Smart approaches to top-level decision making

Reprinted from
Fall 2016 e-newsletter

STRATEGIC FINANCIAL PLANNING

hfma.org/sfp

# 5 Steps for Developing a Cybersecurity Program

By Sara Fay

*Setting a timeline, defining roles, and planning long- and short-term budgets are among the key steps in developing a program to keep patient data secure.*

Cybersecurity breaches are making headlines every day, and healthcare providers are often vulnerable targets. As the stakes are particularly high in healthcare data security, it is essential to develop a program to keep data safe. However, where should healthcare cybersecurity begin? Many organizations look to the IT department, others the board, and some to external resources. The answer usually is a combination of all of the above, as keeping data safe cannot be the responsibility of one person, department, piece of equipment, or vendor.

"Cybersecurity, data breaches, ransomware attacks. … All these phrases can be intimidating, especially when they are displayed so frequently in the headlines," says Michael Haines, assistant vice president, First American Healthcare Finance, Fairport, N.Y. "To make sure your organization and patients are safe, it is crucial to form a strategy with your leadership team so everyone is on board from the top down. Being proactive about data security can have long term effects on patient care and satisfaction."

Below are five tips for establishing a cybersecurity program.

*Plan a short-term and long-term budget.* Some costs need to be absorbed immediately to get a cybersecurity strategy started, but not all of them. Costs that healthcare organizations should absorb immediately are anti-virus and

→

hfma
healthcare financial management association

anti-spyware software, network security systems, and firewalls. These components are essential to keep data secure and protected. Once these items are in place and installed on both the network and all individual devices (i.e., computers, laptops, mobile devices, tablets), organizations should replace or upgrade servers, infrastructure, and switches every three years.

Regardless of whether the investment is needed immediately or in the future, explore multiple funding options, including cash, financing and leasing. If you're considering leasing or financing, a good rule of thumb is to finance assets you'll use for a long-period of time and lease assets which need to be regularly refreshed. All items of equipment, as well as software, can be either financed or leased.

Consider treating your cybersecurity strategy as a recurring item on your long-term budget to keep your network secure and up to date. Being strategic about IT financing and budgeting will not only equip your organization with ways to keep your data safe, but will also save money in the long run by not having excessive costs to replace equipment or pay for a ransomeware attack.

*Define roles within your organization.* The board and C-level executives should agree that cybersecurity should be a priority for their organization, as the purpose is to protect data that affects both patients and staff. Because the board or finance committee often has to approve expenses, it's important they are aligned with the initiative. To start, top level executives should organize a cybersecurity committee, usually with the chief information officer (CIO) or the chief information security officer to lead the initiative, and define roles, such as the following, for each member that pertain to their area of expertise.

> IT team members researching vendors and training staff on new systems
> The finance team looking at the best ways to fund the project
> The legal team verifying that new vendors and systems comply with HIPPA regulations
> Human resources and marketing communicating changes

Dedicating a project manager to work alongside the CIO is a best practice of many organizations, as a cybersecurity strategy is formed from multiple vendors, types of software, and IT equipment, that all need to work together.

*Set a timeline.* Create realistic milestones for when old equipment and software will be replaced during the next three to five years. Make a schedule of when data security equipment and software should be refreshed, when systems should be updated, and when security measures should be tested. For example, the following schedule accounts for updates for five years as well as ongoing maintenance and replacement.

> First, install firewall software, and for endpoint security (all laptops/desktops), install antivirus protection, ensure all workstations have the latest updates/patches installed, and enable drive encryption to protect data if a device is stolen.
> Twice a year, implement third-party security audits/tests that include pen testing and vulnerability scans, which detect weaknesses and security holes in your environment.
> Every 3 to 5 years, refresh security appliances along with other IT hardware.
> On an ongoing basis, keep all appliances up-to-date with the latest software and firmware.

*Update outdated core components.* If IT equipment is more than two or three years old, update your organization's servers, firewalls, and wireless infrastructure immediately. Many data breaches can be avoided simply by replacing outdated equipment with equipment that has new security features in place.

*Utilize external experts.* Healthcare providers do not need to be technology and security experts. Use your leadership team to keep cybersecurity a focus for the organization, but work closely with external vendors and companies that specialize in keeping data safe.

The recent report from the American Hospital Association, "Cybersecurity and Hospitals: What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response," notes that "cybersecurity is not about compliance with regulations and it concerns much more than patient privacy. It is about identifying the systems that are connected to the hospital's information network where the hospital has vulnerabilities—financial data, patient data, personnel files, medical devices—and taking steps to reduce those vulnerabilities."

Hospital leaders should make cybersecurity a priority at all levels of the organization, and ensure every staff member, system, and device meets the standards of patient data security.

"Investment in cybersecurity is crucial in this day and age. Especially with ransomware attacks and data breaches, healthcare organizations have the option of investing up front, or taking the risk of paying later," says Kimberly Moore, assistant vice president, First American Healthcare Finance. "Healthcare organizations need to form a plan customized for their organization and align the entire staff on how they can contribute to keeping data safe. For the peace of mind of any organization the best choice is to plan and make smart investments now."

**Sara Fay**
is an Assistant Vice President, First American Healthcare Finance, Fairport, N.Y.

This article originally appeared in the Fall 2016 enewsletter of *Strategic Financial Planning.*