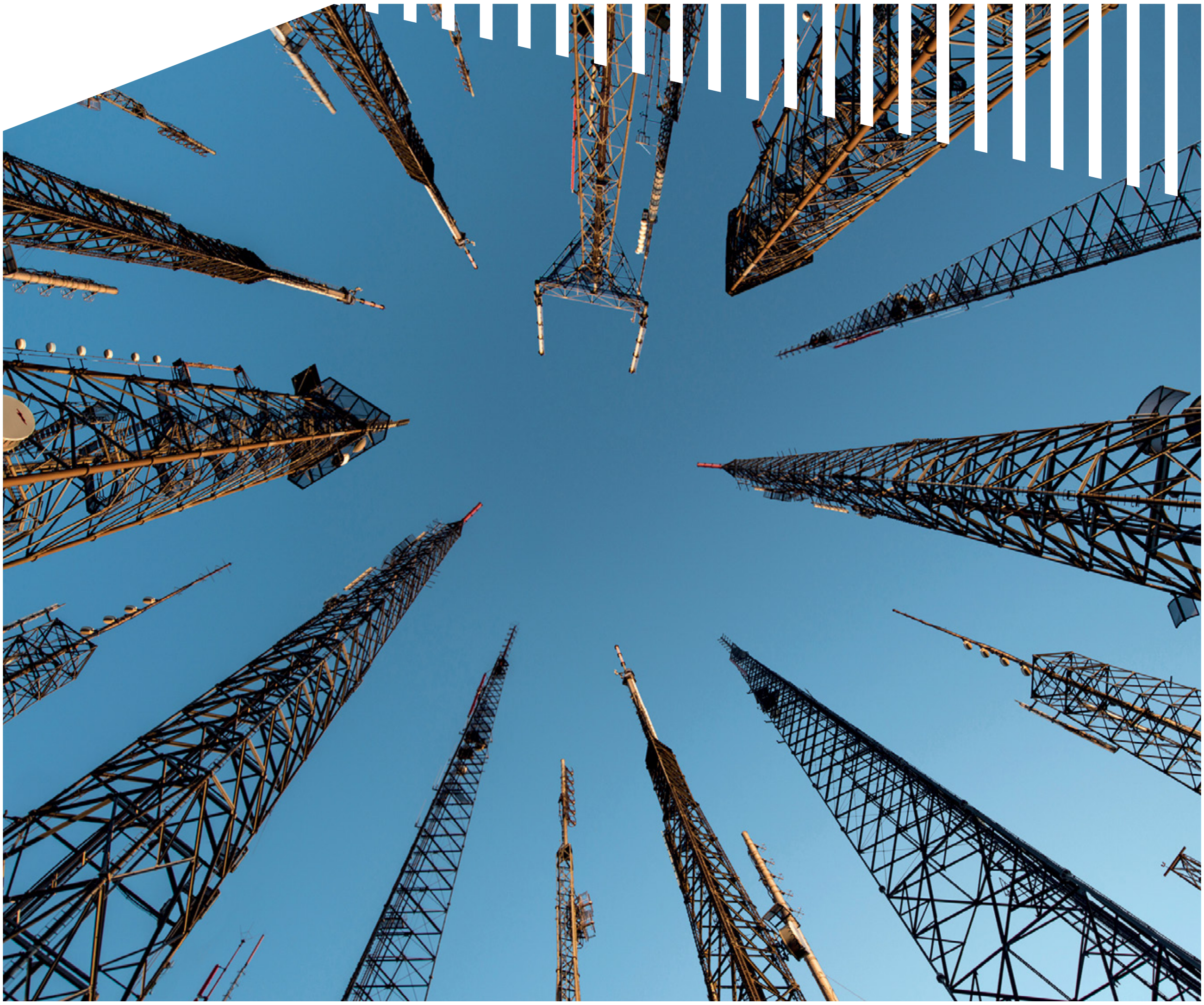
MARSH & McLENNAN COMPANIES | Global Risk Center

GETTING AHEAD IN CYBER RISK

A differentiated approach for Communications, Media and Technology providers



MARSH GUY CARPENTER MERCER OLIVER WYMAN

KEY TAKEAWAYS

1 **Companies in the Communications, Media and Technology (CMT) industry, especially in the telecommunications sector, operate across multiple technology platforms and jurisdictions, exposing them to wide-ranging cyber risks.** The industry often acts as a conduit for information and transaction flows and forms a fundamental component of other key sectors, making it a particularly attractive target.

2 **Business interruptions and reputational damage** are perceived to be the most critical cyber loss scenarios for CMT companies and their stakeholders. A cyber incident can cause significant financial losses stemming from service disruption, as well as loss of trust due to breach of customer privacy. In the case of reputational damage, on average it is much more pronounced for the CMT industry than other industries.

3 **In the face of a cyberattack, the CMT industry is perceived to incur the highest financial cost** across all surveyed industries. Among cyber threats, financially-motivated ones are the biggest concern for CMT companies. As shown by results of the latest **Marsh Microsoft Global Cyber Risk Perception Survey**, more than 80 percent of respondents from the CMT industry expect a cyber breach to cost them more than $1 million per case, as compared to a cross-industry average of 65 percent.[1]

4 **Proactive measures are needed to increase the visibility of cyber risk issues within CMT companies, and cyber risk management should be made a shared responsibility across the firm.** While the risks have been recognized by the industry, more can be done by CMT companies to establish and implement a holistic framework, encompassing cyber hygiene, governance, quantification of risks, and adequate board oversight.

5 **In the past 12 to 24 months, the CMT industry has been taking more cyber risk-related actions than other industries,** particularly in the areas of prevention and preparation. Given their high degree of interconnectivity, CMT companies are vulnerable to human-induced cyber threats and must continue to assess and manage cyber readiness around internal and external parties, including third parties.

6 **This paper highlights some examples of best practices across industries in cyber risk management,** and several key areas for CMT companies to start focusing on, such as preparedness, prevention, detection, response, and recovery, including the use of cyber risk insurance as a risk-transfer tool.

[1] Marsh & Microsoft (2018). By the Numbers: Global Cyber Risk Perception Survey.

CYBER RISK SITUATION AND PERCEPTIONS

COMMUNICATIONS, MEDIA AND TECHNOLOGY COMPANIES ARE EXPOSED TO A BROADENING RANGE OF CYBERSECURITY THREATS

CMT companies, particularly in the telecommunications sector, possess critical infrastructure and are increasingly exposed to cyber threats owing to the trend of rapid digitalization. They are becoming among the prime targets for cyberattacks as companies in this industry – including communications service providers, solutions providers and technology manufacturing firms – often act as conduits for information and transaction flows, forming fundamental components of other sectors such as healthcare, transportation, and financial services. Manufacturers also face an expanded threat landscape as their business operations often rely on information technology (IT), operational technology (OT) or a composite of both – commonly known as convergence IT/OT.[2]

Most industries run on technology, software, and communications infrastructure, and handle large volumes of personal and sensitive data while interfacing on various networks and platforms as part of their business operations. The overlapping lines of business grow more complicated each day, and the CMT industry faces a range of cyber risks and first- and third-party costs. Cybersecurity threats can be internal (for example, corruption of enterprise data), external (for example, capturing of customers' data) or state crimes that are politically-motivated. Some threat actors act for money, data or intellectual property, while others want to destruct, and the defensive measures against each are very different.

The Marsh Microsoft Global Cyber Risk Perception Survey[3] indicates that the prevalence of cyberattacks in the CMT industry is at similar levels to that of other highly targeted industries: 13.5 percent of CMT companies surveyed globally reported that they were victims of a successful cyberattack in the 12 months prior to the survey, as compared to that experienced by financial institutions (17 percent) and the public sector (15 percent). In the same survey, 58 percent of CMT respondents ranked cyber risk among the top five risks, and 9 percent listed it as the top-most risk. This is almost twice the share of those who rated cyber risk as their top concern in a similar survey conducted by Marsh in 2016.[4]

As the potential impact of cyberattacks cuts across boundaries, no country is immune. For companies in Asia-Pacific, it takes almost five times longer to detect an intrusion compared to their global counterparts.[5] Common threats such as distributed denial-of-service (DDoS) attacks and global ransomware attacks (for example, WannaCry) had a global reach, affecting large communications service providers in all regions (Exhibit 1).

Being at the center of connectivity and the forefront of innovation, CMT companies find themselves in a cyber risk-laden business landscape

[2] IT/OT is defined as the integration of information technology systems used for data-centric computing with operational technology systems used to monitor events, processes and devices in industrial operations.

[3] Marsh Microsoft (2018). By the Numbers: Global Cyber Risk Perception Survey.

[4] Marsh (2016). MMC Cyber Risk Handbook 2016. Global Cyber Risk Perception survey 2016 (UK-focused).

[5] FireEye and Marsh & McLennan Companies (2018). Cyber Evolution: En Route to Strengthening Resilience in Asia-Pacific.

