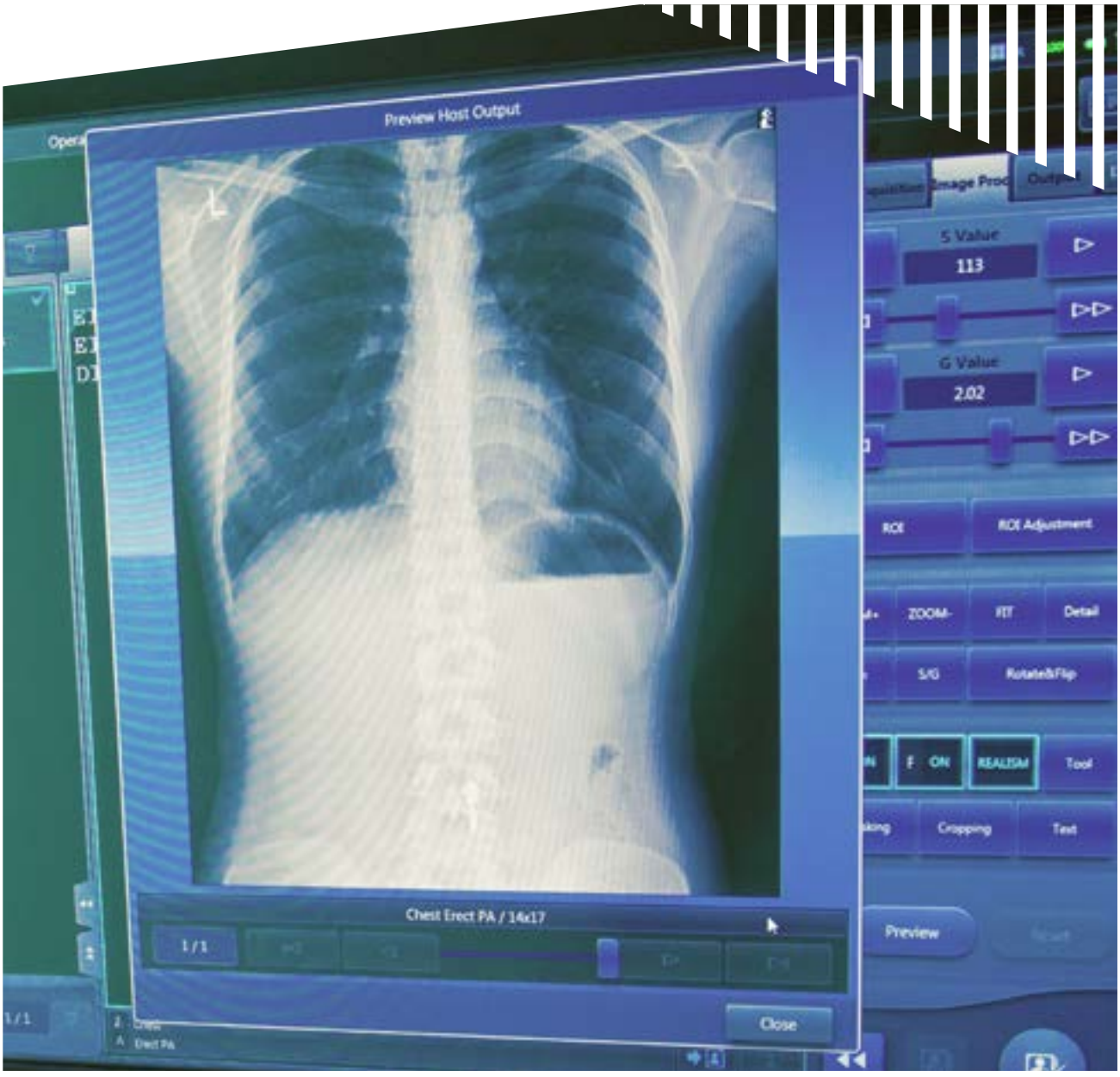
MARSH & McLENNAN COMPANIES | Global Risk Center

HOLDING HEALTHCARE **TO RANSOM**

Industry perspectives on cyber risks



MARSH GUY CARPENTER MERCER OLIVER WYMAN

KEY TAKEAWAYS

1 **Healthcare is among the industries most vulnerable to cyberattacks.** There have been more high-profile attacks in the past few years in the healthcare industry than others, and the sector will likely remain one of the most targeted given its sensitive data.

2 **Business interruptions and the leak of customer information** are the most critical cyber loss scenarios for the healthcare industry. Breaches can have major implications beyond financial losses – they can result in shutdowns and interruptions and impact the well-being of patients.

3 **The healthcare industry incurs one of the highest financial costs,** in the face of a cyberattack. Among cyber threats, financially-motivated threat actors, including internal parties, are the biggest concern for healthcare organizations. As shown by results of the Marsh-Microsoft Global Cyber Risk Perception Survey 2017, more than 70 percent of respondents from the healthcare industry expect that a cyber breach could 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 visibility of cyber risk issues within healthcare organizations and distribute cyber risk management to a responsibility across the firm.** While the risks are real and have been recognized by the industry, many healthcare organizations have yet to set up and implement a holistic framework, governance, and adequate Board oversight.

5 **This paper highlights some examples of best practices across industries in cyber risk management,** and several key areas for healthcare organizations 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, Feb 2018. By the Numbers: Global Cyber Risk Perception Survey

