Stephen M. Yoss
Technology. Instructor. Fireworks.

48 Hours: Anatomy of a Real Cyberattack

Credits	Field of Study	Course Category	Level
2.0	Information Technology	General	Intermediate

COURSE DESCRIPTION

This narrative-driven session provides a minute-by-minute deconstruction of a realistic cyberattack, modeled on actual events. Participants follow the progression of a breach from the initial phishing email on a Monday morning to the final ransom demand on Wednesday night. By examining the attack simultaneously through the eyes of the victim, the attacker, and the incident responder, the course clarifies how technical decisions and human errors intersect to create a crisis. The presentation avoids blame and instead focuses on the technical annotations of the attacker's moves and the first 48 hours of recovery efforts. The session concludes with a postmortem analysis of the specific controls that could have prevented the breach and a defense framework built directly from the narrative events.

LEARNING OBJECTIVES

• Identify the common stages of a multi-day cyberattack including initial access, lateral movement, and data exfiltration.

• Analyze the attacker's decision-making process to understand why specific security controls succeed or fail.

• Differentiate between effective and ineffective incident response actions during the first 48 hours of a breach.

• Evaluate a defense framework designed to mitigate the specific technical and human vulnerabilities exploited in the case study.

MAJOR TOPICS

• Chronological breakdown of a phishing-originated breach

• Technical annotations of attacker lateral movement and privilege escalation

• Psychology of the attacker: Motivations and decision-making during the exploit

• Incident response protocols: The reality of the first 48 hours of recovery

• Postmortem analysis: Critical failure points and preventative measures

• Constructing a narrative-based defense framework for business professionals

ADDITIONAL INFORMATION

- **Who Should Attend:** Business professionals, CPAs, firm partners, and organizational leaders who need to understand the practical mechanics of a security breach beyond theoretical concepts.
- **Prerequisites:** A fundamental understanding of general business technology and common office software.
- **Advanced Preparation:**
- **Tags:** cybersecurity, incident response, risk management, data breach, information security
- **Course ID:** 2205
- **Short Name:** 48 Hours: Anatomy of a Real Cyberattack

Course Created:2026-09-17 • Course Last Updated: 2026-09-17 • PDF Exported On: 2026-09-18