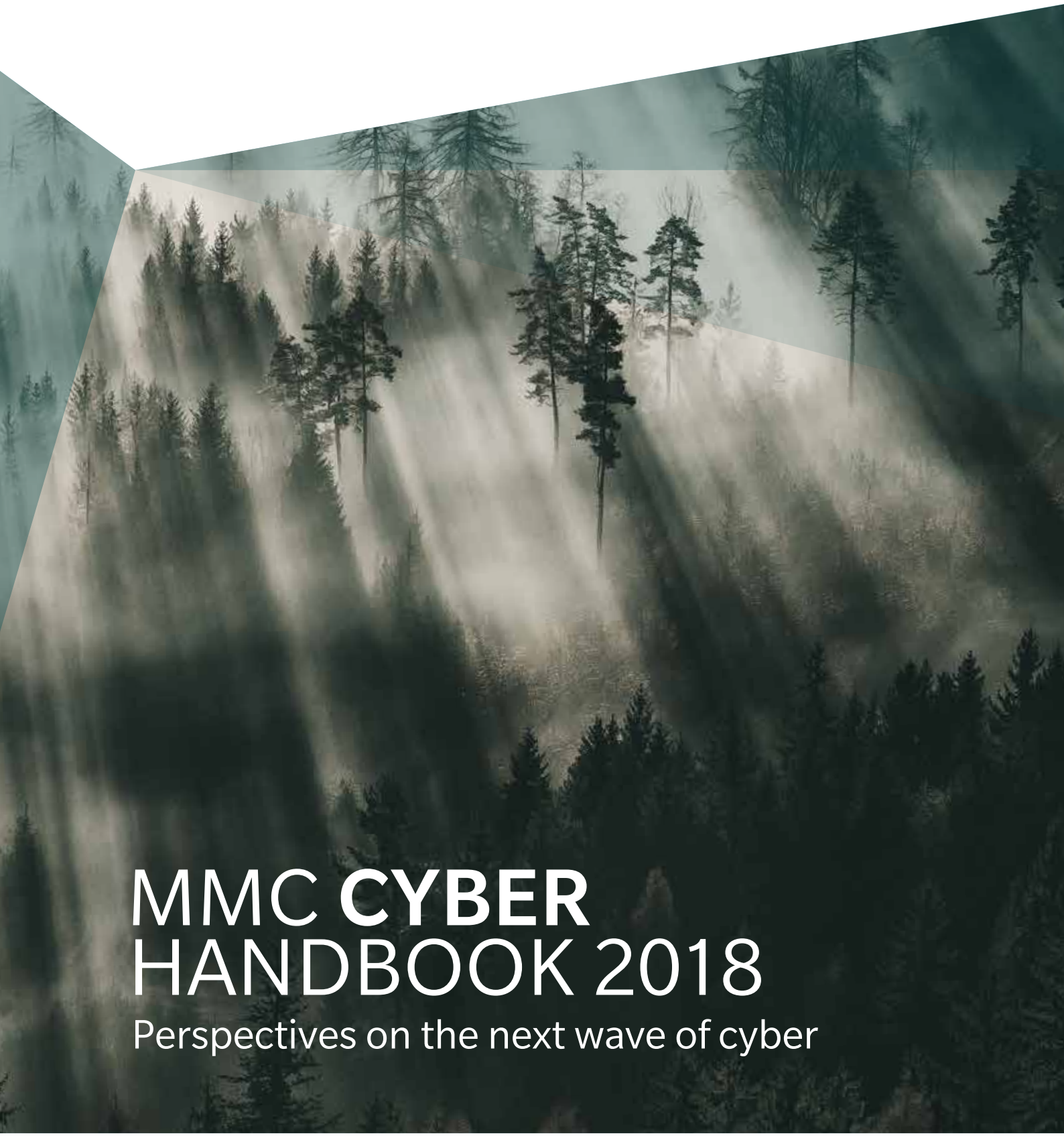
MARSH & McLENNAN COMPANIES | Global Risk Center



MMC **CYBER** HANDBOOK 2018

Perspectives on the next wave of cyber

MARSH GUY CARPENTER MERCER OLIVER WYMAN

FOREWORD

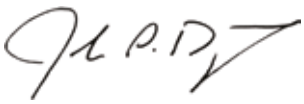
Cyber risk continues to grow as technology innovation increases and societal dependence on information technology expands. A new and important turning point has been reached in the struggle to manage this complex risk. In the war between cyber attackers and cyber defenders, we have reached what Winston Churchill might call "the end of the beginning."

Three characteristics mark this phase shift. First, global cybercrime has reached such a high level of sophistication that it represents a mature global business sector – illicit to be sure, but one which is continually innovating and getting more efficient. In 2017 we have experienced the widespread use of nation state-caliber attack methods by criminal actors. Powerful self-propagating malware designed to destroy data, hardware and physical systems have caused major business disruption to companies worldwide with an enormous financial price. The number of ransomware attacks has also spiked significantly. More attack incidents have impact extending beyond the initial victims with broad systemic ripple effects.

Second, business and economic sectors have high and growing levels of dependency on IT systems, applications and enabling software. Growth in connectivity between digital and physical worlds, and the acceleration in commercial deployment of innovative technologies like Internet of Things (IOT) and Artificial Intelligence (AI) will expand potential avenues for cyberattack and increase risk aggregation effects. These changes will make the next phase of cyber defense even more challenging.

The third shift is the rising importance of coordination among institutions – governments, regulatory authorities, law enforcement agencies, the legal and audit professions, the non-government policy community, the insurance industry, and others – as a critical counter to the global cyber threat. Cyber risk defense can only be effective if these groups share a common understanding of the changing nature of the threat, their importance and increased interconnected nature. Working individually and in concert, these groups can increase our collective cyber resilience. We are beginning to see expectations converge in areas such as increased transparency, higher penalties for failure to maintain a standard of due care in cyber defense, improved incident response, and an emphasis on risk management practices over compliance checklists. It will be vital for this trend to continue in the next phase.

Against this backdrop, the 2018 edition of the *MMC Cyber handbook* provides perspective on the shifting cyber threat environment, emerging global regulatory concepts, and best practices in the journey to cyber resiliency. It features articles from business leaders across Marsh & McLennan Companies as well as experts from Microsoft, Symantec, FireEye and Cyence. We hope the handbook provides insight which will help you understand what it takes to achieve cyber resiliency in the face of this significant and persistent threat.



John Drzik
President, Global Risk and Digital
Marsh & McLennan Companies

CONTENTS

WAKE UP TO THE SHIFTING CYBER THREAT LANDSCAPE

PREPARE FOR EMERGING REGULATIONS

CYBER RESILIENCY BEST PRACTICES

WAKE UP TO THE SHIFTING CYBER THREAT LANDSCAPE

THREAT TRENDS ON MAJOR ATTACKS

BREACHES

	2014	2015	2016
Total breaches	1,523	1,211	1,209
Total identities exposed	1.2 BN	564 MM	1.1 BN
Average identities exposed per breach	805 K	466 K	927 K
Breaches with more than 10 million identities exposed	11	13	15

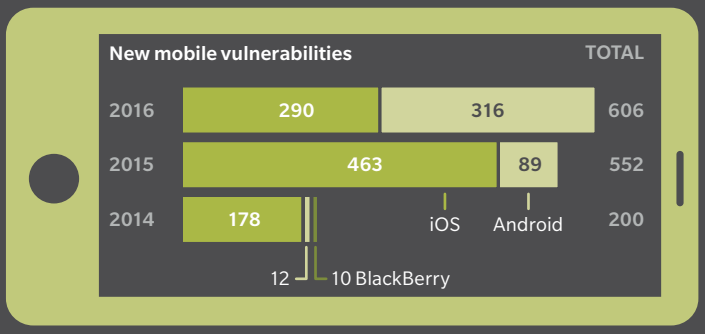
In the last **8** years more than **7.1 BILLION identities** have been **exposed** in data breaches

RANSOMWARE

	2014	2015	2016
Number of detections		340,665	463,841
Ransomware families	30	30	101
Average ransom amount	$373	$294	$1,077

MOBILE

	2014	2015	2016
New Android mobile malware families	46	18	4
New Android mobile malware variants	2.2 K	3.9 K	3.6 K



CLOUD

Average number of cloud apps used per organization

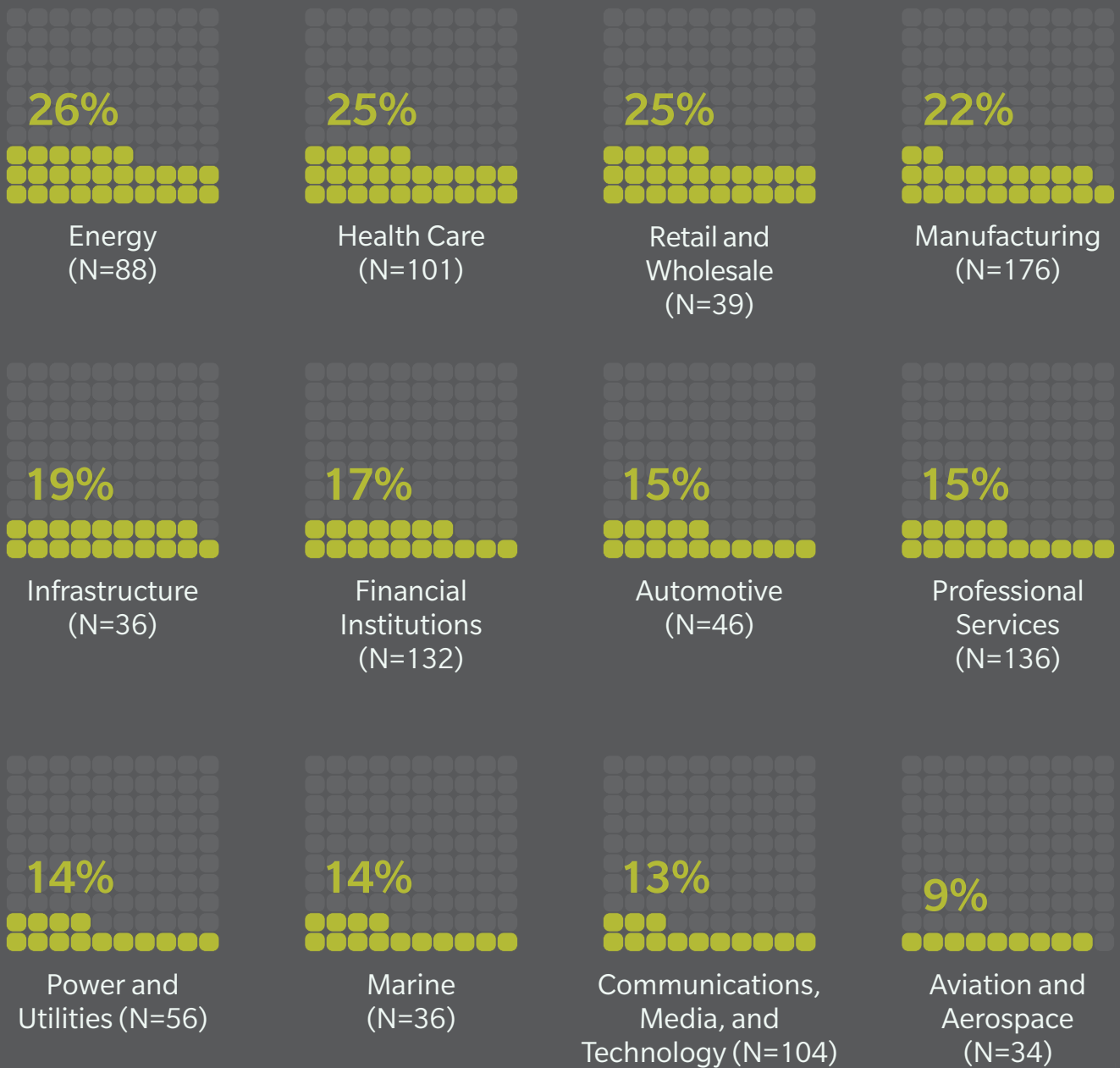
2015 JUL-DEC	2016 JAN-JUN	2016 JUL-DEC
774	841	928
25%	23%	25%

Percentage of data broadly shared

Source: Symantec

INDUSTRIES IMPACTED BY CYBERATTACKS

Percentage of respondents in industry that have been victims of cyberattacks in the past 12 months



Source: 2017 Marsh | Microsoft Global Cyber Risk Perception Survey

EVOLUTION OF CYBER RISKS: **QUANTIFYING** SYSTEMIC EXPOSURES

George Ng and Philip Rosace

Cyberattacks have escalated in scale over the last twelve months. The progression of events has demonstrated the interconnectedness of risks and shared reliance on common internet infrastructure, service providers, and technologies. If the Target, Sony, Home Depot, and JPMorgan Chase data breaches in 2013 and 2014 defined the insured's need to manage their cyber risks and drove demand for cyber insurance, then this year's events have proven the need for insurers to quantify and model their exposure accumulations and manage tail risk.

These recent events have a different texture and a broader impact/reach than the incidents we have grown accustom to seeing over the past decade. A certain trend towards awareness of systemic risk has emerged among cyber insurance markets and their regulators. Exposure modeling around accumulation

exposures such as cloud infrastructure and widely used technologies is advancing. The 2017 Lloyd's Emerging Risk Report *Counting the costs: Cyber risk decoded,* written in collaboration by Cyence and Lloyd's, models losses from a mass cloud service provider outage to have potential for $53 billion in ground up economic losses, roughly the equivalent to a catastrophic natural disaster like 2012's Superstorm Sandy.

Cyence's economic cyber risk modeling platform collects data to quantify systemic risks and assess economic impact to portfolios of companies. It is essential to evaluate the variety of commonalities among companies to identify any non-obvious paths of aggregation that could be a blind spot. The Web Traffic by Sector chart shows a sector breakdown of internet usage. Software and technology companies, unsurprisingly account for a majority of traffic.

But systemic risk also stems from joint usage of common services within an "Internet Supply Chain" including ISPs, cloud service providers, DNS providers, CDN providers, among others. Understanding the many permutations of these accumulation paths is critical for the insurance industry's enterprise risk

EXHIBIT 1: TIMELINE OF RECENT ATTACK EVENTS

OCTOBER 21, 2016...

Dyn Inc.'s DNS provider services were interrupted by a Distributed Denial of Service attack of unprecedented strength from the Mirai botnet of compromised IoT devices. The attack was said to have a flood rate of 1.2 Tbps from 100,000 infected devices. Dyn's 11-hour outage of their DNS lookup services caused availability issues for users of Amazon.com, Comcast, HBO, Netflix, The New York Times, PayPal, Spotify, Verizon, The Wall Street Journal, Yelp, among many other platforms and services reliant upon Dyn as a DNS provider.

FEBRUARY 28, 2017...

Amazon Web Services suffered an outage of their S3 cloud storage service for approximately 4 hours. The outage impacted some popular internet services, websites, and other businesses utilizing that infrastructure. The Wall Street Journal reported that the outage was caused by human error – an employee mistyped a command causing a cascading failure that knocked out S3 and other Amazon services. Cyence estimates that companies in the S&P 500 dependant on Amazon's services lost approximately $150 million as a result of the outage.

MAY 12, 2017...

An aggressive ransomware campaign was deployed infecting hundreds of thousands of endpoints around the world since. The ransomware named WannaCry (AKA WannaCrypt, Wana Cryptor, wcrypt) targeted unpatched Microsoft Windows machines using the EternalBlue exploit. Notable victims included the National Health Service (NHS) in the United Kingdom, Nissan Motor Manufacturing UK, and Renault. The Wall Street Journal reported Cyence's estimate of $8 billion in potential economic losses due to the event arising out of lost income and remediation expenses to organizations with infected or vulnerable systems.

JUNE 27, 2017...

New variants of the Petya ransomware began spreading globally (dubbed NotPetya), though most of activity was reported in the Ukraine. Once the malware first infected its host, it then tried to spread further throughout the local network using the EternalBlue exploit, which was used by WannaCry a month prior. Ukraine's Chernobyl Nuclear Power Plan went offline, India's largest port was brought to a standstill, and a number of global companies were impacted including A.P. Moller Maersk, WPP, DLA Piper, Merck & Co., FedEx, and others. Reuters reported Cyence's $850 million ground up loss estimate from this event.

IT IS ESSENTIAL TO EVALUATE THE VARIETY OF COMMONALITIES AMONG COMPANIES TO IDENTIFY ANY NON-OBVIOUS PATHS OF AGGREGATION THAT COULD BE A BLIND SPOT.

EXHIBIT 2: WEB TRAFFIC BY SECTOR

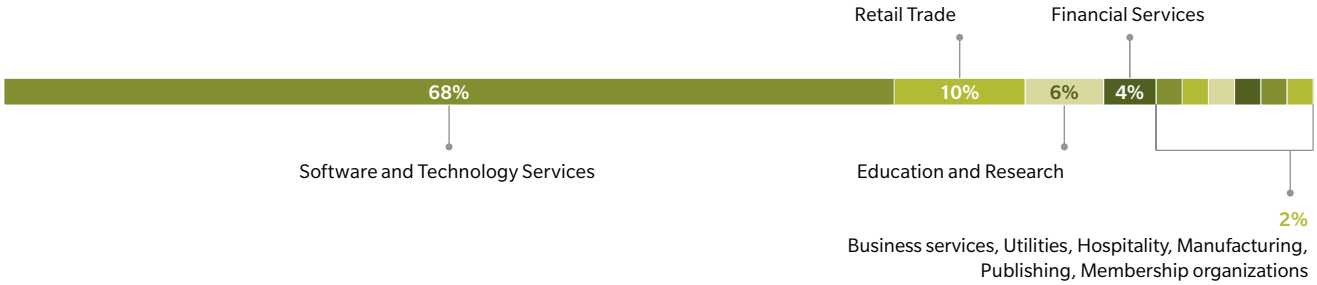
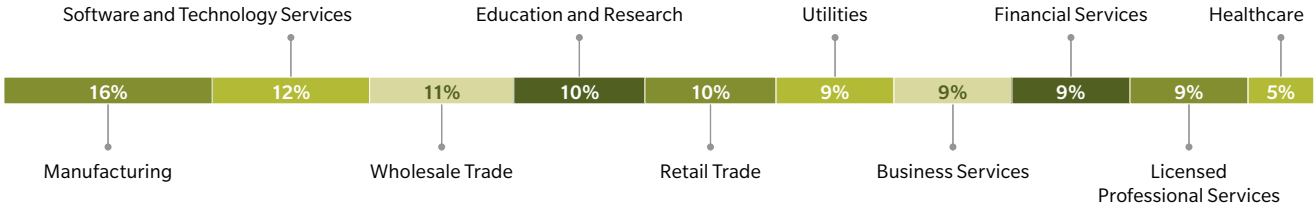


EXHIBIT 3: CLOUD USAGE BY SECTOR



Source: Cyence

management. The Cloud Usage by Sector chart highlights cloud services usage by sector and tells a different story than the first chart; We see more widespread and balanced usage across a variety of industries instead of one sector dominating. A detailed and thorough evaluation of these exposures in dollars and probabilities will be essential for re/insurers enterprise risk and capital management.

Just as our sea levels and weather patterns change over time, cyber temperatures are rising and society's technological advances appear to have a hand in it. The last twelve months have proven that the types of cyber events observed can change dramatically over a short period and create a new normal. A few years ago, we were all suffering from breach fatigue – every week a new retailer, healthcare provider, or financial institution lost their customer's sensitive data. This year we started to see early versions of cyber hurricanes occur – something the market has been concerned with for quite a few years. Like a natural disaster, these events affected wide swaths of enterprises by failures in common points of dependency.

THIS YEAR WE STARTED TO SEE EARLY VERSIONS OF CYBER HURRICANES OCCUR – SOMETHING THE MARKET HAS BEEN CONCERNED WITH FOR QUITE A FEW YEARS.

CONCLUSION

So, what is on the horizon to be the next new normal for the cyber world? At Cyence, our white hats are seeing a lot of new trends, but some areas we see evolving to include increased exposure to Internet of Things (IoT) exposures, increased ransomware efforts, and increased regulations. We believe there will be more attacks disrupting GPS and other geo location systems to cause disruptions in the physical world from supply chains and marine risks, to consumers reliant on GPS based products. As Bitcoin and other cryptocurrencies become more widely adopted, we expect to see more frequent and severe ransomware campaigns like WannaCry and NotPetya. Last, sovereign states are increasingly seeking regulations on data storage locations to provide governments with better control over their data. This control is desired for a variety of reasons including privacy, censorship, and anti-terrorism; compliance will require operational change by companies, but the variety of cloud resources available can simplify that transition for those organizations. ♦

George Ng, based in San Mateo, is the CTO and co-founder of Cyence.
Philip Rosace, based in San Mateo, is a Senior Solutions Manager at Cyence.

THE **DRAMATICALLY CHANGING** CYBER THREAT LANDSCAPE IN EUROPE

FireEye | Marsh & McLennan Companies

Europe is being forced to confront a growing cyber threat against physical assets. Hackers and purportedly nation states are increasingly targeting industrial control systems and networks – Power grids, chemical plants, aviation systems, transportation networks, telecommunications systems, financial networks and even nuclear facilities.

In late 2014, the German Federal Office for Information Security (BSI) reported that a cyberattack had caused "massive damage" to a German iron plant. Utilizing a combination of spearphishing and social engineering, hackers gained access to the iron plant's office network, moved laterally to control the production network and then disabled the shut-off valves on the plant's blast furnaces. In the parlance of the industry, this was a "kinetic" or physical attack against hard assets.

In late 2015, hackers turned their focus to the power industry. In one of the largest attacks of its kind, hackers shut off the power to hundreds of thousands of residents in Ukraine. According to public reports, the attacks that caused the power outage were accompanied by parallel cyber intrusions into Ukraine's train system and TV stations.