CYBER RISK SITUATION AND PERCEPTIONS

INCREASED CYBERATTACKS WITNESSED IN THE HEALTHCARE INDUSTRY

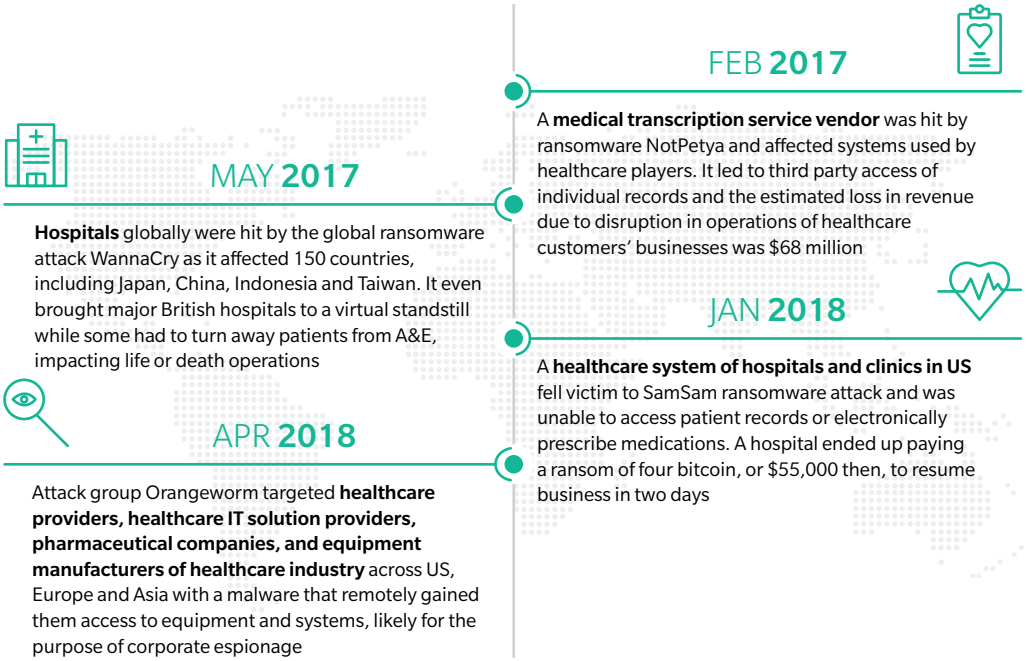
Healthcare is one of the sectors most vulnerable to cyberattacks. Over the past decade, the industry has been haunted by headlines of data breaches. Three of the largest reported incidents impacting healthcare organizations in 2015 alone affected up to 100 million patient records and resulted in hundreds of millions of dollars in settlements.[2] Data and cyber breaches have real financial and reputational impacts. For instance, the heavily-regulated healthcare industry can be penalized up to $380 per patient record, more than double the global industry average of $141 per lost/stolen record.[3]

High stakes *– Human lives and sensitive data – make healthcare the perfect target for cyber crime*

The Marsh-Microsoft Global Cyber Risk Perception Survey 2017,[4] administered between July and August 2017, too indicates that healthcare is particularly vulnerable, with more than one in four (27 percent) healthcare organizations reporting that they have been a victim of cyberattack in the past 12 months. This is more than financial institutions (20 percent) and nearly twice the incidence in the communications, media and technology sector (14 percent).

As the potential impacts of cyberattacks are transboundary, no country is completely immune to this phenomenon. Ransomware attacks such as WannaCry and Petya had a global reach affecting care delivery businesses and insurers in the region. For companies in Asia-Pacific, it takes almost five times longer to detect an intrusion compared to global counterparts.[5]

Exhibit 1: Snapshot of recent attacks in the healthcare industry



Source: Data Breach Today, The Straits Times, Healthcareitnews

2 Reuters (2017) Anthem to pay record $115 million to settle U.S. lawsuits over data breach.

3 Ponemon Institute (2017). 2017 Cost of Data Breach Study.

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

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

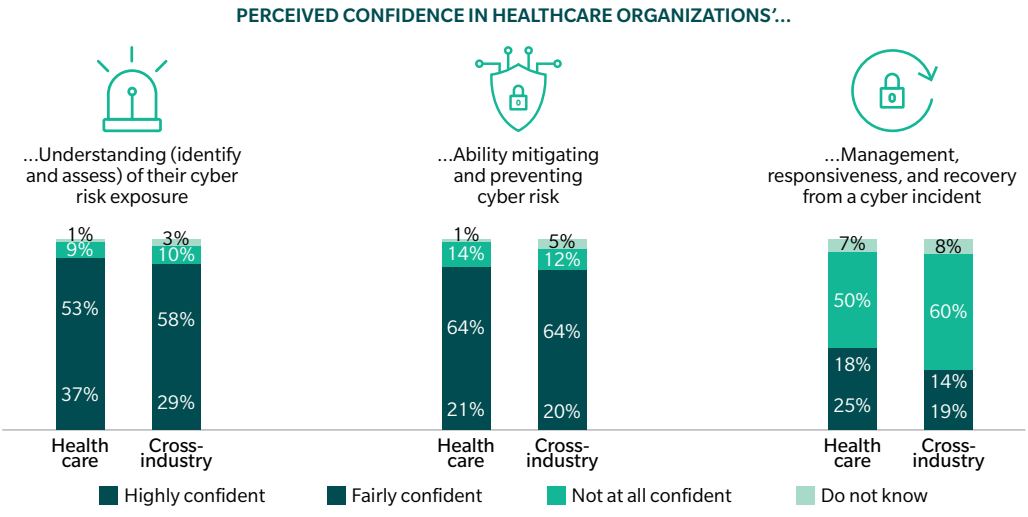
The healthcare industry, in many parts of the world and across service providers, is still in the nascent stage of digitalization and often relies on hardcopy medical records. The wide spectrum of formats in which data can exist within an organization, either digitally or in print, means that the risks of data breaches can be widespread and systemic in healthcare. It can also include internal operational risks, such as lost or stolen paper records or non-employee access to restricted care areas. In fact, error and misuse are notoriously widespread in the healthcare industry. It is the only industry that has more internal threat actors behind data breaches than external.[6] The high stakes involved—human safety and sensitive data—make cyber resilience an imperative for the industry.

ROOM FOR IMPROVEMENT IN HEALTHCARE ORGANIZATIONS' MANAGEMENT, RESPONSIVENESS, AND RECOVERY FROM CYBERATTACKS

Even against this backdrop, respondents from the healthcare industry in the Marsh-Microsoft Global Cyber Risk Perception Survey underestimate the likelihood of a cyberattack, while being slightly more confident of preventing and recovering from a cyber incident than other industries. More than a third (37 percent) of survey respondents in the healthcare industry are highly confident of understanding their cyber risk exposure, as opposed to the cross-industry average of 29 percent (Exhibit 2). However, in the event of a successful cyberattack, 50 percent of the respondents from the healthcare industry and more than half (60 percent) of the cross-industry respondents are not at all confident about managing and recovering effectively from it.

