Future-Proof Your Business: Essential Cyber Incident Response for Irish Businesses

Irish SMEs are increasingly targeted by complex cyberattacks, threatening operations, reputation, and finances. This crucial course empowers non-technical owners and managers with the practical know-how to navigate a cyber incident. By demystifying the **Incident Response Plan**, we enable a structured, compliant, and rapid recovery, protecting your assets, data, and hard-earned trust from panic to prevention.

High-Level Outline:

1. Understanding the Cyber Threat Landscape (Why this Matters to YOU)
2. Your Role in Early Detection & Reporting
3. The Incident Response Journey: From Containment to Recovery
4. Navigating the Aftermath: Communication, Compliance & Learning
5. Staying Ready: Maintaining Your Cyber Resilience

Objectives:

Upon completion of this course, participants will be able to:

- Understand the fundamental principles and importance of a robust Incident Response Plan for small to medium-sized businesses.
- Recognise the common signs of cybersecurity incidents and know the correct immediate actions to take.
- Grasp the purpose and key activities within each phase of the incident response lifecycle (Detection, Containment, Eradication, Recovery, Post-Incident).
- Appreciate their own role and the roles of key personnel within the Incident Response Team during a cyber crisis.
- Understand the critical importance of timely and appropriate communication with internal and external stakeholders.
- Gain awareness of key legal and regulatory obligations, including GDPR, NIS2, and DORA, in the context of cybersecurity incident reporting and compliance in Ireland.
- Recognise the value of continuous improvement, regular training, and testing in maintaining organisational cyber resilience.

Learning Outcomes:

By the end of this course, attendees will be able to:

- Identify common indicators of a cybersecurity incident within their organisation.
- Execute the initial reporting and isolation procedures for a suspected incident.
- Describe the core activities performed by the Incident Response Team during containment, eradication, and recovery.
- Explain why documentation, evidence preservation, and post-incident reviews are crucial.
- Articulate the general requirements for reporting cybersecurity incidents and data breaches under GDPR, NIS2, and DORA, especially as applicable in Ireland.
- Collaborate more effectively with the Incident Response Team during an actual incident.
- Advocate for ongoing training, regular plan reviews, and incident response drills within their organisation.

Course Duration: 2 Hours (Flexible, can be adapted)

Included: Incident Response Plan template (in Word format) and copy of the slides.

Audience: Micro/Small/Medium Business Owners or Managers, responsible for day-to-day operations of the business.

Capacity: Maximum 20 attendees