Internal Audit’s Guide to Ransomware

About This Course

Course Description

Organizations have worked diligently for decades to protect data and information assets. Organizations deploy encryption technology, limit access, and physically and logically segment valuable, sensitive, and proprietary data and information assets in an effort to keep bad actors from viewing, stealing, altering, or destroying it. However, at the same time, the bad actors have improved their craft; they infiltrate and steal these assets by using the same technology designed to protect it.

One of the primary methods used to extort and humiliate organizations throughout the globe is to affect technology with ransomware, which is designed to deny a user or an organization access to files on their computers. By encrypting the files, and demanding a “ransom” payment for the decryption key, this malware places organizations in a position where paying the ransom is the easiest and least expensive way to regain access.

How can internal audit assist their organizations in defending themselves against bad actors who are using their own technology against them? How do we protect ourselves?

Who will benefit from this course?
This course is for internal audit leaders and internal auditors who wish to gain a basic understanding of ransomware.

Course Objectives
Using clear business language, this seminar is designed to familiarize internal auditors and internal audit leaders with ransomware facts and types, as well as the means to reduce threats and improve controls. In this seminar, we will:

- Explore the origin of ransomware.
- Recognize the characteristics of common and emerging ransomware variants.
- Describe the primary ways ransomware is delivered.
- Identify controls to reduce the possibility of infection.
- Explore compensation controls to reduce the likelihood of infection by zero-day attacks.
- Summarize the key components in a ransomware playbook.
- Dramatize a ransomware prevention, detection, and response program audit.
- Discuss how audit leaders can talk to their board of directors and other key stakeholders about ransomware and its impact.

Course Topics
Copyright © 2021 by The Institute of Internal Auditors, Inc., (“The IIA”) strictly reserved. Any preproduction of The IIA name or logo will carry the U.S. federal trademark registration symbol ®. No parts of this material may be reproduced in any form without the written permission of The IIA.
Origin of Ransomware
- History Lesson.
- Types and variants.

Exploitation
- Methods of Exploitation.

Controls
- Preventative controls.
- Detective controls.
- Compensating Controls.
- Incident Response.
- Ransomware and zero-day playbook considerations.

Auditing Ransomware Programs
- Audit considerations.

Management Discussion Points
- Discussions with boards of directors and key stakeholders.

Course Information

Course Duration: 0.5 Day

CPE Hours Available: 4

Knowledge Level: Intermediate

Field of Study: Information Technology

Prerequisites: Participants should come with knowledge of, and experience with the internal auditing process.

Advance Preparation: None

Delivery Format(s): eLearning (Group-Internet-Based); Seminar (Group-Live); On-site Training (Group-Live)