BCG

THE BOSTON CONSULTING GROUP

BUILDING THE CYBERRESILIENT HEALTH CARE ORGANIZATION

By Ryan Goosen, Alex Asen, Stefan Deutscher, Walter Bohmayr, Karalee Close, and Ulrik Schulze

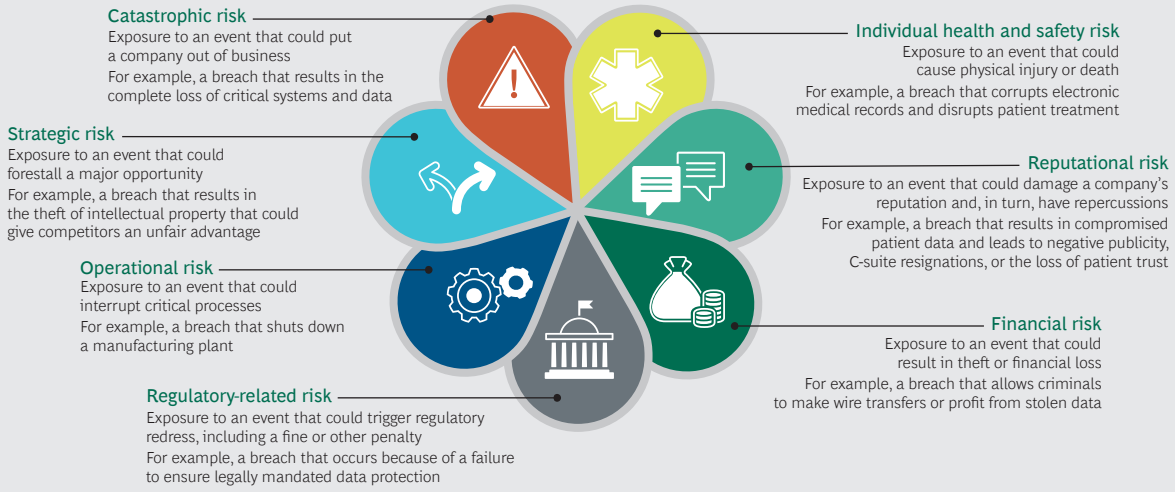
IF EVER A REAL-WORLD cyberwarning drove home the importance of cyberresilience, it was in 2017. The first came in May in the form of the WannaCry ransomware attack that seized hundreds of thousands of computer systems at companies, institutions, and government agencies globally. The second warning came over the summer, when Equifax, a US-based credit agency, was hacked and more than 145 million identities were compromised. Among the victims of the WannaCry attack were hospitals in Britain's National Health Service, many of which lost access to data and networks and were forced to turn away patients.

Fortunately, the WannaCry attack turned out to be ham-fisted in many respects. But if an amateur (or amateurs) can infect more than 200,000 computer systems in a matter of days, and more competent professionals can steal more than 145 million identities over a few months, what do such threats suggest for the malicious abilities of cybercriminals who target health care companies and institutions?

The cyberrisks to the health care industry include much more than ransomware and threaten more than hospitals. Imagine a WannaCry type of attack that targets implanted medical devices, for example. The digitization of health care, which is bringing more digital products and services into more widespread use, puts health care organizations in the cybercriminal's cross hairs. Moreover, because of the data that health care companies collect, the life-and-death nature of their services, and the increasing interconnectivity of tools and devices, cybersecurity is no longer only an IT issue (if it ever was only an IT issue). The potential for strategic, reputational, operational, financial, and regulatory-related risks, as well as individual risk, elevates cyberresilience to the C-suite and the boardroom. (See Exhibit 1.)

All kinds of companies and institutions are vulnerable. A 2016 study by the Ponemon Institute found that, in the previous two years, almost 90% of health care organizations had had a data breach and 45% had had more than five. Ponemon pegged the

EXHIBIT 1 | Cybercrime Poses Serious Threats to Organizations



Source: BCG analysis.

cost to the industry at more than $6 billion. The institute's 2017 data found that the average cost per compromised record in health care approached $400, far more than the cost in any other sector. The question is, are pharma and medtech companies, providers, and payers ready to take the steps that are necessary to turn themselves into cyberresilient organizations?

