Ransomware and Emerging Security Risk Facing Health Systems. Is Your Data Protected?

Program Overview

Many healthcare organizations have invested millions of dollars building massive computer processors, data bases, and wired and wireless networks to connect people together. Their goal is to facilitate communication, improve workflows, improve quality, lower costs, and satisfy customers. But how much attention have these organizations given to protecting these investments from today's cybercriminals? Apparently, not enough as evidenced by the growing incidents of cybercrime and ransomware in healthcare.

Today's most devastating form of cybercrime is known as ransomware, where cybercriminals will hold an organizations data for ransom. No hospital or healthcare provider is immune to the operational chaos and potential financial ruin that can result from sudden cybercrime attacks. Health systems must take prudent steps to identify and address their IT security weaknesses to protect more thoroughly their invaluable data and financial assets from ransomware and other dangerous exposures now and in the future. Their very future depends on it. This presentation will outline concrete methods for mitigating the risk and vulnerability to ransomware.

Program Objectives

At the completion of this program, the participants will be able to:

- Analyze organizational cybersecurity weaknesses that make them vulnerable to a ransomware attack
- Understand how to complete the required security risk assessment
- Review staff education practices and provide insight about patient privacy and security
- Discover how hackers trick employees into revealing information through social engineering

About the Speakers

Jeffery Daigrepont, senior vice president at Coker Group, specializes in healthcare automation, system integration, operations, and deployment of enterprise information systems for large integrated delivery networks. A popular national speaker, Jeffery is frequently engaged by highly-respected organizations across the nation, including many non-profit trade associations and state medical societies

Marissa Maldonado, IT project management, network audit management, and cyber security management consultant with Coker Group. Marissa focuses on identifying key resources ranging in finance, specialists, strategy, and policy for cyber security assessments and network assessments, and specializes in managed IT services which include practice office moves, WAN implementations, desktop and network hardware upgrades, and ongoing Help Desk support. Marissa manages the Coker Group's internal IT support as well.

Who Should Attend

Healthcare personnel interested in learning about the implications of the Internet and medical devices and some methods one can take to better secure them, especially IT staff, executive leaders and managers.

REGISTER NOW

WEBINAR

DATE/TIME

Tuesday
February 28, 2017
1:30 PM - 3:00 PM

PROGRAM FEE

Webinar connection for MHEI Members: $175

Webinar connection & CD recording of the webinar for MHEI Members: $250

Webinar connection for Non-MHEI Members: $300

Webinar connection & CD recording of the webinar for Non-MHEI Members: $375

Registration fee covers one connection per registration. Multiple participants can view the webinar. Payment must be received before connection instructions will be sent

REGISTER

To register, please visit MHEI.org.

Questions? Contact Kelly Yost, Manager of Programs & Membership:

410.796.6239
kyost@mhei.org

mhei Lead. Educate. Inform.

maryland healthcare education institute
6820 Deerpath Rd.,
Elkridge MD 21075
410.796.6239 (p)
www.mhei.org