Incident Response and Review for IT departments. What to do after the Incident Response Plan is activated.

Description:

In this one day session the class will cover how an IT department responds to incidents in the organization. Students will cover the steps to take **after** the Incident Response Plan takes effect, and understand how the department needs to respond to requests, document process and provide deliverables to the Incident Response Manager. This is a highly interactive discussion based class. The students will be reviewing real and mock, large and small incidents.

Background:

Many organizations have a formal Plan for how the organization will respond to incidents. In the event of an incident, IT is heavily involved in the containment and resultant investigation. IT professionals will likely deal with management, legal departments, and law enforcement during the incident. Understanding the requirements of the Plan, and the expectation of the parties involved, will make the process much smoother, and could provide significant value and protection to the individuals and the organization.

Agenda:

Morning:

- What is an Incident Response Plan?
- What is the intended result of the Plan?
- What are the basic questions to address?
- What is the impact of an incident to the organization?
- What is IT's role in the Plan?
- Who will be asking you for information?

Afternoon:

- Define the IT roles of the incident response Plan
- Documentation
  - Request for Action
  - Response
  - Deliverables
  - Evidence
  - Timeline
  - Follow-up's
- Building a checklist
- Scenario practice for incident response
- Reports for your Incident Response Manager
- The day after the incident
- Incident Response Planning
- Practice, Practice, Practice