HOLDING HEALTHCARE RANSOM

INDUSTRY PERSPECTIVES ON CYBER RISKS

Paul Mee
Partner, Strategy, IT & Operations, Oliver Wyman

Jayant Raman
Principal, Financial Services, Oliver Wyman

Kitty Lee
Principal, Health & Life Sciences, Oliver Wyman

Editor's Note: This article is excerpted from Marsh & McLennan Companies' Global Risk Center, Holding Healthcare to Ransom – Industry Perspectives on Cyber Risks *report*[9].

There was an average of at least one[10] cyberattack every single day over the entire course of 2017. High stakes – human lives, big money, and sensitive data – make healthcare a pretty perfect cybercrime target – and an expensive one, at that. For eight consecutive years, healthcare organizations' data breach costs have been the most expensive – costing $408 per lost or stolen record, almost triple the $148 cross-industry average.

BUSINESS INTERRUPTION

is the primary cyber risk concern in healthcare. Last year's WannaCry made many people want to cry, temporarily shutting down hospitals, diverting ambulances, and canceling critical medical appointments. Cyence, a Silicon Valley-based cyber-risk analytics and modeling firm, estimated the financial impact of this attack could reach $4 billion. 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[11] for one machine.

BREACH OF CUSTOMER INFORMATION

is, however, a more daunting scenario in healthcare compared to other industries. For example, when a medical record with information like your address, Social Security number, date of birth, and medical information, is compromised, it cannot be swiftly reissued or instantaneously suspended like a stolen credit card where you check your statement for erroneous charges, open an app and claim card fraud, have a new card swiftly delivered, and continue onward – soon to forget it even happened at all. Healthcare data is very different. For one thing, the black market is hungry – starving, you could say – for patient medical records, which hold great amounts of power. One copy of an electronic medical health record can be priced up to thousands of dollars on the black market, compared to a credit card number worth a quarter, or a Social Security number worth a dime.

Once this valuable medical information is in their hands, cybercriminals have used and even manipulated this highly permanent, personalized data to damage[12] a patient's reputation (such as committing intellectual theft or blackmail, opening bank accounts, or filing tax returns to collect rebates), compromising their corporate accounts or monetizing stolen data. Quite different than a credit card hack, to say the least.

PHYSICAL HARM

and the possibility of death are other potential impacts of a cyberattack. Medical technology and devices, for instance, are particularly vulnerable. The Food and Drug Administration has recently doubled-down to enhance cybersecurity there, albeit not always aligned with rising security concerns, such as malware or utilizing unsecured wireless devices. Yet, imagine when critical operating equipment or devices (such as anesthesia, ventilation, or pacemakers) suddenly stop working, without a shred of warning. For instance, former Vice President Cheney

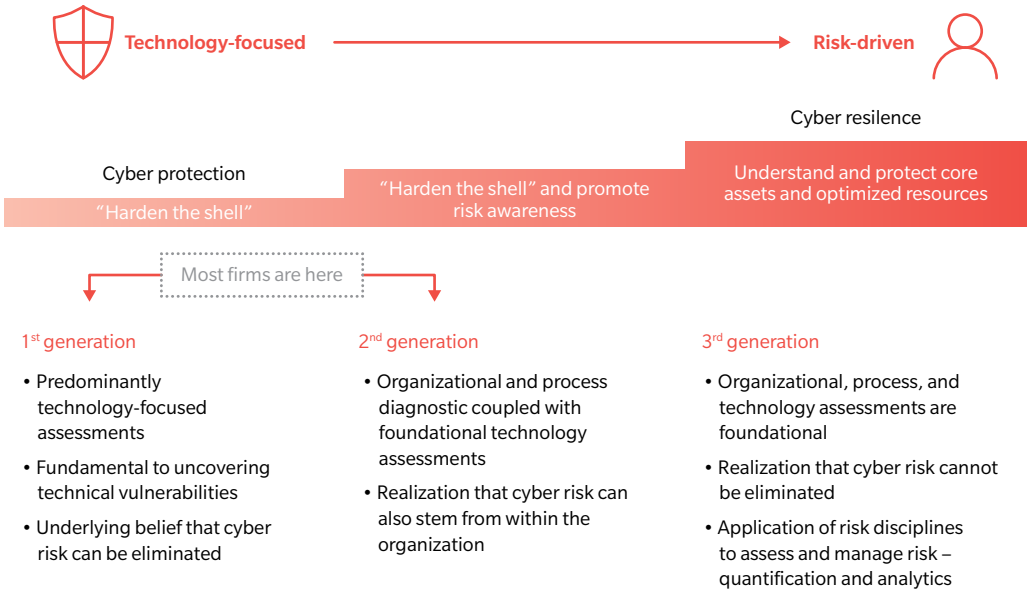
(who has survived five heart attacks and quadruple bypass surgery, for starters) had the wireless capability of his pacemaker disabled. Cheney later described this incident as a possible assassination attempt.

