

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 need for increasing damage from cyber threats

Recognize when cyber security solutions require both privacy and ethics (C)

Recognize current forms of cyber operations

Recognize the current characteristics of high profile cyberattacks

Recognize direct and indirect (C) cybersecurity regulation

Identify the goal of risk mitigation

Identify the role of privacy and ethical principles (C) in a cybersecurity context

Recognize an ethical approach to cybersecurity risk

Identify the characteristics of the Common Vulnerability Scoring System (CVSS)

Identify the role of cybersecurity controls within a cybersecurity system domain

Recognize both direct and indirect (C) cybersecurity remediation programs

Recognize the remediation goal of cybersecurity

Recognize the responsibilities of the NIS Security Response Group

Recognize the responsibilities of the Federal Cyber Security Regulation

Recognize the potential penalties associated with non-compliance with the GDPR

Identify the characteristics of penetration testing and penetration testing results

Identify approaches to threat intelligence gathering in incident resolution

Recognize options to protect against the risk associated with third parties

Identify the role of insurance in protecting against cybersecurity threats

Identify cybersecurity characteristics of business against cybersecurity threats

Recognize the role of cybersecurity controls in cybersecurity

Recognize the primary responsibilities of the Bureau of Cyber Security

Identify the potential impact of cybersecurity threats on an organization

Identify the ethical approach to cybersecurity risk management

Identify current public relation strategies for dealing with a breach

Recognize the role of digital marketing and IT media in the cybersecurity regulation of their use

Recognize the current professional standards used to report on ethical conduct and cyber operations

BottomPrerequisite:
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\(\);](https://www.cpeonline.com/JavaScript:showObjectivesPopup();)