In October 2016, the head of the International Atomic Energy Agency at the United Nations, Yukiya Amano, publicly disclosed for the first time that a "disruptive" cyberattack had been launched against a nuclear facility in Germany. This report came on the heels of an analysis by the Nuclear Threat Initiative warning of lax cybersecurity at nuclear facilities in a number of countries across Europe.

Thus, cyberattacks against critical infrastructure, dubbed a potential "Cyber Pearl Harbor" by US military officials, are no longer the fantasies of Hollywood producers, conspiracy theorists or sci-fi aficionados, but are the reality that governments and businesses across Europe must now confront.

WHAT EU COUNTRIES ARE BEING TARGETED WITH THE GREATEST FREQUENCY?

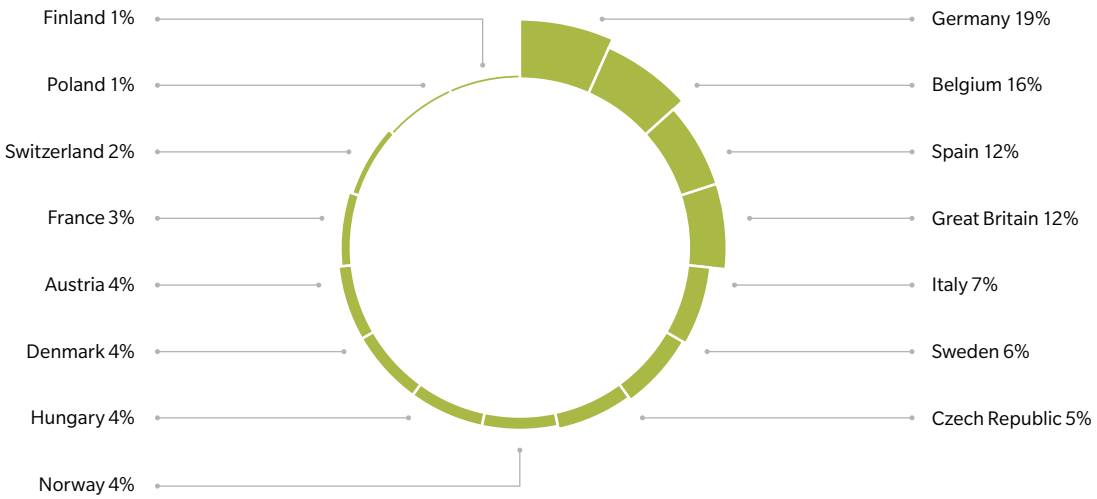
Cyber hackers are increasingly opportunistic – Smart, savvy, and innovative. Hackers are bypassing traditional defenses by continually engineering new methods of attack. Even sophisticated cybersecurity programs are being thwarted, often by targeting weak links in the chain, including vendors and employees. Due to its advanced economies and important geopolitical positioning, Europe is a prime target for these attacks.

TARGETING OF EU COUNTRIES

Europe's largest economies remain the top targets, but the focus ranges broadly across the continent. *Exhibit 1* shows targeted malware detections from January to September 2016 for all EU nations except Turkey and Russia. (Nations not represented on this chart received little or no malware assessments from FireEye). Had

EXHIBIT 1: TARGETED MALWARE DETECTIONS FROM JANUARY 2016 TO SEPTEMBER 2016

In 2016, hackers most often targeted financial, manufacturing, telecom industries and governments in Germany, Great Britain, Belgium, Spain, Denmark, Sweden, Norway and Finland



Source: FireEye|Marsh & McLennan Cyber Risk Report 2017 Cyber Threats: A perfect storm about to hit Europe?

Turkey been included, it would far overshadow the EU nations represented. Turkey accounted for a whopping 77 percent of all targeted malware detections by FireEye in Europe.

Germany powerfully demonstrates the changing cyber environment. Last month, Thyssen Krupp, a large German industrial conglomerate, disclosed that "technical trade secrets" were stolen in a cyberattack that dated back almost a year. The company filed a criminal complaint with the German State Office for Criminal Investigation and stated publicly, "It is currently virtually impossible to provide viable protection against organized, highly professional hacking attacks."

The type of data being stolen in these attacks is particularly revealing. While sensitive personal information like financial or health records remains a key focus, hackers are increasingly targeting higher value data relating to infrastructure systems. Based on FireEye's research, 18 percent of the data that was exfiltrated through cyberattacks in Europe in 2016 related to companies' industrial control systems, building schematics and blueprints, while a further 19 percent related to trade secrets.

The federated nature of Europe also increases the potential cyber risk across the continent. Each EU member state has a different cybersecurity maturity. As more and more components of infrastructure are connected to the Internet and the Internet of Things explodes in popularity, certain countries within Europe may lack the capabilities needed to assess and implement a sophisticated cybersecurity framework to defend against these emerging threats. As a result, hackers can take advantage of the disparate architecture across the EU.

NO SECTOR OF THE ECONOMY IS IMMUNE FROM ATTACK – NOT INDUSTRY, NOT GOVERNMENT AND NOT EVEN THE NOT-FOR-PROFIT SECTOR.

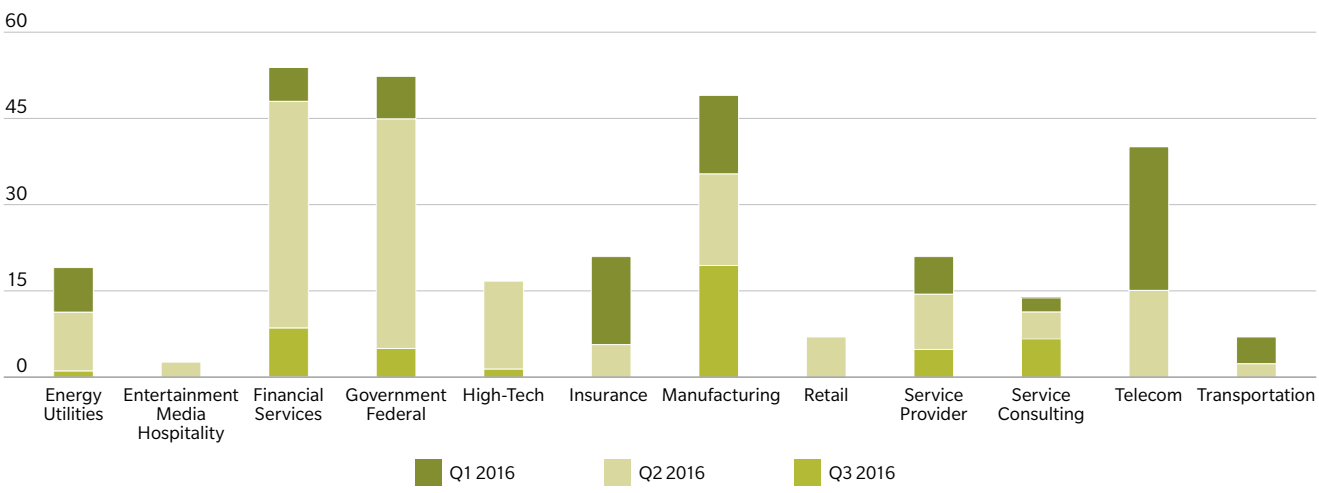
WHAT SPECIFIC INDUSTRIES ARE BEING TARGETED AND HOW?

The vertical industry analysis below reveals which sectors are being targeted with the greatest frequency. The three industries that draw the greatest attention in Europe are:

- Financial Services
- Manufacturing
- Telecommunications

In the third quarter of 2016, threats accelerated in particular against manufacturers and telecom operators. Conversely, retailers, a key focus of cyberattacks in the United States, are virtually at the bottom of the list in Europe.

EXHIBIT 2: TARGETED MALWARE DETECTION ACROSS EUROPE DURING JANUARY – SEPTEMBER 2016



Source: FireEye|Marsh & McLennan Cyber Risk Report 2017 Cyber Threats: A perfect storm about to hit Europe?

In addition, governments are a primary target for hackers across Europe. Indeed, aggregating attacks against national, state and local governments into a single category makes government the number one target in Europe.

To date, there has been an underreporting of cyber incidents in the EU. Nonetheless, a handful of public reports reveal significant cyber incidents across the continent. In 2016, cyber hackers stole more than $75 million from a Belgian bank and $50 million from an Austrian aircraft parts manufacturer through fraudulent emails mimicking legitimate communications to fool companies into transferring money to a hacker's account.

In sum, no sector of the economy is immune from attack – not industry, not government and not even the not-for-profit sector. Accordingly, we need a mindset, particularly between government and industry, that we are all in this together.

COMPANIES IN EUROPE TAKE 3x LONGER TO DETECT CYBER INTRUSIONS

FireEye found that companies in the European Union take three times longer than the global average to detect a cyber intrusion. The region's mean "dwell time" – the time between compromise and detection – was 469 days, versus a global average of 146 days.

The delay in identifying intrusions has profound consequences. At a basic level, the notion that hackers are rooting around in companies' networks undetected for 15 months is sobering, as it allows ample opportunity for lateral movement within IT environments.

Equally important, dwell times of this length allow hackers the opportunity to develop multiple entry and exit doors. When a company does detect an intrusion, the natural first impulse is to shut down its system to "stop the bleeding." Numerous stakeholders then press the organization and its management team to get back online and operating.

In this dynamic, FireEye has found that hackers compromised many organizations in Europe a **second time within months** of the initial breach. Repeated breaches most often result from the use of unsuitable techniques to hunt initially for attacks within their environment. Many companies still opt for a traditional forensic methodology, only analyzing a handful of machines or systems. On average, however, hackers in Europe have infected approximately 40 different machines in any given company during the length of their cyber intrusions.

HOW ARE MOTIVES AND TACTICS CHANGING?

Hackers come in many forms and differing degrees of sophistication. In addition to attacks against critical infrastructure, EU cyber threats are dominated by two distinct groups: hackers with political goals and hackers with financial motives.

IS POLITICALLY MOTIVATED HACKING ON THE RISE?

In 2016, FireEye observed numerous nation-state or nation-sponsored intrusions against EU governments, and specifically against foreign or defense ministries of member states. Recently, nation-state sponsored threat actors have shown strong interest in extending these attacks into the political arena.

In September 2016, politicians and employees of political parties in Germany were targeted with a series of spear phishing e-mails, purportedly from NATO headquarters, regarding a failed coup in Turkey and the earthquakes that hit Italy's Amatrice region. The links to these spurious e-mails contained malware. Arne Schoenbohm, the head of the German BSI, responded swiftly by warning political parties across the spectrum in Germany that the country needed to learn the lessons from the recent elections in the United States.

In December, the focus shifted to France. France's National Cybersecurity Agency, known as the ANSSI, summoned representatives of all political parties to a detailed cyber briefing about the threat posed by cyberattacks.

DWELL TIME UNTIL A COMPROMISE IS DETECTED

469

Days in **Europe**

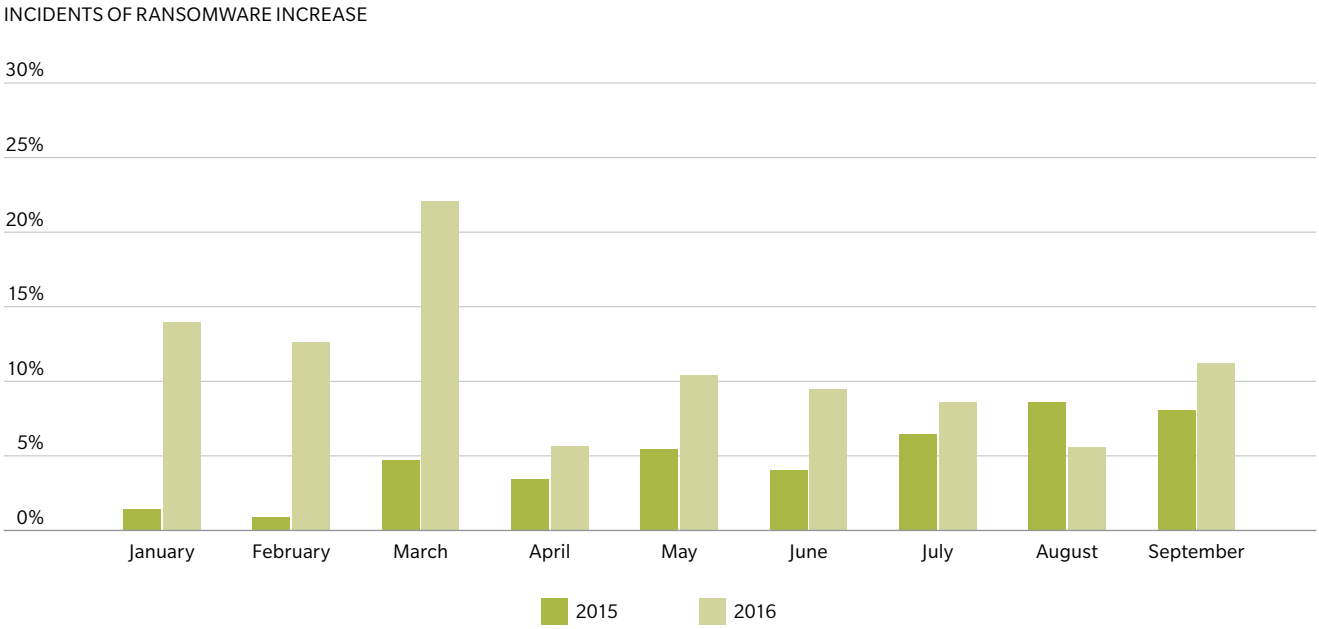
146

Days
Global Average

THE NOTION THAT HACKERS ARE ROOTING AROUND IN COMPANIES' NETWORKS UNDETECTED FOR 15 MONTHS IS SOBERING, AS IT ALLOWS AMPLE OPPORTUNITY FOR LATERAL MOVEMENT WITHIN IT ENVIRONMENTS.

EXHIBIT 3: RANSOMWARE EVOLUTION AND GROWTH IN EUROPE

This chart depicts a monthly average of the ransomware events that occurred from January to September in 2015 and 2016. While the number of events varied, the increase in events in 2016 over the prior year is significant – and worrisome.



Source: FireEye|Marsh & McLennan Cyber Risk Report 2017 Cyber Threats: A perfect storm about to hit Europe?

Prior to the recent attacks in the US, few would have considered political parties and voting machines as part of a nation's critical infrastructure. With national elections looming in the Netherlands (March 2017), France (May 2017) and Germany (late 2017), however, the risk posed to the integrity of the electoral process is all too real.

CRIMINAL HACKERS STILL A DANGEROUS THREAT

Cyber criminals continue to target organizations and private citizens across Europe to steal information, stage cyber extortion attacks, and steal money through fraudulent transactions.

The use of "ransomware" spiked significantly in 2016. Victims are asked to pay a ransom in the form of "bitcoins." Utilizing malware with names like Cryptolocker, TorLocker and Teslacrypt, hackers encrypt your files and then demand a ransom to unlock them. In one recent example, a ransomware variant called "Locky" targeted users in more than 50 countries – many of them in Europe. Locky utilized exploit kits and mass e-mailing campaigns, often seen with spam. The campaign enticed recipients to open e-mail attachments that appeared to be invoices but instead contained malware. Victims are asked to pay the ransom to obtain a decryption key that will then unlock their systems. As more criminals successfully carry out ransomware attacks, others are enticed to try this growing type of malware attack. This form of attack has been particularly prevalent in the health care space, with one report contending that 88 percent of ransomware attacks target the healthcare industry[1].

CONCLUSION

In addition, there has been an increase in targeting of corporate executives across Europe to carry out a scam known as "CXO fraud" or "Business E-mail Compromise." Cyber criminals typically mimic a small to mid-size enterprise with international supply chains requiring regular wire transfer payments. Hackers compromise legitimate business e-mail accounts and then request unauthorized transfers of funds. ♦

This article is an excerpt from the FireEye|Marsh & McLennan Cyber Risk Report 2017 Cyber Threats: A perfect storm about to hit Europe?

1 Solutionary's Security Engineering Research Team Quarterly Threat Report, Q2 2016.)

ASIA PACIFIC – A **PRIME TARGET** FOR CYBERCRIME

Wolfam Hedrich, Gerald Wong, and Jaclyn Yeo

Asia is 80 percent more likely to be targeted by hackers than other parts of the world. The number of high profile cyber incidents has risen in recent years, although we assert that the public sees only a sliver of the real impacts of such incidents.

Reasons for the relatively higher cyber threat potential in Asia Pacific (APAC) are twofold: the growing speed and scope of digital transformation, and the expanding sources of vulnerability stemming from increasing IoT connectivity.

ACCELERATING DIGITAL TRANSFORMATION IN APAC

Digital transformation – the connection of individuals, companies, and countries to the Internet – has emerged among the most transformative means to ignite sustainable growth. This is most evident in APAC where strong economic growth in recent years has been powered by the rapid adoption of Internet and mobile technologies.

Across the region, a few emerging economies have accelerated their digital transformation so rapidly that they have bypassed certain various stages of technology development – just over the past few years many people across several Asian countries have leapfrogged from not having any Internet access at homes to owning multiple mobile devices and accessing the Internet. For example, estimates from The World Bank indicate 22 percent of Myanmar is now online, compared to less than 2 percent in 2013, opening abundant opportunities for the domestic consumer market.

In Indonesia, meanwhile, mobile device subscription rates were estimated to be higher than the rest of Asia in 2015 (132 percent vs. 104 percent). The high subscription rate was one key driving force propelling the domestic mobile-money industry – annual e-money transaction values in Indonesia grew almost to Rp5.2 trillion ($409 million) in 2015 from Rp520 billion ($54.7 million) in 2009.

Unfortunately, there remains a huge gap in cybercrime legislations in these countries – the lack of awareness and knowledge of basic security makes most online transactions highly susceptible to digital theft. While the breakneck speed of digital transformation is generally good news, safeguards must be in place alongside to protect users and sustain the burgeoning digital business.

EXPANDING SOURCES OF VULNERABILITY

The rapid spread of internet-enabled devices – IoT – enables new and more efficient modes of communications and information sharing. Asia-Pacific, in various aspects, leads in the IoT technology: South Korea, Australia, and Japan are among the top five countries, reaping the most benefits from IoT, according to the 2016 International Data Corporation's (IDC) "*Internet-of-Things Index*".

Over time, IoT technology will create and add a significant fleet of digitally-connected devices, most of them originating from APAC – China, Japan, and South Korea are constantly looking to "smartify" all possible consumer electronics, for example.

However, higher interconnectivity through the plethora of IoT devices "opened up new means of attack", according to William H. Sato, Special Advisor to the Cabinet Office, Government of Japan. In October 2016, one of Singapore's main broadband networks suffered a severe Distributed Denial of Services (DDoS) attack, causing two waves of internet-surfing disruptions over one weekend. Investigations revealed the security vulnerability was exposed through compromised IoT devices, such as customer-owned webcams and routers. Such smaller personal IoT devices are increasingly targeted since they potentially provide a backdoor into more robust security systems.

WEAKER CYBER RISK MITIGATION EFFORTS

Despite the ever-present and ever-growing cyber threat potential in APAC, companies in the region appear less prepared. A lack of transparency has resulted in low levels of awareness and insufficient cybersecurity investments.

SURVEY CONDUCTED BY ESET ASIA IN 2015 REVEALED THAT 78 PERCENT OF INTERNET USERS IN SOUTHEAST ASIA HAVE NOT RECEIVED ANY FORMAL EDUCATION ON CYBERSECURITY, HIGHLIGHTING THAT MOST PEOPLE IN THE REGION ARE OBLIVIOUS TO THEIR CYBER VULNERABILITIES.

EXHIBIT 1: A HIGHER THREAT POTENTIAL

SPEED OF DIGITAL TRANSFORMATION

	In 2015/2016	In 2020
More internet users globally	3.7 BN	**4.2 BN** growth led by APAC (60%)
Greater interconnectivity among 4G mobile devices	1 BN connections	**4.7 BN** almost ½ (49%) of the increase attributed to APAC
Higher mobile network traffic	7 EB/mth	**35 EB/mth** APAC accounts for the largest share of traffic (47%)

ASIA PACIFIC LEADS INTERNET-OF-THINGS (IOT) MARKET

TECHNOLOGY ADOPTION PIONEERS
Japan and South Korea pioneered the adoption of IoT and machine-to-machine technology

Top broadband (internet) speed	5.6 Mbps global average	**27 Mbps** South Korea
Global IoT connectivity	4.9 BN units	**25 BN** with APAC countributing 8.6 billion
Exponential growth in IoT market revenue	$656 BN	**$1.7 TN** APAC accounts for the largest share of traffic (47%)

China and Japan alone account for a quarter of global revenue, followed by the US

Source: Cyber Risk in Asia-Pacific: The Case for Greater Transparency

LOW AWARENESS

A survey conducted by ESET Asia in 2015 revealed that 78 percent of Internet users in Southeast Asia have not received any formal education on cybersecurity, highlighting that most people in the region are oblivious to their cyber vulnerabilities.

The lack of disclosure regulation has also created the perception that cyberattacks in the region are relatively lower than those reported in the US or Europe, even though Asian businesses are significantly more likely to be targeted.

LOW INVESTMENTS

The low level of awareness in general leads to an underinvestment of time, finances, and resources in the technologies and processes needed to combat cyber adversaries.

