Incident Response Clinic

Kieran Norton, Deloitte & Touche

Professional Techniques Track – Session T11

Abstract:

While proactive security is the best defense, today's reality is that breaches will continue to occur. Whether a breach involves the loss of confidential customer information, corporate intellectual property or employee protected health information, companies face significant challenges recognizing, responding and mitigating the impact of such breaches.

This session will focus on best practices in the incident response process and will include an interactive walk through of three different breach scenarios that are based on actual events.

This course is designed to provide a high-level overview of incident response processes and practices. It will:

- Discuss the current landscape and common challenges
- Outline best practices in developing an incident response program
- Define the primary steps in the incident response process
- Include multiple incident response scenarios that we will walk through together during this interactive session

Target Audience:

- IT Auditors with 2-3 years' experience
- Anyone interested in gaining a better understanding of the incident response process, or anyone wanting to sharpen their incident response skills
- This will not be an in depth technical session, so no forensics knowledge is necessary

COBIT Objectives:

This course will focus on DS5 primarily

Speaker Bio:

Kieran Norton (CISSP) is a Senior Manager in the Security & Privacy Services practice within Deloitte & Touche's Technology Risk Services group. Kieran is focused on designing, developing and delivering solutions in the areas of network security and data protection. His experience includes network and application security, vulnerability assessment and penetration testing, intrusion detection and incident response as well as security governance and program development/deployment.

Kieran's incident response experience includes: leading a post mortem analysis of the incident response program and handling of one of the largest data breaches in modern history; leading an incident response and forensic investigation engagement for a fortune 500 company focused on employee/insider misconduct; managing an incident response engagement for a major internet services company focused on attack confirmation, identification of malicious activity post compromise and incident containment; leading an investigation into wire transfer fraud for a financial services company; and, advising a major manufacturer as they made critical decisions during the post incident breach notification and remediation process.

In addition, Kieran has significant experience leading data protection projects focused on addressing regulatory and industry requirements. Prior to Deloitte & Touche, Kieran spent more than 12 years in the IT industry and in professional services firms.