HealthManagement.org
Promoting Management and Leadership

# Staff Training Urgently Needed for Healthcare Cybersecurity

In healthcare, digitalisation is playing increasingly more important role in streamlining processes and workflows to improve patient care. Electronic health records (EHRs), for example, make it easier for clinicians to store and retrieve important patient data. It is estimated that nearly 86% of office-based physicians now use EHRs, according to the U.S. Centers for Disease Control and Prevention.

**You might also like:** ***Do you do these 7 things to get C-suite behind cyber-security?***

With increasing implementation of EHRs and other technologies for a more integrated patient experience, there is also a growing concern about the safety of sensitive patient information. Such fears are stoked by reports of recent incidents of data hacking. The U.S.Department of Health and Human Services has reported that, as of 1 January 2019, there had been over 200 hacking/IT-related healthcare organisation incidents affecting 500 or more individuals in the U.S. alone.

The sad thing is that healthcare organisations often fail to implement effective cybersecurity strategies to help protect private patient information. As shown in a December 2018 survey study by Kaspersky – covering 1,758 healthcare personnel in North America – some 40% of respondents are not aware of cybersecurity measures in place at their organisation to protect IT devices.

Kaspersky's study, "Cyber Pulse: The State of Cybersecurity in Healthcare", was carried out to get a better understanding of the state of cybersecurity in the region's healthcare sector. Both American and Canadian healthcare employees participated in the survey.

Other interesting findings of the study include:

· 32% of healthcare workers said that they had never received cybersecurity training from their workplace but should have.

· 19% of respondents said there needed to be more cybersecurity training offered by their organisation.

· Nearly half of respondents (49%) said they didn't know if Canadian patient healthcare information needed to stay in Canada.

Based on the survey results, Kaspersky cites the importance of having a skilled IT security team that can help your organisation identify its unique security risks. These IT pros can also help with implementing the necessary security tools to keep your IT environment safe and secure.

The report further recommends the following steps for protecting sensitive patient health information:

· Implement/strengthen cybersecurity training for employees at all levels, specialising the training based on role and the most common threats employees might be challenged with.

· IT security leaders should be knowledgeable of various training options that they can offer employees from bringing in a consultant, to webinar services, one-day training, etc.

· Establish a clear, company-wide cybersecurity policy and proactively communicate the policy to employees on a regular basis to increase awareness in order to minimise future threats.

Source: Kaspersky

Image credit: iStock

Published on : Tue, 27 Aug 2019