How Health Care Providers Can Thwart Cyber Attacks

APRIL 20, 2021

By Michael Coden and Mike Czumak

> Five quick proven steps can secure patient information, protect intellectual property, and reduce the risk of a shutdown.

The number of cyber attacks on US health care systems has reached epidemic proportions. According to the Protenus Breach Barometer, in 2020 hackings jumped 50%, affecting more than 41 million patient records. COVID-19 has played no small role in the surge, as cyber criminals take advantage of the fact that more people are working from home on insecure devices and are focused more on protecting their health than on maintaining cybersecurity.

Left unchecked, cyber attacks can do incalculable damage to health care providers. Personal health information (PHI) and pharmaceutical research intellectual property are at risk, as is a hospital's ability to deliver health care services.

To stem the tide, we recommend that health care provider systems and hospitals pursue a small number of key actions immediately, from assessing the risk of breaches to conducting tabletop simulations. At the same time, organizations should take steps to ensure a secure cyber environment for the long term.

KEY CYBER ATTACK CONCEPTS

Health care providers and hospitals should focus on six primary threats:

- **Hacking.** The term "hacking" is often used to refer to a security incident that occurs when a cyber attacker finds their way into a system by exploiting a vulnerability or misconfiguration in the software or system. The hacker then uses this access to reach a desired target, such as systems housing a hospital's intellectual property or PHI, to exfiltrate data or implant malware that could disrupt healthcare operations.
- **Phishing.** With phishing, an actor sends an email with a link to a member of the hospital community, such as a physician. When the recipient clicks on the link, they are tricked into providing a user ID and password, which gives the actor access to hospital systems. Phishing attempts have proven particularly successful during COVID-19 because people are more apt to click on links when the email has an emotional urgency, such as a notification that a relative is in the hospital or an offer for a vaccine appointment.
  Phishing is often a leading precursor or contributor to significant security

incidents because of its low cost of entry and wide-reaching potential. It's often easier to get results from sending a phishing email to thousands of people than it is to find a single exploitable vulnerability in an organization's systems or network.

- **Malware.** Malware, or "malicious software," is often delivered through phishing (and executed by an unsuspecting user). Alternatively, it can be installed by a threat actor who has gained unauthorized access to an organization's systems or network. Frequently, an attacker uses malware to repeatedly access a hospital's network and systems, whether to exfiltrate valuable IP or PHI or to disrupt the hospital's ability to provide patient services.

  There are different types of malware. Ransomware is a type that attackers use to both steal information and disable hospital systems, relinquishing control only when the hospital pays up. Cyber criminals use ransomware primarily for financial gain.

- **Espionage.** Cyber espionage, or spying, is the act of gathering information without the knowledge or permission of the holder of that information. A nation state stealing pharmaceutical research data on COVID-19 vaccines is a good example.
- **Compromised Accounts.** Any account that is being used illegally—whether through stolen, guessed, or brute-forced passwords, phishing, or malware—is considered compromised. A security incident typically involves the abuse of a privileged account—that is, a legitimate user's system or network account and access rights. An unrevoked account (one that was not deleted when the user left the hospital community) is another way for hackers and disgruntled employees to gain access to hospital systems.
- **Unauthorized Data Disclosures.** Unauthorized data disclosures are another prevalent risk. This issue is particularly vexing in the health care industry, where safeguarding access to sensitive patient and research data is a

fundamental part of an employee's job. Such disclosures can occur accidentally, such as when a well-intentioned researcher mistakenly includes sensitive information in a publication or when a clinician uses an unsanctioned or insecure method of data storage or transmission out of convenience. Loss and improper disposal of hardware such as laptops, servers, and thumb drives is another reason accidental disclosures occur. Unauthorized disclosures can also be intentional, as in the case of device theft or the actions of a disgruntled employee.