Exhibit 1: Snapshot of recent attacks in the CMT industry

OCT **2016**

Thought to be the largest DDoS attack in history, the hit on **a DNS Provider** caused a massive web outage and affected millions of users from US and Europe, causing hundreds of popular websites to be taken offline for hours, bringing chaos to users and costing businesses millions in lost revenue

FEB **2017**

One of the biggest cloud companies suffered outages in their web-based storage services, affecting millions of cloud service/website users, and businesses utilizing the infrastructure globally, for approximately four hours. Economic losses to S&P 500 companies as a result are estimated at $150 million

MAY **2017**

The aggressive WannaCry ransomware infected hundreds of thousands of endpoints around the world. It targeted **unpatched Microsoft Windows machines** and the incident caused up to $8 billion in economic losses due to lost income and remediation expenses to organizations with infected or vulnerable systems

MARCH **2018**

A security researcher revealed the identity documents of around 45,000 customers, from **one of Thailand's biggest mobile network.** The 32GB data cache included 45,736 files, including scanned ID cards, driving licences and possibly passports. The National Broadcasting and Telecommunications Commission, of Thailand, has since asked Thailand's five main mobile operators to clearly outline their data protection measures

JULY **2018**

A variant of the infamous Mirai botnet was built within a span of 24 hours. The botnet brought down nearly 18,000 IoT devices of a leading global provider of smart devices and information and communications technology (ICT) infrastructure within a day

JULY **2018**

A cyber attack on Singapore's **healthcare database** stole the personal information of about 1.5 million people, including Prime Minister Lee Hsien Loong. The breach was said to be deliberate, targeted and carefully planned, likely to be carried out by a well-resourced, well-funded and highly sophisticated nation state-actor

Source: TechRadar, f5, PacktHub, Channel News Asia

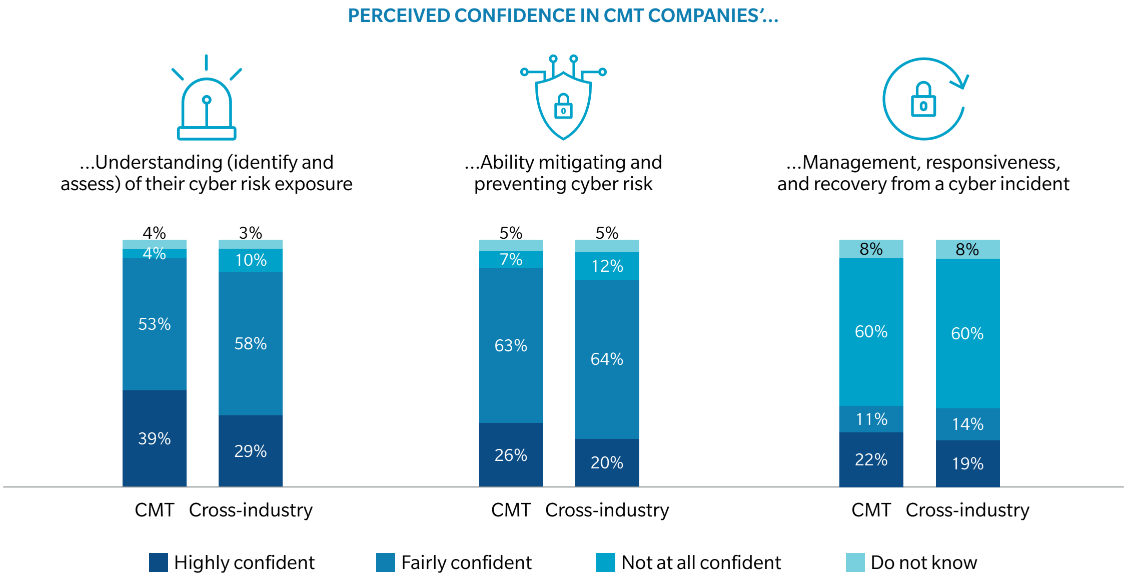
TECHNOLOGY CHANGES OUTPACING ABILITY OF CMT COMPANIES TO MANAGE, RESPOND TO, AND RECOVER FROM CYBERATTACKS

As compared to the cross-industry average, respondents from CMT companies in the Marsh Microsoft Global Cyber Risk Perception Survey are more confident of understanding and mitigating cyber risks, but are just as insecure of recovering from cyber incidents. In fact, 39 percent of survey respondents from the CMT industry are highly confident of understanding their cyber risk exposure, as opposed to the cross-industry average of 29 percent (Exhibit 2). In the event of a successful cyberattack, 60 percent of the respondents are not at all confident about managing and recovering effectively from it.

With rapid innovation and an ever-expanding world of connected devices, CMT companies, particularly communications service providers, are undergoing a transformation of their business models. While they are rapidly digitizing many of their assets, such as networks and channels, they must also respond to evolving cyber adversaries. In some cases, business models are evolving faster than companies' corresponding technical capabilities. Communications service providers are migrating from technology-focused networks towards service-focused ones, and some parts of the networks must also undergo transformation. Some providers remain reliant on legacy systems and protocols to deliver key services.[6] A large share of the infrastructure remains proprietary and is relatively isolated and protected. Infrastructure lagging in technology advancement can limit the sector's ability to deal with cyber shocks efficiently, and the current trends in network management – such as cloud-based, network function virtualization, or software-defined networks – will only increase vulnerabilities.

In addition, the technology sector is affected by a shortage of cybersecurity talent. Overall, there is a lack of qualified cybersecurity specialists who possess the required skills to lead organizations swiftly and confidently to manage cyberattacks.[7]

Exhibit 2: CMT companies' self assessed ability to understand, prevent, and manage cyber risk



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

[6] Dot Magazine (2017). Current challenges in EU Telecom security.

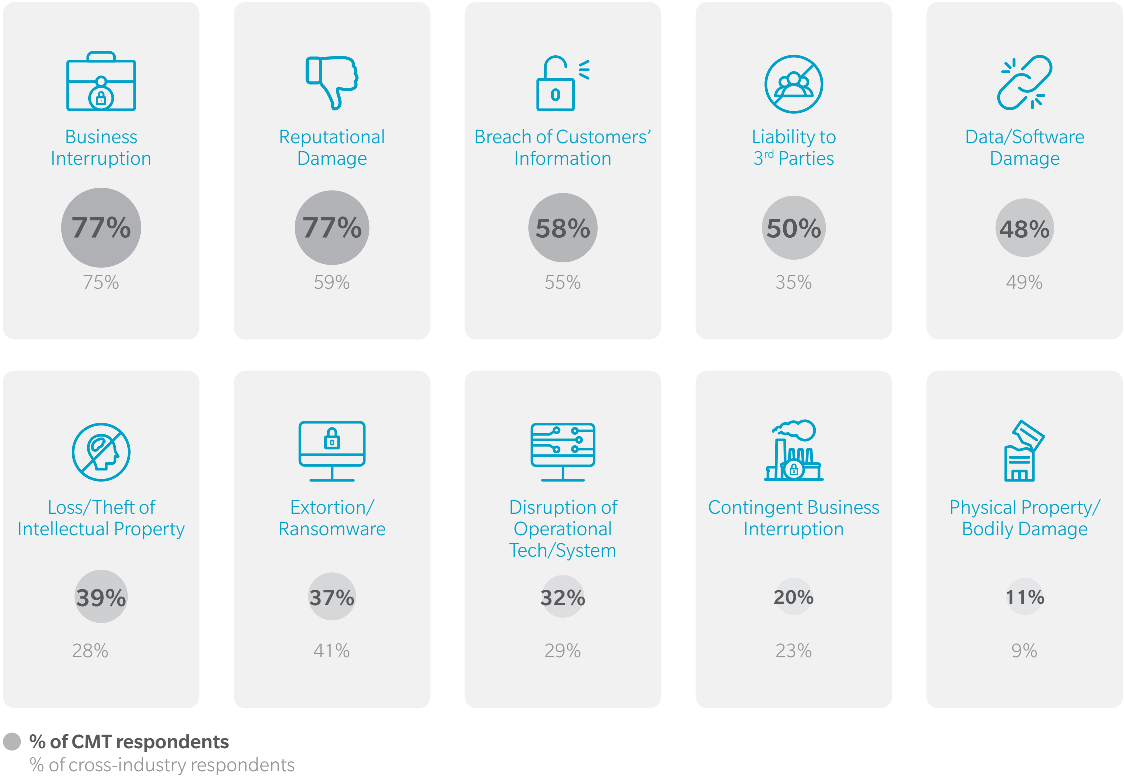
[7] Information Age (2017). Government responds to tech skills gap as employers name cyber security and coding top priorities.

BUSINESS INTERRUPTIONS AND REPUTATIONAL DAMAGE BIGGEST PERCEIVED THREATS

Participants of the Marsh Microsoft Global Cyber Risk Perception Survey were also asked about their perceptions of cyber-loss scenarios that would have the highest impact (Exhibit 3).

Business interruption was highlighted as the primary cyber risk concern in the CMT industry (77 percent), similar to other industries. Communication services companies typically have tight service level agreements and are expected to supply high performance and uninterrupted levels of service to meet customer demands.

Exhibit 3: Top cyber-loss scenarios with the largest perceived potential impact



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

Compromised connectivity or a “failure to perform” could lead to ripple effects and loss events, gravely disrupting an unlimited range of business models and stakeholders. For instance, the business of a global software technology corporation was impacted by NotPetya malware attack in 2017. The attack also disrupted the services of numerous stakeholders, particularly healthcare organizations, around the world. The financial impact due to loss in revenue from business interruption and incremental costs of restoration and remediation efforts amounted to $92 million since the attack.[8]

Even with world-class cybersecurity solutions in place, business operations remain vulnerable to cyber risk. Recently, the world’s largest maker of semiconductor and processors was severely crippled by a WannaCry variant, resulting in major business disruption and incurring additional costs. The estimated impact was up to $300 million.[9]

Reputational damage is perceived to be extremely destructive to the long-term health of the CMT industry (77 percent), while the cross-industry average is 59 percent. Particularly in the telecommunications sector, customers are likely to consider the track record of potential providers as they become more conscious of security.[10] A recently conducted focus group for a multinational telecommunications company indicated that customers have almost blind trust in incumbent providers, resulting in very low-tolerance threshold for cyber risk.

In the context of negative headlines, financial consequences are also indirectly attributed to damage in brand value and loss of trust on the part of investors and customers. The impact on a company’s bottom line can even result in securities class-action lawsuits. Apart from investors and customers, governments also consider the reputation and cybersecurity track record of companies in their consideration of potential vendors or partners. For instance, multinational telecommunications companies have been excluded from Australian federal governments’ trials and auctions of 5G (fifth-generation mobile networks) infrastructure projects, based on cyber and national security grounds.[11]

[8] Cyberscoop (2018). Nuance communications says NotPetya attack has cost it $92 million since June.

[9] Reuters (2018). TSMC says third-quarter revenue hit by computer virus.

[10] Alva Group (2015). The reputational risk of cybersecurity attacks: TalkTalk case study.