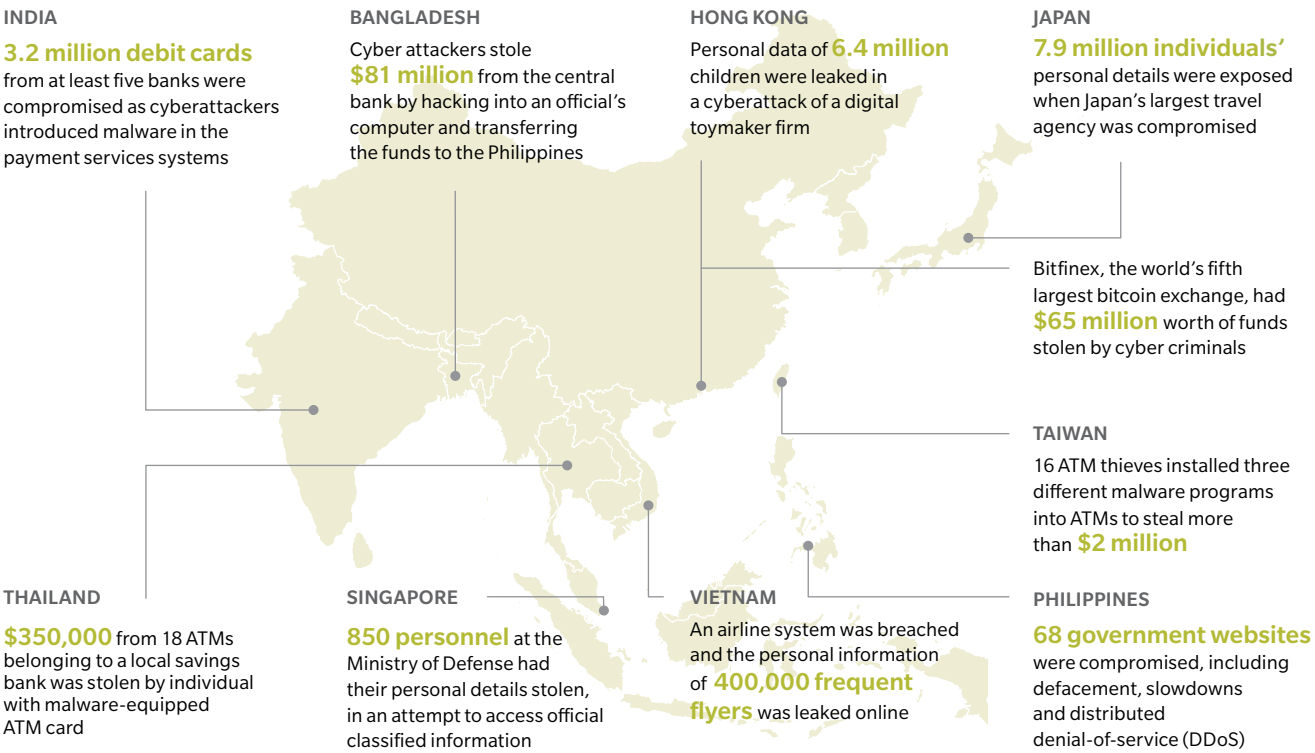
For example, a 2016 Beazley survey found 80 percent of the surveyed small-medium enterprises (SMEs) in Singapore used anti-virus software as their main cyber risk management tool, while only 8 percent allocated more than $50,000 to their cybersecurity budgets. Furthermore, APAC firms on average spent 47 percent less on information security than North American firms in 2015.

The need to combat cyber threat has never been more urgent in the APAC region, and major industries in the region (construction and engineering, financial, high tech and electronics, for example) are especially susceptible to the threats. A series of recent, high-profile cyberattacks that touched multiple countries and industries across the region have brought the issue to the fore.

Yet, these incidents represent only a handful of all attacks. LogRhythm, a security intelligence company, estimated up to 90 percent of APAC companies came under some form of cyberattack in 2016. A survey by Grant Thornton revealed that business revenues lost to cyberattacks in APAC amounted to $81.3 billion in 2015, exceeding those in North America and Europe by approximately $20 billion each.

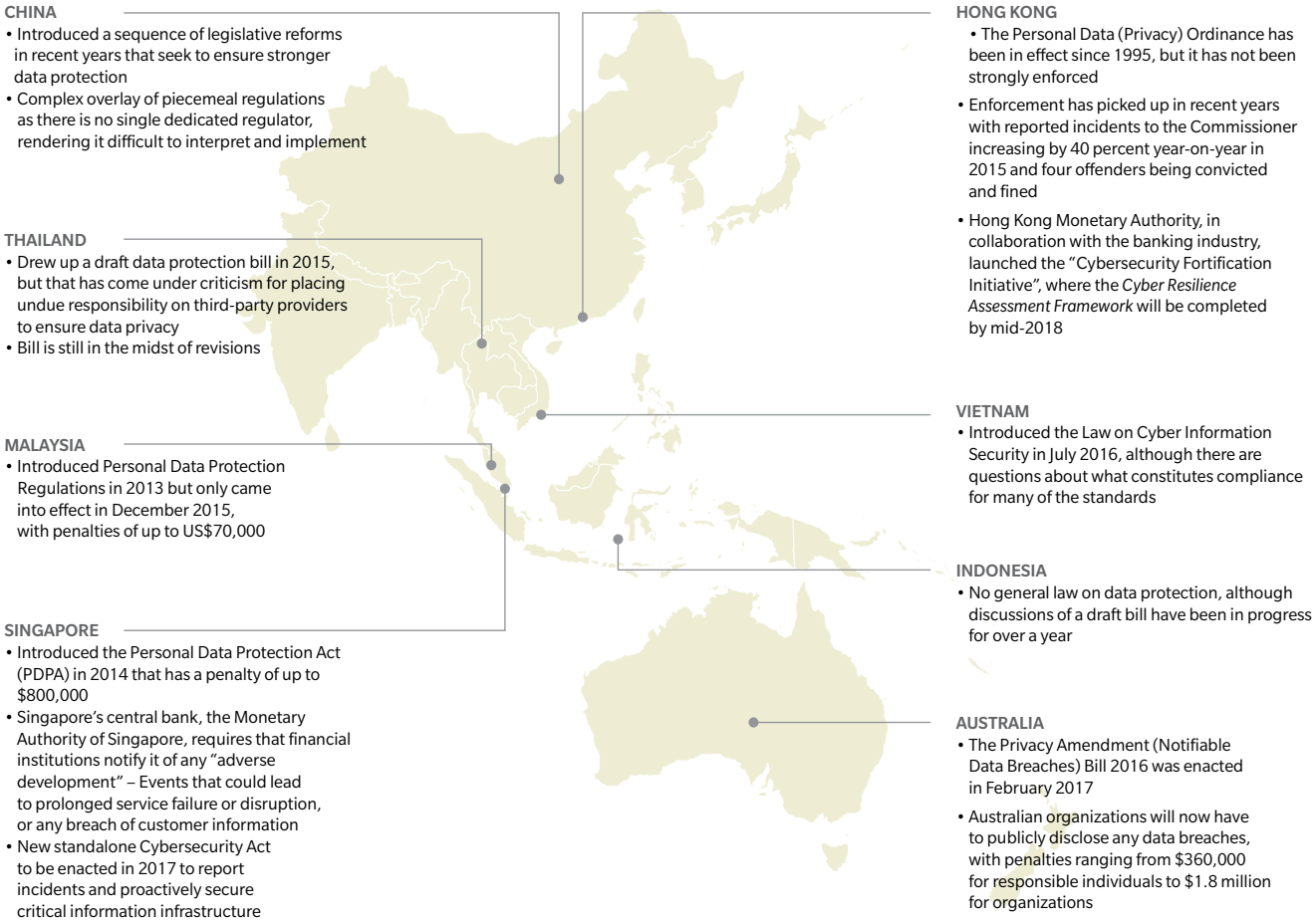
What is worrying is that this is likely only the tip of the iceberg. Cheah Wei Ying, an expert on nonfinancial risk at Oliver Wyman believes that "the majority of

EXHIBIT 2: CYBERATTACKS IN APAC – TIP OF THE ICEBERG?



Source: Cyber Risk in Asia-Pacific: The Case for Greater Transparency

EXHIBIT 3: DEVELOPMENTS IN DATA PRIVACY AND BREACH DISCLOSURE REGULATIONS



Source: Cyber Risk in Asia-Pacific: The Case for Greater Transparency

cyberattacks in the region usually go unreported as companies are neither incentivized nor required to do so. This lack of transparency underpins APAC's susceptibility to cyberattacks".

Apart from selected countries (i.e., Japan, South Korea) and industries (i.e., financial services in Singapore), APAC still lags the West in terms of cyber transparency. Organizations are able to conceal data compromises from regulators and their stakeholders, dulling the true impacts of cyberattacks and impeding the threat awareness required to act against cyber criminals.

CONCLUSION

In the region's battle against cybercrime, the most critical issue is raising the level of transparency. ♦

This article is an excerpt from the report entitled Cyber Risk in Asia-Pacific: The Case for Greater Transparency

Wolfram Hedrich, is the Executive Director of Marsh & McLennan Companies' Asia Pacific Risk Center. Gerald Wong is a Senior Consultant for Oliver Wyman. Jaclyn Yeo is a Senior Research Analyst for Marsh & McLennan Companies' Asia Pacific Risk Center.

CYBER RISK ASIA-PACIFIC IN NUMBERS

THE SEVERITY OF CYBERATTACKS

Hackers are 80% more likely to attack organizations in Asia

$81 BILLION in business revenues **LOST** to cyberattacks

RECENT EXAMPLES IN ASIA

$81 MILLION stolen from cyberattack on a bank in Bangladesh in May 2016

PERSONAL DATA OF 850 personnel stolen from Singapore's defense ministry online database portal in Feb 2017

6.4 MILLION Children's data stolen in Hong Kong hacking of a digital toymaker firm in Dec 2015

Cyberattacks are ranked 5th among **Asian top risks** and 6th among **Global top risks**

68 Philippine government websites simultaneously hacked in July 2016

ASIAN FIRMS LAG IN CYBERSECURITY

78% of Internet users in Asia have not received any education on cyber security

Asian organizations take 1.7 times longer than the global median to discover a breach

Asian firms spent 47% less on information security than North American firms

CHALLENGES FOR FIRMS IN MANAGING CYBERSECURITY

74% of organizations found it "difficult-to-extremely-difficult" to recruit cyber talent

70% of firms do not have a strong understanding of their cyber posture

Primary insurers are reluctant to provide single coverage above $100 million

Source: Cyber Risk in Asia-Pacific: The Case for Greater Transparency

THE **EQUIFAX BREACH** AND ITS IMPACT ON IDENTITY VERIFICATION

Paul Mee and Chris DeBrusk

Does the Equifax data breach mean that existing processes for confirming the identity of customers no longer work? Equifax, a leading US credit bureau, has announced that it suffered a data breach resulting in the exposure of critical personal and financial data for 143 million Americans. The implications for the affected consumers are profound. While their credit cards can be re-issued with new numbers, their legal names, addresses, social security numbers, and birthdates cannot.

Equally profound are the implications for companies who use information stored by credit bureaus as a mechanism for confirming the identity of new and returning customers. At many companies, standard procedures for confirming customer identity involve asking for the "last four" digits of a social security number (SSN). The safety of this procedure is now in question and it is reasonable to assume that all these SSNs are now in circulation among fraudsters and for sale on the dark web.

Other standard procedures for confirming identity require the consumer to answer challenge questions based on the content of their credit files. For example, a consumer may be asked whether or not they took out an auto loan during the last six months; and if so, for what type of vehicle. Or, they might be asked to confirm a prior address. These methods are now far less safe as the underlying information has been hacked. In fact, there is a real question as to which commonly used identity-confirmation processes are still viable.

Banks, mortgage companies, insurance companies, asset managers, telecommunication companies, medical and health companies, hospitals and other organizations hold critical information on their customers, and often their money. These organizations arguably have a moral and fiduciary obligation to prevent fraudsters from obtaining data and using it to takeover accounts or open new accounts fraudulently. If organizations fail to protect their customers, they will expose themselves to legal action as well as potentially punitive responses from regulators.

In this challenging new world, we see three imperatives for chief risk officers, chief security officers, heads of compliance and line of business leadership.

IF ORGANIZATIONS FAIL TO PROTECT THEIR CUSTOMERS, THEY WILL EXPOSE THEMSELVES TO LEGAL ACTION AS WELL AS POTENTIALLY PUNITIVE RESPONSES FROM REGULATORS.

SOCIAL SECURITY NUMBERS SHOULD BE CONSIDERED PUBLICLY KNOWN

Arguably, the safety of using SSNs in authentication has been declining for some years and certainly since the large data breach of the IRS in 2015. However, the last four digits of the SSN are still casually assumed to be confidential information in identity verification processes. Companies need to start relying on information that is truly only known to the company and its customer.

PROCESSES FOR CONFIRMING CUSTOMER IDENTITY TO PREVENT ACCOUNT TAKEOVER AND FRAUD NEED TO BE RETHOUGHT

When considering fraud risk, and procedures for avoiding customer account opening or takeover by fraudsters, the use of third-party information for identity confirmation is now arguably much less reliable than ever before. Adapting to this new reality will complicate many existing processes, especially those that support account password resets because if a customer cannot access his or her account, you cannot readily confirm identity using past transaction history (unless the customer has a really good memory!).

The only information that can be used with confidence for identity confirmation is that which is unique to the consumer and the verifying company. A statistical approach could be taken that relies on a broad range of different types of information, the totality of which is unlikely to be available to a fraudster. However, given constant announcements

regarding data breaches, even this approach could be challenged, especially in light of ongoing innovation by fraudsters and other bad actors.

Another complexity and practical challenge is that many organizations only encrypt and protect key data items such as SSNs in their systems, and don't protect the information that they will now need to use to confirm identity. A comprehensive reevaluation of what information is deemed "sensitive and critical" across databases and customer support systems needs to be performed and the means determined to protect this information from leakage or unauthorized access.

Today, many organizations use two-factor authentication as a mechanism to protect against account takeover attempts, phishing, and other fraudulent activities. The most common approach is to leverage a customer's mobile phone and a text message to confirm identity. It is worth noting that the information that was likely released in the Equifax breach (and others) could also be in use supporting identity processes by mobile phone companies.

Using text messages has always been of dubious merit. Mobile phone companies have themselves had difficulty preventing fraudsters from getting control of their customers' phones. Given the Equifax breach, the use of text messages to support two-factor authentication processes needs to be re-examined and alternative approaches implemented.

One potential new tool that companies can leverage to confirm identity are biometrics, although their use as a primary mechanism to confirm identity is still in question given the numerous examples of mobile phone fingerprint readers being spoofed by fakes. Emerging capabilities to perform facial recognition and iris scanning via mobile phones are worth watching to see how they can be leveraged – but won't address immediate challenges of confirming identity.

A COMPREHENSIVE REEVALUATION OF WHAT INFORMATION IS DEEMED "SENSITIVE AND CRITICAL" ACROSS DATABASES AND CUSTOMER SUPPORT SYSTEMS NEEDS TO BE PERFORMED AND THE MEANS DETERMINED TO PROTECT THIS INFORMATION FROM LEAKAGE OR UNAUTHORIZED ACCESS.

ACCURATELY IDENTIFYING NEW CUSTOMERS JUST GOT A LOT MORE DIFFICULT

Possibly the most difficult part of authentication takes place when a new customer opens an account. For complex financial products, this can be less of a concern due to the larger quantities of information that need to be collected, extensive know-your-customer processes and the sheer amount of time that opening a new account requires. Yet, as more and more consumer account opening processes are digitized and the time-to-first transaction decreases, companies need to redesign the processes by which they confirm that the new customer truly is the person they claim to be. This is going to be even more critical for products that allow a customer to establish an immediate liability such as a short-term loan, or aim to provide an immediate service for a deferred payment.

Industry organizations such as the FIDO Alliance are attempting to create industry-wide standards and support new solutions to the identity problem. This is all to the good but in light of the Equifax data breach, it is imperative that each organization perform a comprehensive audit of its own customer identity processes to ensure they understand where changes are needed, and also that they are accurately assessing the risks of process failures.

Given the increasing sophistication of attackers, the question is more likely "when," not "if" you will be attacked and compromised. Too often organizations focus on the potential for direct losses (fines, litigation and remediation) that result in a customer account being compromised, and not enough on the reputational damage (impact on brand value and customer loyalty) that can result from being inadequately prepared for a major incident or data breach.

With these factors in mind, senior executives need to be asking the questions, **"Are we fully prepared to respond to a large scale information breach?" and "How do we protect our customers in the best possible manner?"** ♦

Paul Mee is a New York-based Partner in Oliver Wyman's Digital and Financial Services practices. **Chris DeBrusk** is a New-York based Partner Oliver Wyman's Finance and Risk, CIB, and Digital practices.

LESSONS FROM WANNACRYPT AND NOTPETYA

Tom Burt

On May 12th, 2017, the world experienced the malicious "WannaCrypt" cyberattack. Starting first in the United Kingdom and Spain, the WannaCrypt malware quickly spread globally, blocking users from their data unless they paid a ransom. The antecedents of this attack occurred when criminals used exploits reportedly stolen from the U.S. National Security Agency (NSA) to develop this malware. By the first week, 45,000 attacks in nearly 100 countries were attributed to WannaCrypt, with 45 British hospitals and other medical facilities being some of the hardest hit.

On June 27th, 2017 – just six weeks after WannaCrypt – the NotPetya cyberattack began in the Ukraine and quickly spread globally by exploiting the same stolen vulnerability used in the WannaCrypt attack. This new attack, which in the guise of ransomware hid malware designed to wipe data from hard drives, also had worm capabilities which allowed it to move laterally across infected networks, with devastating consequences. In Ukraine, for example, workers at the Chernobyl nuclear plant were forced to manually monitor nuclear radiation when their computers failed.

THREE KEY LESSONS TO SURVIVE THE NEXT WANNACRYPT

There are three lessons from WannaCrypt and NotPetya with relevance for technology companies and their customers, as well as our technology-dependent societies. First, technology providers like Microsoft must continue to improve our own capabilities and practices to protect our customers against major cyberattacks. Second, technology companies and their customers must understand that cybersecurity is a shared responsibility, and that each stakeholder must take the actions necessary to improve security in the online ecosystem. Finally, governments must come together, along with technology companies and civil society groups, to pave the way for a new "Digital Geneva Convention" that will establish new international rules to protect the public from peace-time nation-state threats in cyberspace.

Technology companies have an increasing responsibility to strengthen their customers' security. Microsoft is no exception. With more than 3,500 security engineers, Microsoft is working comprehensively to address cybersecurity threats. This includes new security functionality across our entire software platform, including constant updates to our Advanced Threat Protection service to detect and disrupt new cyberattacks. With respect to WannaCrypt and NotPetya, Microsoft released security updates in March of 2017 that addressed the vulnerability exploited by the attacks. But we have not stopped there. Microsoft has been assessing their characteristics with the help of automated analysis, machine learning, and predictive modeling, and then using those lessons to constantly improve the security for all of our customers.

These attacks also demonstrate the degree to which cybersecurity has become a shared responsibility between technology companies and customers. In particular, WannaCrypt and NotPetya are powerful reminders that information security practices like keeping systems current and patched must be a high responsibility for everyone, and it is something every top executive should support. Millions of computers were running terribly outdated software or remained unpatched months after Microsoft released its March updates, leaving them vulnerable. In fact, over 10 percent of the computers that were successfully attacked were running Windows XP – which was originally released in 2001. And, no fully-up-to-date Windows computer was successfully penetrated. As cybercriminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems.

Finally, these attacks provide additional proof of why the stockpiling of vulnerabilities by governments is such a problem. This was an emerging pattern in 2017. As an example, vulnerabilities stored by intelligence agencies were showing up on WikiLeaks, and vulnerabilities reportedly stolen from the NSA have affected technology users around the world. Exploits in the hands of governments have leaked into the public domain and caused widespread damage, including the most-recent example of an NSA contractor who compromised sensitive hacking tools by placing information on his home computer. As Microsoft's

TECHNOLOGY PROVIDERS MUST CONTINUE TO IMPROVE OUR OWN CAPABILITIES AND PRACTICES TO PROTECT OUR CUSTOMERS AGAINST MAJOR CYBERATTACKS.

President, Brad Smith, explained immediately after the WannaCrypt attack, the theft of a nation-state cyber weapon can lead to economic devastation even more significant than theft of a conventional weapon, and when critical facilities such as hospitals or power grids are hacked, can put just as many human lives at risk.

WANNACRYPT IS A WAKE UP CALL

Clearly, governments of the world should treat WannaCrypt, NotPetya, and other nation-state sponsored cyberattacks as a wake-up call. Nation-state conflict – which started on the land, moved to the sea and found its way into the air – has moved to cyberspace with governments increasingly using the internet to hack, spy, sabotage and steal – and most recently, to simply impose economic destruction. This battle is waged on private property: in the datacenters, cables and servers of private companies like Microsoft, and on the laptops and devices owned by private citizens. And increasingly, private companies and individuals are finding themselves in the crosshairs. Nation-states need to take a different approach and adhere in cyberspace to the same rules applied to conventional weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities, inadequate protection of them from theft and the use of these exploits. This is one reason Microsoft called in February 2017 for a new "Digital Geneva Convention" to address these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.

Moreover, industry must also play a role in enabling a more secure Internet. Therefore, in the coming months Microsoft will continue to work across the technology sector to discuss a set of principles that can create the foundation for an industry accord outlining what, as an industry, we will do and what we won't do – all to protect our customers and help law enforcement. One principle that resonates strongly within the tech sector is a commitment to assist and protect customers everywhere, and never to assist in attacking them.

All the norms, rules and agreements in the world will not matter if attackers cannot be held accountable. That needs to start with attributing an attack to the perpetrator, even if it is a state or a state-sponsored group. While attribution could be collaborative between the public and private sector, drawing on the strengths of both technology companies and governments to investigate cyberattacks and identify those behind them, it must be independent and trustworthy. Trusted, credible attribution of cyberattacks would give governments – not just the jurisdiction where a particular victim resides – expert information to determine whether to take further action against the perpetrators. As with other complex and organized criminal networks, multiple jurisdictions may have information or a stake in uncovering the overall crime. Cybercrime is transnational and complex. To this end, the technology sector should work together, and seek the support of other experts in non-profit groups, academia, and elsewhere, to create such an organization to help deter nation state attacks in cyberspace and protect our customers.

CONCLUSION

WannaCrypt and NotPetya were just two of the major cyberattacks this past year, but their origins and impacts should train our attention to more urgent collective action. With help from nation-states, attackers are becoming more sophisticated and better funded. Confronting future nation-state sponsored attacks will only become more difficult, and that is why the tech sector, customers, and governments must work together. In this sense, the WannaCrypt and NotPetya attacks are a wake-up call for all of us. Microsoft recognizes the responsibility to help answer this call, and is committed to doing its part. ♦

Tom Burt serves as Vice President, Deputy General Counsel of Digital Trust at Microsoft.

