# CS 798: Digital Forensics and Incident Response

## Lecture 21 - Pre-Incident Preparation

Diogo Barradas

Winter 2025

University of Waterloo

# Outline

1. Incident Response

2. Pre-Incident Preparation
   - Preparing the organization
   - Preparing the team
   - Preparing the infrastructure

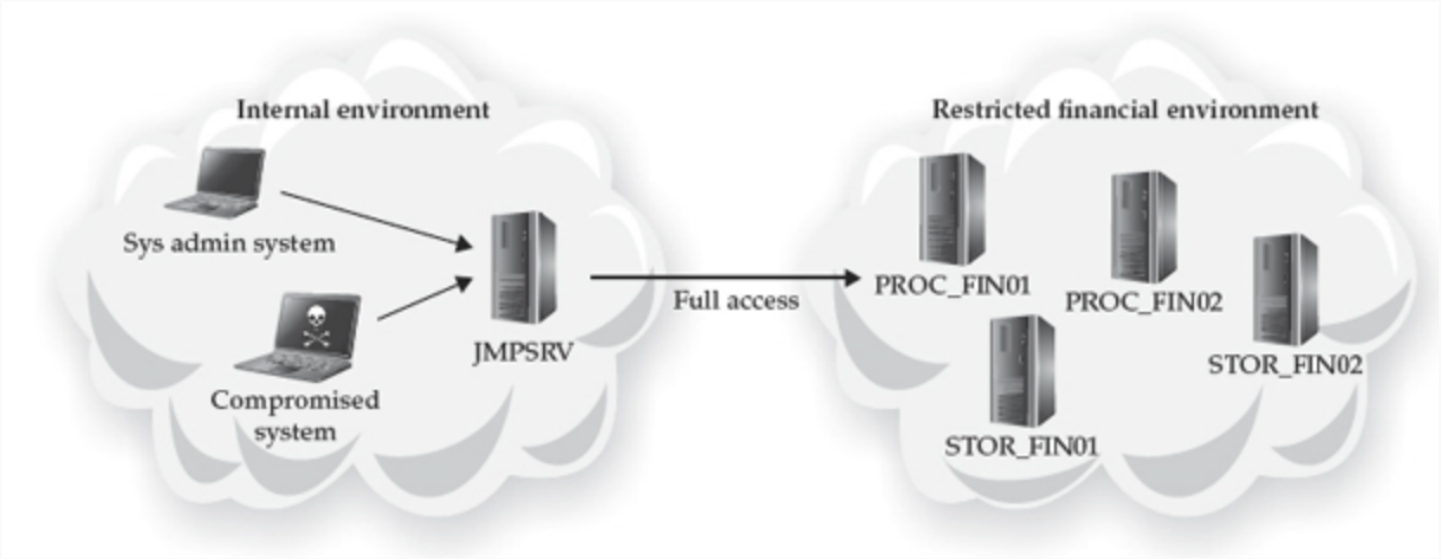
# Incident Response

# What is an incident?

- **Definition by NIST**: An incident is a "violation or threat of violation of computer security policies, acceptable use policies, or standard security practices"

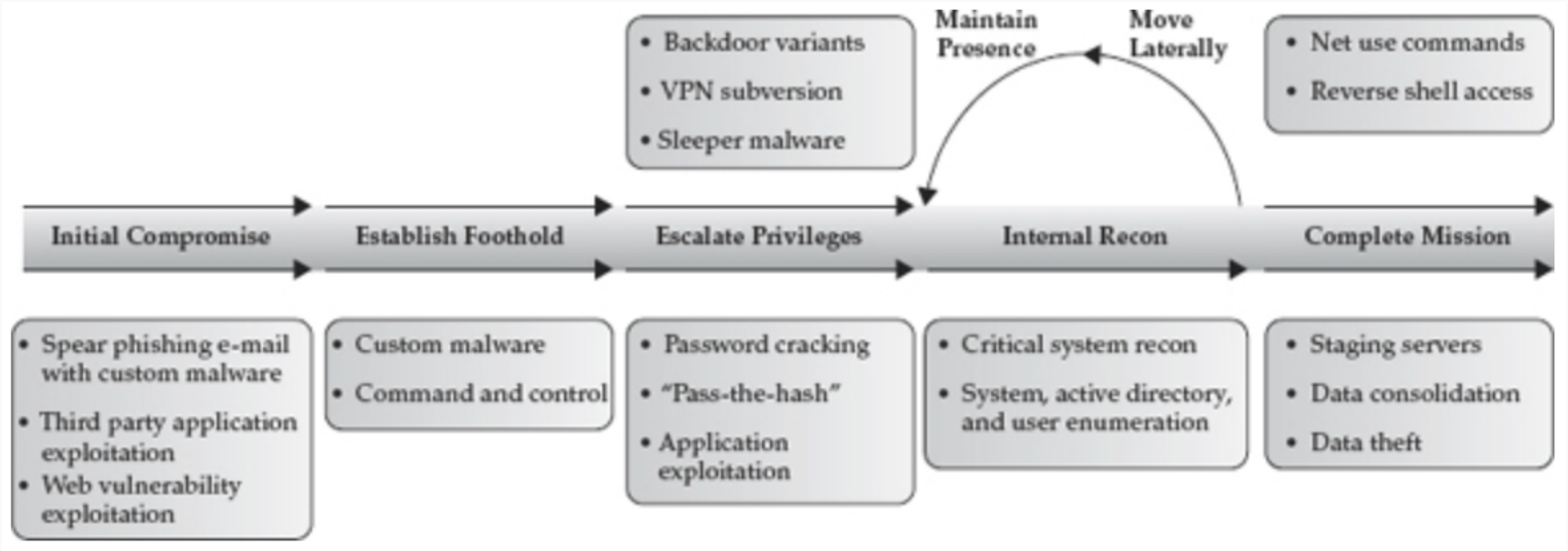
# An example incident

- **Example incident**: an attacker compromises a system in an internal network (e.g., through social engineering) and gains access to a restricted network due to a misconfigured server



# The attack lifecycle

- The typical attack lifecycle can be adapted to fit any incident



# How bad do incidents look today?

- In practice, intrusions are getting more complex over time:
  - May include hundreds of (geographically dispersed) compromised systems
  - Attackers increasingly use anti-forensic techniques
  - Attackers use multiple tactics to access computer systems
- The **goals of an incident response** may vary, depending on:
  - Severity of the incident, the victim's needs, the timing of the incident, the intent of the attack group, the industry or customers impacted, etc.

# Why should we care?

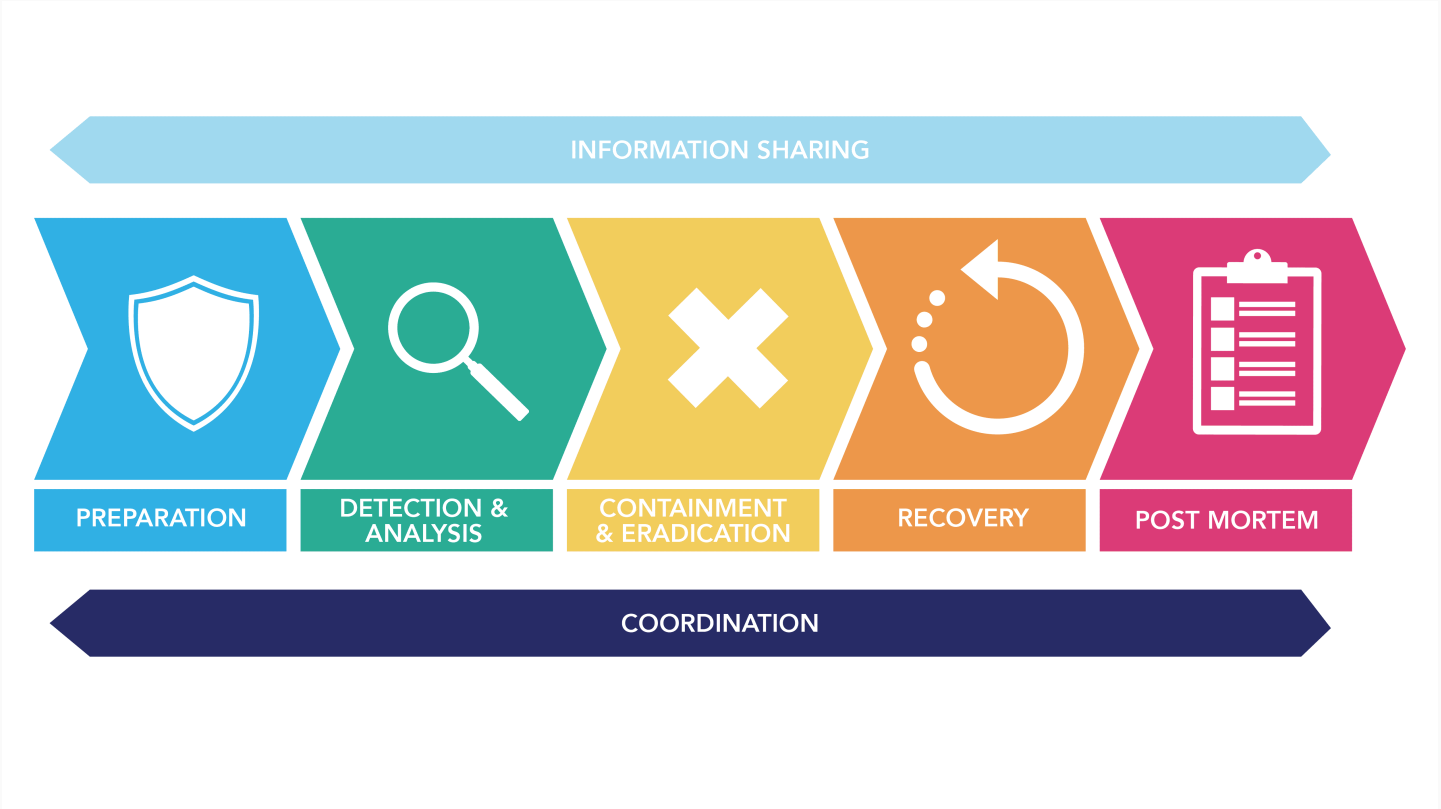
- Many attacks now have a broad scope, affecting the private and public sectors, as well as individual citizens
- Cyber-criminals operate with little risks or repercussions
- Digital investigations get increasingly more complex, requiring incident responders to understand how to normalize, parse, and make sense of large amounts of data

