electronic trading platforms: Brokers, investment banks, exchanges, and others involved in buying and selling of stocks, bonds, and other financial instruments should look at whether they can operate with lost or degraded connectivity.

5. Extended internet service disruption: Determine how your institution will be affected if you, and others that you do business with, are forced offline for an unspecified period of time. Consider whether some, or all, operations can continue offline.

EXHIBIT 18: BLENDING ACTUAL AND PSEUDO DATA TO DETERMINE CYBER-SPECIFIC LOSS



CONTACT

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

Tom Reagan

US Cyber Practice Leader,
Marsh

Thomas.Reagan@marsh.com

Jeremy Platt

Cyber Specialty Solutions Practice Leader,
Guy Carpenter

Jeremy.S.Platt@guycarp.com

Kevin Richards

Global Head of Cyber Risk Consulting,
Marsh

Kevin.Richards@marsh.com

Leslie Chacko

Director, Transformative Technologies,
Marsh & McLennan Insights

Leslie.Chacko@oliverwyman.com

Paul Mee

Partner and Cyber Lead,
Oliver Wyman

Paul.Mee@oliverwyman.com

Victoria Shirazi

Associate Director, Cyber Resilience,
Marsh & McLennan Solutions

Victoria.Shirazi@mmc.com

ABOUT MARSH & MCLENNAN INSIGHTS

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

ABOUT MARSH & MCLENNAN COMPANIES

Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The company's approximately 65,000 colleagues advise clients in over 130 countries. With annual revenue over $14 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. Marsh advises individual and commercial clients of all sizes on insurance broking and innovative risk management solutions. Guy Carpenter develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. Mercer delivers advice and technology-driven solutions that help organizations meet the health, wealth and career needs of a changing workforce. Oliver Wyman serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit mmc.com, follow us on LinkedIn and Twitter @mmc_global or subscribe to BRINK.