THE MIRAI DDOS ATTACK **IMPACTS** THE INSURANCE INDUSTRY

Pascal Millaire

We are entering a new era for global insurers, where business interruption claims are no longer confined to a limited geography, but can simultaneously impact seemingly disconnected insureds globally. This creates new forms of systemic risks that could threaten the solvency of major insurers if they do not understand the silent and affirmative cyber risks inherent in their portfolios.

On Friday, October 21st, a distributed denial of service attack (DDoS) rendered a large number of the world's most popular websites inaccessible to many users, including Twitter, Amazon, Netflix, and GitHub. The internet outage conscripted vulnerable Internet of Things (IoT) devices such as routers, DVRs, and CCTV cameras to overwhelm DNS provider Dyn, effectively hampering internet users' ability to access websites across Europe and North America. The attack was carried out using an IoT botnet called Mirai, which works by continuously scanning for IoT devices with factory default user names and passwords.

The Dyn attack highlights three fundamental developments that have changed the nature of aggregated business interruption for the commercial insurance industry:

1. The proliferation of systemically important vendors

The emergence of systemically important vendors can cause simultaneous business interruption to large portions of the global economy.

The insurance industry is aware about the potential aggregation risk in cloud computing services, such as Amazon Web Services (AWS) and Microsoft Azure. Cloud computing providers create potential for aggregation risk; however, given the layers of security, redundancy, and 38 global availability zones built into AWS, it is not necessarily the easiest target for adversaries to cause a catastrophic event for insurers.

There are potentially several hundred systemically important vendors that could be susceptible to concurrent and substantial business interruption. This includes at least eight DNS providers that service over 50,000 websites, and some of these vendors may not have the kind of security that exists within providers like AWS.

2. Insecurity in the Internet of Things (IoT) built into all aspects of the global economy

The emergence of IoT with applications as diverse as consumer devices, manufacturing sensors, health monitoring, and connected vehicles is another key development. Estimates vary that anywhere from 20 to 200 billion everyday objects will be connected to the internet by 2020. Security is often not being built into the design of these products with the rush to get them to market.

Symantec's research on IoT security has shown the state of IoT security is poor:

- 19 percent of all tested mobile apps used to control IoT devices did not use Secure Socket Layer (SSL) connections to the cloud
- 40 percent of tested devices allowed unauthorized access to back-end systems
- 50 percent did not provide encrypted firmware updates, if updates were provided at all, IoT devices usually had weak password hygiene, including factory default passwords; for example, adversaries use default credentials for the Raspberry Pi devices to compromise devices

The Dyn attack compromised less than one percent of IoT devices. By some accounts, millions of vulnerable IoT devices were used in a market with approximately 10 billion devices. XiongMai Technologies, the Chinese electronics firm behind many of the webcams compromised in the attack, has issued a recall for many of its devices.

Outages like these are just the beginning. Shankar Somasundaram, Senior Director, Internet of Things at Symantec, expects more of these attacks in the near future.

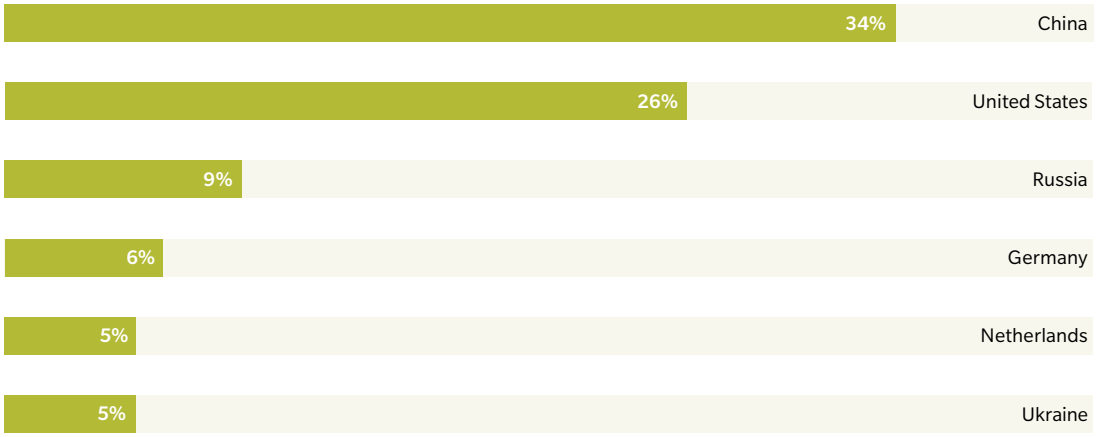
3. Catastrophic losses due to cyber risks are not independent, unlike natural catastrophes

A core tenant of natural catastrophe modeling is that the aggregation events are largely independent. An earthquake in Japan does not increase the likelihood of an earthquake in California.

In the cyber world consisting of active adversaries, this does not hold true for two reasons (which require an understanding of threat actors).

THERE ARE POTENTIALLY SEVERAL HUNDRED SYSTEMICALLY IMPORTANT VENDORS THAT COULD BE SUSCEPTIBLE TO CONCURRENT AND SUBSTANTIAL BUSINESS INTERRUPTION.

EXHIBIT 4: DISTRIBUTION OF ATTACKS



As well as long tail of adversaries from Vietnam, the UK, France, and South Korea.

Source: Symantec

First, an attack on an organization like Dyn will often lead to copycat attacks from disparate non-state groups. Symantec maintains a network of honeypots, which collects IoT malware samples.

Groups, such as New World Hacking, often replicate attacks. Understanding where they are targeting their time and attention, and whether there are attempts to replicate attacks, is important for an insurer to respond to a one-off event.

Second, a key aspect to consider in cyber modeling is intelligence about state-based threat actors. It is important to understand both the capabilities and the motivations of threat actors when assessing the frequency of catastrophic scenarios. Scenarios where we see a greater propensity for catastrophic cyberattacks are also scenarios where those state actors are likely attempting multiple attacks. Although insurers may wish to seek refuge in the **act of war** definitions that exist in other insurance lines, cyberattack attribution to state-based actors is difficult – and in some cases not possible.

WHAT DOES THIS MEAN FOR GLOBAL INSURERS?

The Dyn attack illustrates that insurers need to pursue new approaches to understanding and modeling cyber risk. Recommendations for insurers are below:

- Recognize that cyber as a peril expands far beyond cyber data and liability from a data breach and could be embedded in almost all major commercial insurance lines
- Develop and hire cybersecurity expertise internally, especially in the group risk function, to understand the implications of cyber perils across all lines
- Proactively understand whether basic IoT security hygiene is being undertaken when underwriting companies using IoT devices
- Partner with institutions that can provide a multi-disciplinary approach to modeling cybersecurity for insurer including:
  - Hard data (for example, attack trends across the kill chain by industry)
  - Intelligence (such as active adversary monitoring)
  - Expertise (in new IoT technologies and key points of failure)

CONCLUSION

Symantec is partnering with leading global insurers to develop probabilistic, scenario-based modeling to help understand cyber risks inherent in their standalone cyber policies, as well as cyber as a peril across all lines of insurance. The Internet of Things opens up tremendous new opportunities for consumers and businesses, but understanding the financial risks inherent in this development will require deep collaboration between the cybersecurity and cyber insurance industries. ♦

This article first appeared in the Symantic Thought Leadership Blog

Pascal Millaire serves as Vice President and General Manager, Cyber Insurance, for Symantec.

TIME FOR TRANSPORTATION AND LOGISTICS TO **UP ITS CYBERSECURITY**

Claus Herbolzheimer and Max-Alexander Borreck

When Danish shipping giant A.P. Moller-Maersk's computer system was attacked on June 27 by hackers, it led to disruption in transport across the planet, including delays at the Port of New York and New Jersey, the Port of Los Angeles, Europe's largest port in Rotterdam, and India's largest container port near Mumbai. That's because Maersk is the world's largest shipping company with 600 container vessels handling 15 percent of the world's seaborne manufactured trade. It also owns port operator APM Terminals with 76 port and terminal facilities in 59 countries around the globe.

For the transportation and logistics (T&L) industry, the June 27 cyberattack is a clarion call to elevate cybersecurity to a top priority. Besides Maersk, press reports said other transportation and logistics industry giants were affected including German postal and logistics company Deutsche Post and German railway operator Deutsche Bahn, which was also a victim of the WannaCry ransomware hack in May.

While up until now hackers have seemed more preoccupied penetrating computer systems at banks, retailers, and government agencies – places where a hacker can find access to lots of money and data and create substantial disruption – the most recent ransomware attacks demonstrate that the transportation and logistics industry is now on hackers' radars.

T&L's INCREASED DIGITIZATION

Part of the increased interest in the industry is because of its own efforts to digitize. Over the past couple of years, the industry has been in the process of automating systems, turning paper into digits, and using advanced analytics to stay on top of their customers' needs. That has put more systems online and **vulnerable to various attack weapons now so readily available** on the Darknet – the hidden underbelly of the Internet where hackers, terrorists, and criminals cavort anonymously buying malware, stolen data, arms, and drugs.

The early, more obvious targets have upped their game in cybersecurity, and hackers who are relentless look down the chain for new avenues of entry. Hacking also has become not only a corporate business, but a nation state's business. Here, nation states are looking for places where things are crossing borders regularly and for access to major industries and public infrastructure, such as the airports and ports that transportation and logistics companies operate.

The transportation and logistics industry also has characteristics that make it a particularly tempting target. First, the industry is a global one with tentacles into so many different industries around the world. Complex logistical chains are created around manufacturers, and often logistics companies are embedded within production facilities controlling inventory and handling on-demand needs of a plant. Simultaneously, the industry is fragmented with large transportation and logistical giants working alongside tiny companies responsible for one short leg of a product's long journey from raw materials, to production, to retailer, to consumer. This almost always means multiple technology systems are being employed, and multiple cybersecurity procedures of various degrees of rigor being followed. This fragmentation provides more opportunities for hackers.

LIKE WITH ALL FORMS OF WARFARE, ATTACKERS WILL SEEK OUT THE WEAKEST LINK IN ANY CHAIN – THE MOST VULNERABLE ELEMENT – AS A TARGET. WHY STEAL MONEY FROM THE BANK WITH ALL ITS INFRASTRUCTURE AND PROTECTIONS WHEN YOU CAN STEAL IT ON THE WAY TO THE BANK?

LOOKING FOR THE WEAKEST LINK

Like with all forms of warfare, attackers will seek out the weakest link in any chain – the most vulnerable element – as a target. Why steal money from the bank with all its infrastructure and protections when you can steal it on the way to the bank? While efforts to protect it along the way are made, almost any criminal could tell you, it is almost always more insecure in transit.

We already see malware that allows for hacking of delivery robots and parcel lockers. Drones can be hacked as well as autonomous cars, and as these are used more and more for deliveries the potential for hijack increases. Drones could be flown into no-fly zones posing the possibility of attacks on planes. When we reviewed the Darknet, we found personnel data from a major transportation and logistics company, car entry hacks, and means to create fake parcel station identity.

Until now, the transportation and logistics industry has not prioritized cybersecurity except in cases where life was on the line, such as with aerospace manufacturers or airlines where the most sophisticated protections are used. But the **direct costs from cybersecurity breache**s are growing exponentially, and companies – even small ones – need to invest in new systems and more comprehensive risk management. By our projections, they can be expected to grow from $1.7 billion in 2015 to more than $6.8 billion by 2020.

INDUSTRY FRAGMENTATION IN SECURITY SOLUTIONS

The industry's fragmentation and its requirement to operate within the various IT systems of its customers makes figuring out cybersecurity solutions more challenging and has led to lower investment. The industry also operates on low margins, making extensive capital expenditure on cybersecurity unattractive. That may be offset by the potential liability costs from hacks.

Increasingly, shippers and regulators will require transportation and logistics companies to guarantee the integrity of product and transport data, as well as ensure compliance with stricter cybersecurity laws. This will include carriers and forwarders, who are assuming central roles in supply chains as hubs for data exchange, making them high-value targets.

Taking precautions by installing security systems, such as firewalls and detection systems for denial of services attacks and other malware, is crucial, but insufficient by themselves. **Cyber risk management** also needs to take into account personnel and organization failure.

Ultimately, adopting proactive cybersecurity risk management provides an opportunity for transportation and logistics companies to differentiate themselves. Forward-looking companies will begin to see a safer logistical offering as a competitive advantage, especially if attacks continue.

CONCLUSION

In the end, no industry will be entirely safe from the threat of cyberattacks. But every industry must do its part to at least make hackers' jobs more difficult. ♦

NO INDUSTRY WILL BE ENTIRELY SAFE FROM THE THREAT OF CYBERATTACKS. BUT EVERY INDUSTRY MUST DO ITS PART TO AT LEAST MAKE THE JOB OF HACKERS MORE DIFFICULT.

This article first appeared in Forbes on June 28, 2017.

Claus Herbolzheimer is a Berlin-based partner in Oliver Wyman's Digital practice.
Max-Alexander Borreck is a Munich-based Principal in Oliver Wyman's Transportation and Logistics practice.

ARE MANUFACTURING FACILITIES **AS SECURE** AS NUCLEAR POWER PLANTS?

Claus Herbolzheimer and Richard Hell

With 100,000's of non-Internet IP addresses, cybersecurity means more than internet security. As companies leverage more and more intelligent sensors and cyber-physical systems to aggregate data for algorithms that will control and maneuver machines, they increase the level of cyber risk. Physical machines and tools – or robots – that were once confined by the four walls of a manufacturing plant, are now vulnerable to outside forces.

Imagine if a malevolent outsider were to find a way to change the value of one or more sensor devices, triggering a chain reaction. In a chemical plant, it could change temperature or pressure settings and spark a cascade of negative events, possibly an explosion. In an automotive plant, it could force robots to go wild, or, even worse, covertly embed malware during the automated flashing process into autonomous vehicles.

MANUFACTURING PLANTS ARE VULNERABLE

Nuclear power plants and utility grids have layer upon layer of cyber measures in place, including "air pockets" with neither direct nor indirect internet connections, and defense mechanisms that shut or slow down activity if any abnormality is detected. But corporate manufacturing plants typically don't think in those terms, even though they may now have hundreds of thousands of potentially insecure, non Internet IP addresses that are susceptible to hackers.

The more open the ecosystem, of course, the greater the danger. Manufacturers of autonomous vehicles, for example, are unleashing products – designed to interact with other vehicles and a variety of connected roadside devices – into an open environment more susceptible to hacking than a more closed ecosystem like the manufacturing plant itself, at least in theory.

But that is only true if classic cybersecurity principles developed for the IT world are transferred into the industrial automation and cyber-physical systems world of production and control systems. If, say, a manufacturing plant's system is breached and negative events begin to cascade, you need a control mechanism that will either disconnect the system – or put you in a "safe" mode so you can continue to operate at a reduced level until the problem is isolated and corrected. Just like a nuclear power plant.

Going forward, engineers need to change the way they develop products, and physically embed security in product design. Imagine producing and installing hundreds of thousands of vulnerable devices in cars. What does it mean, from an architectural or infrastructure perspective, to make a sensor or any other IP device, secure? What is the next level of data security?

Companies need to manage the transition from a physically controlled environment to a digital environment. They need to develop policies to protect and monitor their systems, and to react and minimize damage when they are breached. They need to apply decentralized resilience to standards and rules so that intelligent systems stop connecting with each other and lock into "safe" mode when abnormalities are detected.

CONCLUSION

Given the proliferation of non-internet IP addresses in the manufacturing world, private-sector companies should transfer the classic principles of multiple, redundant safety mechanisms and cybernetic control systems of high-resiliency industries to the field of cybersecurity in manufacturing. ♦

Claus Herbolzheimer is a Berlin-based partner in Oliver Wyman's Digital practice. **Richard Hell** is a Munich-based Vice President in Oliver Wyman's Manufacturing Industries practice.

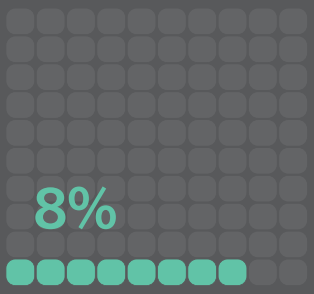

PREPARE FOR
EMERGING
REGULATIONS

PERCENTAGE OF RESPONDENTS AT EACH LEVEL OF GDPR COMPLIANCE

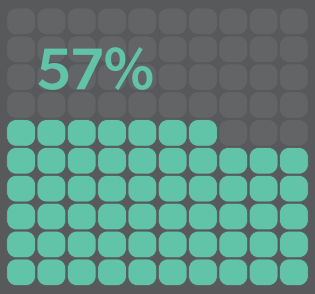
We asked these questions

1. *What progress has your organization made toward GDPR compliance/readiness?*
2. *Does your organization conduct the activities listed above in the European Union or otherwise process personal data of European Union citizens (e.g., names, unique IDs, email addresses or credit card information of customers or employees in the European Union)?*

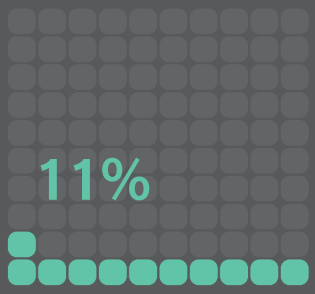
And the results were as follows



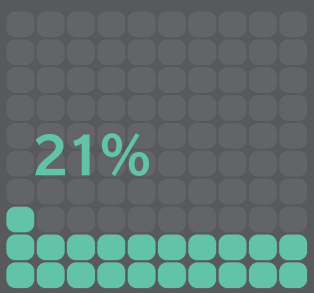
We are fully compliant/prepared



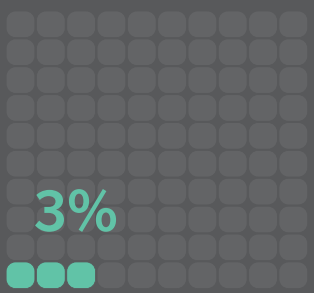
We are developing our plan for GDPR compliance



We have not developed or are not planning to develop a plan for GDPR compliance



I do not know



Other

Source: 2017 Marsh | Microsoft Global Cyber Risk Perception Survey

THE **GROWING WAVES** OF CYBER REGULATION

Paul Mee and James Morgan

In the recent past, there have been three major cyber-related regulatory developments in the US – these include the Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards ("ECRM ANPR"), the Cybersecurity Requirements for Financial Services Companies issued by the New York Department of Financial Services (NY DFS) and the revised version of the FFIEC Information Security Handbook.

As has been reported broadly and discussed in many industry forums, these regulatory documents present some of the most prescriptive cyber risk management requirements to date and include substantial new requirements for an enterprise-wide view of cybersecurity.

We will not present a detailed summary of these regulations, but rather will synthesize the major points where we believe the regulations impose new and challenging pressures.

TOP-TO-BOTTOM CASCADING OF CONTROL

Consistent with other prominent regulatory programs, cyber regulations establish an expectation of direct oversight by the Board of Directors based on policies, standards, and procedures articulated by management. Once a comprehensive cyber risk management strategy is defined and implemented, organizations need to continuously monitor their effectiveness and measure their alignment with business priorities. Regulators want to enforce this philosophy by requiring firms to identify and assess all the activities and exposures that present cyber risk, and subsequently aggregate them to evaluate the enterprise-wide residual cyber risk. Continuous monitoring of such aggregated information will require significant effort from organizations as they will need to design relevant metrics at different levels and make significant changes to their business processes across functions to include cyber risk in consistent ways.

Requirements for certification or attestation of compliance to internal policies, procedures, and regulatory standards will require further process definition and accountabilities clarification.

WHAT WILL NEED TO BE REFINED AND ENHANCED IS THE ALIGNMENT OF CYBER SURVEILLANCE WITH THE CYBER RISK PROFILE AND RISK APPETITE OF THE INSTITUTION.

EXHIBIT 1: SELECT SPECIFIC PRACTICAL EXPECTATIONS

In combination, FFIEC, ANPR, and NYDFS requirements entail a substantial increase in regulatory expectations for information management and security

CATEGORY	NOTABLE EXPANSION OF REGULATORY EXPECTATION	SOURCE FFIEC	ECRM	NYDFS
Scope breadth and depth	• Scope of Non Public Information (NPI) still unclear, but can be interpreted as significantly broader than Non Public Personal Information			●
Strategy and governance	• Integration of Information Security into risk culture and decision-making	●		
	• Prescriptive governance document requirements	●		●
	• Board-approved, enterprise-wide cyber risk appetite and risk tolerances		●	
	• Board-approved, written, enterprise-wide cyber risk management strategy		●	
	• Annual Board certification of compliance and annual Board reporting			●
Framework	• Integration of Information Security into third party risk management program	●		
	• Integration of Information Security into the Lines of Business (LoBs) and support functions	●		
	• Integration of Information Security into enterprise risk management framework	●	●	
	• Specific testing/assessment requirements (e.g., bi-annual vulnerability assessment)			●
Operating model	• Responsibility for cyber risk management across three independent functions		●	
	• Mandated Chief Information Security Officer (CISO) role			●
	• Specific guidelines to be included in policies governing third-party cybersecurity			●
Infrastructure and capabilities	• Two-hour recovery time objective for sector-critical systems		●	
	• Quantification and aggregation of cyber risk with consistent, repeatable methodology		●	
	• Specific data protection requirements (e.g., multi-factor authentication)			●
	• Maintenance of five-year audit trail for material financial transactions			●

Source: Oliver Wyman analysis

MULTIPLE LINES OF MANAGEMENT DEFENSE

Financial institutions have already been extending the "Three Lines of Defense" model to cyber risk management, drawing on experience from other areas of risk management. Regulators appear to be making such a model a formal requirement without specifying all expectations.