[11] Macrobusiness (2018). Why is Huawei banned.

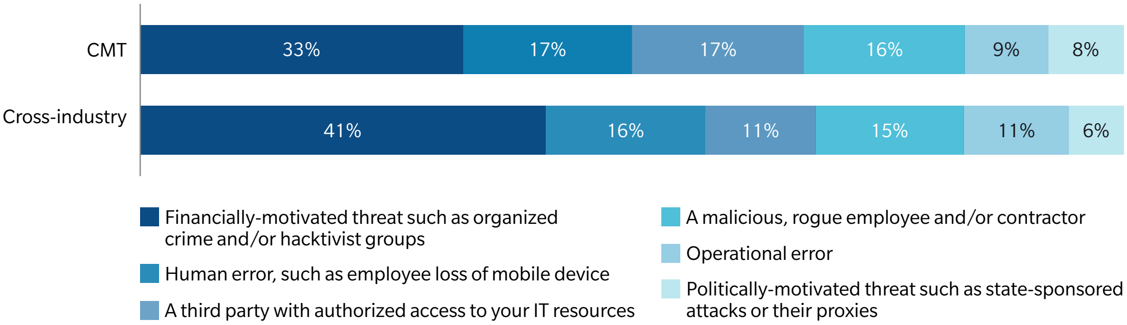
GROWTH OF CYBER THREATS ATTRIBUTED TO SEVERE FINANCIAL CONSEQUENCES AND MORE

Players in the CMT industry are most concerned about financially-motivated threat actors. A third of CMT respondents in the Marsh Microsoft Global Cyber Risk Perception Survey flagged financially-motivated threats such as organized crime or hacktivist groups as the biggest source of such threats (Exhibit 4).

According to the Verizon's 2018 Data Breach Investigation Report, the large web-based presence and technological footprint of CMT companies leave them especially vulnerable to DDoS attacks. In the case of data breaches that concern information services, threat actors are most often financially-motivated external attackers using web attacks, which make up 41 percent of the breaches.[12]

Meanwhile, human error and "rogue" employees are together regarded as the biggest threat-concern by 33 percent of respondents. Human-induced threats can be difficult to predict and anticipate – they could result from a range of factors, including but not limited to the prospect of financial gains and coercion, to deliberate data manipulation or mere carelessness – and their impact can be detrimental. For example, in February 2017, an employee of an American e-commerce and cloud computing company mistyped a command while debugging, and caused an outage that impacted many of its cloud services for approximately four hours. The estimated economic losses to S&P500 companies stood at over $150 million as a result.[13]

Exhibit 4: Threat actors that are of greatest concern with a cyberattack that delivers destructive malware



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

[12] Verizon (2017). 2017 Data breach investigation report.

[13] Wall Street Journal (2017). Amazon finds the cause of its AWS outrage: A typo.

Cyber threats by third parties, such as suppliers, are also a major blind spot and are not receiving adequate attention (only 17 percent of CMT respondents flagged this as their topmost concern). An increasing move towards Open Data and the flow of customer information across multiple parties will result in cyber incidents affecting third parties, while causing significant losses to CMT companies.[14]

While the financial threat will persist for CMT companies and their customers, it is also increasing with hacktivists harboring politically-motivated intent. In the past year, the telecommunications and media sectors have been targeted as convenient entry-points for watering-hole attacks[15] to undermine critical national infrastructure and international government systems.[16] Amid growing geopolitical tensions globally, state-sponsored cyber attackers remain a heightened threat actor that CMT stakeholders need to monitor.

Cyber threats by third parties, such as suppliers, are also a major blind spot and are not receiving adequate attention

The business of CMT companies involves huge amounts of data – some of which are theirs, but most of which are their customers' or the customers' clients'. For instance, the telecommunications sector holds a huge amount of sensitive personal information (such as banking and utilities account details), provides required infrastructure and even offers cybersecurity services themselves. In another case, a CMT company might produce a technology that exposes themselves or other CMT companies to cyber threats, who might end up identifying those exposures, such as during the case of Meltdown and Spectra.[17] Consequently, the CMT industry functions in an ecosystem where business interruption and reputational damage are key issues and it often bears the burden of the losses incurred.

According to the Ponemon Institute, the average total cost of data breaches in FY2017 was $3.6 million per company across all industries.[18] Comparing the perceived cost per cyber breach case across selected industries in the Marsh Microsoft Global Cyber Risk Perception Survey, the CMT industry has one of the largest perceived financial impacts – more than 80 percent of the CMT companies expect losses of more than $1 million per incident (Exhibit 5). These perceptions underscore the extent of possible financial damage for the CMT industry and its stakeholders. For example, in another scenario of an extreme cloud service disruption, the estimated total economic losses could go as high as $53 billion, a financial impact equivalent to a natural catastrophe such as the 2012 Superstorm Sandy.[19]

[14] Tech Crunch (2016). Large DDoS attacks cause outrages at Twitter, Spotify, and other sites.

[15] Watering-hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that the members are known to visit, with a goal of gaining access to the network at the target's place of employment.

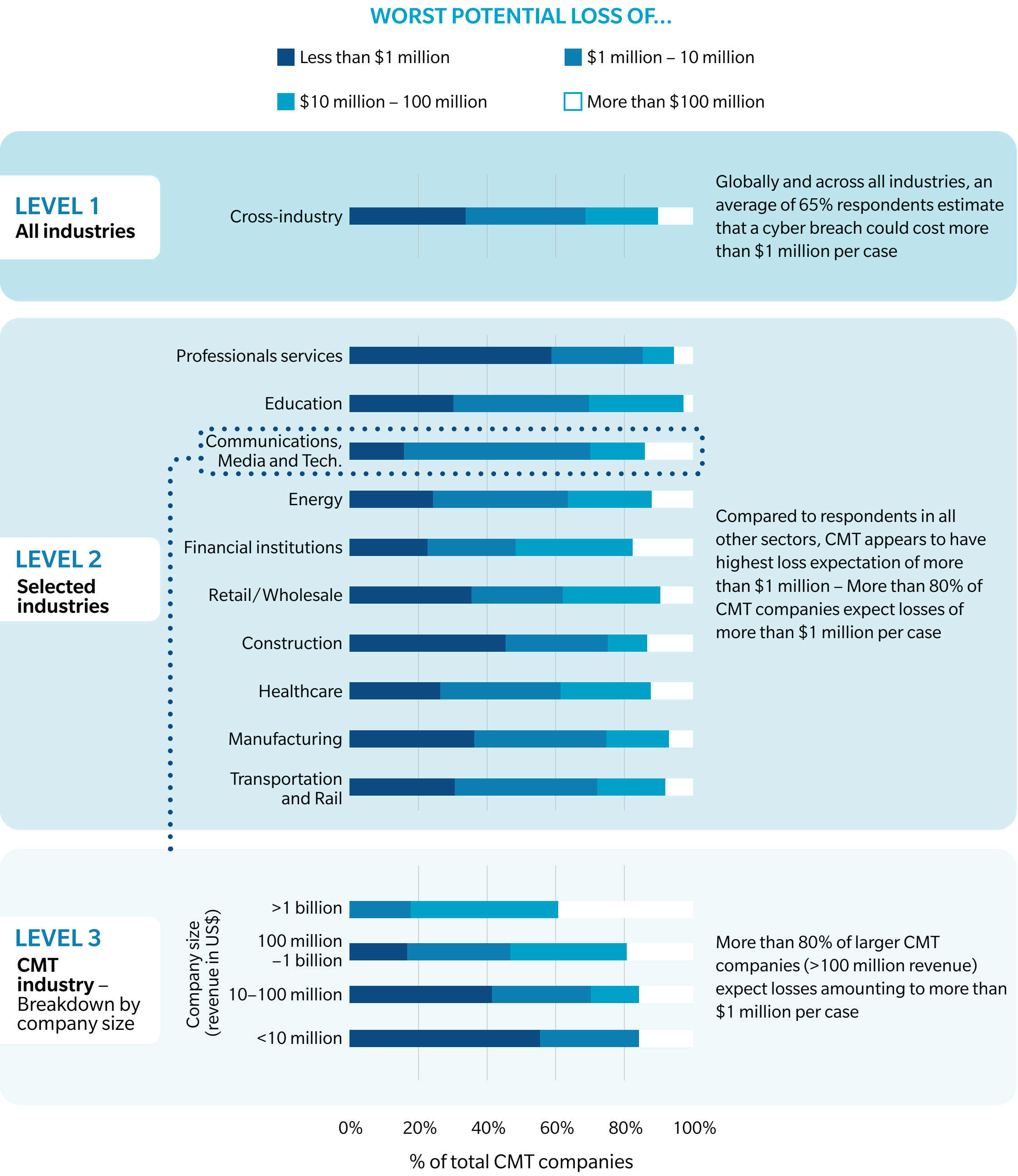
[16] The Guardian (2017). Russian hackers targeted UK media and telecoms firms, confirms spy chief.

[17] Meltdown and Spectre are two reported central processing unit (CPU) bugs that exploit critical vulnerabilities in modern processors, allowing programs to steal data which is currently processed on the computer.

[18] Ponemon Institute (2017). 2017 Cost of Data Breach Study.

[19] Lloyd's (2017). Counting the costs: Cyber risk decoded. The figures represent mean values of simulated loss year severities for large and extreme loss events, taking into account all expected direct expenses related to the events.

