Supporting a Cyber-Resilient Health Care Organization

To maintain operational and financial viability, cyber-vulnerable health care organizations need to become better-prepared and more resilient against attack. This means having in place not only the right technology, but also proper governance, policy, processes, and education to help prevent a cyberattack.

Living in California, we are well-aware of natural threats like earthquakes which can potentially wreak havoc on a health care organization. California hospitals are spending billions to ensure they can remain operational after a major earthquake and meet the 2030 seismic mandate passed after the 1994 Northridge earthquake. Today, health care organizations are faced with another growing threat – cyberattacks – which can be equally disastrous to the ill-prepared.

Like earthquakes, cyberattacks can happen any time and the damage can range from minimal to several millions of dollars, depending on the nature of the attack and the vulnerability of the involved organization. Yet unlike their expenditures against earthquakes, many health care organizations spend just 1-2% of their annual IT budget on cybersecurity — or safeguarding their computer networks and data from penetration and accidental or malicious disruption.

To maintain operational and financial viability, cyber-vulnerable health care organizations need to become better-prepared and more resilient against attack. This means having in place not only the right technology, but also proper governance, policy, processes, and education to help prevent a cyberattack.

How Real is the Threat?

The threat of a cyberattack against any health care organization is very real. Breaches of unsecured protected health information involving 500 or more individuals are tracked nationally by the Department of Health and Human Services Breach Portal, which has recorded more than 400 such incidents within the past year. For example, in 2019, a Montana health care provider suffered a data breach potentially exposing the health care information of 140,000+ patients.

Cyberattacks in health care are typically aimed at accessing, changing, or destroying sensitive data; extorting money; and/or disrupting normal business operations. According to the 2019 HIMSS Cybersecurity Survey, the most prevalent cyberattack method is phishing, in which the perpetrator sends an e-mail to an unwitting health care employee. The phishing e-mail is opened, spreading malicious software across the enterprise. The perpetrator then holds the institution's data hostage in exchange for money.

Health care organizations are particularly targeted because they house private health information and potentially valuable financial and clinical information. Such information is prized on the black market and can be used to create stolen medical identities for fraudulent purposes (e.g. filing claims, obtaining prescription medications). In addition, health care systems integrated with multiple third parties and medical devices often have security flaws which hackers can exploit. On average, there are 10 to 15 e-connected devices per bed in U.S. hospitals, leading to increased access points. In addition, because health care providers are mainly focused on keeping patients healthy, they are often less attuned to data security.

Addressing the Problem

1. Embrace Internal Phishing Campaigns

Health care IT departments are generally good at implementing technology to filter and scan e-mails for malicious intent. However, some potentially harmful e-mails can still make their way to users' inboxes. All it takes is one user's click on a malicious link to infect an entire system. This is where the human firewall – employees following best practices to report and prevent data breaches or suspicious activity — is your last form of defense.

To ensure staff compliance with cybersecurity measures, many organizations regularly conduct phishing security tests to raise staff awareness and gauge which employees need training. Conducted properly, phishing security tests have proven effective in reducing employees' unwarranted clicks on malicious links or attachments.

The key to success for such campaigns is ensuring your leadership supports the effort. The spirit of the campaign should be educational versus punishment. That said, the campaign should be tracked for problematic departments or individuals to ensure complete compliance. Create competitions and reward staff for keeping the organization resilient to cyber threats.

2. Treat Cybersecurity as a Patient Safety Issue

Clinicians will sometimes reference "patient safety" as a trump card to obtain a particular desired outcome regarding operations. In the case of cyberattacks, the issue is undeniably tied to patient safety. A denial-of-service cyberattack could render a critical clinical system inaccessible, stifling a provider's ability to diagnose or treat a patient appropriately.

Incorporate cybersecurity as part of patient safety, and change perception from "it's an IT issue" to "it's a patient safety issue." If you lead or participate in patient safety meetings, ensure cybersecurity is incorporated in discussion. Partner with IT to learn of recent threats and how they were mitigated, and share the incidents with staff who are often unaware of such threats. The sample incidents can be from other organizations. What's important is raising awareness, because technology alone will not solve the problem. The human firewall is equally important.

3. Don't Become Complacent; Work as a Team

Just as health care is ever-changing, so is the nature of cyberattacks. Solutions for today's threats may not work in the future. Thus, continually partner with IT, compliance, risk management, legal, HR, and other pertinent departments to work as a team to develop and implement your cyber-resilient strategy.

For example:

- Support IT's security risk assessments of new devices and services; your desire to use what's new should not supersede your organization's foundational cybersecurity measures.
- Work with your legal department as you build a virtually integrated enterprise. For example, smaller partner organizations such as skilled nursing facilities may not have the same level of cybersecurity resources as your organization, but should still follow your cybersecurity policies.
- Work within your incident command system to ensure cyberattacks are included in planning as well as in regular drill exercises. Knowing and practicing in advance who will make critical decisions (e.g. will a ransomware demand be paid?) and how information will be communicated will reduce chaos if an attack occurs, and potentially lead to faster recovery.

Conclusion

The growing threat of health care cyberattacks will likely hit hardest on those who are unprepared or ill-equipped. Nowadays, a cyberattack is not a question of "if" but "when." Allot sufficient cybersecurity resources, policies, practices and training to help prevent or minimize a cyberattack on your organization.

