HealthManagement.org
Promoting Management and Leadership

10 Ways to Enhance Cybersecurity Protection

2016 was marked by a number of cybersecurity mishaps that caused health data records to be exposed or stolen. The healthcare industry has taken steps to secure its vulnerabilities, but IT security experts say much more needs to be done to protect valuable patient data and keep it out of cybercriminals' hands.

See Also: Cloud Security Toughest Role for HIT to Fill

A report in *Healthcare IT News* offers insights from experts as to what changes are needed to avoid repeating last year's data mishaps.

1. Risk assessments. Most organisations have limited funding. Risk assessments help identify what really needs to be protected, and can help security teams plead the case for funding. Organisations should make recommendations based on assessments to address vulnerabilities.

2. Disaster recovery and contingency plans. An effective plan addresses not only access to medical and billing records, but contingencies for email, departments reliant upon the network and departments with high-tech equipment like, lab, pharmacy or imaging services. Also, practising the plan is crucial. Involve staff, not just IT or managers in exercises ("worst case scenarios" for loss of power, communications, network and others) to ensure staff can actually do their job without the system.

3. Dedicated Sec-Op teams. Organisations need a dedicated Sec-Op team to handle security, hunt threats, educate staff on latest threats and perform pen tests.

4. Business associate/vendor scrutiny. Organisations must review vendors' risk assessments and require indemnification provisions and cybersecurity insurance in business associate agreements. It's important to

select vendors with a demonstrated track record with "security by design" – a security method that uses continuous testing, authentication safeguards and adherence.

5. Better employee training. Organisations should conduct security exercises (e.g., mock phishing attempts) to raise staff awareness, similar to fire drills that are done regularly and frequently in most places. While computer-based training may be easy, other methods involving experiential learning such as tabletops, exercises and tests, may be more effective.

6. Layered defence. As many organisations think they have the capability to detect and respond, they're not layering their defences. "The CISO should be looking at targeted areas where he or she can add to various layers of cyber defence. But there's still not enough movement in this area," says ICIT Senior Fellow James Scott.

7. Improved tech hygiene. System upgrades and patches must be up-to-date and routinely checked to minimise system vulnerabilities and hacking attempts. Systems must also be routinely monitored for inappropriate activity. And, as always, back-up systems to prepare for ransomware attacks or other system outages.

8. Cybersecurity partnerships. Partnering with the right organisations can assure the success of your cybersecurity strategy: for resources, expertise, experience and capabilities. Additionally, organisations need to "embrace sharing of cybersecurity information". For example, you can initiate a local or regional ISAO Standards Organisation with other healthcare entities in your region, according to CynergisTek co-founder and CEO Mac McMillan.

9. Better software. While there is "a whole litany of technologies" healthcare organisations should consider, McMillan said his short list would include: next-generation firewalls, advanced malware detection, email and web gateways, multi-factor authentication, encryption, vaulting solutions and outsourcing security information and event management – among others.

10. Forensic consultants. Organisations should engage a forensic consultant to provide insights on weaknesses, liabilities and security reports.

Source: Healthcare IT News
Image Credit: Flickr

Published on : Tue, 24 Jan 2017