Participant Guide

This four-day class has been developed by DRI International to provide a comprehensive understanding of *Cyber Resilience for the Business Continuity Professional* and their proper application within a business continuity program. It is designed for the business continuity professional with less than two-years' experience.

DRI International
Train. Prepare. Recover.

Cyber Resilience for the Business Continuity Professional

1. Stepping up from Cybersecurity
2. Cyber Threats and Cyberattacks
3. The Value of Cyber Resilience
4. Integrating Cybersecurity and Entity Continuity
5. Cybersecurity Framework
6. Cyber Resilience Planning Phase 1
7. Cyber Resilience Planning Phase 2
8. Maintaining your Cyber Resilience Plan

Cyber Resilience Course Objectives

- Differentiate between cybersecurity and cyber resilience
- Compare cyber threats to cyberattacks
- Explain the value of cyber resilience
- Explain how cyber resilient plans integrate cybersecurity and entity continuity
- Differentiate between cybersecurity and cyber resilience
- Compare cyber threats to cyberattacks
- Explain the value of cyber resilience
- Explain how cyber resilient plans integrate cybersecurity and entity continuity

Table of Contents

3 Lesson Objectives

4 Top Entity Risks

5 The Changing Face of Hackers

6 Cyber Resilience Definition

7 Stepping Up from Cybersecurity and Entity Continuity

8 Two Concepts that Must Work Together

10 Knowledge Checks

Stepping up from Cybersecurity: Lesson 1 Objectives

Upon successful completion of this lesson, you should be able to:

- Describe why resilience is one of the most valuable long-term strengths of an organization
- Explain why it is important to build a cyber resilience strategy
- Compare the differences between cybersecurity and cyber resilience
- Identify some important cyber resilience terms

Class Activity: Cyber Resilience Terminology

Define the following terms:

Bot

Cybersecurity

Cyber Resilience

Hacker

Malware

Spyware

Virus

Worm

DDOS

Top Entity Risks

2013	2015	2017
1. Business Interruption, supply chain risk 2. Natural Catastrophes 3. Fire, Explosion 4. Changes in Legislation and regulation 5. Intensified competition	1. Business Interruption, supply chain risk 2. Natural Catastrophes 3. Fire, Explosion 4. Changes in Legislation and regulation **5. Cyber Incidents**	1. Business Interruption, supply chain risk 2. Market Developments **3. Cyber Incidents** 4. Natural Catastrophes 5. Changes in Legislation and regulation

Organizations today are confronted by a wide range of cyberattacks.

Given the development of technologies and the growth of entity data, this is likely to remain the case moving forward, which may provide new opportunities for hackers to cause such massive disruptions.

Write down the top five global business risks for 2018.

Global Risk 1:

Global Risk 2:

Global Risk 3:

Global Risk 4:

Global Risk 5:

:

The Changing Face of Hackers

Compare and write down the top groups in both 1997 and 2017.

1997	2017
Who are the top group of hackers?	What is the biggest motivation behind the attacks?

Hacker Risk Activity

- Pair up with someone in class
- List at least three risks hackers pose to your entity
- Be prepared to share your discussion

Risk 1:

Risk 2:

Risk 3:

Notes:

Cyber Resilience Definition

Write down the definition of cyber resilience.

Cybersecurity vs Cyber Resilience

Cyber resilience is a strategy appropriate toward cyberattacks used to disrupt your operations, not cyberattacks used to steal your data (once data has been stolen or compromised, resilience becomes a moot point – which is why having a solid cybersecurity program is so critical).

What is the difference between cybersecurity and cyber resilience? Write down the two characterizations of the different types of cyberattacks inside the boxes.

Cybersecurity refers to the methods and processes of protecting electronic data, including identifying it and where it resides, and implementing technology and entity practices that will protect it.

Cyber resilience is the ability to withstand or quickly recover from cyber events that disrupt usual entity operations.

To fully understand the difference, consider these two *broad* characterizations of the different types of cyberattacks:

One is meant to:

The other is meant to:

Cyber Resilience and Cybersecurity Activity

- Pair up with someone in class
- Describe how cyber resilience and cybersecurity is implemented in your entity
- Be prepared to share your discussion

Stepping Up from Cybersecurity and Entity Continuity

The world is changing rapidly, and cyber criminals are adapting to it faster than security solutions are being developed.

Targeted Attacks	• Targeted attacks by skilled and persistent cyber criminals are now a worrying entity reality
Traditional Security Measures	• Traditional security measures such as firewalls and antivirus software are proving inadequate protection in the evolving threat landscape

Preventive Strategies and Breaches

While preventive strategies are important, we must anticipate that there still may be a breach, and so we must build a cyber resilience strategy to reduce the negative impact of that event when it occurs.