Exhibit 5: Estimated financial impact of each cyber incident case from a top-down analysis



Globally and across all industries, an average of 65% respondents estimate that a cyber breach could cost more than $1 million per case

Compared to respondents in all other sectors, CMT appears to have highest loss expectation of more than $1 million – More than 80% of CMT companies expect losses of more than $1 million per case

More than 80% of larger CMT companies (>100 million revenue) expect losses amounting to more than $1 million per case

Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

CHALLENGES IN EFFECTIVE CYBER RISK MANAGEMENT

OPPORTUNITY FOR CMT COMPANIES TO INCREASE RESPONSIBILITY ACROSS THE ORGANIZATION AND DEVELOP AN INTEGRATED FRAMEWORK IN CYBER RISK MANAGEMENT

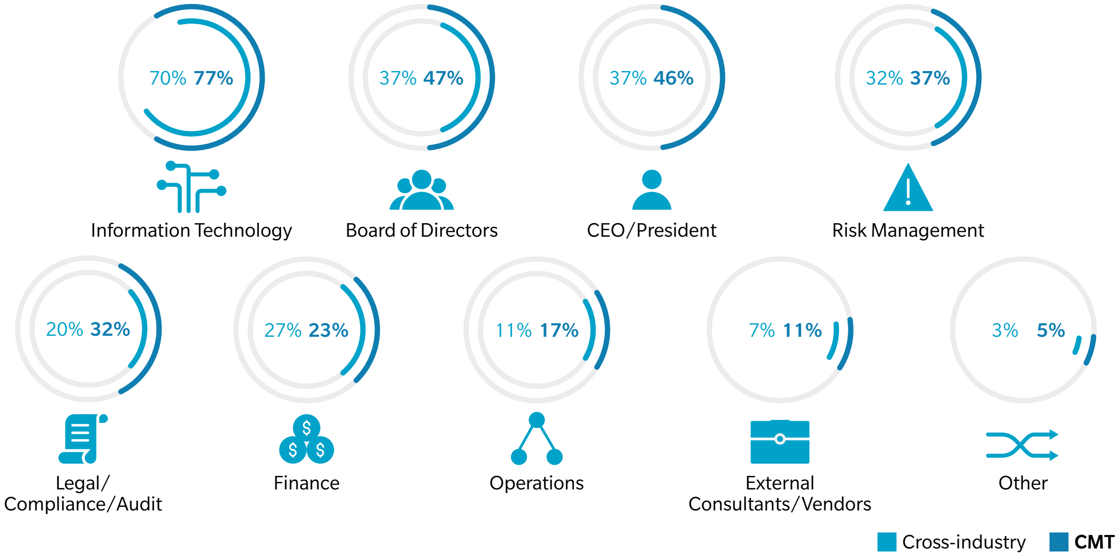
Cyber risk management in the CMT industry is still perceived to be driven by the IT department (Exhibit 6). For instance, 77 percent of CMT survey respondents indicated that responsibility for cyber risk sits mainly with IT, similar to the cross-industry average of 70 percent.

Almost half the CMT respondents believed that the primary responsibility lay with the management – that is, the Board of Directors and CEO/President (47 percent and 46 percent respectively), and only 37 percent believed the risk management team was key in this regard. It is crucial to move towards a more "risk-driven" perception by advocating the importance of embedding cyber risk management as part of an overall enterprise risk management strategy.

At the next stage, CMT companies need to complement their focus on technology with risk management (Exhibit 7).

While technology remains relevant in all stages and can contribute to breakthrough improvements – such as the use of artificial intelligence (AI) to detect cyber irregularities and the introduction of encrypted cloud computing – being "risk-driven" means making cyber risk management a top-down company-wide responsibility that distributes across departments. For instance, the risk management and senior management teams must work together with IT department to define cyber risk-related metrics within an organization's risk appetite. Board members should be attuned to and recognize such risks.

Exhibit 6: Primary owners and decision-makers for cyber risk management in the CMT industry



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

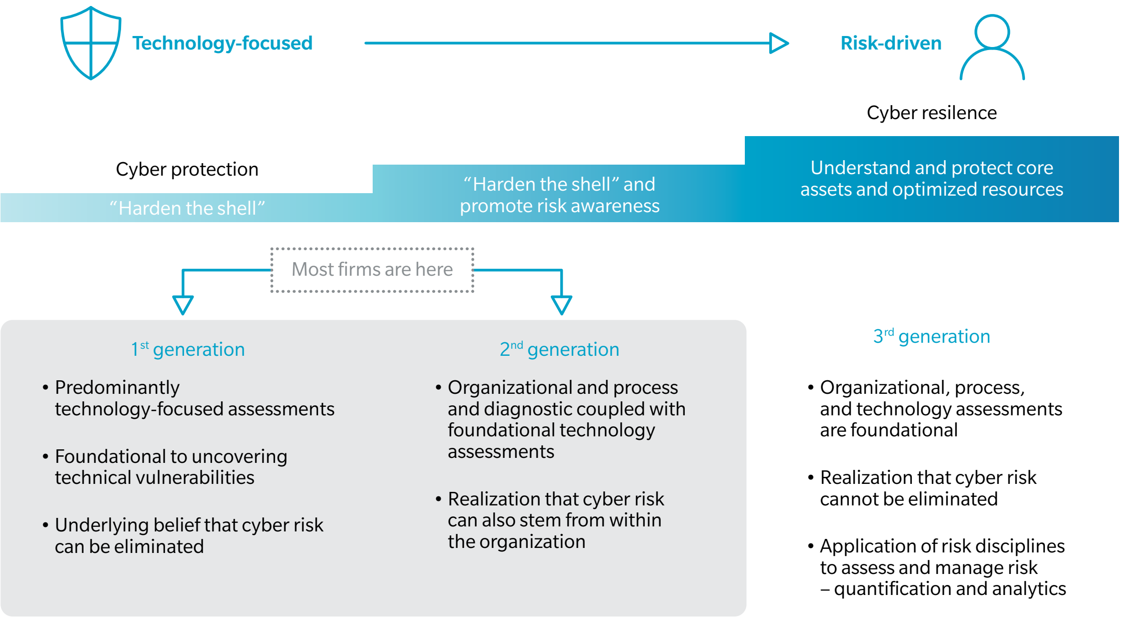
Departments such as Human Resources and Public Relations also must play an integral part in cybersecurity talent management, as well as the processes and communications involved in risk management. Given the volume and velocity of data within the CMT industry, training of all employees and not just cyber specialists around the handling of customer data and policies associated with customer data security, is key.

Many CMT companies need to distribute the responsibility of cyber risk management and shift from a cyber-protection-dominant strategy to one of risk management discipline

On the regulatory front, policy developments have an increasing impact on the CMT industry and they should be on the radar of cyber risk management. The risk of regulatory change has increased significantly and the growing attention on regulatory issues, such as cross-border access to data and the repeal of net neutrality in the US, reflect the growing responsibility placed on telecommunications companies by regulators.[20] Companies in certain jurisdictions are legally required to notify data breaches to their customers and can no longer sweep them under the carpet, while others must now play a greater self-regulatory role in the treatment of data transmissions. For instance, the Electronic Communications Code enacted by the European Commission has outlined new regulatory objectives for the telecommunications sector. It supports the EU's Digital Single Market agenda and significant investment will be required to efficiently comply with multiple, and sometimes conflicting regulations.

The GSM Association[21] has started to work on a cross-industry framework for cyber risk management. Market-specific regulations such as the EU General Data Protection Regulation, China Cybersecurity Law, Singapore Cybersecurity Act, California Consumer Privacy Act and the proposed E-Privacy Regulation will continue to make waves; and regulations around standards and compliance targets, for example, can further complicate the risk-laden operating environment.

Exhibit 7: Shift in focus for cyber risk management



1st generation

- Predominantly technology-focused assessments
- Foundational to uncovering technical vulnerabilities
- Underlying belief that cyber risk can be eliminated

2nd generation

- Organizational and process and diagnostic coupled with foundational technology assessments
- Realization that cyber risk can also stem from within the organization

3rd generation

- Organizational, process, and technology assessments are foundational
- Realization that cyber risk cannot be eliminated
- Application of risk disciplines to assess and manage risk – quantification and analytics

Source: Oliver Wyman

[20] BDO (2017). 2017 Telco Risk Factor Survey.

[21] GSM Association is an originally-European trade body that represents the interests of mobile network operators worldwide.

BOARD MEMBERS NEED MORE INFORMATION ON CYBER RISK MANAGEMENT TO DRIVE MORE PROACTIVE MEASURES

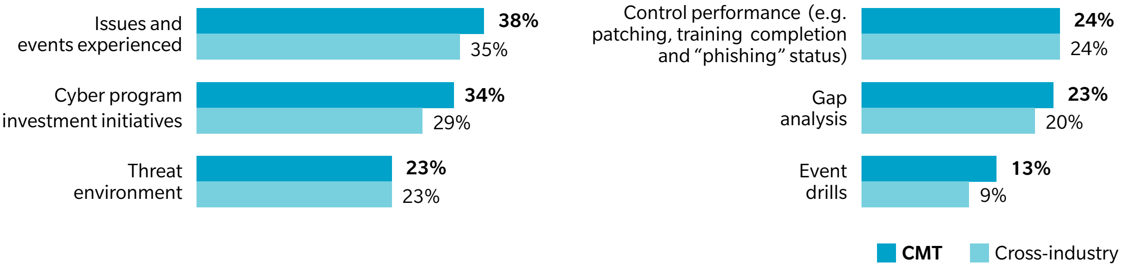
Cyber risk deserves greater visibility on the board agenda – only 38 percent of surveyed CMT companies include cyber risk-related issues in regular reporting (Exhibit 8). Not surprisingly, there is also an apparent lack of gap analysis and event drills conducted across all industries.

Board members need an upfront cyber program strategy and gap assessment to fully understand the context of ongoing event updates and investment initiatives. Director-level cyber experts are often hard to come by and most boards have only one individual serving as the "tech" or "cyber" person. This dearth of talent challenges corporate boards from having sufficient oversight of cyber issues.[22] Participation in event drills is necessary for board members to better understand how their firms are prepared from ground-up to respond to a cyberattack. A lack of familiarity with cyber risk can expose directors to shareholder litigation and regulatory scrutiny.[23] The board does not need to be "tech-savvy" to play an effective role in cybersecurity oversight, but it is critical for it to receive adequate reporting[24] and be acutely aware of key cyber risks to confidently acknowledge, avoid or mitigate them.

"Cyber" can be a catch-all phrase with little meaning – CMT companies need to dig deeper, know specifically which are the most critical scenarios and develop a business model that encourages shared dialogue in a common language among the board, executive management, IT, and operations to catalyze a cross-functional approach to cyber risk governance and reporting.

The results of the Marsh Microsoft Global Cyber Risk Perception Survey show that the CMT industry has taken more actions on average than other industries in the past two years to prevent and prepare for cyberattacks (Exhibit 9). For example, 64 percent of CMT respondents – as opposed to 54 percent of respondents across industries – indicated that they are providing phishing awareness training for employees to engage internal stakeholders in being cyber vigilant. Phishing attacks have been increasingly prevalent in the CMT industry, because they employ deception and leverage weaknesses in human nature (such as fear and greed), which no technology solution can fully guard against.[25]

Exhibit 8: Cyber risk reporting received by Board of Directors of CMT companies



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

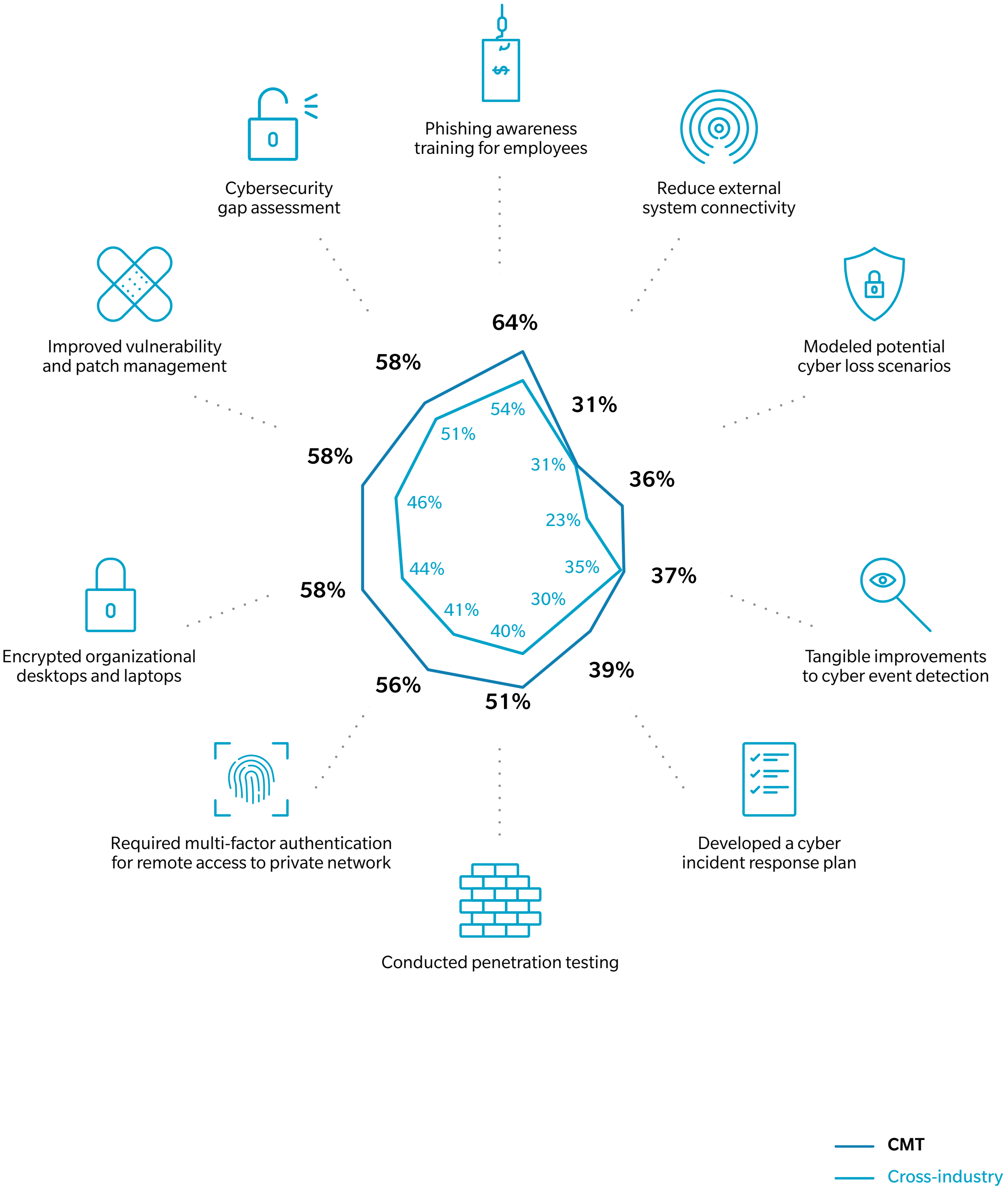
[22] Marsh & McLennan Companies' Global Risk Center & Women Corporate Directors (2018). Cyber Risk Management Response and Recovery.

[23] Marsh (2017). Cybersecurity: Considerations for Directors and Officers.

[24] BRINK (2018). How to stay ahead of cyber breaches, the boardroom's biggest fear.

[25] Infosec Institute. Phishing Attacks in the Telecommunications Industry.

Exhibit 9: Top 10 cyber risk-related actions taken by CMT companies in the past 12-24 months



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

Similarly, the increasingly complex business models of CMT companies comprising multiple third-party suppliers and vendors with access to organizations' internal data, also underscore the industry's vulnerability to human-induced threats. Between 2016 and 2017, there was a two-fold increase in indirect attacks originating from weak links in the supply chain.[26] Given their links to companies in other industries, CMT companies must evaluate and assess the cyber readiness of third parties as part of their selection criteria for a key vendor or partner. The telecommunications sector has already embarked on various strategic initiatives to improve cybersecurity (Exhibit 10).

However, most CMT companies still put more emphasis on prevention or preparedness, and do not focus sufficiently on detection and response.

As illustrated in Exhibit 9, while some proactive measures are being taken to reduce cyber risk, they are largely centered on basic preparation and prevention, such as phishing awareness employee training, cybersecurity gap assessment, improved vulnerability and patch management, and encryption of company computers. Yet, only slightly more than a third of the respondents have a cyber incident response plan in place (39 percent) or have invested in improving cyber event detection (37 percent). Even with awareness trainings, the lack of emphasis on detection and response measures is likely to contribute to CMT respondents' poor confidence in responding to a potential cyber threat.

Exhibit 10: Cybersecurity initiatives taken by communications service providers/telecommunications companies

Cybersecurity tools and capabilities – Telcommunications companies are increasingly employing smart tools like AI/Machine Learning technologies to aid security incident detection in the fast-changing cyber environment

Cybersecurity insurance is being purchased by telcommunications companies to help mitigate the financial losses of cyberattacks where high-profile breaches reportedly recovered tens of millions of dollars

Internal cybersecurity governance has been stepped up by telcommunications companies through the appointment of CISOs and increased levels of Board of Directors' oversight in overall information security strategy

National and internal cybersecurity policies and standards are being adopted more closely into telcommunications companies' cyber risk management technologies, processes and personnel skills

External collaborations with the private sector and government facilitates cybersecurity research and sharing of best practices among industry practitioners to raise overall cybersecurity standards

Source: New releases, Telcommunication companies' websites, Oliver Wyman analysis

[26] Financial Times (2018). Latest hack attacks come through the clouds.

THE MEASUREMENT OF CYBER RISK HAS BEEN LARGELY QUALITATIVE, NOT QUANTITATIVE

68 percent of CMT respondents said their organizations measure their cyber risk exposure, but a significant proportion do so using qualitative methods (Exhibit 11a). 41 percent of CMT companies do so with basic categories on the exposure scale or "maturity levels" to benchmark against their peers; and only a handful of those that measure cyber risk conduct economic quantification such as value-at-risk modeling (15 percent) and numerical rankings (19 percent of those who measure) within a fixed framework (Exhibit 11b).

In response to increased security threats and expected high financial impact, some CMT companies, particularly in the telecommunications sector, are allocating additional resources to strengthen the security of their systems, data and teams.[27] While this is a positive development, there is an ongoing need to better understand the magnitude of cyber risks as part of their overall risk profile, through quantifying the cyber risks and their potential impacts. Greater awareness can be created through quantified economic measures, which can establish a key common language in communicating with stakeholders and catalyze actions to mitigate cyber risk.[28]

Another strategy for CMT companies to adopt is "damage control", such as wording contracts in a way to minimize responsibility in the event of a cyber hack unless it is gross negligence. While this does not eliminate cyber risks, it can limit the company's exposure.

Exhibit 11a: Current state of cyber risk measurement in the CMT industry

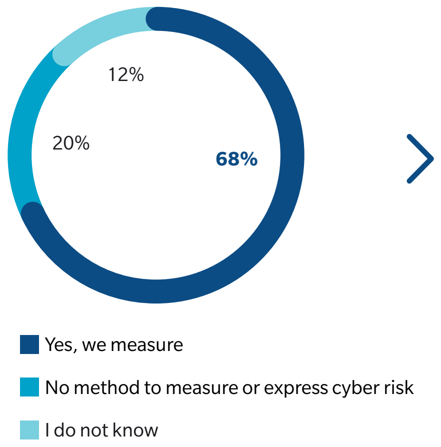
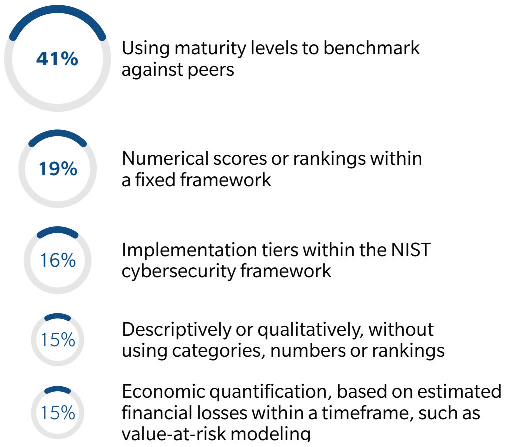


Exhibit 11b: Methods used to measure cyber risk exposure (among CMT companies that do measure cyber risk)



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

[27] DO (2017). 2017 Telecommunications Risk Factor Survey.