The healthcare industry generally lacks qualified IT staff and security specialists, equipped adequately with cybersecurity skillsets, who can lead the organization to swiftly and confidently manage cyberattacks – a key driver of cyber resilience.[7] Misaligned budget and incentive systems are the main barriers to attracting cyber experts and adopting up-to-date digital innovation speedily in the industry.[8]

Exhibit 2: Healthcare organizations' self-assessed ability to understand, prevent, and manage cyber risks



Source: Marsh-Microsoft Global Cyber Risk Perception Survey 2017

6 Verizon (2018). 2018 Data Breach Investigations Report.

7 CSO (2016). Hospitals lack staff needed to combat cyber attacks.

8 Harvard Business Review (2018). Hospital Budget Systems are Holding Back Innovation.

BUSINESS INTERRUPTIONS AND BREACH OF CUSTOMER INFORMATION BIGGEST PERCEIVED THREATS

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

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

Source: Marsh-Microsoft Global Cyber Risk Perception Survey 2017

Business interruption was highlighted as the primary cyber risk concern in healthcare (69 percent), similar to other industries. In 2017, the WannaCry global attack succeeded in temporarily shutting down IT systems of hospitals globally. As a result, ambulances were diverted, and critical appointments cancelled, for instance. Cyence, a Silicon Valley-based cyber risk analytics and modeling firm, estimated that the financial impact of this attack could reach $4 billion.[9] In more life-threatening cases, cyberattackers could compromise medical devices, such as health networked MRI machines, as entry points into unsecured Wi-Fi networks, causing critical medical devices to malfunction. With key equipment out of commission for days, it would cut into healthcare organizations' bottom lines, easily resulting in a daily revenue loss of $1 million for one machine.[10]

Breach of customer information is a more daunting scenario in healthcare (67 percent) than across other industries. A medical record holds powerful data on an individual, and when compromised, it cannot be reissued or suspended, like in the case of a credit card.

9 CBS (2017). "WannaCry" Ransomware Attack Losses could reach $4 billion.

10 Modern Healthcare (2018). Hacked medical devices could wreak havoc on health systems.

Cybercriminals can use, and even manipulate, such data to cause personal distress, damage users' reputation or compromise corporate accounts, or to monetize stolen data. There is high demand for patient medical records in the black market and it fuels malicious cyber activities.[11] A copy of electronic medical health record can be priced up to thousands of dollars each in the black market, as compared to a credit card number that is worth 25 cents and a social security number that is worth 10 cents.[12]

HEALTHCARE INDUSTRY ACUTELY AWARE OF THE **SEVERE FINANCIAL CONSEQUENCES OF A CYBERATTACK**

Healthcare players are most concerned about financially-motivated threat actors – 45 percent of healthcare respondents to the Marsh-Microsoft Global Cyber Risk Perception Survey flagged organized crime/ hacktivist groups as their biggest source (Exhibit 4).

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

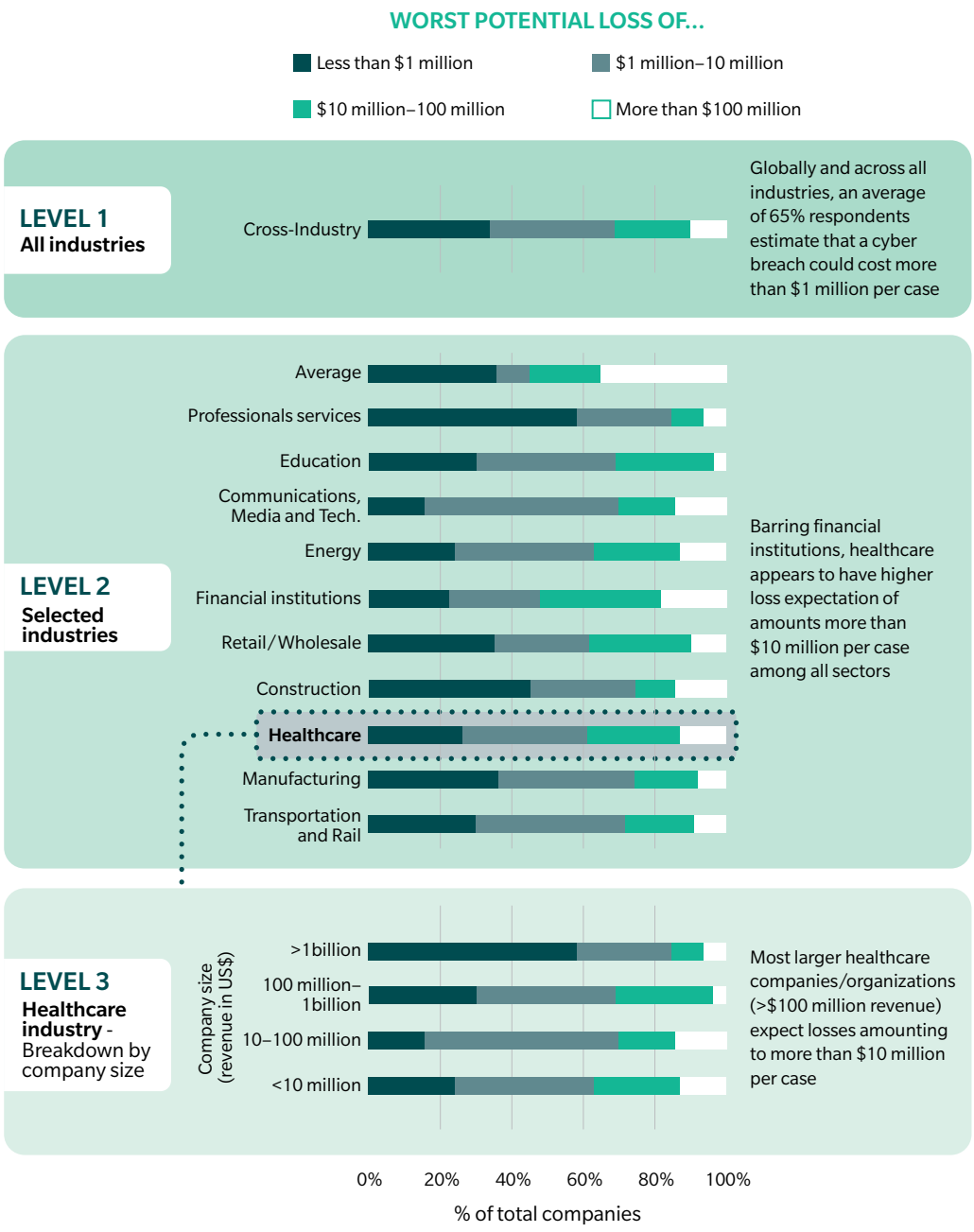
Three in four cyberattackers target the healthcare industry with financial motivations, with ransomware being the most prevalent malware, constituting approximately 85 percent of total malware used in attacks on the industry.[13] In the case of SamSam ransomware attack, the attackers have extorted nearly $850,000 to date.[14]

At the same time, human error and malicious rouge employee, and third parties are other possible human vectors that pose significant cyber threats. Their motivations can be difficult to predict and anticipate, ranging from financial gains to coercion or mere carelessness, and the impact can be detrimental as well.