As we wrote earlier this year, companies can't afford to focus their security efforts solely on their ability to ward off cyberattacks and expect this strategy to fully protect them. (See "Building a Cyberresilient Organization," BCG article, January 2017.) Instead, they must ramp up their resilience—the ability to function during and after a breach and to recover effectively after even a serious security lapse. Building resilience requires marshaling the resources of the full organization; setting priorities and ensuring follow-through needs leadership that comes from the top.

Vulnerabilities Throughout the Sector

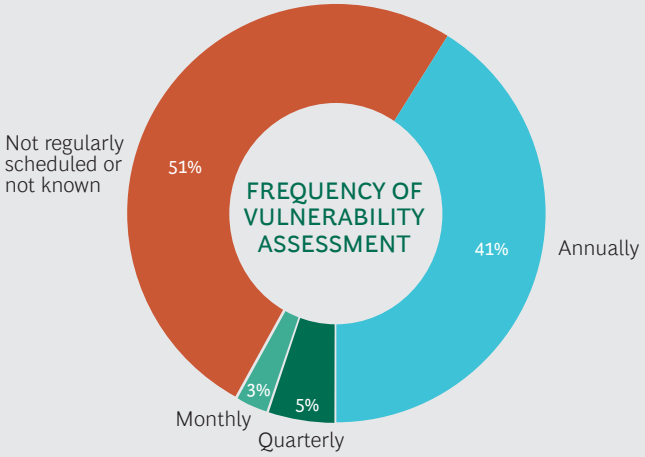
In the health care industry, the nature and type of cyberrisk—and therefore the preparatory steps necessary to strengthen cyberresilience—vary by segment. However, very few organizations conduct frequent checks in order to determine their cybervulnerabilities. (See Exhibit 2.) As a result, all major segments are exposed.

Pharmaceutical Companies. Technology and data—including proprietary R&D data and other highly sensitive information, such as material related to patients, drugs, and trials—have become integral to multiple aspects of the pharma industry. Although they provide enormous value to patients and providers with regard to drug usage, outcomes, and safety, digital technology and information can also attract criminal interest and intent from numerous parties, including nation states and organized crime groups. At least one criminal group, known as FIN4, is thought to be compromising health care companies, particularly in the pharmaceutical segment, by accessing nonpublic information that could affect share price (such as M&A plans) and then trading in these companies' stocks prior to an announcement.

The potential for damage goes beyond financial malfeasance: as supply chains, manufacturing processes, and distribution channels become increasingly digitized, often with outdated devices that have limited vendor support or security management, they present a sabotage risk with potentially disastrous patient health and safety, financial, and reputational consequences. Proprietary digital health software, smart

EXHIBIT 2 | Few Organizations Frequently Assess Their Vulnerabilities

More than 90% of health care organizations fail to conduct frequent vulnerability assessments, yet management needs a clear understanding of its risks before it can take effective corrective action



Sources: Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data,* May 2016; BCG analysis.

devices, and digital health products (such as implants, drug-dispensing wearables, and digital therapeutics) are becoming increasingly important competitive playing fields.

Medtech Companies. More and more medtech equipment is being connected to smart ecosystems that provide greatly expanded functionality—and introduce a host of vulnerabilities and risks. The exposures extend all along the supply chain, which for many companies is global. Software security experts have revealed vulnerabilities in an array of widely used medtech equipment that open these devices to a broad variety of attacks—with potentially life-threatening prospects. Even surgically implanted or daily-use medication devices that can be accessed by remote mechanisms are susceptible to exploitation. In August 2017, the US Food and Drug Administration issued a recall for almost 500,000 radio-frequency-enabled pacemakers because of its concerns that the devices could be hacked, leading the manufacturer to release a firmware update to address the vulnerability. Designing and building cybersecurity into smart devices is essential to the future of the medtech segment.

