Solvay Brussels School
Economics & Management

Seminar on Cybersecurity Response

This seminar is intended to Information Security professional, IT professionals and business managers involved with the implementation of enterprise capabilities for adequately responding to attacks. It involves educating on various drivers, skills and competences.

Location: Brussels (R42 Building, ULB)

Dates: Three days to be determined in Q4 2015 (Early Bird registration is open)

Price: 2000€ plus VAT
Discounted prices for members of partner organizations, Solvay Alumni and ISACA members.
Participants receive the publication "Responding to Targeted Cyberattacks"

Contact: Joanna Jong (joanna.jong@solvay.edu or 02/650 66 34)

Seminar content

1. Introduction and Threat Landscape (4h)
2. Preparation (4h)
3. Investigation (4h)
4. Eradication (4h)
5. Post-eradication (4h)
6. Breakout case studies

Topics that are addressed: A Case Study of the Need for Change; Evolution of the Threat Landscape; Adaptive Attack Vectors; A Watershed Event; The APT Life Cycle ; What Are Others Doing?; Summary ; Build a Team, Make a Plan; Establish Key Relationships; External Relationships; Internal Relationships.; Determine Authorities; Inventory Existing Technologies; Standardize the Investigation Process; Training and Governance; Exercises; Security Program and Response Plan Reviews.; Establish Critical Capabilities; Host-level Activity Awareness; Network-level Activity Awareness.; Search; Computer Forensic Analysis; Malware Analysis.; Threat Intelligence; Vulnerability Identification; Conducting a Security Breach Investigation ; Who Attacked Us?; What Was Targeted? ; When Did Various Events Occur? ; From Where Did the Attacks Come? ; Why Did They Attack?; How Did They Get In, Stay In and Get the Data Out?; Other Important Areas to Consider; On the Quality of Intelligence3.10 Evidence Handling ; Preservation and Collection Memorandum; Chain of Custody; MD5 Hashing ; Write Blockers.; Reconcile Record Counts; Attorney-client Privilege or Attorney Work Product Privilege; Insurance Claims; Investigating Anonymously ; Safeguarding the Investigative Actions.; Data ; Data in Motion ; Protecting the Investigation.; Credential Protection; Plan for Eradication.; Create the Eradication Event Team.; Develop the Eradication Event Plan; Determine the Eradication Event Date; Know the Attacker's Techniques, Tactics and Procedures.; Establish Communication Protocols ; Establish a "War Room" ; Establish Secure Communications and Information Sharing Mechanism(s); Execute the Plan ; Execute a Password Change; Block Attacker Command and Control.; Rebuild Compromised Systems; Submit Malware to Antivirus Vendors; Monitor for Attempted Reentry; Validate Eradication Activities; Maintain a Heightened State of Alert.; Validate Controls; Brief Stakeholders; Lessons Learned; Strategic Change—Cybersecurity Transformation.