It is widely accepted that it's not a matter of "if" but, rather, "when" an organization will suffer a cyberattack … therefore, organizations should assume that they will be breached.

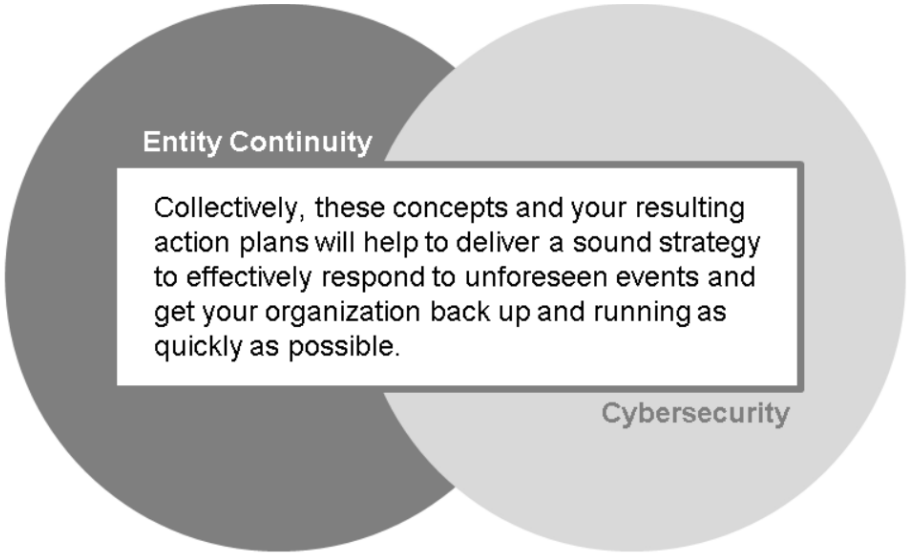
What are two reasons that resilience is one of the most valuable long-term strengths of an organization? Write your answers below.

Reason 1:

Reason 2:

Two Concepts that Must Work Together

We will further develop these concepts to demonstrate that entity continuity and cybersecurity must integrate within every organization. The concepts must work together, however, as they are vital to your organization's ability to survive any pending cyber storm!



Notes:

Class Exercise

1. Work in assigned teams
2. Select a team presenter
3. Be prepared to present your findings to the class
4. Develop a presentation to the leadership of your entity addressing the following:
    a. The importance of implementing cyber resilience and cybersecurity
    b. Any relevant regulations to your entity
    c. The resource requirements to implement cyber resilience and cybersecurity

The importance of implementing cyber resilience and cybersecurity:

Any relevant regulations to your entity:

The resource requirements to implement cyber resilience and cybersecurity:

Notes:

Knowledge Checks
Cyber Resilience 1: Stepping up from Cybersecurity

Circle the best choice for each question below. There is only one correct answer for each question.

---

1. What is the definition of malware?

   a) A type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code

   b) A malicious computer program which misleads users of its true intent

   c) Software that is intended to damage or disable computers and computer systems

   d) Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive

---

2. Why it is important to build a cyber resilience strategy?

   a) To focus directly on threats to your key assets

   b) To focus on the controls that can mitigate threats to your assets

   c) To reduce the negative impact of a breach when it occurs

   d) To reduce the risk of a cyberattack and strives to protect entities, organizations, and individuals from the deliberate exploration of systems, networks, and technologies

---

3. Which of the following statements best describes cybersecurity?

   a) Cybersecurity is the ability to withstand or quickly recover from cyber events that disrupt usual entity operations

   b) Cybersecurity refers to the methods and processes of protecting electronic data, including identifying it and where it resides, and implementing technology and entity practices that will protect it

   c) Cybersecurity action plans include entity continuity strategies that effectively respond to unforeseen events and get your organization back up and running as quickly as possible

   d) Cybersecurity is a strategy appropriate toward cyberattacks used to disrupt your operations, not cyberattacks used to steal your data

---

4. Why is cyber resilience considered one of the most valuable long-term strengths of an organization?

   a) It defines its ability to grow and survive in a changing environment by successfully implementing evolving strategies

   b) It is used as a method to protect electronic data from cyberattacks

   c) As crises are often driven by events that are within their control, resilience focuses on the defenses set up to protect your data

   d) It separates cybersecurity from entity continuity resulting in action plans that will help to deliver a sound strategy to effectively respond to unforeseen events

Notes:

Notes: