HealthManagement
Promoting Management and Leadership

Part 1: Cyber security key obstacles and addressing tech personnel shortage

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 crypto jacking replacing ransomware.

In part 1 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.

There is a view amongst cyber security experts that the healthcare C-Suite is, generally speaking, not taking cyber security as seriously as it is taken in other sectors. What has been your experience in this area?

I agree. It is our observation that the global healthcare industry has been slow to embrace appropriate cyber security measures and faces increasing cyber-attacks with the growth of the Internet of Things (IoT), connected medical devices, and expanded use of Electronic Health Records worldwide.

Why do you think there are obstacles for effective cyber security adoption in healthcare?

Three key obstacles exist:

· Lack of knowledge of the cyber-attack vulnerabilities present within their organisations and the potential significant impacts to their operation and reputation

· False assumptions that cyber liability insurance coverage will cover all of the cost of cyber-attack damages

· The significant time and cost to implement effective cyber security education and training, software encryption, multi-factor authentication, network/email and mobile device monitoring, cyber-attack detection, incident response services, and disaster recovery services.

One major problem facing healthcare is obtaining the tech talent to deal with cyber security. There is a shortage of skilled staff and other sectors like finance and retail tend to soak a lot of them up. How do you think healthcare could address this problem?

There are several options. For larger hospitals and healthcare organisations, I'd suggest making cyber security a high priority with adequate funding to hire the top IT and cyber security talent required. For small to mid-size healthcare organisations, I'd suggest engaging Managed Security Services Providers (MSSPs) to provide the managed monitoring, detection, and response (MDR) cyber security services required. Further, there's the option of using virtual or part-time Chief Information Security Officer (CISO) as a service.

In the BDO report, you identified the top current areas of cyber threat. They were:

- Denial of service attacks
- Business email compromise
- Supply chain attacks
- Internal threats
- Crypto hijacking
- Ransomware
- Computer intrusions

Out of these seven, which do you think represents the greatest threat to healthcare right now?

No question, Ransomware is still the biggest cyber security issue facing the global healthcare industry. However, there are increasing numbers of cyber-attacks focused on the vendor/subcontractors/third-parties who comprise the healthcare supply chain and a growing number of sophisticated Business Email Compromise (BEC) attacks worldwide.

Where does the C-Suite need to take immediate action?

In enhanced cyber security education and training from the top-down within their organisation, combined with improved incident response (IR) training and exercises, and business continuity planning.

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

Published on : Thu, 28 Mar 2019