FIVE STEPS TO TAKE IMMEDIATELY

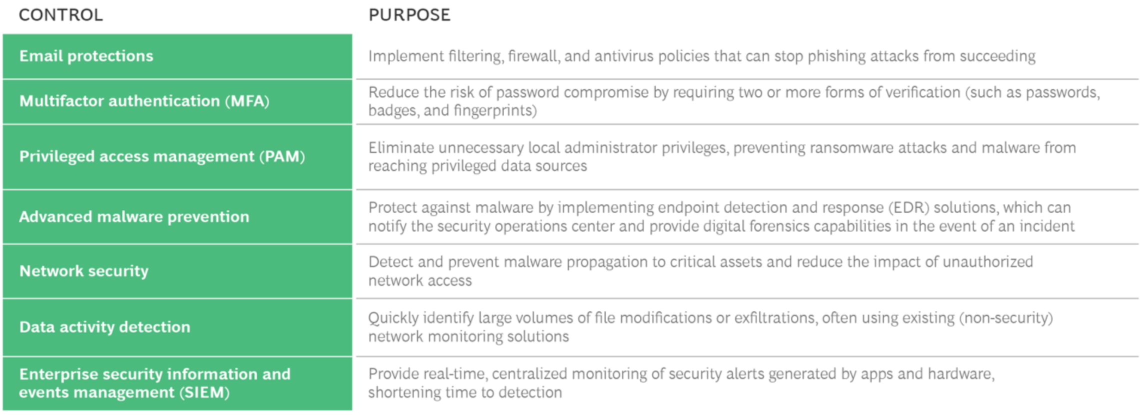
Given the urgency of the situation, health care providers and hospitals need to improve their cybersecurity at once. Five essential steps are key:

- **Determine and prioritize the most critical data and cyber-physical assets.** Organizations should quickly assess which assets are the most essential and focus on protecting them first. Assess which threats (such as malware, espionage, or unauthorized data disclosure) are most likely to be successful against each critical asset and use that analysis to determine which mitigation actions should take priority.
- **Assess the risks and determine the key actions for reducing them**. When considering each threat, it's useful to think of the chain of events that must occur in order for it to be successful (for example, phishing must be followed by account compromise, then malware propagation, and so on). The next step would be to focus mitigation efforts on the weakest or most impactful links in that attack chain.

Perhaps strong phishing controls are in place, but malware prevention capabilities need to be bolstered. Segmenting or isolating critical assets on your network may also be an effective strategy. Since no one control is ever 100% effective, it's important to put in place multiple layers of controls that can interrupt the attack chain of events in as many places as possible.

Memorial Sloan Kettering Cancer Center (MSK) has implemented a number of technical controls to address each step of a ransomware or malware attack. Other hospitals can similarly adopt these actions, which include (among others) email protections, multifactor authentication (MFA), privileged access management (PAM), advanced malware prevention, network security, data activity detection, and enterprise security information and events management (SIEM). (See Exhibit 1.)

Exhibit 1 - Addressing Each Stage of a Ransomware Attack



CONTROL	PURPOSE
Email protections	Implement filtering, firewall, and antivirus policies that can stop phishing attacks from succeeding
Multifactor authentication (MFA)	Reduce the risk of password compromise by requiring two or more forms of verification (such as passwords, badges, and fingerprints)
Privileged access management (PAM)	Eliminate unnecessary local administrator privileges, preventing ransomware attacks and malware from reaching privileged data sources
Advanced malware prevention	Protect against malware by implementing endpoint detection and response (EDR) solutions, which can notify the security operations center and provide digital forensics capabilities in the event of an incident
Network security	Detect and prevent malware propagation to critical assets and reduce the impact of unauthorized network access
Data activity detection	Quickly identify large volumes of file modifications or exfiltrations, often using existing (non-security) network monitoring solutions
Enterprise security information and events management (SIEM)	Provide real-time, centralized monitoring of security alerts generated by apps and hardware, shortening time to detection

Sources: Memorial Sloan Kettering Cancer Center; BCG analysis.

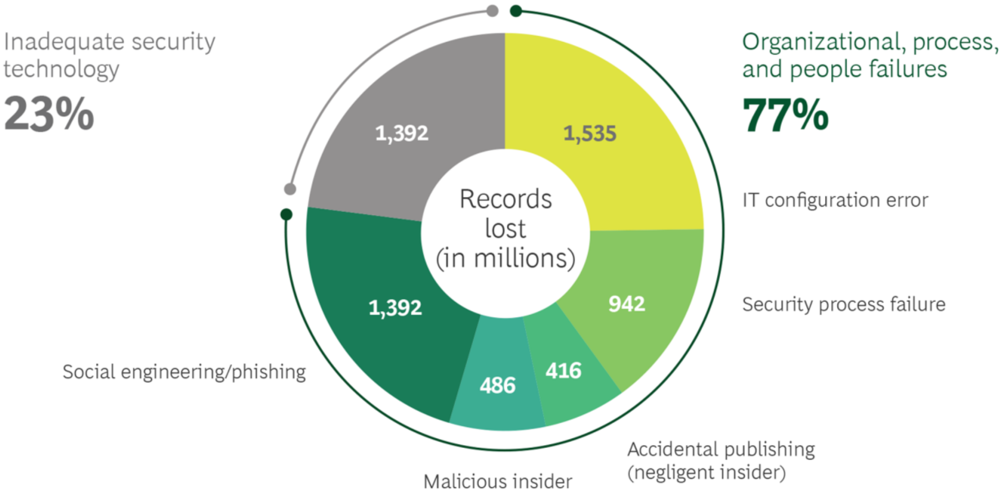
It's equally important to conduct a risk assessment for espionage threats. While this analysis may overlap somewhat with a ransomware assessment, there's a key difference: Ransomware tends to be very easy to detect, because it generates a great deal of "noise"—in other words, network traffic and disk access, which are easy to pick up in a security operations center that uses a SIEM system.