ROOM FOR IMPROVEMENT: CYBER RISK MANAGEMENT CHALLENGES DEMAND AN ENTERPRISE-WIDE VIEW

Responsibility for cyber risk sits mainly in technology in the minds of most. Cyber risk management in the healthcare industry is still perceived to be driven solely by the IT department. Indeed, 83 percent of healthcare respondents to the Marsh-Microsoft Global Cyber Risk Perception Survey viewed technology as the primary owners and decision-makers for managing cyber risks, compared to the 70 percent cross-industry average.

Balance is key. While the healthcare industry understands the key role of risk management teams better than other industries, it is still crucial to appropriately 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", 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 Human Resources and Public Relations also have an integral part to play in processes and communications of cyber risk management.

EXHIBIT 1: SHIFT IN FOCUS FOR CYBER RISK MANAGEMENT

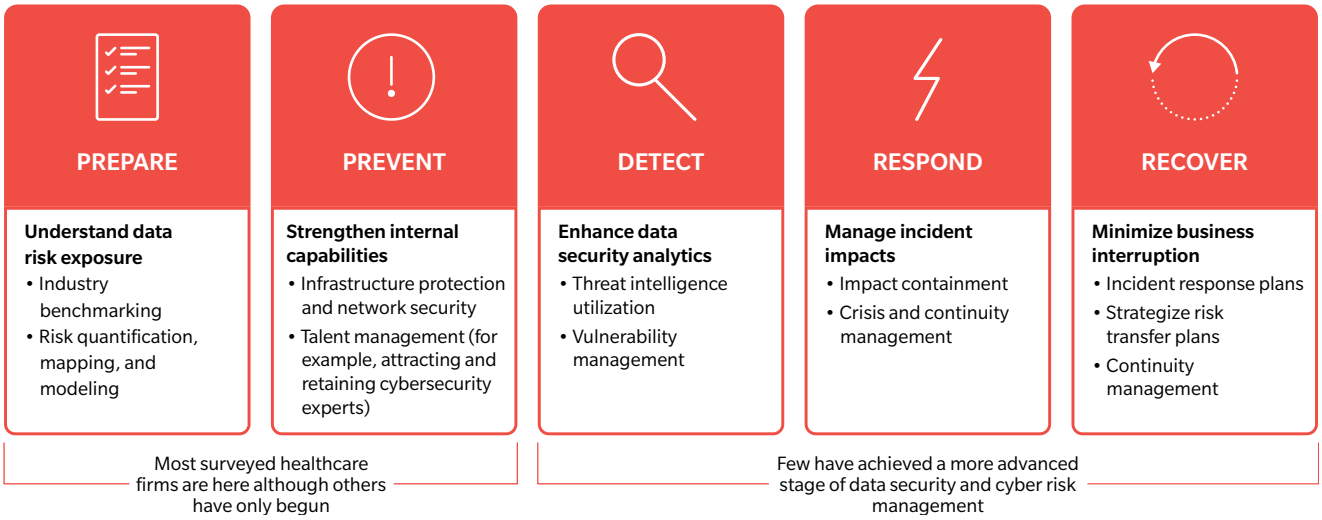


SAFETY FIRST: GETTING CYBERSECURITY ON MORE ORGANIZATIONS' RADARS

Most healthcare organizations still focus more on prevention or preparedness, instead of detection and response. On the one hand, while some proactive measures are being taken to reduce cyber risk, these are largely centered on basic preparation and prevention, like cybersecurity gap assessment, phishing awareness employee training, improved vulnerability and patch management, and encryption of company computers. On the other hand, significantly fewer organizations have a cyber incident response plan in place or have invested in improving cyber event detection.

It's important to prioritize the right skill sets within healthcare organizations to ensure technologies and securities 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 increasingly more devices and platforms.

EXHIBIT 2: FIVE KEY ACTIVITIES OF THE CYBERSECURITY FRAMEWORK AND RECOMMENDED ACTIONS



AN ALL-ENCOMPASSING DATA AND CYBER RISK STRATEGY IS FOUNDED UPON ASSESSMENT, APPETITE, REPORTING, AND EXPOSURE QUANTIFICATION.

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. Actions like these will make the next cybercrime target anyone but you.

KEY TAKEAWAYS

- Every healthcare organization needs to purposely invest in a cyber resiliency program across the lifecycle, from preparation through recovery.
- Organizations must instill a culture of cyber awareness among all stakeholders – the public, patients, and the healthcare workforce, who increasingly have greater access to medical records on more devices and platforms.
- Healthcare is a highly valuable and vulnerable industry. One copy of an electronic medical health record can be priced up to thousands of dollars on the black market, compared to a credit card number worth a quarter, or a Social Security number worth a dime.