Providers. For hospitals and clinics, technology is a key enabler of improved service provision and care, cost effectiveness, workforce efficiency, competitive advantage, and patient safety. This expanding role means cybersecurity is no longer a matter of simply protecting the IT infrastructure. The concern now encompasses safeguarding a sea of digital devices and tools, posing an assortment of significant challenges. Consider digital drug-dispensing machines, for example, which help increase safety for patients and efficiency for pharmacists but are also vulnerable to interference by cybercriminals. One critical need is to effectively coordinate security for these and other devices despite the wide variety of cybersecurity configurations set by manufacturers and users.

Similarly, from a data perspective, digital medical records not only provide a consolidated and easily accessible source of vital information for medical professionals but also present a high-value target to criminals. As the WannaCry attack demonstrated, digital records can be held hostage—or vandalized. Digital records are also potential targets for theft and tampering. Records connected with clinical trials are valuable targets for competitive intelligence; indeed, clinical trial sponsors may increasingly require a demonstration of a hospital's or clinic's cybersecurity program as a prerequisite for participation in trials.

Payers. Health insurers have built massive data collection and storage systems, which

are increasingly important to controlling costs, combating fraud, providing effective and competitive reimbursement services, and using advanced analytics to anticipate patient and provider needs and improve service. Although providers have been more frequently breached than insurers, payers' systems are prime targets for cybercriminals. In 2015, breaches at three big insurers resulted in the theft of almost 100 million records. More than 60 payers were hacked in 2016.

It's little wonder that the bad guys target payers: black market prices for digital records with personally identifiable information and sensitive medical data can range from $200 to $2,000 for a single complete record. By comparison, a stolen credit card record brings only $10 to $40. And as payers develop new digital services and use digital channels more frequently, they become more exposed to a whole new set of risks, such as criminals sabotaging otherwise credible customer communications by embedding malicious links or stealing customers' app credentials in order to file fraudulent claims.

An Issue for the C-Suite

Because cybersecurity and cyberresilience can affect interactions between an organization and its customers, patients, regulators, and service providers in so many ways, these issues are important additions to top management's competitive-advantage and risk-management agendas. Some organizations have established board-level oversight. As the World Economic Forum pointed out in a 2017 report, "Being resilient requires those at the highest levels of a company, organization or government to recognize the importance of avoiding and proactively mitigating risks. While it is everyone's responsibility to cooperate in order to ensure greater cyber resilience, leaders who set the strategy for an organization are ultimately responsible, and have increasingly been held accountable for including cyber resilience in organizational strategy. For businesses, this means that cyber strategy must be determined at the oversight board level."[1]

The Forum's report details a set of principles and tools that are specifically designed for boards and C-suite executives. The tools include questions that facilitate a dialogue with business units to bring about action, a cyberrisk framework to ensure that security measures are integrated into the overall risk management framework, and enablement activities and training sessions to bring boards up to speed on emerging technologies and associated risk profiles. A handful of health care companies are using tabletop exercises that include cyberattack simulations to build organizational awareness and capability. When combined with the tools detailed in the report, such exercises can fundamentally strengthen an organization's readiness for, and capability for dealing with, a cyberattack.

Segment-Specific Steps

In addition to having generally good cyberhygiene, companies in different segments of the health care industry can take specific steps to improve security and strengthen resilience.

Pharma and Medtech Companies. These companies should actively consider cybersecurity's role in the value chain, which comprises corporate strategy, R&D, production (including outsourced production and providers of procured parts), operations, and medical and digital health teams.

With respect to corporate strategy, for example, management should evaluate the organization's cyberresilience and cyberrisks within a comprehensive risk management framework. Cyberresilience awareness should be incorporated at all levels of the enterprise and across all operations. Management should consider expanding the responsibilities of its risk committee to include evaluating and addressing cyberrisk. Management should also formalize the board's cyberrisk responsibilities. Cyberrisk should be a standing agenda item for board meetings, with regular briefings from the chief information security officer (CISO). The board should review the organization's strategic plan and approve the

operating budget for cybersecurity and key cybersecurity strategic priorities.

