Solving Healthcare Security Concerns Will Require a Three-Pronged Effort

AUTHOR | DAVID DINGWALL, VP OF PRODUCT MARKETING

According to a recent KPMG report, four-fifths of executives at healthcare providers and payers say their information technology has been compromised by cyberattacks.[1] That same report presents how the increased risk to healthcare organizations relates to the richness and uniqueness of the information that health plans, doctors and hospitals handle. Apart from typical financial fraud, there is also the possibility of medical insurance fraud, or in the case of providers, attacks on computer-controlled medical devices.

IT'S ALL ABOUT FINDING BALANCE

One of the reasons healthcare organizations face this challenge is the difficult balancing act when it comes to managing electronic medical records. Doctors, nurses and other caregivers as well as patients need online access to information to collaborate on care services. On the other hand, that same information must be protected from unauthorized access and data theft.

So in this battle of accessibility vs. vulnerability, how can internal IT teams strike the proper balance?

There's a lot of contention on what to do within the healthcare industry as there does not seem to be a consensus on the best practices to apply to remain secure. And even if agreed-upon security standards did emerge, frequently-changing HIPAA regulations continue to result in the need to either apply new security tools or change existing security measures. Because HIPAA and the security process make it hard for providers to adapt quickly, the healthcare industry tends to be further behind other industries when it comes to security.

VENDORS WITH PROPRIETARY SOFTWARE IMPEDE PROGRESS

Hospitals and other healthcare organizations also have to contend with the protective ecosystem of medical application vendors. They tend to keep as much of their information proprietary as they possibly can. While this may protect the value these applications deliver to their customers, this approach also limits the extent to which security professionals and third-party security tool vendors can interact with the application vendors—so that they can effectively collaborate together on security measures.

Most security holes within healthcare organizations are largely due to vendors hesitating to release information about their applications. In one case, a large nonprofit health system in the US had to disable the firewall for an application because the vendor would not reveal which ports the application uses and was unwilling to restrict the ports that could be used. This made using a firewall on that application server nearly impossible.

Other medical software vendors are slow to issue updates so that many hospitals are currently using applications that reached end-of-life several years ago. This means the software can no longer be patched, and whenever a new vulnerability emerges, those applications are at risk.

INTERNAL SYSTEM ADMINS ALSO NEED TO ADAPT

But the issues relating to healthcare security go beyond the vendors. Many internal system administrators don't understand security or are unwilling to go through the process of adding the necessary level of security to their systems because it can be a painful process.

The lack of understanding and the inability to implement security is due to some IT pros focusing on other areas of IT as they launch their careers or not taking the time to become cognizant of security issues. That's because in many environments, security knowledge is not required—system admins are used to relying on security pros. But the admins need to assume some of the ownership because access to security pros is not always available in today's cost-cutting environment.

HELP NEEDED FROM MULTIPLE FRONTS

To address the healthcare security issue, it will take a three-pronged effort among internal healthcare IT teams, medical application vendors, and third-party security tool vendors. Internal IT teams must become more knowledgeable about security while the vendors need to provide more information about their application code.

At the same time, third-party tool vendors need to find ways to automate the process for deploying security controls. Today, many require manual intervention, which takes longer to implement and requires security to be managed on a per-server basis. System admins thus have to log onto every server to make changes, which prompts many of them to do nothing at all. The industry as a whole needs to find a way to automate and centralize security tools and then secure participation from the vendors along with educating system admins—so that the tools can be used effectively.

SECURITY SUCCESS IS MISSION CRITICAL

Succeeding in the mission to improve security is critical, because the on-going push to make medical records instantly accessible will likely continue for years to come. Care givers and their patients will always want to have information at their fingertips to help improve patient outcomes.

At the same time, the healthcare industry will continue to wrestle with the added vulnerabilities that the additional accessibility creates. Going forward, the industry thus needs to find that perfect balance between the two. Medical software vendors, security professionals and security tool vendors must all work together to keep electronic medical records secure—so doctors and nurses can provide the best patient care possible without anything holding them back.

---

1. "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities," KPMG, © 2015 KPMG LLP, http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf

ABOUT FOXT

Fox Technologies, Inc. helps companies protect corporate information assets with network security and access management software as well as striving to simplify compliance and streamline administration with an award-winning access management and privileged account control solution. Our access management software centrally enforces granular access entitlements in real time across diverse server environments.

To learn more about Fox Technologies, please visit us at: **www.foxt.com**

CONTACT INFO

North America
3300 Eagle Run Drive NE, Suite 202
Grand Rapids, MI 49525
+1 877 818 3698 (Toll Free)

Sweden
FoxT Sweden AB
Kungsängsgatan 18A
SE-753 22, Uppsala
+46 18 16 00 00 (Main)

United Kingdom
400 Thames Valley Park
Reading , Berkshire RG6 1PT
+44 1189 637 681 (Main)

www.foxt.com | info@foxt.com

foxtechnologies.

You may also be interested in: Best Practices for Unix/ Linux Privileged Identity and Access Management