[28] Oliver Wyman and Marsh & McLennan Companies' Asia Pacific Risk Center (2017). Cyber Risk in Asia-Pacific: The Case for Greater Transparency.

WHAT’S NEXT: MANAGING THE EVOLVING CYBER RISKS

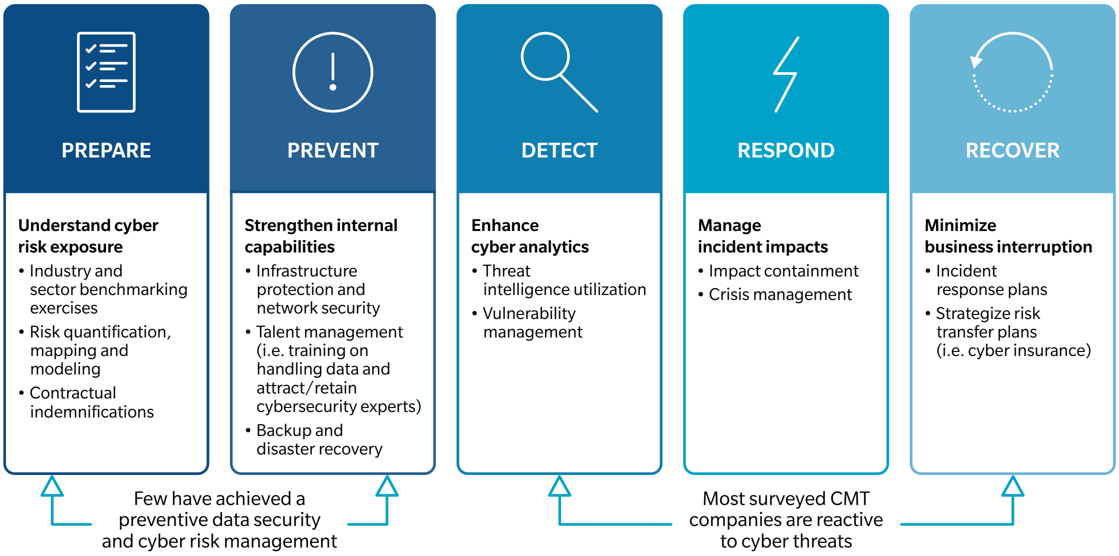
HOLISTIC APPROACH IN MANAGING DATA BREACHES AND CYBER RISK

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

PREPARE AND PREVENT: RISK DIAGNOSTICS, EDUCATION AND STRENGTHENING OF NETWORK SECURITY

A strong internal risk diagnostic is required to assess a company’s cyber risk vis-à-vis industry peers through available benchmarking tools. As shown in Exhibit 9, 42 percent of CMT companies have not conducted a cybersecurity gap assessment in the past two years, suggesting that there is room for improvement in understanding and managing their overall risk exposure.

Exhibit 12: Five key functions of the cybersecurity framework and recommended actions



PREPARE

Understand cyber risk exposure
- Industry and sector benchmarking exercises
- Risk quantification, mapping and modeling
- Contractual indemnifications

PREVENT

Strengthen internal capabilities
- Infrastructure protection and network security
- Talent management (i.e. training on handling data and attract/retain cybersecurity experts)
- Backup and disaster recovery

DETECT

Enhance cyber analytics
- Threat intelligence utilization
- Vulnerability management

RESPOND

Manage incident impacts
- Impact containment
- Crisis management

RECOVER

Minimize business interruption
- Incident response plans
- Strategize risk transfer plans (i.e. cyber insurance)

Few have achieved a preventive data security and cyber risk management

Most surveyed CMT companies are reactive to cyber threats

Source: Oliver Wyman

For CMT companies, the risks of a technology failure are more than data breaches and cyberattacks as they can manifest in various types of losses. The CMT industry understands the complexity of and connections among the risks, and most CMT companies purchase a Cyber/Tech Errors and Omission (E&O) policy to manage and transfer these risks.[29] CMT companies need to identify, define and map the specific cyber threats to their tangible and intangible assets.

Educate workforce and build a cyber-secure culture to combat increasingly complex and frequent cyberattacks. The need to shift from an IT-driven cyber protection strategy to a mature risk management discipline includes creating a more cyber-savvy workforce and strengthening the culture of cybersecurity (such as data privacy, information security, cyber awareness, and accountability). In 2017 alone, for instance, human error was found to increase cloud-related cyberattacks by 424 percent globally, and inadvertent activity such as misconfigured cloud infrastructure was responsible for almost three out of four compromised records.[30] CMT companies must continue to prioritize training for employees as it has been proven that effective cyber resilience has its roots in organization culture.

The expansion of the cybersecurity program should be a priority given the proliferation of the Internet of Things (IoT) and mobile devices with access to corporate networks, and increasing digitalization of physical networks in the CMT industry. Companies should emphasize proven cybersecurity hygiene practices which are missing for almost half of the CMT companies at present. For instance, companies should secure by design – device safe modes and encryptions into their digital assets during development.[31] As shown in Exhibit 9, CMT respondents to our survey admit to not having hardware encryption (42 percent) and multi-factor authentication for corporate networks (44 percent). Furthermore, only 58 percent of the CMT respondents improved vulnerability and patch management in the past year. This is worrying as some major cyberattacks, such as WannaCry and NotPetya, relied on vulnerabilities that could have been remedied through software patches.

Holistic cybersecurity is an integral part of the digital transformation journey

DETECT, RESPOND, AND RECOVER: CYBER-EMBEDDED RISK MANAGEMENT PLAN, DATA RESILIENCE, AND TRANSFER OF RISK

Embed cyber in enterprise risk management plans, even though it is not a commonly accepted practice yet.[32] Globally, IT departments are the primary owners and decision-makers for cyber risk management across the CMT industry (Exhibit 6). Often, cyber risk appears as an add-on, not part of a holistic risk management which presently segments risks into financial, strategic, and/or operational. In taking a more proactive approach to enhance cybersecurity, companies are encouraged to better understand the return on risk, through quantification, and to build in-house capabilities across multiple interconnected functional areas aligned with their cyber strategy.

Underpinning advanced data resilience frameworks is a strong detection mechanism and part of a holistic incident response plan. Almost two-thirds of CMT companies have not developed cyber incident response plans yet.[33] Most alarmingly, 32 percent of CMT respondents claim that their companies lack the expertise to develop one, while only 33 percent are confident that their organization's cybersecurity measures and firewalls are adequate (Exhibit 13).

Transfer risk with cyber insurance as a tool to manage exposure. Key risks that CMT companies face today include integrated risk, alternative risk capital, parametric risk solutions, commercial cyber risks and captives[34] (See "In Focus").

[29] Marsh (2018). Communications, Media, and Technology Risk Study.

[30] Tech 2, (2018). Human error caused by cloud-related cyberattacks to increase by 424 percent in 2017: IBM.

[31] Marsh & McLennan Companies (2018). Cyber Handbook 2018.

[32] Marsh & McLennan Companies' Asia Pacific Risk Center (2017). Risk in Asia: Ramifications for Real Estate and Hospitality 2017.

[33] Marsh Microsoft (2018). By the Numbers: Global Cyber Risk Perception Survey.

[34] Marsh (2018). Communications, Media, and Technology Risk Study.

Given their large capital bases and the need to protect massive research and development (R&D) investment, CMT companies must identify a range of alternative solutions to carefully manage these risks. Though the CMT industry tends to have an above-average ability to retain losses, companies must be cognizant about their increasing exposure to limit financial losses.

According to Marsh Global Analytics, CMT companies can bear an average of 44 percent more risk than comparable companies in other industries. Similarly, their working capital as a percentage of revenue is 75 percent greater than firms in other industries.[35] However, these deep reserves are vital for CMT companies to respond to technology disruption, fund growth and spur innovation, rather than to pay off losses. Increasingly, CMT companies are recognizing the value of cyber insurance and are getting more involved in negotiating for and building of effective cyber policies that cover operational technological risks.

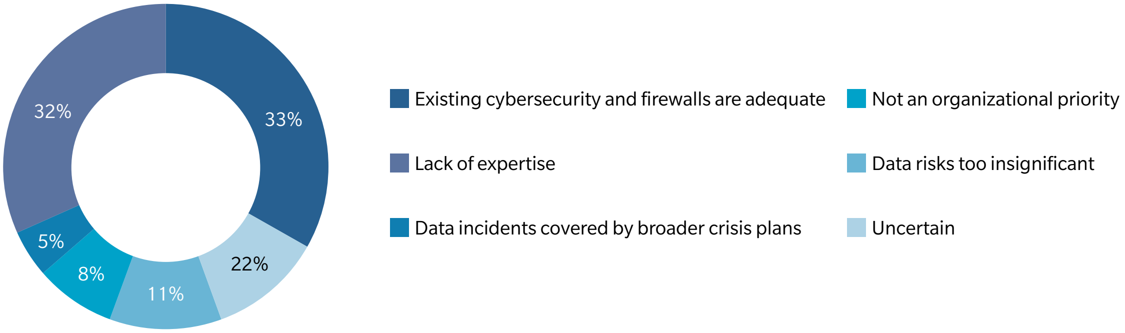
Across all industries, prompted by the wave of high-profile attacks and new data protection legislations, annual gross written cyber insurance premiums have grown by 34 percent annually over the past seven years.[36]

A recent example was Marsh's placement of the largest cyber insurance policy ($100 million in limit) in Asia for a multinational electronics company.

