IMpulse news CLIP
Intermountain Media Pulse
A TRUETONE INCORPORATED COMPANY
11623 Lake Shore
Nampa, ID 83686
(208) 880-9814

FOR YOUR INFORMATION
**Idaho Business Review**
Boise, Idaho
**Wednesday May 30, 2018**
**by Gina Ballucci-White**
Page 1 of 2

# Hospitals must remain vigilant with cyber security

When it comes to patient health records, employee information and data from medical technology devices, hospitals have a treasure trove of sensitive, private information to keep confidential.

"The whole idea of having electronic records positions hospitals to provide better care and services to the patients they are working with but at the same time, obviously, (there is a) risk associated with this information being shared in electronic format," said Harry Holt, vice president of operations of the Baltimore, Maryland-based BITHGROUP Technologies.

Hospitals continue to be heavily targeted by very sophisticated adversaries including internationally based criminal organizations and nation- states such as Russia, China, Iran and North Korea. Sometimes nation states working in collusion with criminal organizations to target healthcare and hospitals.

John Riggi, senior advisor for cybersecurity and risk for the American Hospital Association, notes cyber adversaries will seek to exploit personal and confidential medical information for criminal purposes such as fraudulent billing and general monetization of the information gathered.

"Nation-states could seek to target that health information for intelligence purposes such as the health information of individuals working for the government with security clearances — military personnel, politicians, folks in the intelligence community as well," he noted.

Complicating the matter further is the fact many hospitals incorporate a number of machines in patient care such as laptops and iPads.

"Often just understanding and conducting an inventory of how many devices they have within the hospital that are connected to their networks can be a tremendous challenge," Riggi said. "So not only are the devices connected to their networks but many of these devices are connected to external networks, connected to the Internet so having good end point security on these devices … including antivirus software, having encrypted communication between the device and network is essential."

In June 2017, the Healthcare Industry Cybersecurity Task Force released a report detailing improvements that need to be made. While information

technology security falls under IT management, the report emphasizes the need to also include additional people, processes and policies that generate, use and manage the data and information required for care.

"The employees and the staff of a hospital can either be their best defense against cyber threats or the weakest link," Riggi said. "The most common method adversaries use to deploy malware is by targeting employees through phishing emails or some other type of social engineering tactic. … So everyone being extremely conscious and understanding that they have a fundamental role and responsibility to protect the organization from cyber attack, I think, is critical (and) essential to keeping organizations safe from cyber threats."

In response to the report, the American Health Information Management Association put together a list of 17 best practices regarding a hospital cybersecurity plan. One of the most critical is immediately updating systems when patches are released by the manufacturer.

"A lot of the attacks, unfortunately, could be prevented if people were keeping their systems up to date with the patches," said Kathy Downing, AHIMA's vice pesident of information governance and informatics and author of the report.

The vast size of hospital systems can make patching difficult. Some are legacy systems, or a vendor doesn't support a software anymore.

"It creates this real complicated situation in getting patches out and it has created a lot of risk in healthcare," she said. "Hackers are out on networks looking for people who have not taken that patch and that is how they will get you."

Hospitals should encrupt high-risk work stations, laptops, smartphones, tablets, portable media and backup tapes if still in use, according to AHIMA. Downing notes that if a laptop is stolen from an employee, data could be compromised and alerts would have to be sent out to thousands of patients. Yet if the laptop was encrypted, thieves would not be able to take the data as well.

"Encryption, to me, seems like one of those low-hanging fruit things where if you've got devices on the move, whether it is a mobile device or a laptop or an iPad with patient information on it, it's time to encrypt it," she said.

One of the hardest best practices to implement is evaluating business associates. While hospitals may have privacy and security protocols in place in addition to rigorous training of staff, entities that work with healthcare facilities might not be as vigilant. AHIMA encourages hospitals to obtain reasonable assurances of compliance with HIPAA Security Rule from current business associates.

Riggi believes cybersecurity should first and foremost be viewed through the lens of patient safety and care.

"Cybersecurity is not just an IT issue. It really is an enterprise-wide risk issue and should be incorporated into an enterprise-wide risk management issue."

# # #