In R&D, cybersecurity should be a top consideration in all stages, including the software and hardware design stage of digital health products and services, the development and implementation stage, and the life cycle planning stage. Ensuring the security of digital components over a lifespan of ten years or more, a time by which there will be no security support for many of today's commercial operating systems, is a challenge many companies have yet to address. Companies should also make sure that CISOs or cybersecurity professionals have a seat at the R&D table or are assigned to work with digital innovation-specific or cross-functional project teams. If product developers look at security as a nuisance as opposed to a lifesaver, both the common good and the business foundation of their company will be at risk.

Pharma and medtech companies should conduct cybersecurity health checks in key areas, such as manufacturing (particularly assessing the integrity, accountability, and traceability of data, devices, and device components) and the supply chain. Companies should also assess the cultural readiness of the organization to respond to a cyberattack. Incident response exercises and emergency simulations are effective vehicles for making sure that the organization is well prepared.

Commercial teams increasingly conduct business using digitized processes, mobile devices, and cloud-based services, such as customer relationship management programs, that bypass in-house IT. Companies need to ensure that cybersecurity best practices are well integrated into the ways that people work and interact with each other (internally and externally) as well as into the technology used by employees at all levels.

Providers. Infrastructure (including technology and data availability) is crucial to care provision, patient well-being, efficiency, and regulatory compliance. Data and device integrity, accountability, and traceability are also increasingly important to providing health care. Devices connected to the Internet of Things are of particular concern if they have controls with immature security features. Cybersecurity should be a key priority for hospitals and clinics, but it does require a significant commitment of management's and staff's time and an organization's financial resources.

Providers can start by conducting a health check of all categories of devices used to provide care in the ward, the intensive care unit, and surgical theaters. Regular tabletop exercises that focus on an organization's reaction to, and recovery from, potential cyberincidents (such as when hackers cause critical care devices in an operating room or intensive-care unit to malfunction or stop working and then demand ransom) will help ensure readiness.

Payers. Patient data is a big-time target. Payers that have not yet done so should conduct a full audit of corporate risk management policies and procedures to ensure adequate protection against identity fraud and theft. They should pay particular attention to the protection of identifiable personal information. Payers should also review cybersecurity's role in data integration practices as well as in analytics services, especially if third parties are involved. Going forward, cybersecurity needs to be a key element during the design, development, and implementation of patient-facing digital services. As in other types of health care organizations, health checks, tabletop exercises, and incident simulations will help payers explore how ready they are for a leak, a data-tampering incident, or the theft of patient data.

A century ago, criminals robbed banks because that's where the money was. Today's cybercriminals look at the health care industry in a similar light. Unlike the bank robbers of the past, cybercriminals can take many forms, strike from anywhere, and exploit any number of vulnerabilities. In today's environment, building a cyberresilient health care organization is

essential to both patient and institutional well-being. The ability to provide digital health products and services with built-in cybersecurity is also critical to competing in all segments of the increasingly digitized health care sector.

NOTE

1. *Advancing Cyber Resilience: Principles and Tools for Boards,* a World Economic Forum report, produced in collaboration with The Boston Consulting Group and Hewlett Packard Enterprise, January 2017.

About the Authors

Ryan Goosen is a consultant in the Zurich office of The Boston Consulting Group. You may contact him by email at goosen.ryan@bcg.com.

Alex Asen is a senior knowledge analyst in the firm's Boston office. You may contact him by email at asen.alex@bcg.com.

Stefan Deutscher is an associate director in BCG's Berlin office. You may contact him by email at deutscher.stefan@bcg.com.

Walter Bohmayr is a senior partner and managing director in the firm's Vienna office. You may contact him by email at bohmayr.walter@bcg.com.

Karalee Close is a partner and managing director in BCG's London office. You may contact her by email at close.karalee@bcg.com.

Ulrik Schulze is a senior partner and managing director in the firm's Zurich office. You may contact him by email at schulze.ulrik@bcg.com.