ECRM specifically suggests increased responsibilities for business lines, Audit, an independent Risk function, and the Board. Starting from the base of the 'Three Lines of Defense' model, business units and technology still form the First Line of Defense. However, business units now face the added responsibility of identifying activities that contribute to cyber risk and measuring cyber risk on a continuous basis. In addition, business units will be required to frequently conduct assessments to evaluate the cyber risk across their activities and report them to the independent risk management function and senior management.

Regulators are favoring the CISO role reporting to the Risk function – implying a change in the interaction model where the historical reporting line of a CISO was to the Chief Information Officer (CIO). The new paradigm expects a CISO to drive the execution of cyber risk management strategy from top-down with an enterprise wide remit. At the same time, the CISO also needs to focus on identifying, measuring, and managing the cyber risk at a business activity level with front line business unit management and the technology organization.

In addition to strengthening the role of business units and elevating the cyber risk function and CISO to the enterprise level, regulators are also prescribing that Audit play an elevated role. The Audit function has been traditionally responsible for conducting an independent assessment regarding cyber risk controls compliance. Going forward, Audit teams will be required to assess whether the established Cyber Risk management strategy is appropriate for the nature of the business, strategic objectives, and the board-approved residual cyber risk goals.

While the roles of business units and IT as the First Line of Defense and Audit as the Third Line of Defense are consistent across the industry, the design of the Second Line of Defense (made up of the CISO and the enterprise risk function) still varies. The role of the CISO and the definition of second line risk oversight will likely become an important area for achieving further organizational clarity, and an important one to get right to ensure effectiveness of activities without duplication of effort, diffusion of expertise, or a blurring of accountabilities. An organization's ability to effectively define and deploy their Lines of Defense will be critical in accelerating their readiness to monitor their primary assets and respond in the event of a cyberattack.

INSTITUTIONAL AND SYSTEMIC RESILIENCE

The new regulation is clearly oriented towards establishing greater institutional resiliency in being able to detect and manage inevitable cyberattacks through a more explicit risk-based approach.

Further, there is a push towards promoting resiliency of the financial services system through regulation – a rationale for the imposition of controls to prevent interconnected institutions from negatively impacting each other and the financial system more broadly. We can expect this to lead to common checklists, standard reporting, regulatory submissions, etc., all aimed at establishing a level of certainty or confidence across the financial services sector. Such reviews would certainly be more intrusive and subjective – similar to qualitative aspects of CCAR reviews where fundamental risk management capabilities have been questioned.

The more traditional approach to cybersecurity has focused on strengthening the perimeter by investing in a broad spectrum of sophisticated technical capabilities and process controls across the organization. However, as recent regulation has identified, this approach has become less effective because organizations do always not have a clear understanding of their cyber adversaries and their related motives. In addition, cyber adversaries constantly evolve their attack methods and vectors. What will need to be refined and enhanced is the alignment of cyber surveillance with the cyber risk profile and risk appetite of the institution. In addition, the scope of surveillance will need to broaden and deepen as firms seek to confirm internally that cyber risk mindfulness is present and sufficiently effective throughout the organization.

EXPANDED VIEW OF THE ATTACK SURFACE TO INCLUDE THIRD PARTIES

One of the prominent features of the proposed regulations is the expansion of the notion of situational awareness. As a corollary of the risk-based approach to cybersecurity, the scope of situational awareness has expanded beyond organizational boundaries.

Keeping the interconnectedness of the financial sector in mind, regulators want financial institutions to think carefully about the impact they can have on the rest of the financial sector while managing the cyber risk they face from external dependencies and third-party relationships.

Regulators are also expecting institutions to expand the view of cyber threats to fully consider third parties (including vendors, partners and peers in the network) – both in terms of vulnerabilities that could undermine critical services they provide to regulated financial institutions and the potential for them to be the weak point of defense through which cyberattackers infiltrate the critical systems of a financial institution.

Practically, it is also important to understand the nature of third-party access. Increasingly, adversaries are exploiting the electronic access consumers, corporates, and others have via their multi-channel, multi-device connections to financial institutions. In these arrangements, an institution needs to look at methods to help protect the customer as both a means to protect themselves and demonstrate client support and due care.

Considering the cyber exposure of the many third parties is critical, but this also exponentially increases the complexity of the problem for financial institutions. Many organizations struggle to scale up their Information Security and IT Risk assessment and monitoring processes to keep up with the proliferation of third party vendors and partners within their ecosystem (and further, to deal with providers to these third parties, typically defined as fourth parties). The scoping of regulation to the largest institutions creates room for potentially unregulated contractors, vendors, and clients who have some degree of interface with enterprise systems to create transmission vectors.

Organizations will need to carefully evaluate the cyber resiliency of their overall ecosystem in the broadest sense and lay the necessary groundwork with key vendors, allies, and partners to address "weak links" in their overall business supply chain.

INTEGRATED, PROGRAMMATIC APPROACH TO CYBER RISK

Cyber regulation is focused on defining a distinct "cyber defense program", that can be identified and documented for supervisors, and establishing a "cyber risk management strategy" that will provide guidance to all business activities. Given regulatory insistence on multiple lines of governance and control, an institution's cyber program needs to be broader than the IT or Risk organization, with clear linkages to the institution's strategy and controls. Policies and procedures are one form through which cyber considerations are meant to be promoted through institutions, with accompanying training and positioning of specialized personnel in various parts of the organization also suggested.

Choreographing the interactions of standards and procedures, their enforcement, and the various accountabilities throughout the organization in a consistent manner will be particularly difficult.

We can expect that the Board, senior executives, all the way down to front line supervisors, will seek evidence that policies, procedures, training, and expertise are effectively resulting in a much broader understanding of cyber aspects of the business – which is a significant change for a risk type that is not intuitive for many, nor is an existing element of their day-to-day operations.

INCREASINGLY, ADVERSARIES ARE EXPLOITING THE ELECTRONIC ACCESS CONSUMERS, CORPORATES, AND OTHERS HAVE VIA THEIR MULTI-CHANNEL, MULTI-DEVICE CONNECTIONS TO FINANCIAL INSTITUTIONS.

CONCLUSION

The new and emerging regulations are a clear directive to financial institutions to keep cyber risk at the center of their enterprise-wide business strategy, raising the overall bar for cyber resilience. The associated directives and requirements across the many regulatory bodies represent a good and often strong basis for cyber management practices but each institution will need to further ensure that they are tackling cyber risk in a manner fully aligned with the risk management strategy and principles of their firm. ♦

Paul Mee is a New York-based Partner in Oliver Wyman's Digital and Financial Services Practices.
James Morgan is a New York-based Partner in Oliver Wyman's Digital and Financial Services Practices.

This article is an excerpt from the Oliver Wyman report entitled Deploying A Cyber Risk Strategy: Five Key Moves Beyond Regulatory Compliance

REGULATING CYBERSECURITY IN THE NEW YORK FINANCIAL SERVICES SECTOR

Aaron Kleiner

Regulation of cybersecurity practices is a challenging process, especially when local regulations can have global ramifications. There is a strong argument that prescriptive mandates can interfere with security professionals' agility in a highly-dynamic environment, or slow the pace of innovation and negatively impact economic growth. However, there is a compelling counterargument that certain standards should be followed and minimum requirements set so that organizations meet a baseline level of cybersecurity protection, which can help protect societal values surrounding consumer protection and even public safety.

The essence of the regulatory challenge is not to choose sides, but rather how to make progress against several goals concurrently: empowering security practitioners and supporting innovation while ensuring baseline protections and advancing societal goals. Regulators have recently demonstrated an increased understanding and willingness to embrace this approach, often in collaboration with stakeholders from within regulated communities and others who would support their compliance. These regulatory development processes bear some characteristics of the "multistakeholder" model that has underpinned Internet governance dialogues for many years, in which a diverse group of representative communities engage collaboratively to address shared issues.

NEW TEMPLATE FOR CYBERSECURITY REGULATION

The cybersecurity regulation issued by the New York Department of Financial Services (the Department) was developed through an open consultative process and, as a result, has the potential to create an appropriate level of cybersecurity readiness without compromising security professionals' agility or organizational capacity for innovation. Microsoft provided input to the Department when the regulation was under development as part of our ongoing engagement with global financial services regulators to share perspectives on cloud computing and best practices for cybersecurity risk management. With implementation now underway across regulated institutions, Microsoft continues to partner with organizations to support compliance and determine the best approaches to address regulatory requirements.

There are several elements of the Department's rule that should serve as examples, or at least helpful reference points, for other regulators considering how to craft cybersecurity regulations. Specifically, three areas of the Department's focus should inform the development and growth of cybersecurity regulations:

- First, the Department's emphasis on having appropriate organizational infrastructure in-place to manage cybersecurity risk on an ongoing basis;
- Next, the Department's recognition of how a risk-informed approach enables appropriate cybersecurity investments; and
- Finally, the Department's reliance on a narrow set of proven cybersecurity tools as mandatory requirements to protect regulated entities and their customers.

Building an organizational infrastructure for cybersecurity risk management means more than protecting a network perimeter or investing in cutting-edge tools. Having effective leaders positioned in appropriate roles is equally as important as the processes they implement or technologies they leverage, and the Department's approach reflects this reality. For example, the Department's requirement that organizations have a Chief Information Security Officer with responsibility for the organization's Cybersecurity Program, as well a mandate to inform the Board of Directors, reflects a vision for cybersecurity risk management that is inherent to the organization's internal functions. In addition, the Department appropriately emphasizes keeping cybersecurity professionals current with trends and best practices by requiring organizations to provide ongoing education.

The Department's approach also reinforces the centrality of a risk-informed approach to cybersecurity. The regulation positions an organizational Risk Assessment as a key input into the Cybersecurity Program, and further mandates risk assessments when engaging Third Party Service Providers. However, the regulation does not prescribe a particular model or framework to assess risk, which empowers organizations to make their own determinations about their risk appetite. Given the

HAVING EFFECTIVE LEADERS POSITIONED IN APPROPRIATE ROLES IS EQUALLY AS IMPORTANT AS THE PROCESSES THEY IMPLEMENT OR TECHNOLOGIES THEY LEVERAGE, AND THE DEPARTMENT'S APPROACH REFLECTS THIS REALITY.

broad range of cybersecurity guidance available to critical infrastructure organizations, like the NIST Cybersecurity Framework, the Department's non-prescriptive formula helps to avoid duplication of existing and relevant risk assessment tools that organizations can use.

The Department is prescriptive in some respects, but these prescriptions often reflect practices that should be implemented regardless of whether they are required by law. Use of multifactor authentication, encryption, vulnerability assessments, penetration testing, and similar measures set forth in the regulation are recognized as effective. To the extent that cybersecurity practices should be mandated, the Department's approach reflects what many practitioners would likely require themselves. Nonetheless, proper configuration and other implementation details are essential to whether these requirements have a meaningful impact on cybersecurity. For example, not all encryption is created equal, and organizations should ensure that they are not using outdated algorithms like SHA-1.

CLOUD COMPUTING AS COMPLIANCE ENABLER

Cloud computing offers a unique model for organizations to manage compliance with the regulation, particularly in its more prescriptive aspects. Organizations may have the competence and resources to implement these requirements on their own, but often the expertise does not reside in-house or the budget will not accommodate all necessary investments. In other cases, organizations simply may not want to take on all the work to make their on-premise deployments compliant. Because the regulation allows for technology outsourcing subject to appropriate controls, organizations have the option to leverage cloud services while remaining compliant with the regulation.

Looking ahead, a major test facing the Department will be the incident reporting requirement. Such reporting has high potential for distorting the signal-to-noise ratio; the Department may need to help inform decisions about which incidents are truly material to regulated organizations as well as offer insight into whether reported incidents provide guidance about effective cyber defenses or attacker behavior. Moreover, the Department must demonstrate that it can securely manage the incident data reported through its new online portal, which will inevitably draw considerable interest from malicious actors determined to assess vulnerabilities across the financial sector. Indeed, the incident data reported to the Department could significantly enable attackers if not protected properly.

ORGANIZATIONS MAY HAVE THE COMPETENCE AND RESOURCES TO IMPLEMENT THESE REQUIREMENTS ON THEIR OWN, BUT OFTEN THE EXPERTISE DOES NOT RESIDE IN-HOUSE OR THE BUDGET WILL NOT ACCOMMODATE ALL NECESSARY INVESTMENTS.

For technology providers and their regulated customers, the regulations offer a unique opportunity to begin the journey towards a world where cybersecurity is regulated in new ways by different regulatory actors. Many observers of the cybersecurity policy space would not have anticipated that a state financial services regulator would be among the first to develop and enforce new cybersecurity rules. Moreover, the same observers may not have immediately grasped that regulations implemented in New York would effectively have global resonance, but the concentration of globally-significant financial institutions expands the Department's impact.

CONCLUSION

Microsoft looks forward to continued dialog with stakeholders across the public and private sectors to drive the development of cybersecurity policy. The Department's new rules will certainly move this dialogue forward and provide learnings about how to strengthen cybersecurity readiness without compromising security practices' flexibility or opportunities for innovation. ♦

Aaron Kleiner serves as the Director for Industry Assurance and Policy Advocacy for Microsoft

THE REGULATORY ENVIRONMENT IN EUROPE IS **ABOUT TO CHANGE**, AND PROFOUNDLY

FireEye | Marsh & McLennan Companies

While the front pages of the Wall Street Journal, USA Today and the New York Times regularly feature reports of breaches against US-headquartered companies, the situation appears on the surface to be blissfully different in Europe. It is exceedingly rare that Der Spiegel, Le Monde or Corriere della Sera carry accounts of high-profile breaches against large European companies.

Why is that? The fundamental difference in the two continents is that in the United States, more than 50 federal, state and local laws mandate disclosure of cyber breaches to regulators or affected consumers. Until recently, the regulatory regime in Europe was far different.

That is about to change profoundly. With the recent passage of the European Union's General Data Protection Regulation (GDPR), companies will soon be required to publicly disclose data breaches to national data protection authorities and, where the threat of harm is substantial, to affected individuals. Failure to do so could result in fines of as much as four percent of a company's global turnover – a staggering sum.

This sea of change in the public reporting obligations of companies will carry significant ramifications for governments, businesses and consumers across Europe. In addition, the Network Information Security Directive, adopted by the EU in July 2016, will place further demands on governments and the operators of critical infrastructure.

EU GENERAL DATA PROTECTION REGULATION

Jan Philipp Albrecht, a member of the European Parliament from Germany and the Rapporteur for the GDPR, captured the awesome aspirations of European policymakers in approving this new regulation: "The GDPR will change not only the European Data protection laws but nothing less than the whole world as we know it."

Albrecht's comment reflects the strength of the belief in Europe that privacy constitutes a fundamental human right.

With the growth of Internet-related technology, companies have accumulated troves of personal data. Business procedures have typically been focused on aggregating broad categories of data gleaned from consumers. Fearing the impact to the privacy rights of individuals, the European authorities are now strengthening privacy law to control, limit and expose the sweeping collection and use of data by many organizations.

> THE GDPR WILL CHANGE NOT ONLY THE EUROPEAN DATA PROTECTION LAWS BUT NOTHING LESS THAN THE WHOLE WORLD AS WE KNOW IT.
>
> **— Jan Philipp Albrecht**

Once implemented in May 2018, the GDPR will introduce a seismic shift in how companies retain and utilize personal data of individuals subject to the EU's jurisdiction. To prepare for implementation, companies must begin assessing the current state of their operations and the sweeping breadth of the new requirements.

While the regulation is nearly 90 pages long, there are four broad themes that are worth emphasizing:

- Individuals will have enhanced rights.
- Companies will be forced to reassess the manner in which they process and retain data.
- Companies will need to review their contractual arrangements with a host of third parties.
- Companies will be held to far stricter accountability and sanctions.

SWEEPING JURISDICTION

The GDPR purports to extend its reach far beyond the borders of the European Union to any organization that might collect or process "personal data" of an individual subject to EU jurisdiction (known as "EU data subjects"). Extending data protection beyond EU borders reflects the EU's view that data privacy protections should apply wherever data may travel. In practice, the broad jurisdictional provisions signal a clear hope that the GDPR's complex regulations will have a global impact.

PRIVACY IMPACT ASSESSMENTS

Businesses can expect both regulatory authorities and individuals to make inquiries about how data is being processed. Individuals can object to any data collection made without an adequate basis and can demand correction of inaccurate information. Organizations must perform so-called "data impact assessments" prior to collecting data. The GDPR provides guidance on practices to protect data, such as de-linking data from identities ("pseudonymisation"), encryption, regular assessments of technical controls, and incident response plans that account for maintaining the confidentiality and integrity of data.

AFFIRMATIVE CONSENT AND THE RIGHT TO BE FORGOTTEN

The GDPR makes clear that no company may collect personal data without first notifying users of how their data will be stored, protected and shared with third parties. In order to collect data, the company must first

EXHIBIT 1: COMPONENTS OF GDPR IMPLEMENTATION

Source: FireEye|Marsh & McLennan Cyber Risk Report 2017 Cyber Threats: A perfect storm about to hit Europe

obtain the individual's "freely given, specific, informed and unambiguous" consent for the collection. The GDPR will require users to give consent by affirmatively clicking on a consent notice or opting for specific technical settings that allow for the data collection.

Lastly, the GDPR codifies "the right to be forgotten." Already recognized by European courts and some member states, the right to be forgotten allows data subjects to demand that their personal data be erased and no longer used for processing.

So that is the dramatically altered regulatory regime that will begin to take effect in early 2018. What insight do we have about how sweeping its impact will likely be?

THE DUTCH "MINI-GDPR"

This is where the Dutch "mini-GDPR" comes into play. After a series of cyberattacks in 2015, the Dutch Parliament passed a Personal Data Protection Act, known as the Wet Bescherming Persoonsgegevens ("WBP"), in late 2015. In the time since the Dutch "mini-GDPR" took effect on January 1, 2016, companies have already notified the Dutch authorities of more than 5,500 cyber "incidents." Extrapolating these figures across the EU gives a glimpse of what management will likely confront in response to inquiries from regulators, supervisory boards and the press.

NETWORK INFORMATION SECURITY DIRECTIVE

To enhance focus on the specific vulnerabilities regarding critical infrastructure, the EU separately enacted the Network Information Security (NIS) Directive. Also scheduled to take effect in 2018, the NIS Directive will impose additional obligations on EU member states and infrastructure operators to raise the baseline of their cybersecurity capabilities. For example, the NIS Directive will require all member states to have a cybersecurity strategy, a national competent authority, and national cybersecurity incident response teams.

Several EU nations have already demonstrated early leadership. For example, Germany announced the creation of a mobile Quick Reaction Force as part of its Federal Office for Information Security. Businesses can expect both regulatory authorities and individuals to make inquiries about how data is being processed.

WITH THE THREAT ENVIRONMENT INTENSIFYING AND THE REGULATORY ENVIRONMENT ABOUT TO CHANGE PROFOUNDLY, THE QUESTION BECOMES WHETHER INDUSTRY AND EVEN GOVERNMENT ARE READY FOR THESE CHANGES.

Marsh surveyed the cyber practices at more than 750 of its clients across continental Europe in the fall of 2016. The study found that while high-profile events, government initiatives, and legislation have pushed cybersecurity to the forefront, far more work needs to be done.

For example, Marsh found that the percentage of companies indicating that they assessed "key suppliers" for cyber risk actually decreased from 23 percent in 2015 to 20 percent in 2016. As numerous attacks in the US and elsewhere have shown, hackers often gain access to larger organizations by initiating attacks against smaller vendors that provide services like air conditioning or takeout food.

General awareness of the risk posed by cyberattacks, while increasing, remains low. The percentage of companies that report having a strong understanding of their cyber posture increased from 21 percent in 2015 to 31 percent in 2016. Similarly, companies that regard cybersecurity as a top-five risk increased from 17 percent in 2015 to 32 percent in 2016, and the percentage of organizations that did not even include cyber on their risk register dropped from 23 percent in 2015 to 9 percent in 2016.

CONCLUSION

Despite this progress, European companies, like their counterparts around the world, have a long way to go to keep pace with the dramatically changing threat and regulatory environments. ♦

This article is an excerpt from the FireEye|Marsh & McLennan Cyber Risk Report 2017 Cyber Threats: A perfect storm about to hit Europe?

CYBERSECURITY AND THE EU GENERAL **DATA PROTECTION** REGULATION

Peter Beshar

The countdown has begun. In less than a year, tough new rules on data protection will come into effect in the European Union. For the first time, companies will be required to notify regulatory authorities, and potentially consumers, in the event of a significant cyber breach. In elevating the rights of consumers, the EU General Data Protection Regulation (GDPR) represents a sea of change in how companies will have to operate – and many are not ready.

NEW CYBER REGULATIONS WITH BROAD IMPACTS

Oliver Wyman, one of the Marsh & McLennan Companies, predicts that fines and penalties in the first year alone may total £5 billion, or more than $6 billion, for FTSE 100 companies. Adherence to GDPR requirements will require senior management – and not solely IT departments – to assume greater responsibility for cybersecurity. This shift means more than drafting a new organizational chart. It represents a profound transformation in how industries retain, use, and manage data and how leaders understand, mitigate, and respond to cyber intrusions.

To compound matters, the WannaCry worm showed just how vulnerable companies are. In the span of 48 hours, the WannaCry malware infected more than 300,000 computers across multiple continents. The attack provides a glimpse into a dark future, where cybercriminals operate with growing ease and impunity. Given the array of hacking tools reportedly stolen from the US National Security Agency in April, experts believe that more variants of WannaCry will be deployed shortly.

As the cyber threat landscape grows more complex, European regulators are not alone in mandating greater accountability at the executive level. For example, in May, New York state adopted a sweeping new regulation requiring financial services institutions to perform risk assessments, meet minimum protection standards, report breaches, and certify compliance. The Chinese government has also imposed broad new cyber requirements.

These myriad changes will impact virtually every aspect of a company's operations. In Europe, for example, newspapers will likely be filled next spring and summer with stories of significant breaches as companies begin reporting under the GDPR. And as consumers are alerted to breaches, regulators and data protection authorities will likely jump into the fray.