# What is incident response?

- **Incident response** is a coordinated and structured approach to go from incident detection to resolution. It includes:
  - Confirm whether or not an incident occurred
  - Provide rapid detection and containment
  - Determine and document the scope of the incident
  - Minimize disruption to business and network operations
  - Restore normal operations
  - Manage the public perception of the incident
  - Allow for criminal or civil actions against perpetrators
  - Enhance the security posture of a compromised entity

# Incident response

- Today, we will focus on preparing an organization's response to an incident



# Pre-Incident Preparation

# Preparing for incidents

- An organization should be prepared to methodically conduct an investigation and remediate potential incidents
- However, the chances of performing a successful investigation are low unless an organization commits resources to appropriately prepare for such an event
- The larger the organization, the more difficult this gets

# Three main areas of focus

- Preparing an organization against incidents involves three main efforts:
  - Preparing the organization itself
  - Preparing the incident response team
  - Preparing the infrastructure

# Pre-Incident Preparation

## Preparing the organization

# Preparing the organization

- Organizations tend to focus on technical issues first
  - e.g., buy traffic inspection middlebox, acquire IDS systems
- However, it is often the neglect of non-technical issues that hinder proper incident response capabilities
- We will cover:
  1. Identifying risk
  2. Policies that promote a successful IR
  3. Working with outsourced IT
  4. Thoughts on global infrastructure issues
  5. Educating users on host-based security

# 1. Identify risks

- The initial steps of pre-incident preparation involve understanding the **risks** faced by the organization
- By identifying risk, resources can be managed effectively to better respond to the incidents that are most likely to affect the organization
  - i.e., not all incidents require the same attention
- Useful questions:
  - What are the critical assets? Payment info? PII?
  - What is their exposure? Who gets access?
  - What are the threats?
  - What regulations must the organization comply with?

# 2. Enact policies

- Every step made during an investigation should be directed by a pre-existing **policy** (typically drafted by the CISO's office)
- Delineate expectations on the coverage of search and seizure of the organization resources and interception of network traffic
- Typical policies include:
  - **Acceptable Use Policy** - What's users' expected behavior?
  - **Security Policy** - How are sensitive resources protected?
  - **Remote Access Policy** - Who can connect to the organization's resources, and how?
  - **Internet Usage Policy** - What is an appropriate general Internet usage within the organization?