By contrast, espionage is very quiet. Cyber espionage attackers patiently and slowly exfiltrate the valuable information they are seeking because they don't want to be noticed by generating network and disk traffic. So depending on your threat profile, more controls may be required, such as additional layers of cyber protection and special training for researchers.

Depending on the threat, there may be many other layers of controls that an organization will want to consider (data loss prevention (DLP) software, encryption, and so on), but there may be competing priorities and resource restraints to deal with. Taking into account existing controls and using a risk-based approach can help hospitals determine which processes, procedures, and technologies to invest in for the greatest reduction in cyber risk.

- **Educate and render risky employee cyber behaviors "irrelevant."** BCG analysis found that 77% of all cyber attacks are due to human failures and only 23% to tech glitches. (See Exhibit 2.) Consequently, it's paramount for hospitals to assess behaviors that put health care systems at risk and make those behaviors "irrelevant" so that employees default to more-secure behaviors.

Exhibit 2 - Most Security Breaches Are Due to Human Failures



Source: BCG analysis of 50 major data breaches, February 2021.

But getting employees to adopt different behaviors is difficult. Many users are simply looking for the quickest and easiest way to get their job done. Rather than outright prohibiting things like collaboration or file sharing, hospitals should consider providing securely configured and managed enterprise solutions like Box, Office 365, G-Suite, or Slack, which can help reduce the use of personal accounts while putting the necessary oversight and risk reduction controls in place. Additionally, technical safeguards like disabling unsigned macros and sandboxing (separating apps from critical resources) can mitigate the fallout from users opening attachments or clicking malicious links.

While technical controls are key to a robust risk mitigation strategy, they are not a replacement for a strong culture of security awareness. It's critical both to show employees why cybersecurity is as vital as safety and ethics and to teach them how to avoid causing an incident in the future. In addition, hospitals should consider not only punishing risky behavior but also acknowledging and rewarding good security practices. MSK has implemented a security awareness program that leverages activities such as formal training, webinars, office hours, contests, and organization-wide phishing assessments.

- **Develop crisis management and cybersecurity incident response teams.** Significant incidents will require the participation of stakeholders from across the organization. Many hospitals have both a multidisciplinary crisis management team (CMT) and a cybersecurity incident response team (CSIRT) that are responsible for directing the two major aspects of such efforts. The CSIRT should deal with the actual cyber attack as well as restoring systems, assessing impacts, and implementing business continuity plans. The CMT should coordinate the activities of external forensic analysis, public relations, and legal experts. And it should manage internal and external cybersecurity communications so that employees, patients, the public, law enforcement, regulators, and the hospital's management, trustees, and board of directors are kept up to date. Coordination between these two teams is essential. At MSK, they are combined into one team called the hospital incident command (HIC).

Developing the necessary playbook and response plan is also essential. Like MSK, many hospitals already have an incident command team that responds to significant events. Instead of creating a completely new team, organizations may prefer to develop response plans that leverage the processes, participants, and command structure of the existing group. Cyber events may require additional participants and workstreams, but using familiar, well-tested procedures can ensure a more seamless response.

Conduct tabletop exercises (TTXs). Very few cyber incidents follow a script, of course. Nevertheless, it's important to test all plans well in advance of any incident. As part of this testing, a hospital should conduct TTXs so that senior executives, the CMT, and the CSIRT can develop the necessary knowledge and muscle memory to respond effectively in the event of an attack, when they could have only a few seconds to make decisions. They can use the opportunity to learn about restoring backups, contacting law enforcement, issuing press releases, and ensuring continuous patient care operations.

> “
>
> Few cyber incidents follow a script, of course, but it's still important to test all plans well in advance.

This also means that hospitals need to determine ahead of time who should have the authority to make monumental decisions, such as shutting down the network. It's essential to delegate this authority to someone who can make those decisions without fear of recrimination. And everyone on the CMT and the CSIRT should have at least one delegate with full authority to act in their absence.