Moreover, the GDPR grants EU consumers broad rights to access, correct, and delete their personal data. As a consequence, Oliver Wyman estimates that at least 90 million gigabytes of data may be implicated. Supervisory boards will demand assurances from management teams that are likely not yet accustomed to this level of scrutiny.

Even those companies that do not fall under the new regulations should take proactive measures to protect their businesses against a cyber breach.

RESPONDING TO EMERGING REGULATIONS: FIVE IMPORTANT STEPS

Steps that businesses may wish to consider include:

- **Set a tone at the top of awareness and urgency.** In heightening anxiety worldwide, the WannaCry attack provides an opportunity for executives to demonstrate leadership by prioritizing cyber preparedness. Companies should use this moment – with memory of the attack still fresh – to remind their teams of the importance of good cyber hygiene.
- **Identify translators**. Too often, the technical team that defends systems and detects and combats cyber incidents speaks a language the C-suite does not understand. Executives need to have the right people in place who can provide them with timely and

EVEN THOSE COMPANIES THAT DO NOT FALL UNDER THE NEW REGULATIONS SHOULD TAKE PROACTIVE MEASURES TO PROTECT THEIR BUSINESSES AGAINST A CYBER BREACH.

strategic advice. These translators need to be able to understand both the reputational risk to the company's brand and the technical requirements of the company's systems.

- **Implement best practices.** Senior management cannot afford to be detached from their company's cybersecurity plans any longer. A vital lesson from WannaCry is the importance of developing consistent protocols for patching known software flaws. Executives should engage directly with their IT teams around emerging best practices like multifactor authentication, encryption tools, and penetration testing.
- **Start communicating with customers and shareholders now.** Companies should prepare their stakeholders for an era of greater transparency and disclosure and the almost inevitable day when cyber intrusions occur. Help your customers understand how you collect and use their personal data. Nothing will be worse for your company – or your customers – than over-promising and under-delivering on cybersecurity.
- **Make up for lost time.** The penalties for non-compliance with the GDPR are severe – up to 4% of a company's total turnover. For companies with annual revenues of $12 billion for example, potential fines will run up to $500 million. Companies should test their cyber incident response plans through drills or simulations, and develop cross-department muscle and relationships of trust that will be needed in the event of a serious breach. Executives should also reach out to regulators, law enforcement authorities, and policymakers – not so much to lobby but rather to share insight, information, and help shape the rules as they evolve. No one has all the answers.

CONCLUSION

Sound practices and sheer chance ultimately stopped the WannaCry malware and saved countless institutions from even worse breaches. It is unlikely the unprepared will be so lucky next time. Corporate leaders must act today to ensure their companies can adapt and excel in a world of growing risk, opportunity, and significant new regulations. ♦

Peter Beshar, based in New York, is the Executive Vice President and General Counsel for Marsh & McLennan Companies, Inc.

CYBERATTACKS AND LEGISLATION: A TIGHTROPE WALK

Jaclyn Yeo

The increasingly worrying global cyber risk trend has prompted lawmakers in many countries to either introduce or update their data privacy laws. This is a first step to ensuring better management, security and data control, which ultimately builds cyber resilience.

China will officially roll out its new Cybersecurity Law on June 1, signifying the government's intent to strengthen cyber regulations. Up to this point, China only had some general directives and localized guidelines for a secure and controllable internet. This new national law, however, is a head-turner for everyone doing business with China and will have implications on those business' operations.

SIGNIFICANT PROVISIONS OF THE CYBERSECURITY LAW

This law is the first legislation at the national level to establish legal principles for data privacy, and the financial penalties for data breach incidents are severe. In the event of a compromise to personal data, companies can be charged penalties of up to RMB1 million ($150,000) or ten times the illegal income, while penalties for individuals directly in charge can be up to RMB100,000.

In terms of data localization, the new Cybersecurity Law will require critical information infrastructure (CII) facilities to store personal information and other important business data collected or generated in China to be stored physically in China. CII operators must have government approval to transfer this data outside the country if it is "truly necessary." Companies that do not localize their data face potential financial penalties, including possibly losing their ability to conduct business in mainland China.

Furthermore, "network operators" are required to provide technical support to security authorities for the purposes of upholding national security and conducting criminal investigations under the data residency clause.

Finally, for data security purposes, both CII facilities and network operators in China are needed to comply with national standards and mandatory requirements such that equipment and products are safety-certified by inspection.

A MUCH-NEEDED MINDSET SHIFT

Since its announcement in late 2016, China's Cybersecurity Law has received much attention for the wrong reasons. Additional barriers to trade and innovation, greater complexity and higher-risk concerns for foreign companies doing businesses in China are some criticisms of the law by foreign business communities.

ARE OUR CURRENT CYBER LEGAL SYSTEMS AGGRESSIVE ENOUGH TO TAKE ON EVER-GROWING AND EVER-PRESENT CYBER ADVERSARIES?

However, the recent global extortion cyberattack may significantly shift these negative mindsets and change perspectives on the new law.

Massive ransomware cyberattacks hit critical information infrastructures around the world on May 12, ranging from the UK's National Health Service to a Spanish telecom giant and one of the world's largest international courier services companies headquartered in the United States. The unprecedented cyberattack over that weekend affected more than 200,000 computers across 150 countries, according to Europol, with the numbers expected to increase in the aftershocks ahead.

Asia-Pacific countries were not spared either. According to China's official Xinhua News Agency, more than 29,000 educational institutions were affected by similar attacks. Other infected computers were detected at railway stations, hospitals, office buildings, retail malls and government agencies. Over the next few days, more reports of similar attacks surfaced, impacting dozens of other countries, including Singapore, Japan and Australia.

In the face of this unprecedented scale of ransomware cyberattack, tighter cybersecurity legislation has been cast in the limelight. Are our current cyber legal systems aggressive enough to take on these ever-growing and ever-present cyber adversaries? Are our cybersecurity protection schemes and cyber risk management frameworks comprehensive enough to minimize and mitigate future attacks of similar or greater scale?

While the financial and economic impacts are still being assessed in the aftermath of events, the extent of psychological implications could be far more substantial. This rude wakeup call might just be what is required right now. The need for transparency through

stricter and more robust legislation is emphasized time and again, as it is a critical first step in risk management, driving awareness critical to initiate actions required to overcome adversaries and mitigate cyber risks.

Expectedly, the ransomware attack should lead to addressing the complacency in boardrooms at business levels regarding the seriousness of cyber threat. Perhaps it could even shift mindsets and perceptions of the foreign business community toward China's Cybersecurity Law, which is coincidentally timely in its implementation – just after the attack.

IN LIGHT OF CHINA'S NEW LAW, WHAT SHOULD BUSINESSES DO?

In addition to the Chinese government strengthening cyber regulations, the public needs to focus on being cybersecure and responsible, while companies (both local and foreign) need to ensure their businesses are in compliance with the new cybersecurity regulations and take corporate actions for managing cyber risks.

As part of enterprise-wide cyber risk management, foreign companies looking to do business in China should conduct an additional overall China risk assessment to assess their cyber risk exposure in the China market. Specific reference to the Cybersecurity Law is recommended as the focal point to ensure effective and efficient strategic business plans.

Marsh recently released a risk alert to its clients on China's Cybersecurity Law and its impact to Multinational Companies (MNCs), which highlighted three key recommendations for MNCs:

Conduct comprehensive risk identification for cybersecurity threats (for example, virus/ spyware/ malware, distributed denial-of-service attack, phishing) followed with proper insurance coverage plans.

Enhance the cyber risk management framework, including a clear definition of role and responsibilities, robust risk management process, advanced technical means, information technology (IT) operation control and log record.

Establish and improve business continuity plans and develop contingency plans related to cybersecurity threats.

Furthermore, robust cyber risk management skills begin with leadership from the boardrooms. In general, boards can consider the following questions when evaluating the impact of China's new Cybersecurity Law:

EXPECTEDLY, THE RANSOMWARE ATTACK SHOULD LEAD TO ADDRESSING THE COMPLACENCY IN BOARDROOMS AT BUSINESS LEVELS REGARDING THE SERIOUSNESS OF CYBER THREAT.

- Does our business fall under the definition of "Critical Information Infrastructure"? If so, will there be significant impacts on our internal plans for data storage, transmission and network security in China? Do we understand the parameters we must all work within and do we have the correct safeguards in place to be compliant?
- Are we storing information generated or gathered in mainland China on servers in mainland China? Do we need to create separate IT systems for China-specific data? Are we reliant on cross-border data transfers, and how would we approach this need with the Chinese government?
- What is our risk exposure stemming from the potential loss of intellectual property or encryption information as a result of this law? How would our business be affected should our Chinese competitors gain access to this information?
- What additional investments do we need to comply with this law and ensure the business is cybersecure?

CONCLUSION

It is true that the new regulations in China – as they will elsewhere – pose a few challenges for businesses. Indeed, they will also raise questions around data control and privacy. However, given the increasing frequency of cyberattacks, other countries are likely to follow suit and tighten regulations as well. ♦

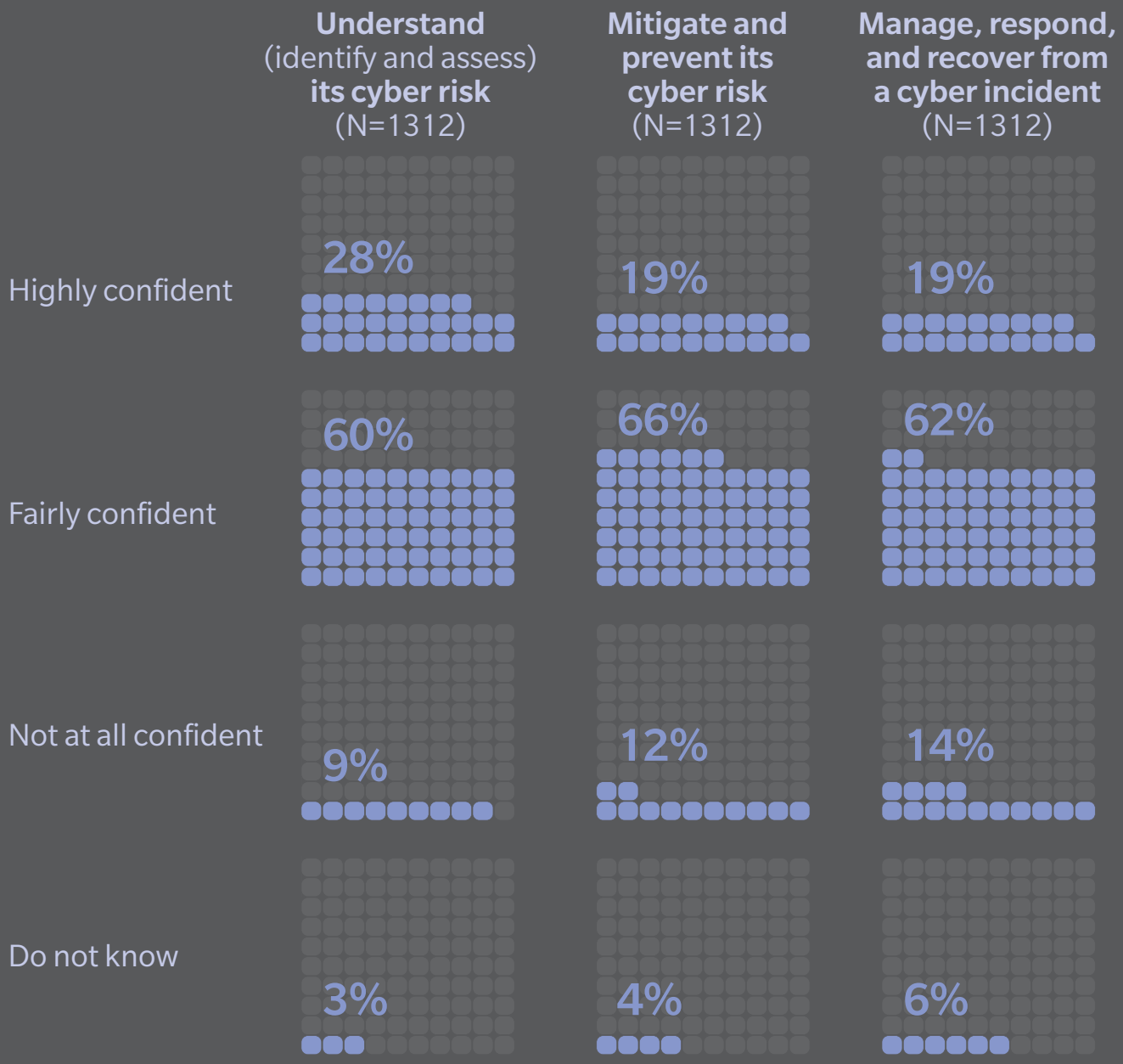
This article first appeared on *BRINK* on May 22, 2017. BRINK is the digital news service of Marsh & McLennan Companies' Global Risk Center..

Jaclyn Yeo, based in Singapore, is a Senior Research Analyst at Marsh & McLennan Companies' Asia Pacific Risk Center.

CYBER RESILIENCE BEST PRACTICES

CYBER PREPAREDNESS ACROSS INDUSTRIES AND REGIONS

Percentage of respondents who are confident in their organization's ability to ...



Source: 2017 Marsh | Microsoft Global Cyber Risk Perception Survey

DEPLOYING A **CYBER STRATEGY** – FIVE MOVES BEYOND REGULATORY COMPLIANCE

Paul Mee and James Morgan

Financial institutions are acutely aware that cyber risk is one of the most significant perils they face and one of the most challenging to manage. The perceived intensity of the threats, and Board level concern about the effectiveness of defensive measures, ramp up continually as bad actors increase the sophistication, number, and frequency of their attacks.

Cyber risk management is high on or at the top of the agenda for financial institutions across the sector globally. Highly visible attacks of increasing insidiousness and sophistication are headline news on an almost daily basis. The line between criminal and political bad actors is increasingly blurred with each faction learning from the other. In addition, with cyberattack tools and techniques becoming more available via the dark web and other sources, the population of attackers continues to increase, with recent estimates putting the number of cyberattackers globally in the hundreds of thousands.[1]

Cyber offenses against banks, clearers, insurers, and other major financial services sector participants will not abate any time soon. Looking at the velocity and frequency of attacks, the motivation for cyberattack upon financial services institutions can be several hundred times higher than for non-financial services organizations.

Observing these developments, regulators are prescribing increasingly stringent requirements for cyber risk management. New and emerging regulation will force changes on many fronts and will compel firms to demonstrate that they are taking cyber seriously in all that they do. However, compliance with these regulations will only be one step towards assuring effective governance and control of institutions' Cyber Risk.

In this paper, we explore the underlying challenges with regard to cyber risk management and analyze the nature of increasingly stringent regulatory demands. Putting these pieces together, we frame five strategic moves which we believe will enable businesses to satisfy business needs, their fiduciary responsibilities with regard to cyber risk, and regulatory requirements:

- Seek to quantify cyber risk in terms of capital and earnings at risk.
- Anchor all cyber risk governance through risk appetite.
- Ensure effectiveness of independent cyber risk oversight using specialized skills.
- Comprehensively map and test controls, especially for third-party interactions.
- Develop and exercise major incident management playbooks.

1 Joint Chiefs of Staff

While this paper is US-centric, especially with regard to regulation, these points are consistent with global trends for cyber risk management. Further, we believe that our observations on industry challenges and the steps we recommend to address them are applicable across geographies, especially when considering prioritization of cyber risk investments.

FIVE STRATEGIC MOVES

The current environment poses major challenges for Boards and management. Leadership has to fully understand the cyber risk profile the organization faces to simultaneously protect the institution against ever-changing threats and be on the front foot with regard to increasing regulatory pressures, while prioritizing the deployment of scarce resources. This is especially important given that regulation is still maturing and it is not yet clear how high the compliance bars will be set and what resources will need to be committed to achieve passing grades.

With this in mind, we propose five strategic moves which we believe, based on our experience, will help institutions position themselves well to address existing cyber risk management challenges.

1. Seek to quantify cyber risk in terms of capital and earnings at risk

Boards of Directors and all levels of management intuitively relate to risks that are quantified in economic terms. Explaining any type of risk, opportunity, or tradeoff relative to the bottom line brings sharper focus to the debate.

For all financial and many non-financial risks, institutions have developed methods for quantifying expected and unexpected losses in dollar terms that can readily be compared to earnings and capital. Further, regulators have expected this as a component of regulatory and economic capital, CCAR, and/or

LOOKING AT THE VELOCITY AND FREQUENCY OF ATTACKS, THE MOTIVATION FOR CYBERATTACK UPON FINANCIAL SERVICES INSTITUTIONS CAN BE SEVERAL HUNDRED TIMES HIGHER THAN FOR NON-FINANCIAL SERVICES ORGANIZATIONS.

resolution and recovery planning. Predicting losses due to Cyber is particularly difficult because it consists of a combination of direct, indirect, and reputational elements which are not easy to quantify. In addition, there is limited historical cyber loss exposure data available to support robust cyber risk quantification.

Nevertheless, institutions still need to develop a view of their financial exposures of cyber risk with different levels of confidence and understand how this varies by business line, process, or platform. In some cases, these views may be more expert based, using scenario analysis approaches as opposed to raw statistical modeling outputs. The objectives are still the same – to challenge perspectives as to how much risk exposure exists, how it could manifest within the organization, and how specific response strategies are reducing the institution's inherent cyber risk.

2. Anchor all cyber risk governance through risk appetite

Regulators are specifically insisting on the establishment of a cyber risk strategy, which is typically shaped by a cyber risk appetite. This should represent an effective governance anchor to help address the Board's concerns about whether appropriate risks are being considered and managed effectively.

Setting a risk appetite enables the Board and senior management to more deeply understand exposure to specific cyber risks, establish clarity on the Cyber imperatives for the organization, work out tradeoffs, and determine priorities.

Considering cyber risk in this way also enables it to be brought into a common framework with all other risks and provides a starting point to discuss whether the exposure is affordable (given capital and earnings) and strategically acceptable.

Cyber risk appetite should be cascaded down through the organization and provide a coherent management and monitoring framework consisting of metrics, assessments, and practical tests or exercises at multiple levels of granularity. Such cascading establishes a relatable chain of information at each management level across business lines and functions. Each management layer can hold the next layer more specifically accountable. Parallel business units and operations can have common standards for comparing results and sharing best practices. Finally, Second and Third Line can have focal points to review and assure compliance.

FROM OUR PERSPECTIVE, FIRMS FACE CHALLENGES WHEN ATTEMPTING TO PRACTICALLY FIT CYBER RISK MANAGEMENT INTO A "THREE LINES OF DEFENSE" MODEL AND ALIGN CYBER RISK HOLISTICALLY WITHIN AN ENTERPRISE RISK MANAGEMENT FRAMEWORK.

A risk appetite chain further provides a means for the attestation of the effectiveness of controls and adherence to governance directives and standards. Where it can be demonstrated that risk appetite is being upheld to procedural levels, management will be more confident in providing the attestations that regulators require.

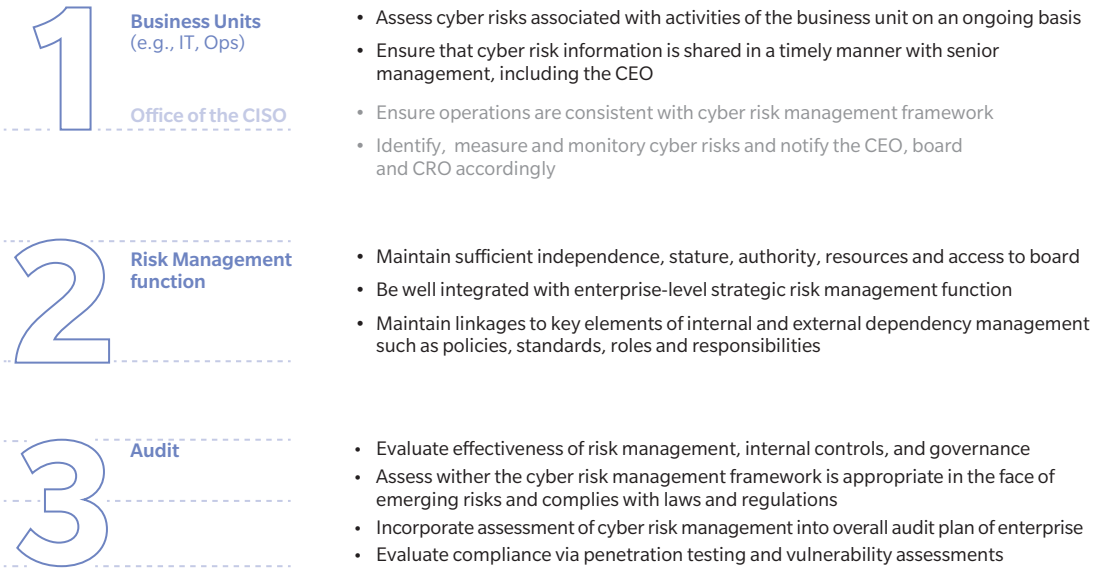
3. Ensure effectiveness of independent cyber risk oversight using specialized skills

From our perspective, firms face challenges when attempting to practically fit cyber risk management into a "Three Lines of Defense" model and align cyber risk holistically within an enterprise risk management framework.

CROs and risk management functions have traditionally developed specialized skills for many risk types, but often have not evolved as much depth on IT and cyber risks. Organizations have overcome this challenge by weaving risk management into the IT organization as a First Line function.

In order to more clearly segregate the roles between IT, business, and Information Security (IS), the Chief Information Security Officer (CISO) and the IS team will typically need to be positioned as a 1.5 Line of Defense position. This allows an Information Security group to provide more formal oversight and guidance on the cyber requirements and to monitor day-today compliance across business and technology teams.

