Cybersecurity: How to Deal with the Risks, Hidden Threats & the Latest Financial Reporting Disclosures Self-Study Webinar (11 Hours)

SA36723H
SA367

Self Study Webcast
Dec 20 - Dec 21

Overview:

Today, your organization’s information systems are the target of continuous, online, malicious attacks. Thwarting these cyber attacks requires expertise and 24/7 diligence. In this self-study webinar, you’ll discover the best ways to stop these attacks before they damage your organization’s reputation and finances. Plus, you’ll find out the quick steps that must be taken to contain the impact when a breach occurs. You’ll learn how to:

- Apply your cybersecurity program—what to do and how to do it
- Create a multi-layer program to reduce and eliminate risk
- Deal with the wide-ranging implications on a company’s accounting and financial reporting, including SOX audits and SEC filings
- Build an integrated and comprehensive company-wide cybersecurity plan

Objective:

This self-study webinar is designed to show financial and accounting professionals the best ways to deal with today’s toughest cybersecurity issues. You’ll learn core principles and proven techniques to successfully safeguard your organization from cyber attacks and effectively deal with breaches when they occur. It also emphasizes how to build communications, share information, and get everyone in the company focused on the same goals and working together.
Detailed Learning Objectives [1]

Emphasis:

- Identify the cyber risks and align your cybersecurity program with the company’s goals
- What questions you can expect from the Audit Committee
- How to deal with the latest SEC and other cybersecurity disclosure regulations
- Public Relations and Cybersecurity: striking the balance of not creating fear while still being accurate
- The flow of Objectives to Risks, to Controls, to Audit plans
- Dealing with multiple divisions and corporate structures
- Methods for preventing cyber events
- Techniques for responding to incidents to contain the damage
- Jurisdictional issues:
  – China data location requirements
  – The new European Union GDPR
  – California consumer protections and other US state requirements
- How cloud computing affects compliance and controls
- How IT outsourcing impacts cybersecurity
- Best practices for organizing staff and vendors
- Real-World Incident Response Success Strategies

- Identify the overall key to minimizing damages from cyber breaches
- Recognize recent cyber security statistics, applicable both globally and within the US
- Recognize current forms of cloud exploitation
- Recognize the common characteristics of high profile cyberattacks
- Recognize direct and indirect US cybersecurity regulators
- Identify the goal of risk mitigation
- Identify the role or potential role of Artificial Intelligence (AI) in a cybersecurity context
- Recognize an overall approach to cybersecurity risk
- Identify the characteristics of the Common Vulnerability Scoring System (CVSS)
- Identify the role of compensating controls within a cybersecurity system structure
- Recognize both US sourced and non-US sourced cybersecurity compliance programs.
- Recognize the overreaching goal of Sarbanes-Oxley
- Recognize the characteristics of the PCI Security Standards Council
- Recognize the characteristics of the General Data Protection Regulation
- Recognize the potential penalties associated with noncompliance with the GDPR
- Identify the characteristics of penetration testing and penetration testing vendors
- Identify approaches to threat elimination following an incident containment
- Recognize options to protect against the risk associated with third parties
- Identify the role of insurance in protecting against cybersecurity breaches
- Identify various policy characteristics of insurance against cybersecurity breaches
- Recognize the role of compensating controls in cybersecurity
- Recognize the primary characteristics of SOC Release #2/2/3/+2
- Identify the potential impact of a cybersecurity breach on an organization
- Identify the optimal approach to cybersecurity crisis management
- Identify suggested public relation strategies for dealing with a breach
- Recognize the role of cloud computing and IT vendors and the cybersecurity implications of their use
- Recognize the current professional standards used to report on internal controls and service organizations

Bottom**Prerequisite:**
None.

Preparation:

No advance preparation required.

Level of Knowledge:
Overview.

NASBA & State Sponsor Information | Policies, Terms & Conditions

Source URL:
https://www.cpeonline.com/selfstudycourse/webcast/cybersecurity--how-to-deal-with-the-risks%2C-hidden-threats--and--the-latest-financial-reporting-disclosures-self-study-webinar-%2811-hours%29-2

Links:
[1] https://www.cpeonline.com/JavaScript:showObjectivesPopup();