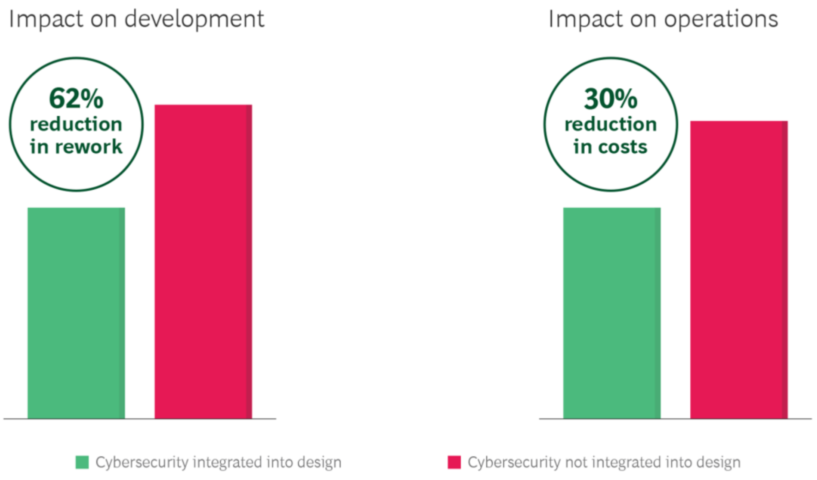
Conducted properly, these TTXs will uncover gaps well before an incident occurs.

SECRETS TO LONG-TERM SUCCESS

To ensure their systems are protected by cyber threats over the long haul, hospitals need to consider six strategic imperatives:

- **Design cybersecurity measures into systems from the start**. There are clear advantages to designing cybersecurity into systems at the beginning of a digital transformation rather than adding it later on. Designers are able to move faster when they know a system is secure. There's also less need for expensive rework—and less risk of introducing new errors. Shorter development times also allow a hospital to generate revenue faster. (See Exhibit 3.)

Exhibit 3 - Designing Cybersecurity into Systems Up Front Saves Time and Reduces Costs



Source: BCG analysis.

This approach also makes it easier to design secure software in a uniform way across the entire organization. Not only will development costs will be lower as a result, but operating costs will be, too, since operations and maintenance processes are the same for many applications. Training costs will also be lower, and security and operations teams will be more efficient and effective.

- **Ensure continued IT system hygiene and governance.** What is secure today may not be tomorrow. So rapid implementation of security patching, system upgrades, and other "IT hygiene" practices are key. To reduce the scope of overall risk, we recommend data and IT governance practices that will ensure an accurate system and data inventory, enforce life cycle management, and minimize the duplication of data and IT investments. These activities should be validated by regular vulnerability scanning and penetration testing.

- **Map the cybersecurity strategy to the business strategy.** Many organizations design cybersecurity to protect their systems today, while the board is focusing on five years from now. To be sure, it's important to aim mitigation efforts at the most critical risks being faced in the present—especially if the hospital in question is just starting to implement a security strategy. But it's also important to develop a cybersecurity program that will accommodate future-state business strategy, such as plans to expand into new markets or different therapeutic areas. Doing so can save costs down the line.

> "
>
> Developing a cybersecurity program that will accommodate future-state business strategy can save costs down the line.

- **Scale systems safely and cost-effectively.** As hospitals increasingly move from the physical realm to the digital, they will need to scale and grow their digital systems. Since building data centers is an expensive and time-consuming way to get more computer capacity and data storage, we recommend partnering with public cloud service providers instead. Moving to the cloud is the best way to scale, provided organizations take the steps we are advocating in this article.

- **Assume an attack is inevitable.** Since it's virtually impossible to provide 100% protection against a cyberattack, incident response, business continuity, and data backup and recovery plans are critical for minimizing impact. When it comes to selecting cybersecurity projects to invest in, hospitals need to be able to quantify the risk of a successful attack and the effect such an attack could have. They can then select the most appropriate portfolio of projects. Monte Carlo simulations can help identify which initiatives might provide the greatest reduction in cyber risk for any given amount of spending.

> “
>
> When it comes to selecting cybersecurity projects to invest in, hospitals need to be able to quantify the risk of a successful attack and the effect such an attack could have.

- **Prepare for simultaneous disasters.** All hospitals know that business continuity and disaster recovery plans are critical for mitigating the impact of cyber attacks. Most hospitals have emergency response plans for each type of disaster: natural, cyber, active shooter, and so on. But it’s key to have plans that can handle more than one emergency at the same time—a cyber attack, a hurricane, and a pandemic, for example. Tabletop exercises are the best and most cost-effective way to test these plans out. Waiting until a real situation occurs can be very costly.

As the pandemic has so vividly demonstrated, health care provider systems and hospitals need to make cybersecurity a top priority today. The health and well-being of the patients they serve depend on it.

Authors

Michael Coden
Managing Director, BCG Platinion
New York

Mike Czumak
Chief Information Security Officer, Memorial Sloan Kettering Cancer Center

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting Group on Facebook and Twitter.