While the average total cost of data breaches in FY2017 is $3.6 million per company across sectors,[15] a cyberattack is perceived to have more severe financial impact for the healthcare industry than most others. More than 70 percent of healthcare respondents expect that each cyber breach scenario in the industry could cost more than $1 million, as compared to a cross-industry average of 65 percent who feel the same way (Exhibit 5).

11 Infosec Institute. Top Cyber Security Risks in Healthcare.
12 Forbes (2017). Your Electronic Medical Records could be worth $1000 to Hackers.
13 Verizon (2018). 2018 Data Breach Investigations Report.
14 CSO (2018). SamSam ransomware attacks have earned nearly $850,000.
15 Ponemon Institute (2017). 2017 Cost of Data Breach Study.

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



Source: Marsh-Microsoft Global Cyber Risk Perception Survey 2017

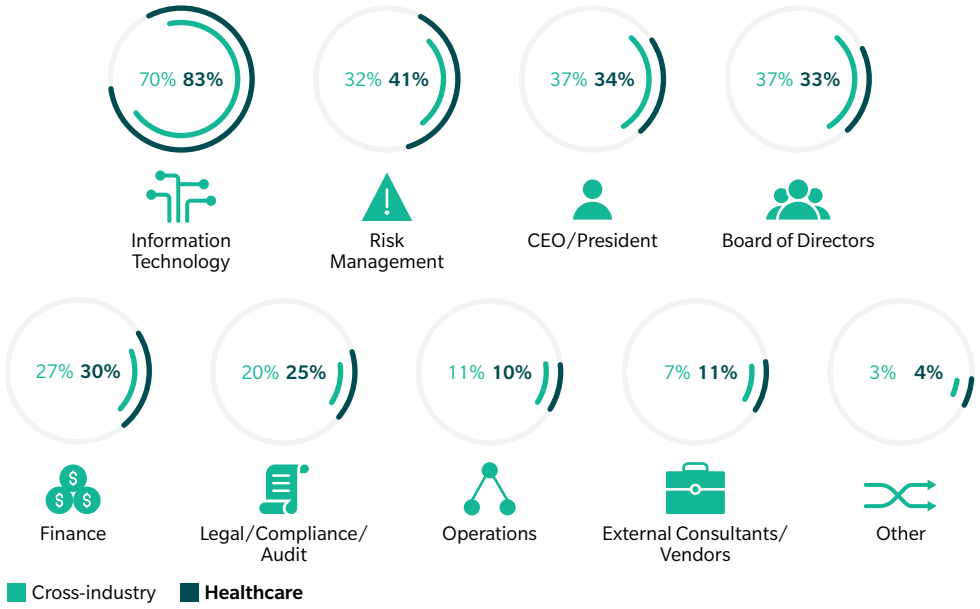
CHALLENGES IN EFFECTIVE CYBER RISK MANAGEMENT

LACK OF FIRM-WIDE RESPONSIBILITY AND AN INTEGRATED FRAMEWORK IN CYBER RISK MANAGEMENT IN HEALTHCARE

Cyber risk management in the healthcare industry is still perceived to be driven by the IT department only (Exhibit 6). Eighty-three percent of healthcare respondents to the Marsh-Microsoft Global Cyber Risk Perception Survey indicated that responsibility for cyber risk sits mainly in IT and they are the primary owners and decision-makers for managing cyber risks, as compared to the 70 percent cross-industry average.

The organization is not yet coming together as a whole in the healthcare industry's fight against cyberattacks

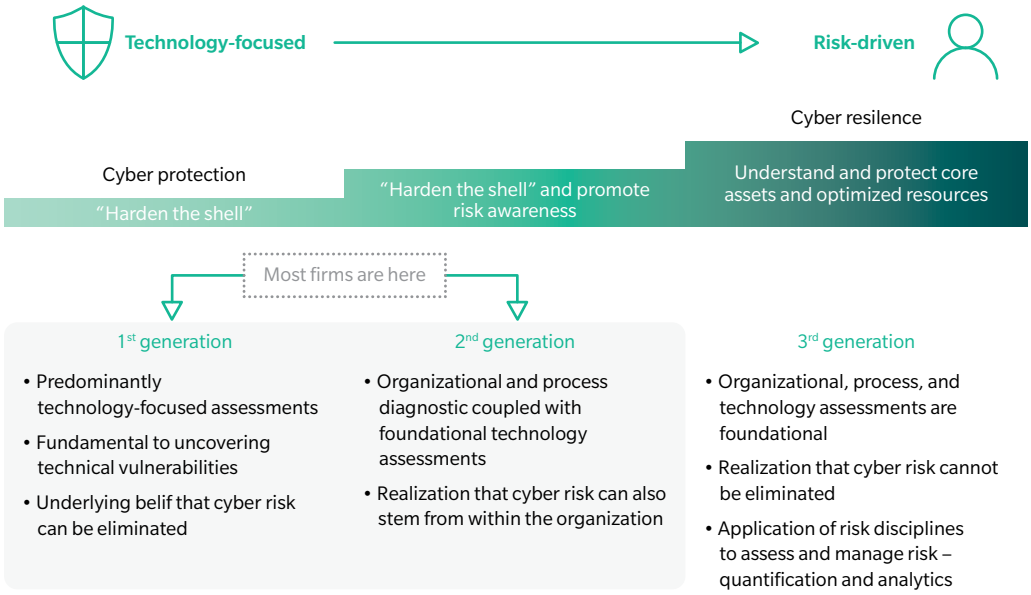
Exhibit 6: Primary owners and decision-makers for cyber risk management in the healthcare industry



Source: Marsh-Microsoft Global Cyber Risk Perception Survey 2017

While the healthcare industry understands the key role of risk management teams better than other industries, it is still crucial to distribute the management of cyber risk to a responsibility across the organization. The next stage of focus for these companies is to transition cyber risk from being "technology-focused" to "risk-driven" (Exhibit 7), and making it a top-down company-wide responsibility that cuts across department horizontals. For instance, risk teams and senior management must work with IT to define cyber risk-related metrics within an organization's risk appetite. Roles such as HR and Public Relations also have an integral part to play in processes and communications of cyber risk management.

