DOTmed HealthCareBusiness news

An effective cybersecurity policy starts with a well-trained hospital staff

February 16, 2018

From the February 2018 issue of DOTmed HealthCare Business News magazine


Seana-Lee Hamilton

HealthCare Business News recently spoke to Seana-Lee Hamilton, manager of information privacy and privacy officer at Fraser Health Authority, regarding cybersecurity and the need to maintain patient privacy and protect health care information.

HCB News: What are the major cybersecurity threats that health care organizations face right now?

Seana-Lee Hamilton: The most significant threat to cybersecurity and patient privacy is literacy of users, making sure they understand the need for safeguarding patient data and protecting the hospital's network. BYOD and staff properly using the hospital's network are among the greatest issues facing cybersecurity professionals in hospitals today. Whether it's employees accessing their Facebook page or checking their personal web mail, or plugging in their own USB memory stick, they're introducing network threats and making the hospital, its staff and their patients significantly more vulnerable to the ugliness of a cyber event. BYOD initiatives need to be rolled out utilizing best practices in technology, user terms of use and corporate policy. Hospital policies have allowed these sort of things, and now we need to review policies and probably create new ones that will both allow people some privileges when they're working, but seal contain or entirely close off vulnerabilities that come with a BYOB environment.

From another literacy-level view, one of the biggest areas we can't control is phishing, and this is how many ransomware attacks and other items are originating. Employees must understand how phishing works and how their actions affect the network. A basic understanding starts with emphasizing that the service desk will never ask you for your user ID and password.

Health care is different and more vulnerable to cyber events because of the advanced technical tools utilized, including diagnostic and imaging tools, as well as biomedical equipment. For instance, our medical imaging equipment, our CT scanners and our MRI machines are all very advanced, technical units, and the technology involved affords a vulnerability, and thereby, must be strategically checked.

Health care organizations must have policies and assessments in place for patches and security upgrades for clinical information systems and EHRs. Security and privacy professionals must look at these systems and ensure all necessary security upgrades are complete.

These systems also introduce the insider threat to protecting patient data. Hospitals must know who is accessing patient data and why. Auditing patient data access is the only way to truly understand how patient data is being accessed, providing an opportunity to better protect that data. To get a true look at this data, technology must be implemented. We use Security Audit Manager from Iatric Systems to show us a clear picture of how patient data is being accessed, so we can properly address any issues.

HCB News: What cybersecurity strategies has your health care organization been focusing on in the last year?

SH: The past year, which has been a major reality check for the health care industry, has made us honestly assess our vulnerabilities so we understand our risks. After this assessment, we created an action plan and timeline for fixing risks or any other identified issues. We have also worked on making sure we are adequately staffed from cybersecurity and privacy perspectives.

We also conducted a cybersecurity audit and are now looking at creating a cybersecurity response team. This team would look at incidents to determine if they are cyber in nature, and who needs to respond, with the ultimate goal of containing any breaches. Through this team, we would also evaluate how privacy comes into play in our cyber response, and how to determine if a breach occurred. Our assessments show how our response plan must go even deeper to include questions such as who do we key up from our media people, how do we involve the quality care office, what is the role of administration and other key factors. It is quite an undertaking, and why we are evaluating the need for a cyber response team.

We know it's not a matter of if a breach happens, but when, and we must be organized and understand how we will address these things when they do happen. It must be an organizational plan, not just privacy or just security. We know personal health information is the most valuable information on the black market, meaning privacy should always be involved, but we also must consider what role we play in touching the data forensically. We want the right people touching and analyzing the data.

HCB News: Have you encountered any challenges in implementing those strategies? If so, how did you overcome them?

SH: To be honest, the answer is no. Maybe it's because of the times we're living in or the numerous incidents happening to organizations of all sizes and types accompanied by backlash and other issues. Our organization leaders are understanding that time is beneficial for both being prepared and in terms of responding. We have received total buy-in from everyone in the organization, including the administration and the board. This is a great development, as the trust demanded from patients must come from the top down. Our board and executives are buying in, and wanting to know more as they're seeing the backlash and the effect on the organization's reputation in the media. The time is right, and the support is incredible, as we continue our readiness assessment and establishing cybersecurity task force and response teams.

Social media has really helped these efforts, showing the severity of these attacks happening worldwide. This has led employees from across the enterprise to ask what are we doing and working from security and privacy perspectives. It is an advantage to have an entire organization care about what we are doing to secure our network and protect the privacy of the patient data entrusted to us.

HCB News: What advice would you give to another health care organization as they begin to focus on cybersecurity?

SH: I advise organizations to start with a strategic review to understand where the vulnerabilities and risks exist. A strategic review will be essential in developing a strategic plan. Strategic reviews need to happen separately, looking from a security perspective, then vulnerability and state of the network assessments.

These assessments need to address patches and how servers are updated, coordination of equipment pulse checks, how are we handling vendors and their access to the network and patient data. We must determine how we are auditing who is in the network and how they're getting in. Additionally, we have to determine our internal literacy level, and ask if our people are aware of what phishing attacks are, are they aware of what they're doing when they're plugging in their BYOD device.

Organizations must understand you can have security without privacy, but you can't have privacy without security. Privacy and every privacy legislation is based on a framework and those frameworks have safeguards involved that are both physical and technical to protect personal information and sensitive health information from unauthorized collection, use, disclosure and disposal.

The biggest piece of advice is to move forward. We must go beyond talking and planning and put these policies and plans into action. But policies must be continually assessed in a way where you walk through use cases of potential attacks and how to involve various organization areas.

HCB News: What do you think the future of health care cybersecurity will look like?

SH: I believe the future of cybersecurity and patient privacy in health care will be more comprehensive in terms of every organization having a strategic plan they put into place and review annually. In conjunction with these plans, I think we will see expanded and enhanced auditing, both from a patient privacy and security perspective, which will provide clear pictures of who is accessing patient records, as well as how that data is being secured.

In the future, I see health care organizations hiring highly credentialed privacy and security individuals, taking the necessary steps to maintain these professionals through establishing departments in various areas of practice. These areas of practice, including technology, cybersecurity and patient privacy, will be increasingly accountable to the CEO and CFO, showing the expanded priority placed on the need for privacy and security.

In my 16 years of work in privacy, I've never seen an impetus like what we are currently in, with privacy and security becoming more predominant in all organizations, specifically health care. Patients trust us to care for their ailments and sickness, but they now trust us to keep their data secure. This trust is paramount and the responsibilities are incredible. But our patients truly deserve to be confident that their sensitive health information is safeguarded against unauthorized collection, use, disclosure and disposal, only being accessed on a need-to-know basis. The future of cybersecurity and patient privacy will hinge on understanding and protecting this trust.