The European Union Agency for Network and Information Security has also found a positive correlation between cyber insurance take-up and the level of preparedness,[37] but there is still an apparent coverage gap.[38] While just over one-third of the CMT respondents' companies (38 percent) have cyber insurance coverage (Exhibit 14a), the number is slightly more than the cross-industry average of 34 percent, but lower than it is for financial institutions (52 percent) and healthcare organizations (49 percent).[39] While the CMT, financial services, and healthcare industries suffer the greatest financial impact, CMT companies tend to not undertake as much cyber insurance coverage. However, it is important to note that the numbers shown in Exhibit 14a might not flag out CMT companies' cyber coverage under Tech E&O insurance policies. In addition, 28 percent of CMT respondents do not know whether their companies have purchased cyber insurance.

Among those respondents who plan to purchase or increase cyber coverage, more than half are driven internally, with 39 percent citing cyber risk management plan and 28 percent citing board mandate as main drivers.

Exhibit 13: Reasons for not having a cyber incident response plan



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

[35] Marsh (2018). Communications, Media, and Technology Risk Study.

[36] Marsh & McLennan Companies (2018). Cyber Handbook 2018.

[37] Marsh & McLennan Companies & OECD (2018). Unleashing the Potential of the Cyber Insurance Market: Conference Outcomes.

[38] Lloyd's (2017). Counting the costs: Cyber risk decoded.

[39] Marsh Microsoft (2018). By the Numbers: Global Cyber Risk Perception Survey.

For those that do not have cyber insurance in place, 25 percent indicate that the current offerings do not provide enough coverage to cover for the cost (Exhibit 14b). While cyber insurance policies vary with respect to coverage for costs of notification, compensation to third-parties, or lost revenue, it is critical for CMT companies to understand the available tools and limit structure that best suit their financial conditions and risk tolerance.[40] In other cases, third-party liability may also be limited by CMT companies' tight service level agreements. Recent cyber claims scenarios, which a notable cyber insurer has paid for, can move CMT companies to re-evaluate their understanding or status of cyber insurance coverage[41]:

- **A cloud service provider** was alleged to have infringed on the Digital Millennium Copyright Act and knowingly permitted unauthorized publication. Statutory damages for willful infringement could have been more than $1 billion, but a pre-suit settlement was reached and total payout was $3 million
- **An information services company** was a victim of a DDoS attack, which brought their systems down, disrupted its business and halted operations. Costs incurred were due to the retention of a forensics firm and privacy counsel. In addition, potential reduction in business income was covered and the total payout was $100,000
- **A computer network services company** had the email accounts of two finance employees hacked. Privacy counsel was engaged, and appropriate notification and credit monitoring was provided. Under the Data Breach Response and Crisis Management Coverage Insuring Agreement, coverage was provided and the approximate payout was $220,000

| **IN**FOCUS |

KEY RISK TRANSFERS DEFINED

Integrated risk management is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision-making and performance through an integrated view of how well an organization manages its unique set of risks.

Alternative risk transfer allows companies to purchase coverage and transfer risk without having to use traditional commercial insurance. The alternative risk transfer market includes risk retention groups as well as insurance pools and captive insurers.

Parametric risk solutions are a type of insurance that covers the probability of a predefined event happening instead of indemnifying actual loss incurred. It is an agreement to make a payment upon the occurrence of a triggering event, and as such, is detached from an underlying physical asset or piece of infrastructure.

Commercial cyber risks coverage is a broad and competitively priced risk transfer option that has evolved from a predominantly 3rd party liability coverage to the inclusion of critical 1st party coverage. Losses can stem from business interruption, rectification of digital assets, IT forensics, ransomware and more.

A captive insurer is generally defined as an insurance company that is wholly owned and controlled by its insured. Its primary purpose is to insure the risks of its owners, and its insured benefit from the captive insurer's underwriting profits.

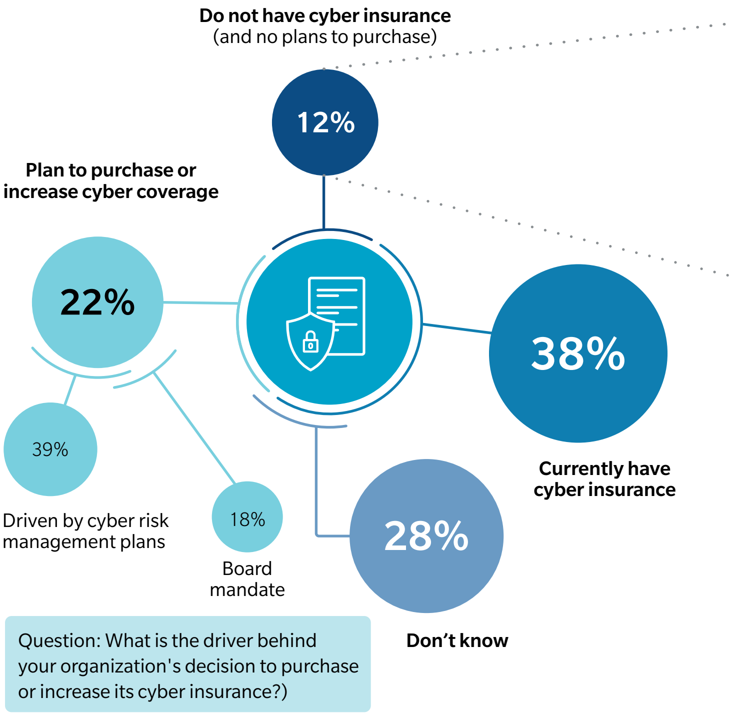
Source: Marsh, Gartner, Investopedia, Swiss Re and Captive

[40] Federal Trade Commission (2017). Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?

[41] XL Catlin (2018). Cyberattacks: claims scenarios ripped from today's headlines.

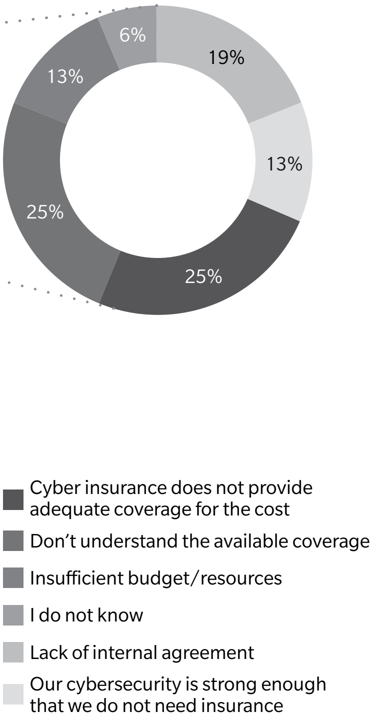
The dearth of understanding around available coverage and the lack of an internal agreement on the need for cyber insurance are also major impediments (with 44 percent of respondents citing them as reasons) to cyber insurance penetration in the CMT industry. However, it must be recognized that cyber insurance is intended to serve as a backstop to a robust cybersecurity strategy and ongoing risk management and not as a solution on its own.

Exhibit 14a: Current state of cyber risk insurance in the CMT industry


Do not have cyber insurance
(and no plans to purchase)
12%
Plan to purchase or increase cyber coverage
22%
39%
Driven by cyber risk management plans
18%
Board mandate
38%
Currently have cyber insurance
28%
Don't know

Question: What is the driver behind your organization's decision to purchase or increase its cyber insurance?)

Exhibit 14b: Reasons for not having cyber insurance



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

INCREASING GLOBAL CONNECTIVITY WILL SHAKE UP THE CMT INDUSTRY

Advancing in the current era of the Fourth Industrial Revolution (4IR), the unprecedented pace of digital transformation will drive the CMT industry to develop more expertise in emerging technologies such as AI, blockchain, or IoT in one way or another. In the next three to five years, massive rise of digital data and IoT are expected to be a major growth opportunity for the CMT industry. By 2030, there will be an estimated 30 billion devices connected to the IoT.[42] The ubiquity of cyber risks in societies will be reinforced by the growth of IoT, and the CMT industry will be at the center of the creation and mainstream use of emerging technologies. The associated and evolving cyber risks, such as the increasing prevalence of Botnet DDoS attacks on IoT devices, will pose significant threats to the development of 4IR. It is likely that CMT companies will be forced to accept more liabilities in the event of failures.

Another enabler of emerging technologies and an infrastructure opportunity for the CMT industry – particularly communications service providers – is 5G spectrum capacity. This will be a game-changer in the next five to ten years[43] and is expected to be commercially available by 2020.[44]

As demand in fixed-line and mobile broadband grows exponentially, it will drive media consumption, infiltrate the entire value chain, and support the dense deployment of sensors and other network-connected devices. For example, ultra-reliable low-latency networks, an upcoming concept in 5G, will empower autonomous systems such as connected cars and futuristic services based on virtual or augmented reality of healthcare solutions. This will not only further integrate sectors and complement the proliferation of internet-enabled devices and cloud computing, but also particularly expose CMT companies to supply-chain cyber risk.

Every company wants to be the next generation technology leader, and it will be a high-speed race in an environment of rapidly evolving uncertainties for the CMT industry. Expanding and shifting exposure will challenge CMT companies to manage cybersecurity and keep data secure. These companies must carefully consider the network-security architecture needed to achieve the right balance between security and flexibility of use to address technology challenges.[45] Only with a stronger position in cyber risk management, and with cyber embedded into their business cases, CMT companies can potentially differentiate themselves and bring greater value to their customers and clients.

[42] BRINK (2018). Risk and Opportunity of the Internet of Things.

[43] Oliver Wyman (2017). On the technical future of the telecommunications industry.

