Healthcare Cybersecurity: Moving from Awareness to Action

In healthcare, cybersecurity threats tend to elicit a type of normalcy bias where leaders who have yet to experience an attack, or those who have weathered less significant attacks, underestimate the likelihood that a disastrous event will impact their organization. Moreover, in the past there was a level of risk organizations were willing to tolerate when it came to data breaches.

Recent Huron research reveals that attitudes may be changing. In a survey of healthcare providers, executives named data security as the top industry trend impacting their organization now and in the next three to five years.

Elevated Risk and Consequences

Cyberattacks and resulting data breaches hold devastating consequences for healthcare organizations, including massive financial payouts, disruption of business operations and the inability to adequately and safely care for patients. Equally as costly is the loss of consumer trust and damage to brand reputation as organizations struggle to compete in a new era of healthcare consumerism.

Recent reports found that 93% of healthcare organizations have faced a data breach in the last three years. The uptick in known data breaches may be due in part to more accurate reporting and heightened public awareness, but there is no doubt that the severity and sophistication of cyberattacks are at an all-time high with the average cost of recovery totaling $1.4 million per attack.

Thinking Differently About Security

Despite the threat level and acknowledgment from leaders that security is vital, as well as the existence of federally mandated security risk assessments, healthcare organizations remain highly susceptible to attacks.

The complexity of the healthcare environment makes defending against cyberattacks and data breaches difficult, but that doesn't mean that security is impossible. As organizations move care outside the hospital, smaller facilities may have vulnerability points such as on-site servers that could easily be accessed or stolen. Below are steps organizations can take to better align resources and shift mindsets about information security in healthcare:

Right-size security. Budget constraints and competing lists of priorities make it hard for leaders to prioritize cybersecurity over adoption of new revenue-generating technology such as analytics platforms or robotics.

Critics are quick to compare healthcare's cybersecurity performance with that of other major sectors such as banking and financial services, which consistently outspend healthcare on IT security. At the same time, organizations have to be careful not to equate spending with protection.

Leaders need to be aware of what best practices apply to organizations of their size and complexity and plan accordingly. A thorough risk assessment and strategically selected improvements can have a big impact on how well an organization avoids and responds to attacks.

Think broader about technology — and risks. New technology and third-party vendors are regularly added to the hundreds of applications already running on a health system's network. Each creates vulnerabilities that malicious actors can exploit.

As healthcare organizations deploy more consumer-centric strategies, consumers will need assurances that the private information they share through wearables, mobile apps, virtual visits and patient portals is protected alongside their electronic health record.

Medical devices, which are often neglected information technology (IT) assets when evaluating risk strategy, present one of the largest-growing areas of risk for organizations as they can be used to gain access to higher-value areas of a network. Consumers need to know that their devices are safe and can't be compromised to harm them.

Cloud-based systems allow organizations to scale their information security functions and offset security risks associated with local servers, but there are other considerations when migrating to the cloud, such as ensuring the organization can retrieve its data at any given time. Also, not all third-party cloud services vendors are equal.

Stratifying vendors according to risk — how much data is managed, the sensitivity of that data and how mission-critical the data is — helps to guide the type of business relationship and level of oversight required with each vendor.

Actively prepare for evolving threats. In addition to malware and phishing emails aimed at stealing valuable patient data, healthcare organizations now contend with increasingly sophisticated ransomware. In the past, attackers would paralyze a health system's operations and care delivery by taking control of financial or patient data until a sum of money was paid. The latest ransomware perpetrators leverage stolen data by publishing small subsets of data publicly in order to accelerate payments from breached organizations fearful of additional exposure.

Information security and compliance officers should stay informed by following sources that monitor new and growing cyberthreats, such as the Office for Civil Rights (OCR) privacy and security group email list and the United States Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), the agency responsible for protecting the nation's infrastructure from cybersecurity threats.

Build the right culture — it matters. Technical security is not a substitute for culture. A positive security culture is one in which people at every level of the organization take security seriously. Employees should have a mechanism to report issues or mistakes without fear of retribution, and there must be trust between employees and leadership that concerns will be addressed once reported.

Invest in your employees and leaders. One of the most important steps organizations can take is to continue educating employees about the risks around them, such as phishing emails or other common areas of infiltration.

Federal regulations require that healthcare organizations designate a named individual for the role of chief information security officer (CISO). Too often organizations undervalue the importance of this role in building an effective security program and designate an individual without the proper training or experience. Healthcare organizations should invest in building out a full job description for their CISO and allocate the resources to fill the job with a fully qualified candidate.

Key Takeaways

The healthcare industry is defending itself against unprecedented levels of cyberthreats. To reduce susceptibility to attacks, organizations should:

Think differently.

Don't allow complacent attitudes and reactionary behavior to steer cybersecurity strategy; security programs should be proactive and always evolving just like threats.

Plan differently.

Take risk assessments to the next level in order to identify the right level of security investment needed for organizations of your size and complexity.

Act differently.

Resource security programs adequately with the tools, information, skilled leaders and culture that are needed to protect healthcare organizations against growing threats.

HURON

huronconsultinggroup.com