EXHIBIT 1: THREE LINES OF DEFENSE CONCEPT AS APPLIED TO CYBER



Source: Oliver Wyman

Further independent risk oversight and audit is clearly needed as part of the Third Line of Defense. Defining what oversight and audit means becomes more traceable and tractable when specific governance mandates and metrics from the Board down are established.

Institutions will also need to deal with the practical challenge of building and maintaining Cyber talent that can understand the business imperatives, compliance requirements, and associated cyber risk exposures. At the leadership level, some organizations have introduced the concept of a Risk Technology Officer who interfaces with the CISO and is responsible for integration of cyber risk with operational risk.

4. Comprehensively map and test controls, especially for the third party interactions

Institutions need to undertake more rigorous and more frequent assessments of cyber risks across operations, technology, and people. These assessments need to test the efficacy of surveillance, the effectiveness of protection and defensive controls, the responsiveness of the organization, and the ability to recover in a manner consistent with expectations of the Board.

Given the new and emerging regulatory requirements, firms will need to pay closer attention to the ongoing assessment and management of third parties. Third parties need to be tiered based on their access and interaction with the institution's high value assets.

Through this assessment of process, institutions need to obtain a more practical understanding of their ability to get early warning signals against cyber threats. In a number of cases, a firm may choose to outsource more IT or data services to third party providers (e.g., Cloud) where they consider that this option represents a more attractive and acceptable solution relative to the cost or talent demands associated with maintaining Information Security in-house for certain capabilities. At the same time, the risk of third party compromise needs to be fully understood with respect to the overall risk appetite.

INSTITUTIONS NEED TO UNDERTAKE MORE RIGOROUS AND MORE FREQUENT ASSESSMENTS OF CYBER RISKS ACROSS OPERATIONS, TECHNOLOGY, AND PEOPLE.

EXHIBIT 2: KEY CYBER CONTROL TESTS, ALIGNED TO THE NIST CYBERSECURITY FRAMEWORK

1. IDENTIFY

CYBER RISK ASSESSMENT
Baseline assessment of threat profile, and expected loss

OVERALL TECHNICAL SECURITY ASSESSMENT
Assessment of technical security effectiveness

2. PROTECT

THIRD PARTY SECURITY REVIEWS
Assessment of third party security capabilities

SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) SECURITY TESTING
Assessment of the security control functionality against security requirements

IMPACT ANALYSIS OF PATCHES
Assessment of internal and third patch impact on security and functionality of the application environment

3. DETECT

APPLICATION SECURITY TESTING
Independent assessment of security capabilities of an application

VULNERABILITY SCANS
Periodic scans of internally and externally facing servers for known security issues and vulnerabilities

NETWORK PENETRATION TESTING
Assessment to identify vulnerabilities in network security

PHYSICAL PENETRATION TESTING
Assessment to identify vulnerabilities in physical security

RED TEAM EXERCISES
Stealth assessment of organization's digital infrastructure and defenses

4. RESPOND

TABLETOP EXERCISES
Assessment of incident response capabilities across pre-determined threat scenarios

SIMULATION/WAR GAMING
Dynamic simulation of a threat facilitated by a third party to assess incident response readiness and effectiveness

5. RECOVER

BC/DR TABLETOP TESTING
Assessment of stakeholders response preparedness and effectivenee of business continuity plan

REMEDIATION
Initiation of action plans and mobilization of resources to remediate following a cyber incident

Source: Oliver Wyman

5. Develop and exercise incident management playbooks

A critical test of an institution's cyber risk readiness is its ability to quickly and effectively respond when a cyberattack occurs. As part of raising the bar on cyber resilience, institutions need to ensure that they have clearly documented and proven cyber incident response plans that include a comprehensive array of attack scenarios, clear identification of accountabilities across the organization, response strategies, and associated internal and external communication scenarios.

Institutions need to thoroughly test their incident response plan on an ongoing basis via table top exercises and practical drills. As part of a table top exercise, key stakeholders walk through specific attack scenarios to test their knowledge of response strategies. This exercise provides an avenue for exposing key stakeholders to more tangible aspects of cyber risk and their respective roles in the event of a cyberattack. It also can reveal gaps in specific response processes, roles, and communications that the institution will need to address.

Last but not least, incident management plans need to be reviewed and refined based on changes in the overall threat landscape and an assessment of the institution's cyber threat profile; on a yearly or more frequent basis depending on the nature and volatility of the risk for a given business line or platform.

EXHIBIT 3: KEY THIRD PARTY CYBER RISK MANAGEMENT CONTROLS

1	**DUE DILIGENCE REQUIREMENTS (Initial and ongoing)**	• Company background accreditation • Financial reviews • Insurance liability coverage validation • Business license certification • Information security assessment and onsite visit
2	**SECURITY ASSESSMENTS (Onsite and remote)**	• Ongoing outside-in external security scans • Security recertifications (e.g., annually) • Changes in regulations and/or compliance requirements
3	**SECURITY SCORECARDS**	• Technology operational metrics (availability, reliability) • Reported cyber security events (time to detect, respond, communicate, resolve, associated impact) • Vendor/partner security training compliance
4	**ESCALATION AND REPORTING**	• Third party review meetings • Escalation and tracking of issues/concerns identified • Board and Risk governance reporting

Source: Oliver Wyman

CONCLUSION

Cyber adversaries are increasingly sophisticated, innovative, organized, and relentless in developing new and nefarious ways to attack institutions. Cyber risk represents a relatively new class of risk which brings with it the need to grasp the often complex technological aspects, social engineering factors, and changing nature of Operational Risk as a consequence of cyber. Leadership has to understand the threat landscape and be fully prepared to address the associated challenges. It would be impractical to have zero tolerance to cyber risk, so institutions will need to determine their risk appetite with regard to cyber, and consequently, make direct governance, investment, and operational design decisions.

The new and emerging regulations are a clear directive to financial institutions to keep cyber risk at the center of their enterprise-wide business strategy, raising the overall bar for cyber resilience. The associated directives and requirements across the many regulatory bodies represent a good and often strong basis for cyber management practices but each institution will need to further ensure that they are tackling cyber risk in a manner fully aligned with the risk management strategy and principles of their firm.

In this context, we believe the five moves advocated in this paper represent multiple strategically important advances almost all financial services firms will need to make to meet business security, resiliency, and regulatory requirements. ♦

This article is an excerpt from the Oliver Wyman report entitled Deploying A Cyber Risk Strategy: Five Key Moves Beyond Regulatory Compliance

Paul Mee is a New York-based Partner in Oliver Wyman's Digital and Financial Services Practices.
James Morgan is a New York-based Partner in Oliver Wyman's Digital and Financial Services Practices.

QUANTIFYING CYBER **BUSINESS INTERRUPTION** RISK

Peter Beshar

As we prepare for the next global pandemic cyberattack, one clear lesson is that the technological infrastructure on which we rely is more fragile than is often appreciated. The WannaCry attack reinforced the need for businesses to address the growing risk and financial consequences of Cyber Business Interruption (Cyber BI).

Although historical data can be relied on to estimate the impacts of data breaches, Cyber BI costs can be more difficult to determine because every company's IT systems, infrastructure, and exposures differ. How much an event costs will depend on several factors, including the organization's business operations model, incident response capabilities, actual time to respond, and the associated insurance coverages. By undertaking a Cyber BI risk quantification analysis, you not only gain a better understanding of the status quo and associated costs, but a foundation for making more informed risk mitigation and transfer investment decisions and improving cyberattack resiliency.

To more accurately quantify Cyber BI risk, businesses can use scenario-based analyses. In the wake of the WannaCry incident, potential disruption scenarios should be reconsidered to include complex ransomware events and their second- and third-order consequences, such as supply chain disruptions or physical damage.

A scenario-based analysis should focus on three factors:

- **Estimating the severity and likelihood of a Cyber BI event.** Using realistic scenarios can allow organizations to more accurately quantify the potential financial loss from a cyber BI event. Equally important is to scope these scenarios such that their likelihood of occurrence falls within a preselected range based on enterprise risk appetite and tolerance considerations.
- **Identifying mitigation options.** Depending on the significance of an organization's Cyber BI exposures, risk mitigation options could include changing business processes, re-architecting IT infrastructure to improve resilience, enhancing IT restoration capabilities, or strengthening technical cybersecurity controls. To properly evaluate these choices and identify the strategies that will have the greatest impact, it's important to have a credible estimate of potential Cyber BI exposure.
- **Evaluating risk transfer options.** Cyber BI is often underinsured or uninsured because many businesses do not fully quantify their risk prior to suffering a loss. But insurers are increasingly offering broader coverage for these exposures in both cyber policies and traditional property all-risk policies. A scenario-based cyber BI risk quantification analysis can support the proper structuring of these insurance options, including selecting appropriate limits. ♦

Peter Beshar, based in New York, is the Executive Vice President and General Counsel for Marsh & McLennan Companies, Inc.

This article is an excerpt from the Marsh Insight entitled #WannaCry: Lessons Learned and Implications

CYBERSECURITY: THE **HR IMPERATIVE**

Katherine Jones, Ph.D., and Karen Shellenback

Cybersecurity is a shared responsibility: it is a board-level concern, an executive concern and a mandate for all employees. Every organization today must plan for "when"– not for "if" – a cybersecurity breach happens. Companies and roles of all industries, types, and sizes are targets. With the enormity of this issue, data breaches are no longer solely the bailiwick of IT.

HR also has an important dual role to play when it comes to cybersecurity: creating and managing a cybersecure enterprise comprising the entire workforce and working to ensure the hiring, retention, and development of cybersecurity professionals.

CREATING A CYBERSECURE ENVIRONMENT

Many cybersecurity breaches affect HR because of the employee identification data that may become accessible. The results of an identity theft can be costly and far-reaching such as when the data is resold and used in further theft such as the fraudulent filing of tax forms to claim refunds.

While the extent of the problem may appear insurmountable, HR can play a major role in helping to prevent cybercrime and data breaches.

Cybersecurity requires a comprehensive, multidimensional approach to governance, requiring the engagement of the board and the executive leadership team. Beyond the technology risk itself, breaches are an overall business hazard and pose a talent strategy imperative. Mercer Select Intelligence research reveals that HR has the opportunity to play a more significant role in strategic planning regarding cyber risk-mitigation. Only half of senior cybersecurity leaders report that HR helps create corporate risk tolerance strategies (50%) or contingency plans for addressing a breach of employee data (45%).

BOLSTERING CYBER RISK MITIGATION WITH AWARENESS TRAINING

In addition to addressing the cybersecurity challenge by shaping hiring and management practices, HR can contribute to corporate security through the development of a risk mitigation governance policy that includes a comprehensive learning strategy on cyber risk issues.

One early step for HR professionals is to familiarize themselves with the recommended data security protocols of their HR information system vendors and ensure that those policies are being observed. For example, Mercer Select Intelligence research shows that over 80% of ex-employees retain access to their previous employer's file-sharing service.

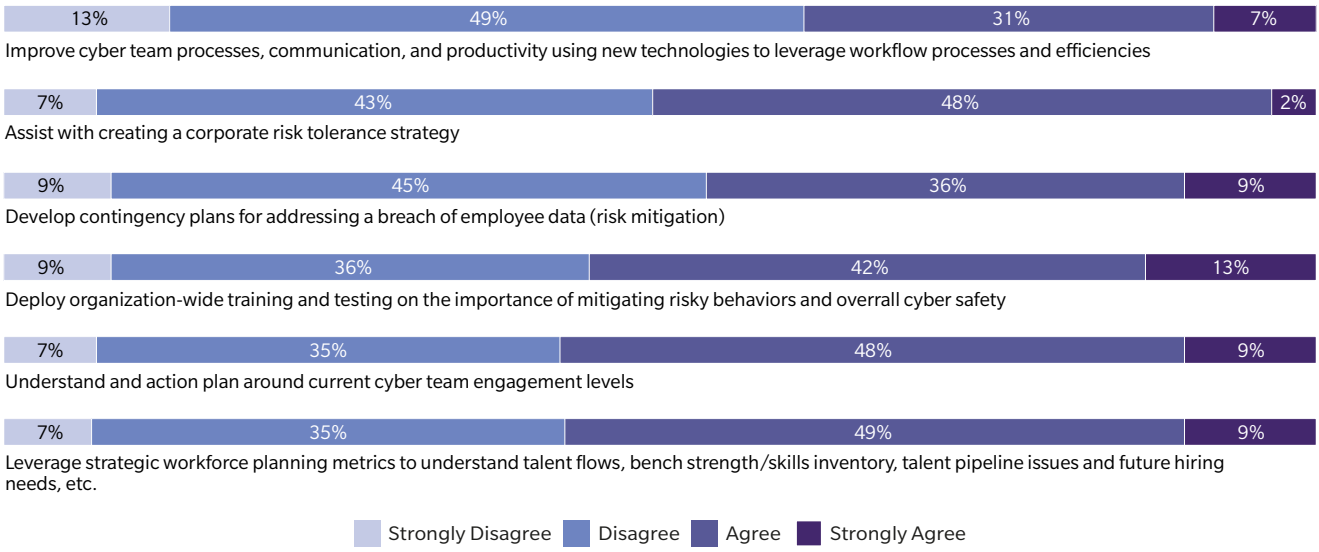
Security awareness training for employees is expected to become a fundamental cyber defense strategy by 2021. This effort must include all employees: from new-hire training that includes education on cyber risk best practices, to ongoing security education for more seasoned employees. This regularly scheduled employee education can better ensure that data security is top of mind. According to corporate cybersecurity leaders, only 55% of HR departments currently deploy organization-wide training and testing on the importance of mitigating risky behaviors and overall cyber safety *(see Exhibit 1)*.

SECURITY AWARENESS TRAINING FOR ALL EMPLOYEES IS EXPECTED TO BECOME A FUNDAMENTAL CYBER DEFENSE STRATEGY BY 2021.

KNOW YOUR INSIDERS

Think about your current workforce and any past breaches or issues that may have occurred. Was it an accident on the part of the employee? Opening a legitimate-seeming email is a common cause of data breaches, and it's a problem that can be addressed by education. Other times, tech-savvy employees may "go rogue" if permitted. Using their knowledge, they may download applications to their laptops or mobile devices that could intentionally

EXHIBIT 1: HR'S ACTIVITY IN CYBER MITIGATION STRATEGIC PLANNING



Source: Mercer Select Intelligence, 2017

or accidentally open the backdoor for ransomware or malware to enter and put the computer network at risk. Innocence, however, is not universal. Malicious employees may enter corporations with an agenda to sabotage. Here, diligent hiring practices, enforced system access controls, and sentiment-monitoring can combat the issue.

EMPLOYEE SENTIMENT: A PRIME PREDICTOR OF INSIDER ATTACKS

There are common events at work that adversely affect employee sentiment – and HR professionals know best when those potential flash points may occur. To meet the cybersecurity challenge, HR professionals must leverage that knowledge. HR should monitor employee sentiment for alienation and disengagement during reorganizations, corporate mergers, buyouts or divestitures, layoffs, and other internal or external events that affect the workforce. It is important to plan for alienation abatement through positive, honest communication and to monitor those employees who are most likely to be affected. Anticipating and planning for extra risk protection during tense periods that affect the workforce can significantly mitigate the potential risk during these periods.

Unfortunately in today's world, a cyberattack is almost as inevitable as death and taxes – but there are ways HR can educate employees about the risks of security breaches and what they can do to help prevent them.

FINDING AND FOSTERING CYBERSECURITY PROFESSIONALS

It is critical to create a comprehensive cyber risk mitigation strategy, provide awareness training, and understand risky employee behaviors, but protecting your organization against the ongoing barrage of daily hacks requires a cohort of talented and energized cyber professionals. There is a severe cybersecurity workforce shortage, with one million unfilled cybersecurity jobs in 2016 anticipated to grow to an expected shortfall of 1.5 million by 2019, according to Cybersecurity Ventures. Mercer Select Intelligence

INSIDER ATTACKS USUALLY FALL UNDER ONE OF THE FOLLOWING THREE CATEGORIES: ACCIDENTAL, RENEGADE, OR MALICIOUS

surveyed senior cybersecurity leaders on their view of HR's role in cybersecurity , and the results showed that HR can do more to help the organizations' cyber risk functions attract, train, and retain cyber professionals.

KEY ISSUES CITED IN HIRING CYBERSECURITY STAFF

Our research shows that while approximately 90% of senior cybersecurity leaders report that HR helps them recruit from diverse labor pools and 62% report that their HR recruiting team partners with universities to access potential new hires, only a little over a half (54%) report that HR actively recruits from military communities, and only 35% report that HR works with them to use crowdsourcing and other innovative strategies to attract the best and the brightest *(see Exhibit 2)*.

THE CYBER SKILL DEVELOPMENT IMPERATIVE

HR has an essential role in assessing and providing career development opportunities for cyber risk teams. While managers hiring for the cybersecurity function look for candidates with training and experience, HR should look to develop those qualifications within existing staff and among new hires. More than two-thirds (68%) of senior cybersecurity leaders report that their HR teams help build managerial skills to effectively coach and develop their cyber staff members; however, nearly two-thirds don't believe that HR helps create enticing career paths or developmental opportunities for those cyber professionals. Additionally, 62% do not believe that HR helps their staff obtain line-of-business experience – an important factor for the effective development and execution of business-driven mitigation strategies. Finally, fewer than half (48%) of respondents believe that their organizations provide mentorship, sponsorship, or "visibility" opportunities for female cyber talent. Only 33% of HR departments help provide skill development opportunities, including relevant games

PROBLEMS FACED BY HR WHEN HIRING CYBERSECURITY STAFF

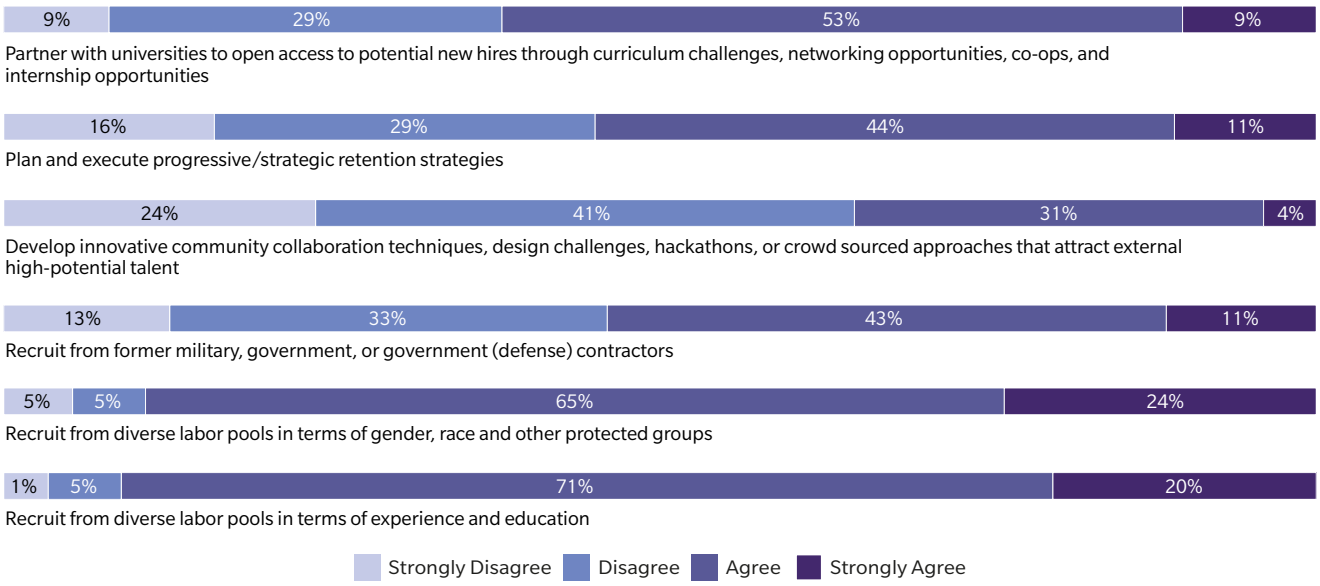
46%

Failure to locate talent with the right **educational** credentials

89%

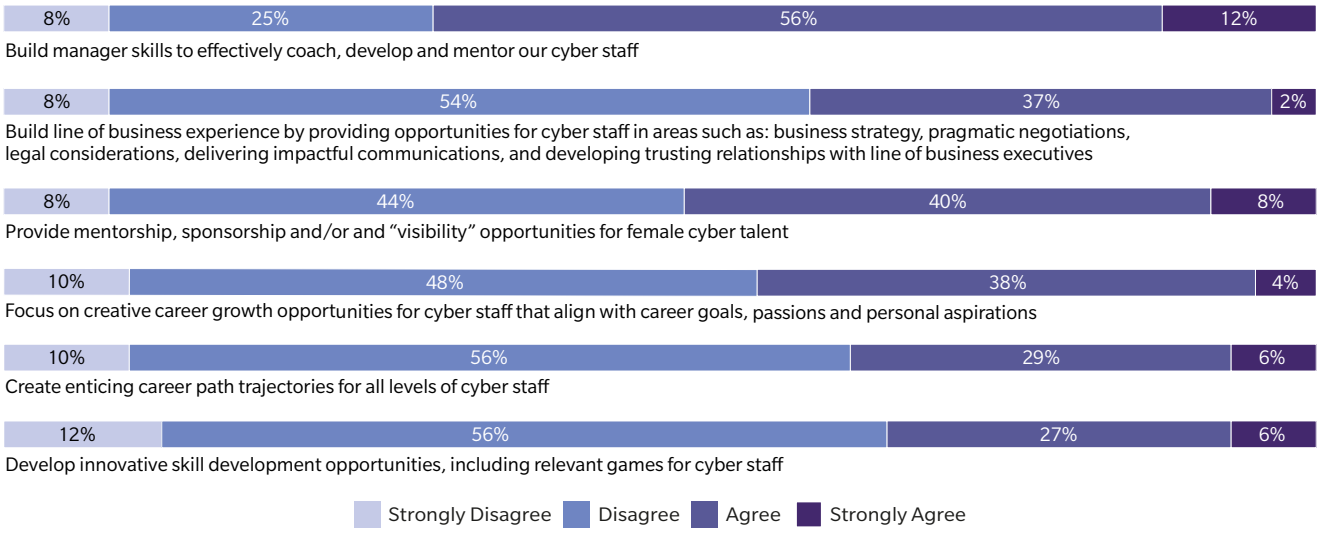
Inability to locate talent with the **experience** needed

EXHIBIT 2: HR'S ACTIVITY IN CYBER TALENT RECRUITMENT AND RETENTION STRATEGIES: WHAT CYBER LEADERS TELL US



Source: Mercer Select Intelligence, 2016

EXHIBIT 3: HR'S ROLE IN CAREER DEVELOPMENT OF CYBERSECURITY TALENT



Source: Mercer Select Intelligence, 2016

for cyber staff (hackathons, for example) and only 42% focus on creative career growth opportunities for these strategic staff members *(see Exhibit 3)*.