# 3. Establish agreements with contractors

- IT functions are oftentimes outsourced to contractors and other companies
- Investigations that require work by contractors may be stalled due to long approval processes, extra costs, or contractually innacessible data
- Organizations should make arrangements for ensuring responsiveness during critical events and draft options for work that may be out of the scope of the initial contract
- Flexibility is key to respond rapidly to an incident

# 4. Reason about a global infrastructure

- Incidents that affect multinational companies might face difficulties tied to different privacy laws and regulations
- Coordinating incident response teams across different timezones might be a difficult task, and requires additional efforts of synchronization
- Investigators will need to collect and analyse vast amounts of data. Data transfer procedures will also potentially stall investigation efforts

# 5. Educate users

- Users play a critical role in the security of an organization
- An effective security training is one of the best initiatives that an organization can take to decrease the chance of incidents
- Users should be typically made aware of the dangers of installing unknown software in the organization's machines and have a clear communication line with an expert to report suspected attack attempts

# Pre-Incident Preparation

## Preparing the team

# Who is involved

- The **incident response team** is interdisciplinary in nature, and consists of:
  - An **investigation team**: determines what happened and performs a damage assessment
  - A **remediation team**: removes the attacker from the environment and enhances the victim's security posture
  - Some form of **public relations team**

# Define the mission

- The **mission** of the incident response team helps keep the team focused and sets expectations for their work
- The mission may include:
  - Respond to all (suspected) security incidents
  - Conduct a complete and impartial investigation
  - Control and contain the incident, assessing damages
  - Protect privacy rights set by laws and regulations
  - Provide upper management with reccommendations

# Define communication procedures

- Defining **communication procedures** in advance of an incident is crucial for an organized incident response
  - Sub-teams will have to work simultaneously
- **Tips for internal communications**:
  - Encrypt e-mails
  - Properly label all documents and communication
  - Monitor conference call participation
  - Use case numbers or project names to refer to an investigation
- **Tips for external communications**:
  - Assess the best time to externally disclose the incident
  - Consider the language of the report
  - Choose an appropriate channel for the disclosure
  - Consider how disclosure might affect the ongoing investigation