Exhibit 7: Shift in focus for cyber risk management



Source: Oliver Wyman

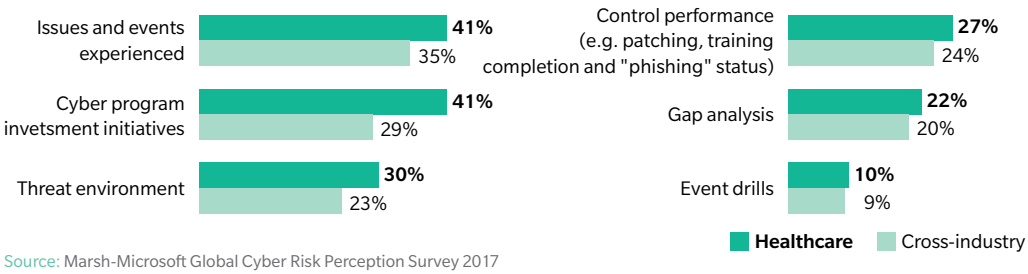
Regulatory developments should also remain on the radar of healthcare organizations. In 2017 alone, the US Department of Health and Human Services' Office for Civil Rights enforced nine resolution agreements against healthcare organizations and imposed higher post-breach monetary fines.[16] Similarly, the National Institute of Standards and Technology (NIST) in the US has recently released updated standards for cybersecurity,[17] and is aligning the requirements for medical devices with its overall cybersecurity framework.[18] Notification of data breaches is also becoming a subject of increased scrutiny in key Asia-Pacific markets such as China, Singapore, Hong Kong, Australia, and South Korea. In Europe, the enactment of General Data Protection Regulation (GDPR) in May 2018 will have a major impact on data and cyber risk management strategy in the healthcare industry.[19]

NOT ENOUGH BOARD VISIBILITY INTO CYBER RISK ISSUES DRIVES THE NEED FOR MORE PROACTIVE MEASURES

Cyber risk is not receiving sufficient visibility at the board level – less than half (41 percent) of surveyed healthcare organizations include cyber risk-related issues in regular reporting (Exhibit 8). There is also an apparent lack in gap analysis and event drills conducted across all industries. This is a concern as it might expose the board to Directors and Officers (D&O) Liability.[20]

16 Beazly (2018). 2018 Breach Briefing.
17 National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity.
18 Health Law Advisor (2018). Thought Leaders on Laws and Regulations Affecting Healthcare and Life Sciences.
19 Frost & Sullivan, May 2018. Impact of EU GDPR on Healthcare Data Management in a Value-based Care Paradigm.
20 Chubb. Readings in Healthcare Governance.

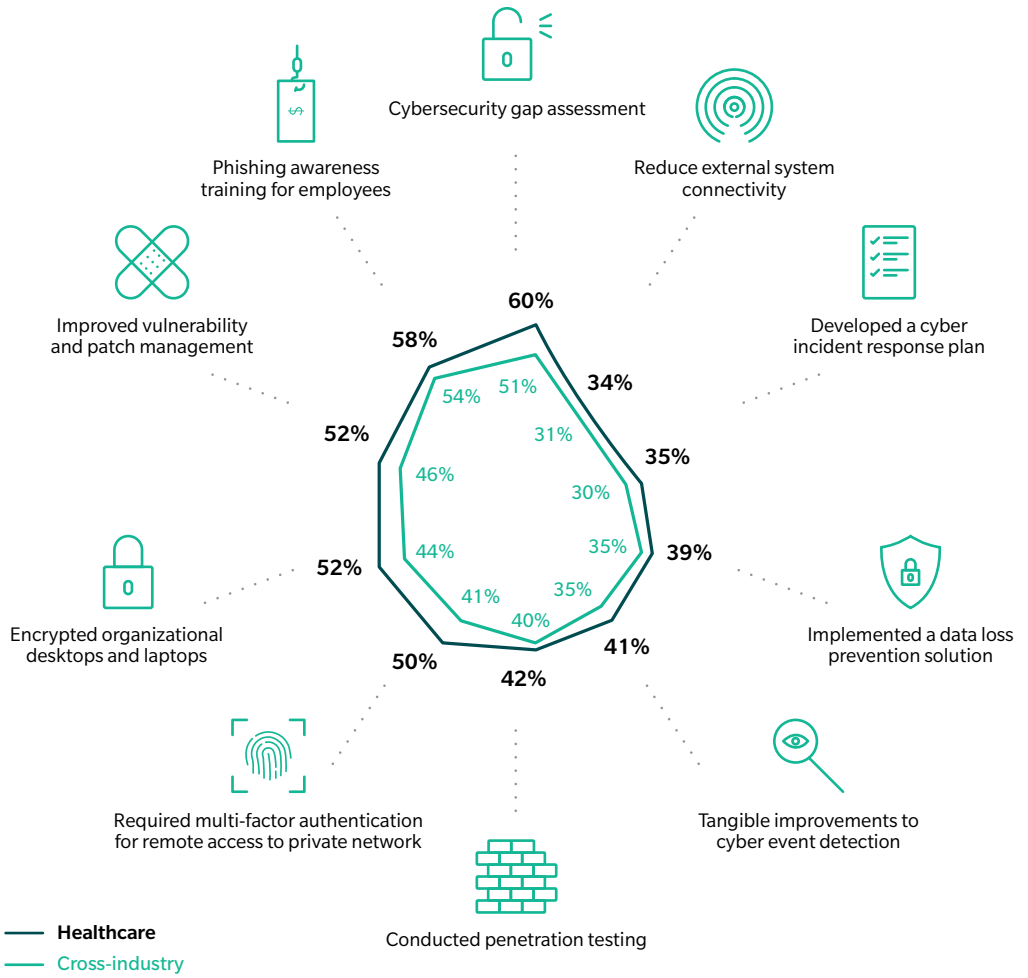
Exhibit 8: Cyber risk reporting received by board of directors of healthcare organizations



Source: Marsh-Microsoft Global Cyber Risk Perception Survey 2017

Given the spate of cyberattacks being seen around the world, cyber risk has climbed higher up the ladder of C-Suite executives' priorities, and is, for the first time, among the year's top five risks.[21] Although the reporting trend is slightly more positive in healthcare than the cross-industry average, cyber risk management should continue to be viewed as part of overall enterprise risk management. Healthcare organizations should 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.