Understanding the current talent pool for cyber, the future capabilities that will be needed, and the best methods for addressing the cyber talent team's professional needs is a priority. HR has the capabilities and resources to help cybersecurity leaders attract, retain, and build the cyber workforce of the future. The imperatives of cyber risk mitigation, corporate boards, executive leadership teams and internal risk management departments should encourage HR to bolster the capabilities and retention of their cyber risk staff as a business priority.

CONCLUSION

Cybercrime is growing at a furious pace, costing organizations trillions globally with an expected increase to $6 trillion annually by 2021, according to DarkReading. The chance of avoiding an attempted breach is almost nonexistent, but the odds of preventing a successful breach will increase with HR's attention to areas discussed in this report.

We suggest that organizations ascertain their own risk tolerance and plan a cybersecurity strategy accordingly. Educating employees enterprise-wide, hiring right, and fostering cyber staff development are critical for HR professionals who face the growing cybercrime challenge.

This article is an excerpt from the report entitled Cyber Security: The HR Imperative for Today.

Katherine Jones is a Partner in Mercer's San Francisco office, and serves as the Products and Insights Leader of Mercer Select Intelligence.
Karen Shellenback is a Principal in Mercer's Denver office, in addition to being the Research and Insights Leader of Mercer Select Intelligence.

LIMITING CYBERATTACKS WITH A **SYSTEM WIDE** SAFE MODE

Claus Herbolzheimer

Cyberattacks cost companies an estimated half a trillion dollars in damages every year. The main reason they can harm companies to such a staggering degree is that today's cybersecurity systems use centralized monitoring, with little beyond their main firewalls to protect the rest of an organization. As a result, when companies are hacked, it can take days for information technology teams to isolate infected systems, remove malicious code, and restore business continuity. By the time they identify, assess, and resolve the incident, the malicious code has usually proliferated, almost without limit, across any connected or even tangentially related systems, giving hackers even more time to access sensitive data and to cause malfunctions.

To stay ahead of new intrusion techniques, companies need to adopt decentralized cybersecurity architectures, armed with intelligent mechanisms that will either automatically disconnect from a breached system or default to a "safe mode" that will enable them to operate at a reduced level until the effects of cyberattacks can be contained and corrected. Like the general security systems at high-risk sites such as nuclear power plants, companies require multiple layers of redundant safety mechanisms and cybernetic control systems. The goal should be to create "air pockets," with neither direct nor indirect internet connections, that can protect critical equipment and internet-connected devices.

Every company's cybersecurity program will have unique attributes, but there are several fundamentals to this decentralized architecture that can help companies shift the balance of power away from the attackers.

DETECTION

Even the most expertly designed cyber architecture is useless if it can't detect and understand the threats it faces. Companies are experiencing more cyber viral outbreaks because they often can't even detect them until it is too late. Today's cybersecurity systems have been built to detect previously identified malicious codes and malware. But cyberattacks are morphing so fast that threat patterns are unpredictable.

To identify and mitigate evolving new attack scenarios, security systems need to search for anomalies, analyze the probability that they are hostile acts, and incorporate them into a continually expanding list of possibilities. This level of detection should be carried out by components on many different levels to cover the multitude of devices and system components connected to the internet and physical environments. Together, these form several layers of cybernetic systems that can identify unknown and new forms of attacks by comparing what they understand to be their normal, uncompromised state – both on their own and in combination with other systems.

Rather than reacting to a defined set of indicators, these systems detect and react to irregularities in data flows, involving anything from the amount, type, origination, or timing of data. For example, to determine whether someone should be locked out of an online bank account, some banks' cybersecurity systems are starting to use artificially intelligent technology to compare how a person normally types or uses their computer mouse.

THE GOAL SHOULD BE TO CREATE "AIR POCKETS," WITH NEITHER DIRECT NOR INDIRECT INTERNET CONNECTIONS, THAT CAN PROTECT CRITICAL EQUIPMENT AND INTERNET-CONNECTED DEVICES.

HARM REDUCTION

The next step is to make sure that decentralized, intelligent systems minimize the impact of attacks by independently starting a protocol that takes potentially compromised systems offline, disconnects them from other critical equipment, or locks them into a safe mode. Current cybersecurity systems usually trigger an alert if they have identified a specific

attack. But they continue to operate and communicate with other systems until information technology teams shut them down and correct the malfunction.

SECURE-BY-DESIGN

Finally, all companies' products will eventually have to become secure-by-design. So far, it seems that companies pay little heed to cybersecurity during product development. That needs to change. Hackers have remotely accessed and controlled everything from network-connected electricity "smart meters" to security cameras. In 2015 Chrysler announced vehicles after a pair of cybersecurity researchers demonstrated that they could remotely hijack a Jeep's digital systems over the internet. In Germany, nearly one million homes suffered brief internet outages in 2016 after criminals gained access to and remotely shut down their internet routers. The U.S. Food and Drug Administration warns that medical devices connected to hospital networks, other medical devices and smartphones – such as implantable heart monitors – are now at risk of remote tampering that could deplete devices' batteries or result in inappropriate pacing or shocks.

Companies need to build kill switches, safe modes, and encryptions into their products during development. This will protect not only the companies' systems but also their customers'. Apple, for example, installs layers of data encryption into its products and will permit customers to run only Apple-approved software programs on their devices. Such practices need to become standard operating procedure across all industries.

CONCLUSION

Stopping cyberattacks will never be cheap or easy. Developing decentralized, intelligent cybersecurity systems will likely happen in fits and starts as devices learn through trial and error not to react to false positives or to go into safe mode more often than is necessary. Managers will have to show leadership, since most customers remain unaware of the extent that cyber risks now pose a threat to the products in their possession, and so are likely to be impatient with glitches and delays. The good news is that the technology exists to make good cybersecurity a reality. Decentralized, intelligent systems can significantly decrease the risk of cyberattacks and minimize their damage. The savings will be enormous. ♦

This article first appeared in Harvard Business Review on May 17, 2017.

Claus Herbolzheimer, based in Berlin, is a Partner in Oliver Wyman's Digital practice.

RECOGNIZING THE ROLE OF INSURANCE

Wolfram Hedrich, Gerald Wong, and Jaclyn Yeo

A key role of insurance is risk transfer. Having recognized that cyber risk cannot be eliminated; companies must be prepared for a cyberattack. The challenge with cyber risk is that it has the potential to be a tail risk to data, reputation, or the ability to do business. A 2016 study by Ponemon found that the average total cost of a breach is $4 million, up 29 percent since 2013 and persistently rising. The magnitude of a potential, sudden loss forces firms to scrutinize their ability to withstand such impact, and after rigorous analysis, part of the solution almost always involves looking to insurance as a way of transferring the risk away.

The role of cyber insurance is also useful in quantifying the price of cyber risk. Insurance premiums can serve as benchmarks to the risk modeling output and should be used as part of profitability analyses to determine the financial feasibility of a project, or executing cyber risk mitigation efforts. For instance, if a cybersecurity feature costs less than the net present value (NPV) of the resulting reduction in cyber insurance premiums, it is a worthwhile endeavor.

Prompted by the wave of high profile attacks and new data protection rules introduced around the world, annual gross written cyber insurance premiums have grown by 34 percent per annum over the last seven years, from $500 million in 2009 to $3.9 billion in 2016. Strong and long-term growth is expected in the global cyber insurance market, which is projected to reach $9 billion by 2020.

However, the cyber insurance market remains heavily skewed towards the US: Insurance take-up rate was 55 percent in the US in 2016, compared to 36 and 30 percent in the UK and Germany respectively. The take-up rate in APAC was even lower even though data is scarce. The distribution is worse for cyber insurance premiums, which was again largely dominated by the US.

The US is expected to continue dominating the global cyber insurance market over the next few years. A key driving force is the mandatory breach notification laws, the first of which was enacted in California in 2002. Today, 47 out of the 50 US states have enacted the legislation, following the basic tenets of California's original law.

Despite the proliferation of technology and cyberattacks in APAC, there lies significant opportunities for insurers here since APAC's cyber insurance market share remains negligible.

This suggests strong growth potential and significant opportunities for insurers in the region – the cybersecurity market in APAC is projected to grow over 15 percent per annum till 2019. Munich Re expects Asian market volumes for cyber covers to grow to $1.5 billion by 2020, while AIG estimates cyber insurance penetration in Singapore could increase to 40 percent in 2020 from 9 percent today.

There are key insurability challenges that need to be addressed so insurers can fully capture the growing market share, while the insured are adequately protected at fair prices.

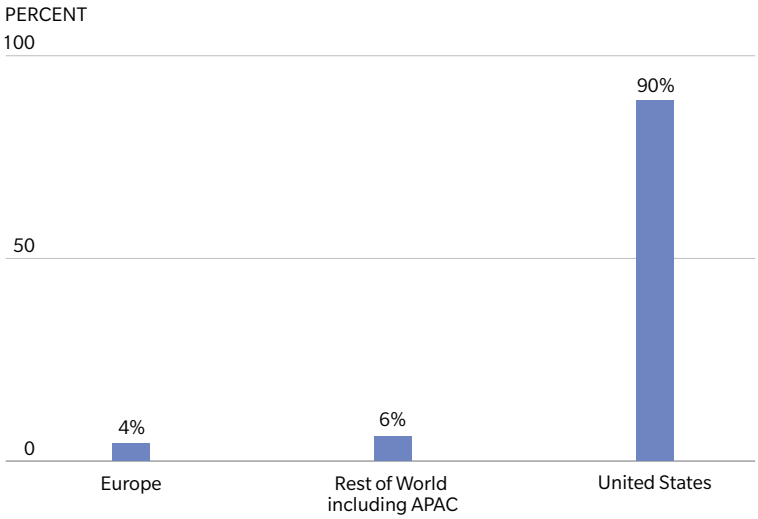
CHALLENGE #1: HIGH SPECIFICITY AND STRICT LIMITATIONS IN CYBER INSURANCE PRODUCT OFFERINGS

The scope of cyber insurance coverage remains highly specific as the characteristics of cyber threats across geographical locations, industries, and size of corporations vary widely. With little standardization across the products offered, companies need to have a deeper understanding of their own cyber risk exposures to determine the appropriate type and amount of coverage required based on their own risk tolerances. However, 49 percent of respondents surveyed by Marsh admitted that they possess "insufficient knowledge" about their own risk exposures to assess the insurances available.

Thus, even corporations with some form of cyber insurance may be unprotected against indirect losses that cannot be measured (reputational losses,

EXHIBIT 1: GLOBAL CYBER INSURANCE MARKET

2016 INSURANCE PREMIUMS
$3.9 BILLION GLOBAL FIGURES



Source: Oliver Wyman

for example), or not relevant to their risk exposure, leaving many corporations exposed to larger losses. On the other hand, cyber policy limits from a single underwriter typically range up to $100 million. Furthermore, with layered programs, a consortium of insurers and reinsurers can provide a tower of cyber insurance easily beyond $500 million in limits, which usually involve a series of insurers writing coverage each one in excess of lower limits written by other insurers.

It is imperative that companies put in place processes for proper assessment of their cyber risk exposure, as that will lead to more targeted and effective mitigation, and greater ability to judge the value of the risk transfer options available in the market.

There is no one standard policy to cover cyber risk as the characteristics of cyber threats vary widely across industries and corporation size, while the terms and coverage of policies are complicated in nature. Thus, companies need to have a deeper understanding of their own exposure as it will help determine the appropriate type and amount of coverage required based on their risk tolerances (Exhibit 2 provides an example of different loss categories deriving from cyberattacks and non-malicious IT failures).

CYBER INSURANCE IS NOT A HOLISTIC SOLUTION IN DEALING WITH CYBER EXPOSURE AND COVERS ONLY CERTAIN SPECIFIC EVENTS AND OUTCOMES.

—Douglas Ure
Practice Leader (Asia) at Marsh Risk Consulting,

EXHIBIT 2: DIFFERENT LOSS CATEGORIES AVAILABLE IN THE CYBER INSURANCE MARKET

Intellectual property(IP) theft	• Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share
Business interruption	• Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a results of cyberattacks or other non-malicious IT failures
Data and software loss	• The cost to reconstitute data or software that has been deleted corrupted
Cyber extortion	• The cost of expert handling for a extortion incident, combined with the amount of the ransom payment
Cybercrime/ cyber fraud	• The direct financial loss suffered by an organization arising form the use of computers to commit fraud or theft of money, securities or other property
Breach of privacy event	• The cost to investigate and respond to a privacy breach event, including IT forensics and notify affected data subjects • Third-party liability claims arising for the same incidents. Fines from regulators and industry associations
Network failure liabilities	• Third-party liabilities arising from certain security events occurring within the organization's IT network or passing through it in order to attack a third party
Impact of reputation	• Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event
Physical asset damage	• First-party loss due to the destruction of physical property resulting from cyberattacks
Death and bodily injury	• Third-party liability for death and bodily injuries resulting from cyberattacks
Incident investigation and response costs	• Direct losses incurred in investigating and "closing" the incident and minimizing post-incident losses. Applies to all the other categories/events

Source: Oliver Wyman

CHALLENGE #2: EVOLVING NATURE OF TECHNOLOGY AND THE INTERNET

The rapidly evolving nature of the Internet sets the speed not just for technological advancements but also severe cybercrimes with increasingly complex capabilities. Insurers need to constantly adapt to the dynamic digital landscape to improve their risk exposure models when designing more innovative cyber insurance products.

The constantly evolving nature of exposure also limits the usefulness of any historical data gathered, since they are most likely not going to be representative of future projections, hampering the development of accurate and robust models.

The low take-up rates of cyber insurance are often attributed to the mismatch of needs and offerings between the insured and the insurers. Whether it is in addressing the overpriced premium for a limited coverage, or offering products offered are better-suited and without many exclusion clauses, it is imperative for insurers to innovate and work on bridging the expectation gap.

One potential innovative product is a shared limits policy amongst firms with non-correlated risk. Marsh believes this should provide firms with access to $1 billion or more of coverage at a fraction of the cost of a stand-alone policy, sufficient to protect against a worst-case scenario. In 2016, Marsh launched Cyber ECHO, a global excess cyber risk facility underwritten by Lloyd's of London syndicates, offering up to $50 million in follow-form coverage for clients across all industries around the world.

CHALLENGE #3: EXPANDING CYBER INSURABILITY

Risk pooling has become an ineffective diversification mitigation tool in the cyber insurance landscape due to the underwhelming market share and smaller-than-required risk portfolios. Conventional strategies such as geographic or industrial diversifications also present greater challenges for cyber insurance as compared to other traditional insurance policies.

Tom Ridge, former Secretary of the US Department of Homeland Security, recently highlighted a key role for insurance-linked securities (ILS) in enabling cyber risks to be transferred to capital market investors. With growing cyber threats in terms of both systemic risks and financial impacts, the insurance industry alone may not be able to fully absorb the risk transfer.

Thus, it becomes critical for the insurance industry to innovate beyond the usual underwriting, and into the broader landscape involving capital markets, industries, and governments. This public-private partnership approach allows stacking multiple layers of both coverage and liquidity in the fight against cybercrimes.

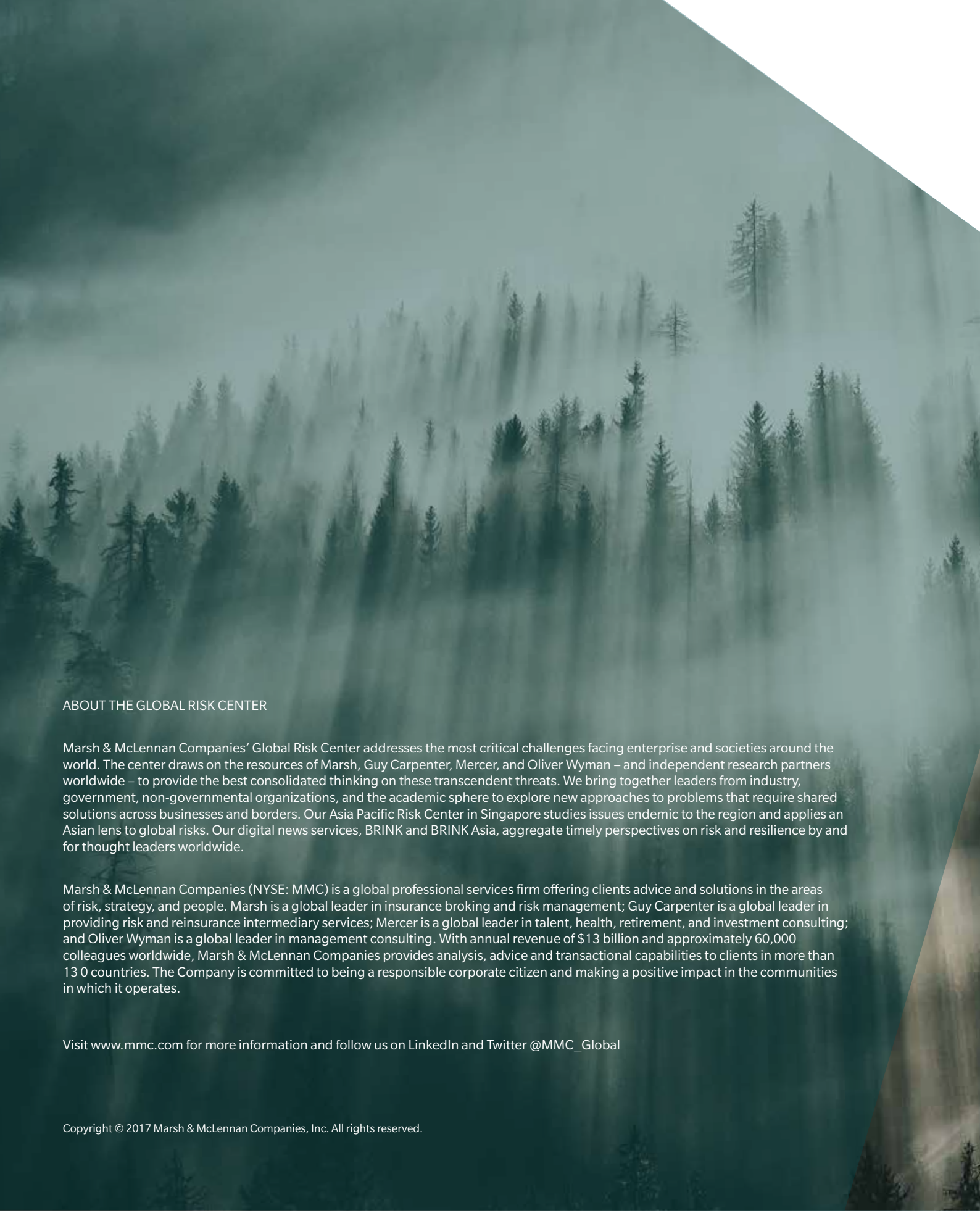
> TO MEET THE GROWING NEEDS OF OUR CUSTOMERS, GUY CARPENTER IS EXPANDING OUR EXPERTISE IN ASSESSING CYBER RISK BY WORKING CLOSELY WITH EXTERNAL EXPERTS AND INDUSTRY PLAYERS.
>
> **—Michael Owen**
> Chief Actuary at Guy Carpenter

CONCLUSION

Without a doubt, insurance has a key role to play in cyber risk management. However, organizations need to be cognizant that a cyber insurance policy is one of the many tools that form a more comprehensive cybersecurity management strategy. Business executives need to find the right balance between cybersecurity investments and securing appropriate insurance plans suitable to the unique needs of their industry or organization. ♦

This article is an excerpt from the report entitled Cyber Risk in Asia-Pacific: The Case for Greater Transparency

Wolfram Hedrich, is the Executive Director of Marsh & McLennan Companies' Asia Pacific Risk Center.
Gerald Wong is a Senior Consultant for Oliver Wyman.
Jaclyn Yeo is a Senior Research Analyst for Marsh & McLennan Companies' Asia Pacific Risk Center.



ABOUT THE GLOBAL RISK CENTER

Marsh & McLennan Companies' Global Risk Center addresses the most critical challenges facing enterprise and societies around the world. The center draws on the resources of Marsh, Guy Carpenter, Mercer, and Oliver Wyman – and independent research partners worldwide – to provide the best consolidated thinking on these transcendent threats. We bring together leaders from industry, government, non-governmental organizations, and the academic sphere to explore new approaches to problems that require shared solutions across businesses and borders. Our Asia Pacific Risk Center in Singapore studies issues endemic to the region and applies an Asian lens to global risks. Our digital news services, BRINK and BRINK Asia, aggregate timely perspectives on risk and resilience by and for thought leaders worldwide.

Marsh & McLennan Companies (NYSE: MMC) is a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. Marsh is a global leader in insurance broking and risk management; Guy Carpenter is a global leader in providing risk and reinsurance intermediary services; Mercer is a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman is a global leader in management consulting. With annual revenue of $13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies provides analysis, advice and transactional capabilities to clients in more than 13 0 countries. The Company is committed to being a responsible corporate citizen and making a positive impact in the communities in which it operates.

Visit www.mmc.com for more information and follow us on LinkedIn and Twitter @MMC_Global

MARSH & McLENNAN COMPANIES