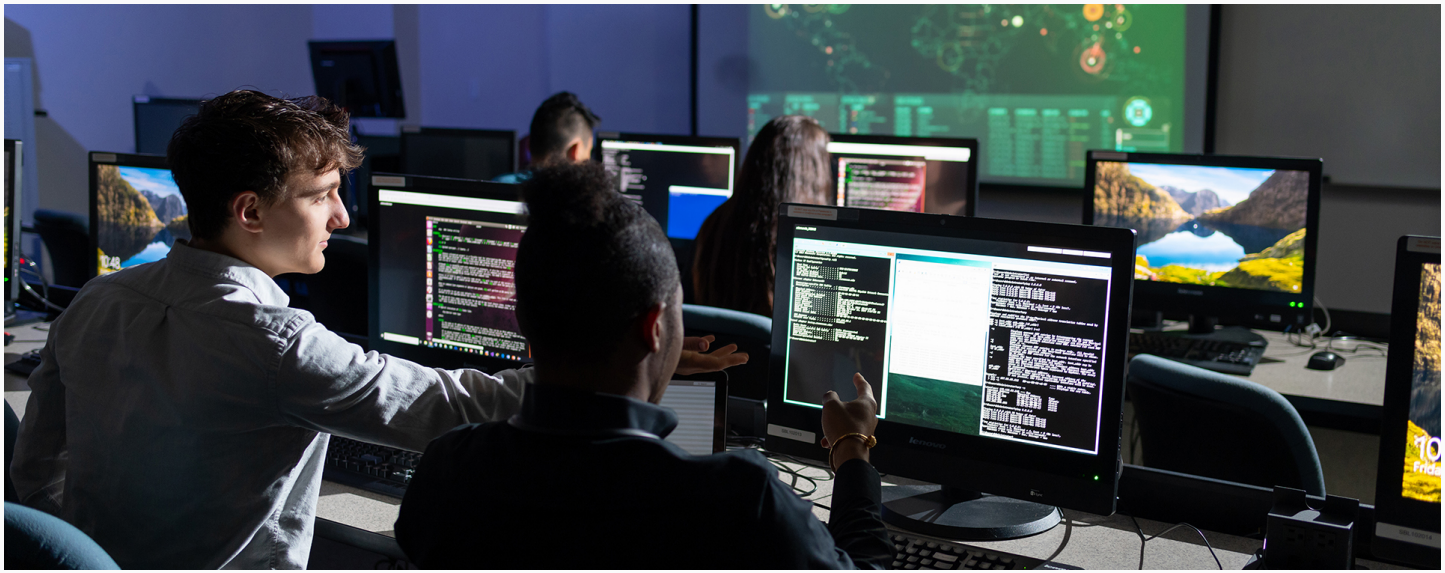
# Define deliverables

- The incident response team should define its primary **deliverables**, e.g., frequency, completion timeframes
- The most important kind of deliverable for an incident response team will typically be in the form of investigative reports, e.g., forensic reports

| Name | Purpose | Delivery Target |
|---|---|---|
| Case Status Report | Update stakeholders on progress of an individual case. | Recurring: Daily or as required |
| Live Response Report | Document findings from initial live response triage of a single system. | Draft: Within one business day<br>Final: Within two business days |
| Forensic Examination Report | Document the detailed findings from forensic analysis performed on an item of evidence. | Draft: Within four business days<br>Final: Within six business days |
| Malware Analysis Report | Document the findings from analysis of suspected malicious software. | Draft: Within three business days<br>Final: Within five business days |
| Intrusion Investigation Report | Consolidate all reports and findings related to a single incident and create a high-level executive summary. | Draft: Within five business days of completion of the investigation<br>Final: Within eight business days of completion of the investigation |

# Define resources needs

- Incident response teams will typically have special hardware and software requirements (at least the forensics team will)
- The team will need training with such tools and/or systems
- Many commercial training programs exist for DFIR
  - e.g., SANS Institute



# Define documentation procedures

- In the context of an incident investigation, **documentation** may refer to policy, procedures, knowledge management, or workflow within the team
- While reporting is flexible and can be decided on an organization basis, it is crucial to properly document evidence (we saw this before!)

# Pre-Incident Preparation

## Preparing the infrastructure

# Preparing the infrastructure for incident response

- The incident response team should have the ability to acquire data and search for relevant material across the organization as easily as it does on a single machine
- Thus, the forensics team must be able to be in control of the organization's infrastructure and have awareness over multiple vantage points

# Computing device configuration

- Computing devices like servers, desktops, and laptops harbor a vast amount of evidence that might be relevant
- An organization should configure these systems to facilitate an effective investigation (and minimize the chances of an incident, e.g., apply patches)
- Two things are crucial:
  - **Understand what you have**: Difficult to protect systems we don't know about
  - **Improve and augment**: Ensure that the organization's systems are set up with proper logging, antivirus, HIDS, and forensic helper software

