HealthManagement
Promoting Management and Leadership

Healthcare IT Security Problems, People and Solutions

Wayne Richards
******@***gmail.com

Graduate Student, University of Maryland Baltimore County &
Cybersecurity Professional

LinkedIn

Like other sectors whose mission depends on network-connected technology, healthcare is in crisis. In addition to the need for confidentiality, people's lives depend on the integrity of the health information system. Incorrect decisions based on incorrect information could mean the difference between life and death. Finally, the information must be available when needed by a caregiver.

Similar to many companies, which view themselves as non-technology companies, a common problem with hospitals is that they make heavy use of technology but refuse to spend the money to secure and use it properly. The common theme is usually: Where is my return on investment? CFOs, CEOs, and even CIOs, are usually not technically savvy; therefore they are very shortsighted when it comes to seeing how technology is critical to the mission of the organisation. Therefore, we have to explain the risks and opportunities and the vital role technology plays in mission of healthcare organisations: the very safety and well being of their patients.

Ransomware such as Cryptolocker, a recent phenomenon on the hospital scene seems to be the new threat, but not the most dangerous by far. Locking hospital data is more of an inconvenience at this point. Take Hollywood Hospital Healthcare systems for instance, a well-maintained backup system would have allowed them to abandon the old system, format the hard drives and upload the backups to critical systems overnight. Lack of planning cost them an extra $17,000 dollars, and maybe millions in lawsuits. In 2013 over 250,000 victims and about 90,000 machines per day were affected according to www.privacyandsecuritymatters.com.

Regardless of this, the attacks I am most worried about are command and control type attacks. These attacks could be leveraged against pacemakers, and other electromechanical devices that send wireless signals over the internet to doctors and caregivers. In some cases, manipulation of these devices can have immediate and deadly consequences.

The investment in healthcare Information technology would have four meaningful effects:

Investment in better technology that can detect a real-time intrusion attack on the system and automate its response;

The weakest link in the IT chain can be the people. However, with proper training in incident response and intrusion mitigation, this weakest link situation can be solved. An attack on a SCADA type system would mean the attacker would need to do reconnaissance on the people and system. Trained personnel would know to look for system enumeration, scanning events and change in data traffic flow. Most attacks can be avoided with knowledge and vigilance. Patients' information would be more protected, risk to data breach would be minimised, and return on investment would be realized over the long term.

What management also needs to realise is spending money on the system does not make it hack proof. What it does is reduce the chances of a breach, not eliminate it.

Most CIOs, CFOs, and CEOs would ask: What happens when I invest in training for personnel and they take that training and find a better job? Well, finding well-trained people that work cheap is not an option. For the training, ask employees to stay for two years in return and train junior employees. Discuss salary increases so employees can feel compensated for their work. The alternative is, you do not train employees and they stay with the company for 20 years collecting a pay check while the problem escalates. Healthcare management has the power to create the healthcare technology of the future they desire. This is not the responsibility of their employees.

Biography

Wayne Richards is a Graduate Student at University of Maryland Baltimore County and a Cybersecurity Professional. His main focus is on Cyber Threat Management and Mitigation in the federal government and healthcare workplace. He currently holds 12 Information Technology (IT) Certifications and is a Subject Matter Expert (SME) on IT threat detection, mitigation and remediation. He also works as a consultant for the

federal government as an expert on insider threat, Network infrastructure, Security Operation Center (SOC) Monitoring and incident mitigation, Network protocols and best practices and Certification and Accreditation Process for federal government enterprise network operations. Currently he lives and works in the Washington DC Metro area.

Curated and edited by cybersecurity and healthcare speaker and author Dr. Mansur Hasib, CISSP, PMP, CPHIMS, Programme Chair, Cybersecurity Technology, The Graduate School, University of Maryland University College (UMUC). www.cybersecurityleadership.com

Published on : Tue, 25 Oct 2016