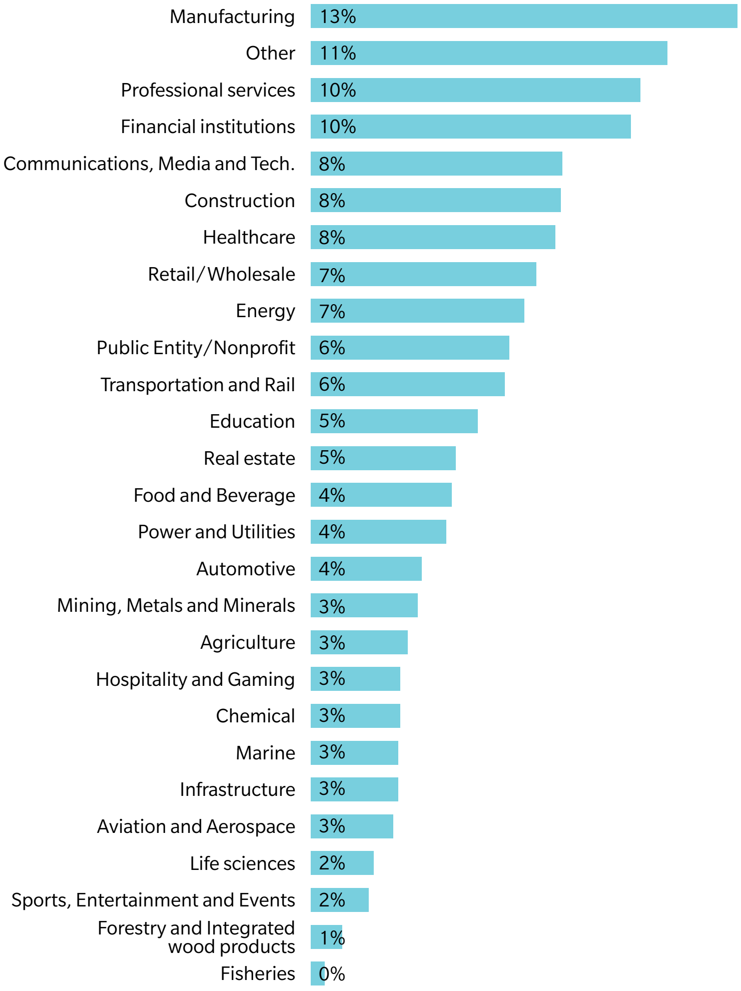
[44] BDO (2017). 2017 Telecommunications Risk Factor Survey.

[45] Ericsson (2017). 5G security—scenarios and solutions.

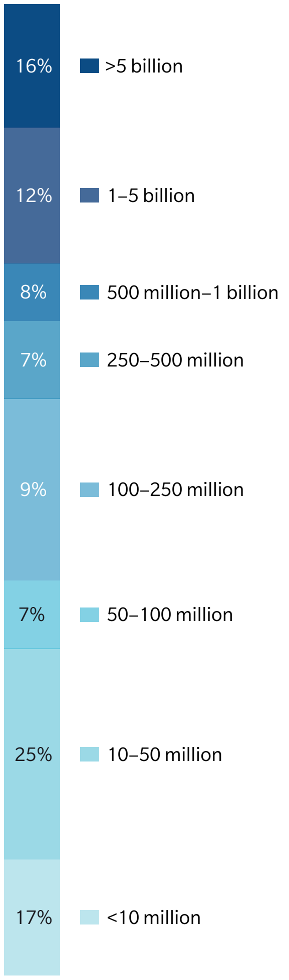
ABOUT THE MARSH MICROSOFT GLOBAL CYBER RISK PERCEPTION SURVEY

This paper is based on findings from the Marsh Microsoft Global Cyber Risk Perception Survey administered between July and August 2017. Overall, more than 1,300 senior executives participated in the survey, representing a wide range of industries and key functions, including information technology, risk management, finance, legal/compliance, senior management and boards of directors. Of the 1,312 respondents surveyed in all, 104 (8 percent) are from the CMT industry with businesses across various regions, and having at least $10 million in annual revenue.

Industry breakdown of all survey respondents (N=1,312)



Surveyed CMT organizations' annual revenue in $ (N=104)



ACKNOWLEDGEMENTS

To read the digital version of this report, please visit here.

SPONSORS

UWE LAMBRETTE

Partner; Digital, Technologies & Analytics Practice
Oliver Wyman

TOM QUIGLEY

US Practice Leader; Communications, Media & Technology Practice
Marsh

AUTHORS

SAAHIL MALIK

Principal; Consumer, Industrial & Services Practice and Digital, Technologies & Analytics Practice
Oliver Wyman

LESLIE CHACKO

Director
Marsh & McLennan Companies' Global Risk Center

NAUREEN RASUL

Cyber Leader, Asia Region
Marsh

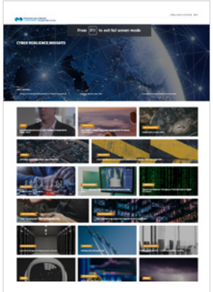
RACHEL LAM

Research Analyst
Marsh & McLennan Companies’ Asia Pacific Risk Center

MARSH & MCLENNAN COMPANIES CONTRIBUTORS

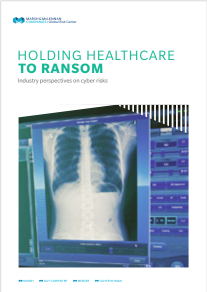
Marsh: Kevin Richards, Thomas Reagan, David Finz, Florence Levy, Alexander Chao, Lynne Burns, Michael Connolly, Linden Reko
Oliver Wyman: Paul Mee, Claus Herbolzheimer, Javier Pedro Gonzalez Pinal, Augusto Baena Reig, Mohssen Toumi, Jayant Raman
Marsh & McLennan Companies’ Asia Pacific Risk Center: Wolfram Hedrich, Jaclyn Yeo

RECENT PUBLICATIONS



MMC CYBER INSIGHTS MICROSITE

An evolving microsite with intellectual capital from Marsh & McLennan Companies and cyber partners. The site includes thought leadership on identified trending themes such as cyber, workforce of the future, and more

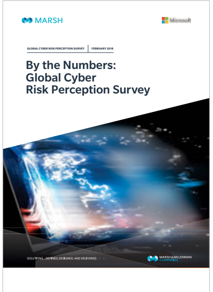


HOLDING HEALTHCARE TO RANSOM

The paper highlights the vulnerability of healthcare players to cyberattacks, clarifying its importance for all stakeholders to understand and to take proactive measures in managing cyber risks. It examines the current situation of cyber risks in the healthcare landscape and illustrates key observations and common challenges faced by the industry

FROM THREATS TO IMPACT: EVOLVING RISK CONCERNS IN ASIA PACIFIC VOL. 3

Leveraging the 2018 Global Risk Report, the report builds on previous iterations by providing insights regarding the risk landscape for businesses operating in Asia-Pacific. It also drills down into the risks of critical infrastructure failure/shortage and talent shortage, before exploring several options to mitigate such risks going forward



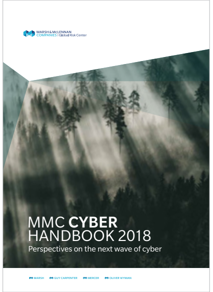
BY THE NUMBERS: GLOBAL CYBER RISK PERCEPTION SURVEY

A global survey of more than 1,300 executives, undertaken by Marsh in partnership with Microsoft, examines cyber risk concerns and management strategies by organizations of all sizes in a range of industries worldwide

MARSH & McLENNAN COMPANIES | Asia Pacific Risk Center
CYBER
EVOLUTION
En Route to Strengthening Resilience in Asia-Pacific
FireEye

CYBER EVOLUTION: EN ROUTE TO STRENGTHENING RESILIENCE IN APAC

A collaboration between FireEye and Marsh & McLennan Companies – each a leader in their own fields – the white paper includes a full overview of the fundamental cyber challenges facing the APAC region, and the appropriate risk management tools needed to address those challenges



MMC CYBER HANDOOK 2018: PERSPECTIVES ON THE NEXT WAVE OF CYBER

The handbook provides insights on the shifting cyber threat environment, emerging global regulatory trends, and best practices in the journey to cyber resiliency. It features articles from business leaders across Marsh & McLennan Companies and our expert and notable collaborators

2018 COMMUNICATIONS, MEDIA, AND TECHNOLOGY RISK STUDY

Pushed on by a data-driven economy and the ubiquity of technology in society, CMT companies are meeting the challenges by taking a hard look at their traditional way of doing business. This paper examines the shift and is based on more than 200 survey responses from risk professionals and other executives from CMT sectors globally

THE GLOBAL RISKS REPORT 2018

The World Economic Forum highlights the issue that will exacerbate volatility and uncertainty in the next decade – while also presenting opportunities for government and businesses to build resilience and deliver sustainable growth. Marsh & McLennan Companies has been a strategic partner of the report since 2006

ABOUT MARSH & MCLENNAN COMPANIES

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 leader in insurance broking and risk management; Guy Carpenter is a leader in providing risk and reinsurance intermediary services; Mercer is a leader in talent, health, retirement and investment consulting; and Oliver Wyman is a 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 130 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.

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.

This report and any recommendations, analysis or advice provided herein (i) are based on our experience as insurance and reinsurance brokers or as consultants, as applicable, (ii) are not intended to be taken as advice or recommendations regarding any individual situation, (iii) should not be relied upon as investment, tax, accounting, actuarial, regulatory or legal advice regarding any individual situation or as a substitute for consultation with professional consultants or accountants or with professional tax, legal, actuarial or financial advisors, and (iv) do not provide an opinion regarding the fairness of any transaction to any party. The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. We are not responsible for the consequences of any unauthorized use of this report. Its content may not be modified or incorporated into or used in other material, or sold or otherwise provided, in whole or in part, to any other person or entity, without our written permission. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Information furnished by others, as well as public information and industry and statistical data, upon which all or portions of this report may be based, are believed to be reliable but have not been verified. Any modeling, analytics or projections are subject to inherent uncertainty, and any opinions, recommendations, analysis or advice provided herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. We have used what we believe are reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied, and we disclaim any responsibility for such information or analysis or to update the information or analysis in this report. We accept no liability for any loss arising from any action taken or refrained from, or any decision made, as a result of or reliance upon anything contained in this report or any reports or sources of information referred to herein, or for actual results or future events or any damages of any kind, including without limitation direct, indirect, consequential, exemplary, special or other damages, even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. No responsibility is taken for changes in market conditions or laws or regulations which occur subsequent to the date hereof.