HealthManagement
Promoting Management and Leadership

Part 2: How to be one step ahead of healthcare cyber hackers

Gregory Garrett
******@***bdo.com

Head of U.S. & International
Cybersecurity Advisory Services -
BDO

A recent report from advisory BDO has highlighted 'the most underrated cyber threats' in the healthcare sector. 'Brace for the Breach', showed a growing trend in decentralised cyber attacks and nation state cyber attacks on hospitals in addition to a movement towards rypto jacking replacing Ransomware. In part 2 of a 2-part interview, HealthManagement.org spoke to Gregory A. Garrett, Head of BDO U.S. & International Cyber Security Advisory Services, BDO for further expert insights into the healthcare cyber threat landscape.

How do you see the healthcare cyber threat landscape evolving in the near future?

The cyber threat landscape is becoming more challenging every year. As the use of IoT grows to save time and money, so does the number of cyber-attack vulnerabilities, which create significant potential operational, financial, and reputational risks for the healthcare industry globally.

What points of attack will hackers target?

Cyber-attackers typically pursue the cyber vulnerabilities that are the fastest and easiest points of entry or access to the information they seek.

Blockchain technology is attracting attention in healthcare. Do you think this technology could go some way to eradicating cyber threats on patient data, for example?

Yes, Blockchain technology does provide the potential to provide much greater information security. Private Blockchains could be formed to create enhanced security for electronic health records (EHRs).

Regarding the growth of crypto jacking, how is this impacting healthcare cyber security?

Sometimes, insider attacks occur resulting in crypto jacking and sometimes the database outside the Blockchain, storing the quick cash is not as secure. Today, crypto jacking is very widespread in the financial services industry worldwide, but, while still a threat, crypto jacking is not yet very widespread in the healthcare industry.

Is there any particular healthcare organisation that is especially vulnerable to decentralised cyber attacks?

Based upon our experience nearly all healthcare organisations are vulnerable to decentralised cyber-attacks worldwide.

Cyber hacking is always one step ahead of cyber security? How can healthcare organisations keep pace?

It is far easier to be a cyber-attacker to find one cyber vulnerability to gain access to valuable information, than to be the cyber security analyst (defender) and try to defend a large organisation with a small information security budget and little focus on information security as a real business, organisational, and patient priority.

Healthcare needs to make real cyber security a top organisational, business, and patient priority. Invest in Threat-based Cyber security through the following measures:

- Provide cyber security education and training from the Top-Down to create a human-firewall
- Ensure the board & C-Suite understand the cyber threats and cyber risk factors facing your organisation
- Conduct periodic vulnerability assessments and penetration testing to detect the threats
- Conduct periodic email attack assessments and spear-phishing campaigns
- Enhance software encryption measures
- Implement multi-factor authentication (MFA)
- Conduct network, email, and mobile device managed monitoring, detection, and incident response services
- Ensure appropriate business continuity planning and disaster recovery

You might also like: Part 1: Cyber security key obstacles and addressing tech personnel shortage

Source: HealthManagement.org
Image Credit: iStock

Published on : Wed, 3 Apr 2019