SQUIRE PATTON BOGGS

Thinking About Healthcare Cybersecurity

How to Get Organized and Better Manage Risk

Another month, another round of data breaches – seem like a familiar refrain when healthcare providers, health plans and their counsel think about cybersecurity? But what if instead we could get organized and manage this growing business risk in a more proactive manner?

It sounds like a good idea, but for many counsel, who view themselves as less than tech-savvy, it is hard to put together the pieces and formulate a strategy. And for highly regulated industries, holding highly sensitive personal information, like healthcare, making mistakes is costly. Here, we have laid out a simple set of key steps for thinking about cybersecurity at the organizational level. Keep an eye out for future alerts where we will explore cybersecurity in more detail – and we promise, no computer science degree or extensive IT experience required!

Key Steps for a Sound Cybersecurity Program – First, it is critical that organizations consider cybersecurity (or "information security" or "data protection," if you prefer) to be a program, an ongoing part of the business that demands leadership and commitment, and not a one-time project. Successful organizations develop sound practices and then maintain constant vigilance, using a risk management mindset. Next, a few key steps help organize the work and provide a structure for regular leadership discussions.

1. **Know Your Information Assets**
   It is as simple as this: if you do not know about it, you cannot protect it. For many organizations, information technology (IT) infrastructures grow organically and over time through individual business unit activities, discrete projects and acquisitions/changes in business structure. Taking an overarching view of the IT infrastructure (sometimes called an "enterprise architecture" view), helps identify how and where sensitive information is stored, and who needs access. A well-maintained asset inventory, including the data maintained, can also help the information security program recognize asset and risk categories, as well as affinities among business groups – improving their risk assessment capabilities. These categories can also help to better segment your internal network and limit access to only those who have a need-to-know. Segmentation is a valuable cybersecurity strategy, because it can limit the damage hackers (internal or external) can do when your environment is compromised.

2. **Recognize and Understand Legal Obligations**
   Healthcare organizations often equate cybersecurity with the HIPAA Security Rule, but HIPAA is just one of many legal obligations in the information security area (and such thinking can leave serious risks unaddressed, since the HIPAA regulations were primarily developed before external, Internet-based threats became a common part of our world).

   At the federal level, healthcare groups should also understand and track the US Federal Trade Commission's (FTC) current activities in data privacy and information security, as well as Congressional efforts aimed at improving information sharing and standardizing breach notification. The US Food & Drug Administration (FDA) has also issued guidelines to improve cybersecurity for medical devices, and the White House recently proposed legislation in support of its Consumer Privacy Bill of Rights. From a state-level perspective, it is critical for healthcare organizations to understand general data protection and breach notification requirements, in addition to healthcare-specific laws. For example, organizations that hold certain personally identifiable information for Massachusetts residents (whether patients, members, employees or others) must implement and document a proactive information security program that includes specific safeguards and vendor governance – similar requirements have arguably become the industry-wide de facto standard of care.

3. **Implement and Maintain a Standards-Based Information Security Program**
   A risk management based information security program should have clear executive ownership and address **people, process, policy and technical controls**. Treating cybersecurity as just another IT project or "IT's problem" invites serious gaps and significant risk. Moreover, as technical controls become increasingly sophisticated, people become more common targets through e-mail phishing and social engineering. Cybersecurity – like patient care, customer service and expense management – is an issue for every team member. A variety of resources are available to structure (and measure) your comprehensive cybersecurity program. Two great places to start are the National Institute of Standard & Technology's (NIST) Cybersecurity Framework – a product of the Administration's 2013 Executive Order 13636, Improving Critical Infrastructure Cybersecurity – and HITRUST's Common Security Framework (CSF), while others, such as the ISO 27000 Series of information security program standards, NIST's 800-53 controls for federal systems, under the Federal Information Security Management Act (FISMA), the Top 20 Critical Security Controls (also known as the Consensus Audit Guidelines, or CAG), ISACA's Control Objectives for IT (COBIT) and the Payment Card Industry Data Security Standards (PCI-DSS), can also be invaluable, according to specific organization needs.

4. **Seek External Review/Certification**

   A variety of external reviews and certifications are available to assess an organization's cybersecurity program. Independent, third-party reviews against industry standards can provide an unbiased view of current status and opportunities, while certifications (such as those from HITRUST and others) can provide market differentiation by offering assurances to business partners and customers. Increasingly, underwriters also require such assessments to obtain cyberinsurance coverage – another key component in the cybersecurity risk management toolbox.

5. **Monitor and Report**

   Finally, ongoing monitoring and reporting for your cybersecurity program allow for continuous improvement and leadership visibility. NIST's Cybersecurity Framework provides a concept (and structure) for "profiles" that help organizations describe and communicate their current ("as is") state as well as a target (or "to be") state – helping to lay out a strategy and maintain focus.

Finally, healthcare organizations may wish to seek out opportunities to share information and collaborate with others in trusted forums, as they develop and maintain their cybersecurity programs, whether through standards organizations, or an information sharing and analysis center, like the National Health ISAC (NH-ISAC). For more details on furthering development of Information Sharing and Analysis Organizations (ISAOs), see Executive Order, Promoting Private Sector Cybersecurity Information Sharing.

Contacts

Stephen P. Nash
T +1 303 894 6173
E stephen.nash@squirepb.com

John E. Wyand
T +1 202 626 6676
E john.wyand@squirepb.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations nor should they be considered a substitute for taking legal advice.