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



Source: Marsh-Microsoft Global Cyber Risk Perception Survey 2017

21 Marsh & McLennan Companies' Asia Pacific Risk Center & World Economic Forum (2018). 2018 Global Risks Report.

According to the Marsh-Microsoft Global Cyber Risk Perception Survey, the healthcare industry has been taking more actions on average than other industries in the past 12-24 months to prevent and prepare for cyberattacks (Exhibit 9). For example, 60 percent of healthcare respondents – as opposed to 51 percent of respondents across industries – indicated that they are assessing the cybersecurity gap to uncover what more needs to be done in protecting themselves against future threats.

That notwithstanding, most healthcare organizations still focus more on prevention or preparedness and not 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 a cybersecurity gap assessment, phishing awareness employee training, improved vulnerability and patch management, and encryption of company computers. On the other hand, only slightly more than one-third of the respondents have a cyber incident response plan in place (35 percent) or have invested in improving cyber event detection (41 percent).

MEASUREMENT OF CYBER RISKS HAS BEEN **LARGELY QUALITATIVE**, NOT QUANTITATIVE

More than half (56 percent) of healthcare respondents in the Marsh-Microsoft Global Cyber Risk Perception Survey say their organizations measure the cyber risks that they are exposed to, but a significant proportion do so using qualitative methods. Three in four organizations 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 (30 percent) and numerical rankings (16 percent of those who measure) within a fixed framework.

Considering the expected high financial impact of cyberattacks and data breaches, healthcare organizations should allocate more resources to better understand the magnitude of cyber risks as part of their overall risk profile, through quantifying the potential impacts.

Exhibit 10a: Current state of cyber risk measurement in the healthcare industry

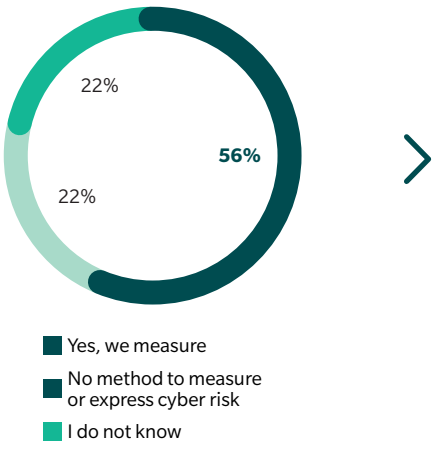
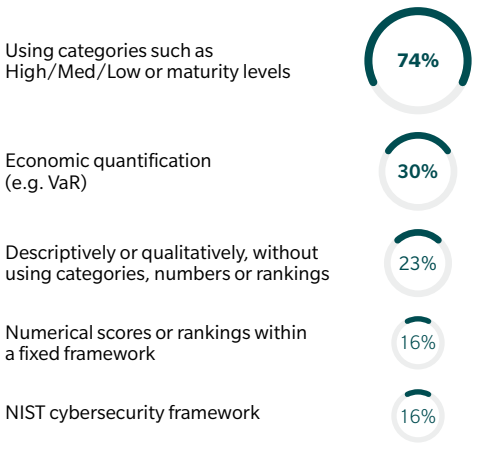


Exhibit 10b: Methods used to measure cyber risk exposure (among healthcare organizations that do measure cyber risk)



Source: Marsh-Microsoft Global Cyber Risk Perception Survey 2017

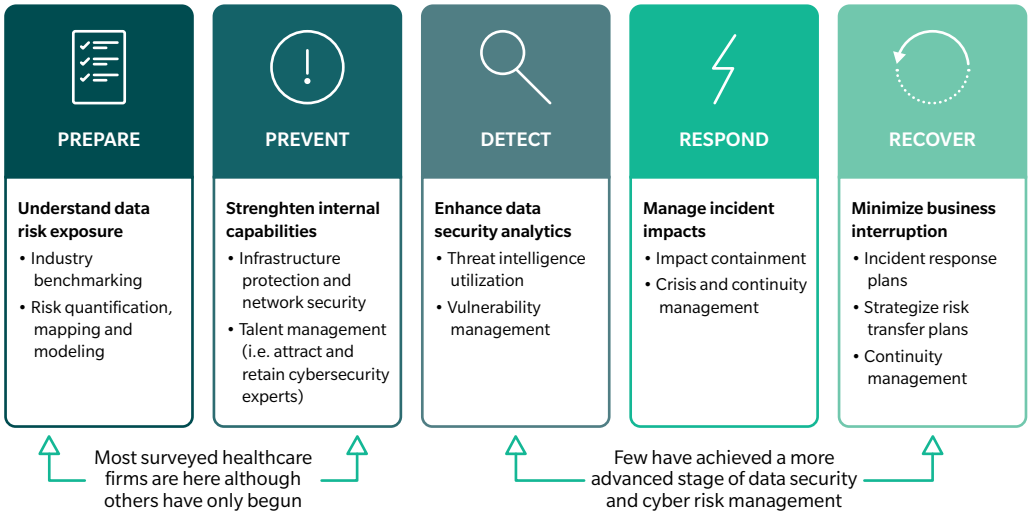
WHAT'S NEXT: STAYING SAFE FROM CYBERATTACKS

HOLISTIC APPROACH IN MANAGING DATA BREACHES AND CYBER RISK

Protect lives and build a ***cyber immune system***

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 expectations from Management, Shareholders, Regulators, and rating agencies (such as Standard & Poor's), industry-specific mechanisms should be designed to safeguard against incidents as well as implement an up-to-date proven cyber incident playbook in case of breaches.

Exhibit 11: Five key functions of the cybersecurity framework and recommended actions



Source: Oliver Wyman analysis; Marsh-Microsoft Global Cyber Risk Perception Survey 2017

Prepare and **Prevent: Risk Diagnostics, Education, and Strengthening of Network Security**

A strong internal risk diagnostic, as a start, is required to assess a company's cyber risks vis-à-vis industry peers. As shown in Exhibit 9, 40 percent of healthcare organizations still haven't conducted a cybersecurity gap assessment in the past two years and there is room for improvement in understanding and managing their overall risk exposure. Healthcare organizations need to identify, define, and map specific cyber threats and scenarios to their tangible and intangible assets. Such tailored practices need to become a standard operating procedure across the healthcare industry.

