Cyber Resilience

Cyber Resilience for the Business Continuity Professional
Duration: 4.5 Days (Four full days of instruction 8:30 a.m. - 5:00 p.m., followed by one half-day Cyber Resilience Examination 8:30 a.m. - 12:00 p.m.)

Cost: $2,750.00

Description
Organizations today are confronted by a wide range of cyberattacks, and your organization is no exception. There are countless opportunities for hackers to cause massive disruptions, all of which you will require a response that will involve you. That's why this course is an absolute must. More than just another statement of the problem, Cyber Resilience for the Business Continuity Professional is an information-packed four-day experience that will provide an understanding of how to address cyber disruptions within a business continuity framework.

You'll discover how business continuity and cybersecurity must integrate within every organization, using the five elements of cyber resilience: prepare/identify, protect, detect, respond, and recover. Collectively, these concepts and the resulting action plans will help to develop a strategy to effectively respond to unforeseen events and get your organization back up and running as quickly as possible. These two traditionally separate functions must work together, and with this course, you'll be able to take steps to make that happen in your organization. Doing so will streamline well-coordinated identification and response to attacks or data breaches, minimize costs, protect the organization's reputation, and give you the professional advantage of bringing the most current information and skills to the table.

Objective

1. Provide students with detailed instruction, framework, and guidance for implementing the concepts essential to combining cyber security and business continuity into an effective Cyber Resilience program.
2. Prepare students with actionable recommendations to represent an appropriate "value proposition" to an organization's executive management that will help to ensure any investment necessary to step up to a strong Cyber Resilience program.
3. Have students engage in cyber/BCM based exercises to help understand the issues you will face.
4. Share experiences with other professionals.
5. Prepare to pass the Cyber Resilience Examination, so you can be certified as a DRI International Certified Cyber Resilience Professional.

DRI International

For more information, visit **drii.org**.

Outline

DAY 1

- Introduction to concept of cyber resilience
- Types of cyber events
- How cybersecurity events impact business continuity
- Integrating cybersecurity into business continuity
- Organizational considerations
- Stepping up from cybersecurity and business continuity to achieve cyber resilience

DAY 2

- Develop an effective incident response
- Identify specific means to bringing cybersecurity incident response planning and entity continuity planning together
- Design strategies that mitigate loss should a breach occur
- Identify critical parameters of IT-related operations with an entity impact assessment
- List entity recovery strategies crucial to re-establishing technology and continuity of critical entity processes
- Advantages of identifying cyber-related risks and integrating them into entity planning and administration

DAY 3

- Creating cybersecurity framework
- Examine the latest cybersecurity framework
- Review existing regulations that govern cyber security protection and reporting
- Explain how to develop and implement safeguard protection for critical technology infrastructure and services in order to contain the impact of a cyberattack
- Discuss how to detect and monitor network attack indicators to ensure the effectiveness of safeguards
- Describe the importance of regular cyber awareness training
- Monitoring internal security events and correlate them to external threats

DAY 4

- Creating an effective response plan
- How to restore data and services that may have been impacted during a cyberattack
- Understand how Cybersecurity and Entity Continuity both work with reputation management
- Cybersecurity monitoring
- Creating effective crisis communication plans for cyber incidents
- List recommendations for preparing key suppliers in the event of a cyberattack
- Discuss how training and awareness initiatives should be employed to embed cyber resilience within the entire organization and ensure that personnel know the function of response plans