# Asset management

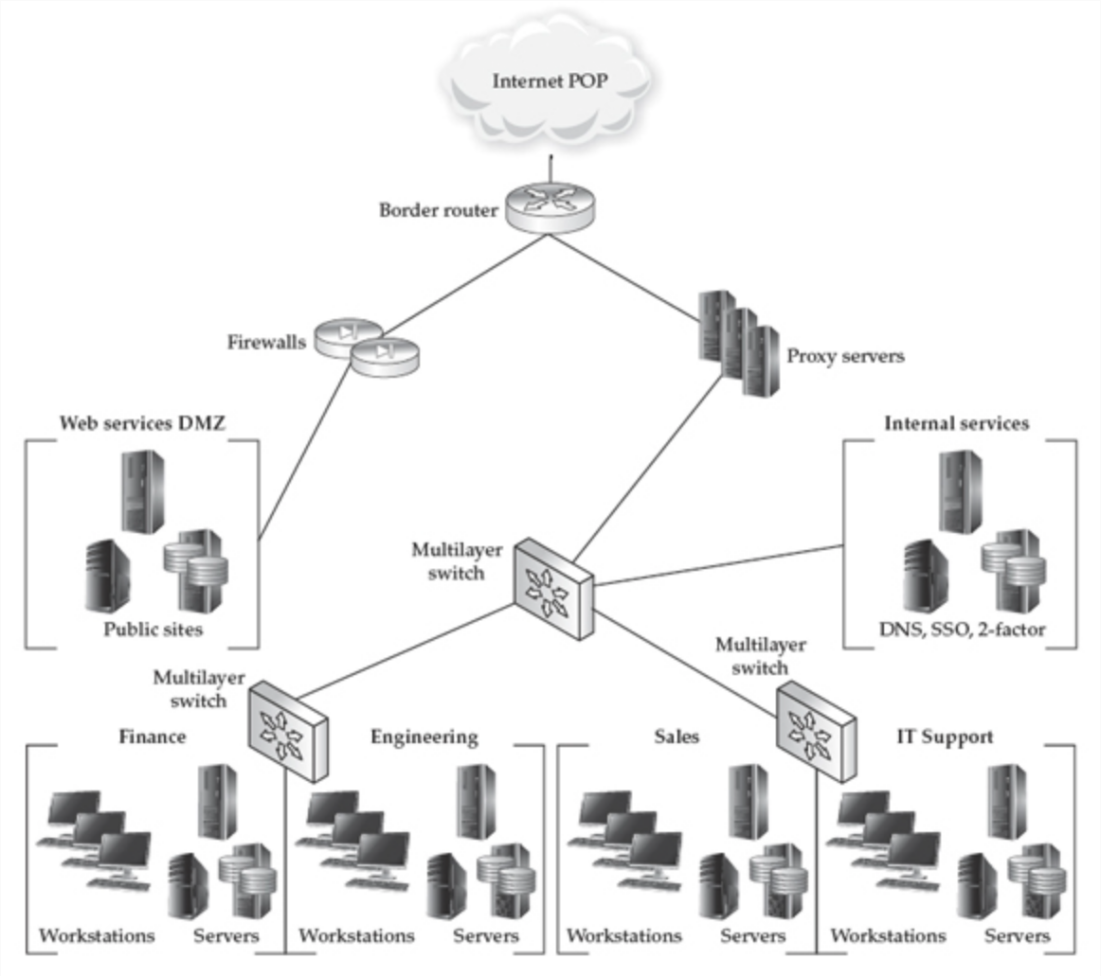
- It is important to keep a record of what systems exist within the organization, and what their details are:
  - Date provisioned
  - Ownership
  - Business unit
  - Physical location
  - Contact information
  - Role or services
  - Network configuration
- If necessary, this information can be acquired (or refreshed) through surveys

# Host instrumentation

- The initial phases of an investigation require the collection of evidence and following leads
- How should the organization's machines be instrumented to help this process? Is the team in control?
  - **Event logs**: Centralized logging may help have all information in a single place. However, how are logs collected? Where are they stored? For how long?
  - **Antivirus and HIDS**: How do these log events? Will they delete malware samples upon detection? Are these sending detection data back to the software vendor?
  - **Investigative tools**: Investigative tools should be deployed one the standard build for new systems and provide increased awareness about artifacts over multiple machines

# Network configuration

- An organization's network is often a large and dynamic system
- It is important to design it in such a way that the chances of an incident are minimized



# Network Segmentation and Access Control

- A common practice is to **segment** a network based on the information processed by the systems within each segment
- Controlling traffic between segments offers enhanced monitoring opportunities and more effective reactive measures:
    - **Traffic filtering**: Ingress and eggress filtering is essential to protect the network's perimeter
    - **Web, chat, and file transfer proxies**: Traffic to external resources should be inspected by a proxy w/ advanced filtering
    - **Two-factor authentication (2FA)**: VPN traffic originating from the Internet should be controlled with 2FA credentials, as well as servers, jump boxes, admin worstations, etc.

# Documentation

- Through growth, mergers, and acquisitions, maintaining accurate and current network diagrams is a tough task
- However, the incident response team uses this **documentation** during an investigation to determine risk, scope, and remediation measures
- Part of a good documentation plan is the storage of various devices' configuration. The team also needs access to network configurations, e.g., routers, firewalls, and switches

# Takeaways

- Computer incidents are on the rise. Tackling them effectively requires multi-disciplinary teams with proper coordination.
- Organizations must understand their assets and risks, have well-equipped response teams and clear processes put in place to efficiently address incidents.
- Incident preparation spans multiple concerns beyond IT, which encompass overcoming non-technical organizational challenges.

# Pointers

- **Textbook:**
  - Luttgens – Chapters 1–3
- **Literature:**
  - NIST - Computer Security Incident Handling Guide