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 requires a bottom-up approach, such as creating a more cyber-savvy workforce and strengthening the culture of cybersecurity (such as data privacy, information security, cyber awareness, and accountability). Many successful and attempted cyber incidents in healthcare organizations have been attributed to human error, with a reported 30 percent of phishing messages being opened by targeted users and 12 percent of

those users falling for the malicious attachments or links.[22] Healthcare organizations should continue to prioritize trainings for employees as effective cyber resilience has its roots within the culture of an organization and its people.

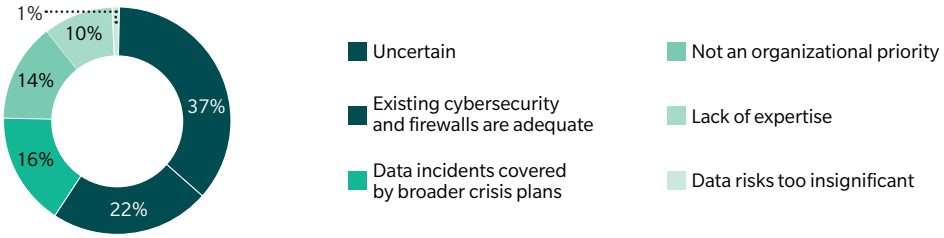
Strengthening network security should be a priority given the proliferation of the Internet of Things (IoT) and mobile devices with access to corporate networks. Organizations should emphasize proven cybersecurity hygiene practices which are missing for half of the healthcare industry at present. For instance, organizations should secure by design – devise safe modes and encryptions into their digital assets during development.[23] Healthcare respondents to the Marsh-Microsoft Global Cyber Risk Perception Survey admit to not having hardware encryption (47 percent) and multi-factor authentication for corporate networks (50 percent). And only half of the healthcare respondents improved vulnerability and patch management in the past year.

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.[24] IT departments are the primary owners and decision-makers for cyber risk management across the healthcare sector globally, as shown in Exhibit 6. Often, cyber risks appear 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, organizations are encouraged to better understand the return on risk, through quantification, and to build in-house capabilities across multiple interconnected functional areas aligned with their cyber strategy. A management-led approach to set out cyber risk appetite is a first step to recognizing that cyber is a firm-wide risk.

Underpinning advanced data resilience frameworks is a strong detection mechanism and holistic incident response plan. Almost two-thirds of healthcare organizations have not developed a cyber incident response plan. Most alarmingly, 37 percent of respondents are not sure of the reasons behind the lack of a cyber response plan while only 22 percent are confident that their organization's cybersecurity and firewalls are adequate.

Exhibit 12: Reasons for not having a cyber incident response plan



Source Marsh-Microsoft Global Cyber Risk Perception Survey 2017

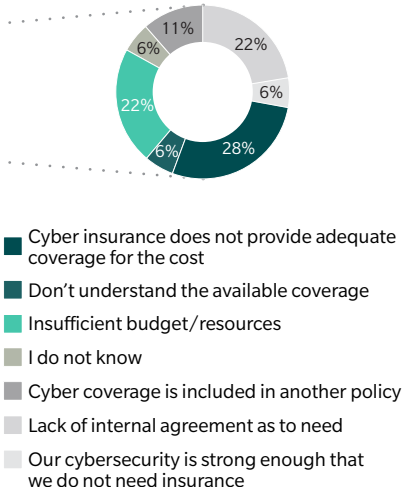
22 Verizon (2017). 2017 Data Breach Investigations Report.
23 Marsh & McLennan Companies (2018). Cyber Handbook 2018.
24 Marsh & McLennan Companies' Asia Pacific Risk Center (2017). Risk in Asia: Ramifications for Real Estate and Hospitality 2017.

Transfer risk with cyber insurance as a tool to manage exposure. Key risks that healthcare organizations face today include patient data exposure, shared system data exposure and employee exposure. Recognizing that cyber risks cannot be eliminated, healthcare organizations are beginning to look to insurance or cyber risk transfer programs as a way to shift the risks, not just as a solution for balance sheet protection but also for contractual evidence and compliance.[25] Prompted by the wave of high-profile attacks and new data protection rules, annual gross written cyber insurance premiums have grown by 34 percent per annum over the past seven years.[26] 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, [27] and healthcare organizations are only beginning to recognize this.

While less than half of the healthcare respondents' organizations (49 percent) have cyber insurance coverage (Exhibit 13a), the number is comfortably more than the cross-industry average of 34 percent, but marginally behind financial institutions (52 percent). We understood from respondents that have estimated their losses from cyber incidents that both healthcare and financial institutions suffer the greatest financial impact. Quantifying cyber risks and creating greater awareness can catalyze actions – such as increasing cyber insurance coverage – to mitigate cyber risks.[28]

Exhibit 13a: Healthcare organizations' status of cyber insurance

Exhibit 13b: Reasons for not having cyber insurance



Source: Marsh-Microsoft Global Cyber Risk Perception Survey 2017

25 Marsh, 2015. Cyber Risk Healthcare Brochure.

26 Marsh & McLennan Companies (2018). Cyber Handbook 2018.

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

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

Among respondents who plan to purchase or increase cyber coverage, 38 percent are driven internally, citing cyber risk management plan as the main driver.

For those that do not have cyber insurance in place, 28 percent indicate that the current offerings do not provide enough coverage to cover for the cost (Exhibit 13b). While some cyber insurance policies do not cover costs of notification, penalties, or lost revenue, it is critical for healthcare organizations to understand the available tools and limit structure that best suit their financial conditions and risk tolerance.[29] Recent cyber claims scenarios, which a notable cyber insurer has paid for, might indicate that healthcare organizations need to re-evaluate their understanding or status of cyber insurance coverage[30]:

- An **assisted living facility** experienced a "brute force" ransomware attack and several critical systems became inoperable. It incurred losses of more than $250,000 to get affected systems back online and $50,000 for incident response and IT forensics services.
- A **hospital** fell victim to a ransomware attack and was unable to bill the insurance carrier, process payroll, or produce MRI and CT scan images. Expenses of more than $700,000 were incurred in IT forensics, data recovery, business interruption and crisis management costs.
- A **business associate of the insured healthcare organization** was the subject of a ransomware attack, putting the insured customers' personal health information at risk. After consultation with the incident response manager, it was determined that no data was breached, but an approximate $20,000 in incident response costs was incurred.

The lack of internal agreement on the need for cyber insurance and insufficient budget/resources are also major impediments (with 22 percent of respondents citing them as reasons) in cyber insurance penetration in the healthcare industry. These numbers further support the observation that budgeting in healthcare organizations is misaligned and technology modernization should be prioritized.

At the same time, it must be recognized that cyber insurance is not a silver bullet and must be augmented with robust risk strategy and ongoing management.

29 Healthcare IT news (2017). What to know about risk, coverage before you buy cyber insurance.
30 Chubb (2018). Cyber Claims Scenarios: What we have paid lately.

RISING CYBER RISK WITH INCREASED DIGITALIZATION OF THE HEALTHCARE INDUSTRY

Moving into the future of the healthcare industry, organizations will find that end-of-life applications, legacy systems, and the current way in which sensitive data are stored – Electronic Medical Record, are no longer sufficient for maintaining health data. Patients are going to continuously integrate health devices, such as adding Fitbit information, downloading genetics information, and feeding additional personal data through wearable and implantable technologies. In the future, they would all make up a part of a medical record. It is also not going to be just about health records on the server or cloud of a hospital, but also health data held by us on our private phones. The introduction of 5G network will contribute to the high potential for compromise.[31]

Other emerging technologies will also lead the healthcare system to evolve into a more data- and analytics-driven one that can enable healthcare organizations to translate data into information that we can base decisions on. This will allow us to continuously monitor, treat, and see the development of patients not just during appointment time. It will require the whole suite of integrated technologies – IoT, Artificial Intelligence, and Machine Learning, based on various hardware and software.[30]

With these technologies on the horizon and their implications on healthcare cybersecurity, there is a need to advocate a security-privacy layer in the design of these devices and technologies.[30] It is also important to prioritize the right skillsets within healthcare organizations to ensure that technologies and security can continually improve. Most importantly, there must be a mindset and behavioral shift, through education or campaigns, to instill a culture of cyber-awareness among all stakeholders – the public, patients, and the healthcare workforce, who will have greater access to medical records on more devices and platforms than before.

31 Sam Hanna and Oliver Wyman (2018). The Oliver Wyman Health Podcast; Wearables, Ingestibles, and (the Inevitable) Cyberattack.

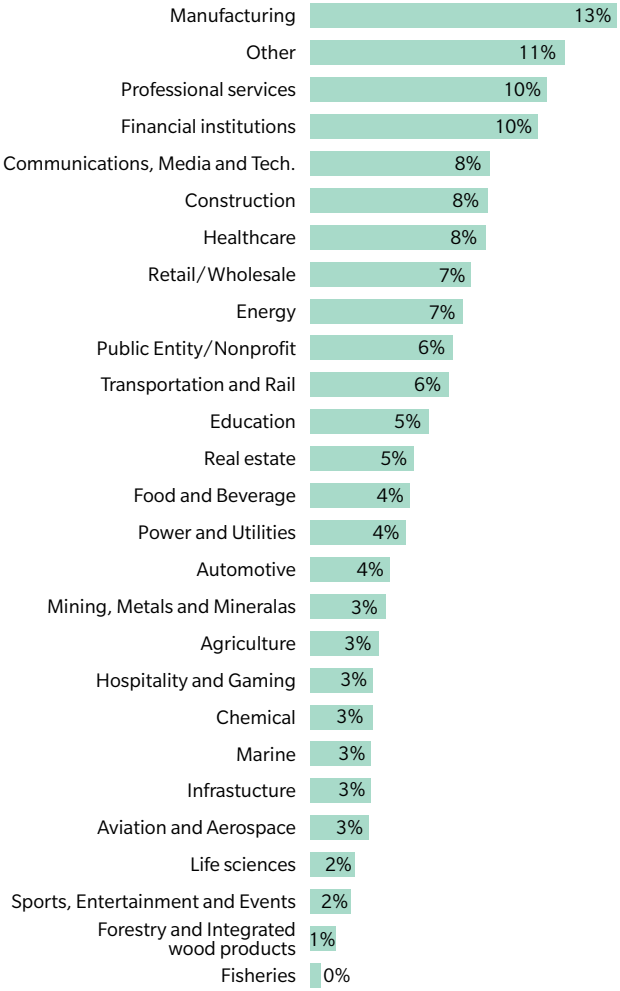
About the Marsh-Microsoft Global Cyber Risk Perception Survey

This paper is based largely on findings from the Marsh-Microsoft Global Cyber Risk Perception Survey administered between July and August 2017.

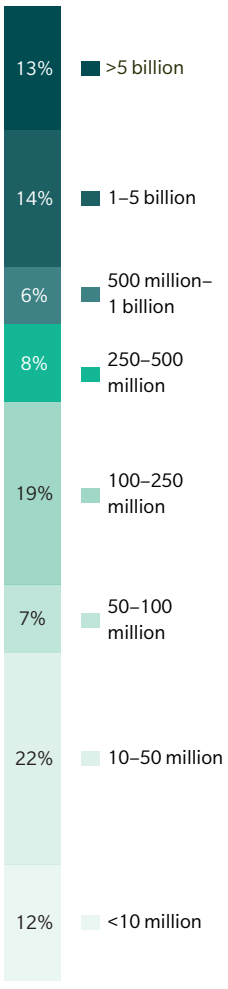
More than 1,300 senior executives participated in the survey, representing a wide range of industries and key functions, including information technology, risk management, finance, legal/compliance, senior management and boards of directors.

Of the 1,312 respondents surveyed in total, 101 respondents (8 percent) were from the healthcare industry identified with businesses across various regions and were from organizations with at least $10 million in annual revenue.

Industry breakdown of all survey respondents (N=1312)



Surveyed healthcare organizations' annual revenue in $ (N=101)



To read the digital version of Holding Healthcare to Ransom – Industry Perspectives on Cyber Risks, please visit: **www.mmc.com/global-risk-center-overview.html**

AUTHORS

Jayant Raman
Principal, Finance & Risk Practice, Oliver Wyman

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

Prashansa Daga
Health & Life Science Industry Leader Asia, Marsh

Wolfram Hedrich
Executive Director, Marsh & McLennan Companies' Asia Pacific Risk Center

Rachel Lam
Research Analyst, Marsh & McLennan Companies' Asia Pacific Risk Center

MARSH & MCLENNAN COMPANIES CONTRIBUTORS

Marsh: Richard Green, Lynne Burns, Thomas Reagan
Oliver Wyman: Sumit Sharma, Mark James, Paul Mee, Terry Stone, Sam Glick
Asia Pacific Risk Center: Jaclyn Yeo
Global Risk Center: Leslie Chacko

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.

For more information, please email the team at contactaprc@mmc.com.

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.