Incident Response

Lecture 7

What is an Incident?

- A **computer security incident** is any action or activity – accidental or deliberate – that compromises the confidentiality, integrity, or availability of data and information technology resources.
- Incidents also include the use of technology for criminal activities such as: fraud, child porn, theft, hacking etc…
- Policy violations may also be considered security incidents.

- **An incident response plan (IRP)** ensures that in the event of a security breach, the right personnel and procedures are in place to effectively deal with a network security incident as it occurs.
- Having an incident response plan in place provides a targeted response to contain and remove the threat.
- A proper incident response starts by determining your most critical data and backing it up in a remote location like the cloud.
- **The most vital systems and data should receive prioritized backups.** Along with backing up data, you should have a backup plan until critical systems and functions are restored.
- Employees understanding their roles and knowing how to execute them during a breach is also crucial for quick cyber incident recovery.

Team Leadership and Duties

- CISO or Operations Team Lead usually acts as CSIRT Leader
  - ❑ Convene the **CSIRT (Computer Security Incident Response Team).**
  - ❑ Select additional support members as necessary for the reported incident.
  - ❑ Contact the Chief Information Officer.
  - ❑ Conduct meetings of the CSIRT.
  - ❑ Ensure meetings are documented.
  - ❑ Direct team training on an ongoing basis.
  - ❑ Periodically report status of incidents to the CIO.
  - ❑ Manage incidents.
  - ❑ Ensure incidents are documented.
  - ❑ Coordinate team incident research and response activities.
  - ❑ Conduct a debriefing of lessons learned and report to the CIO.

Team Expertise

- ❑ **Chief Information Office (CIO)**
- ❑ **Chief Auditor Office**
- ❑ **Legal**
- ❑ **Human Resources**
- ❑ **Information Security (CISO or Representative)**
- ❑ **Registrar**
- ❑ **Public Information Officer**
- ❑ **Platform Specialists**
- ❑ **Financial Administrators**
- ❑ **Law Enforcement**

Incident Response Goals

- Preserving the confidentiality, integrity and availability of enterprise information assets.
- Minimizing the impact to the organization.
- Providing management with sufficient information to decide on appropriate course of action.
- Providing a structured, logical, repeatable, and successful approach.
- Increase the efficiency and effectiveness of dealing with an incident
- Reduce the impact from both financial and human resources perspectives.
- Provide evidence that may become significant should legal and liability issues arise.

Incident Models

- There are always some incidents which are not new. They may happen again over a period of time. Therefore it is best practice to have pre-defined model to handle such incidents.
- An incident models should include:
- Steps that should be taken to handle the incident: chronological order of the steps that should be taken, with any dependences or co-processing defined
- Responsibilities – who should do what
- Timescales and thresholds for completion of the actions
- Escalation procedures; who should be contacted and when
- Any necessary evidence-preservation activities

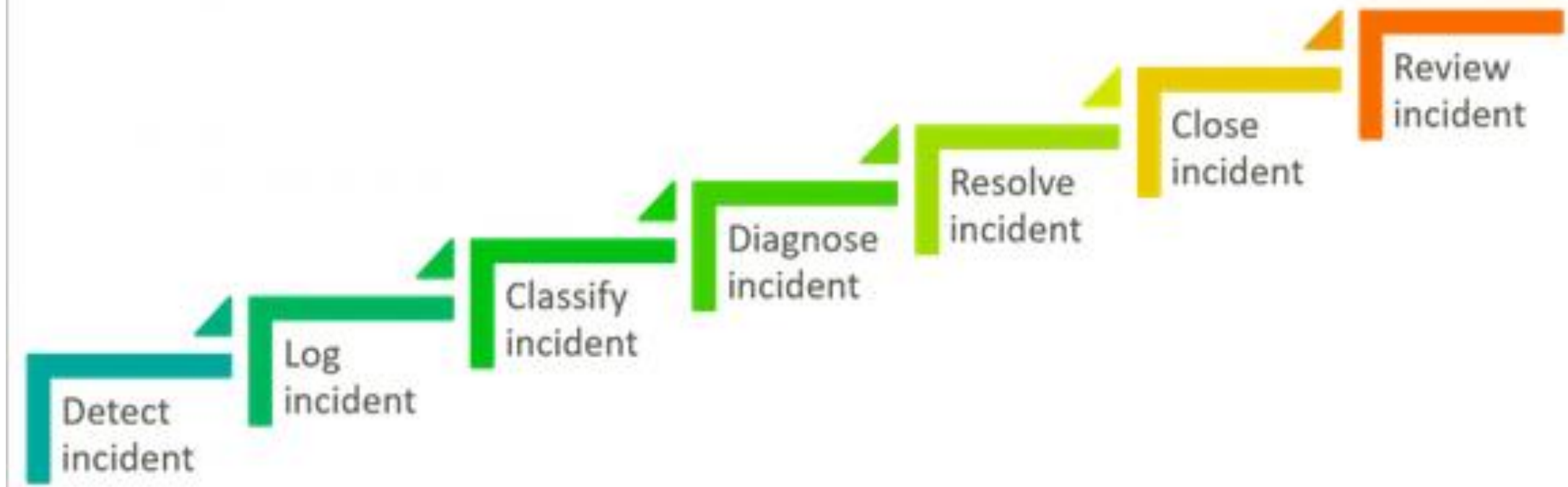
Incident Management Process

- The incident process provides efficient incident handling, which in turn ensures continual service uptime

1. **Incident Identification, Logging and Categorization**
2. **Incident Notification & Escalation**
3. **Investigation and Diagnosis**
4. **Resolution and Recovery**
5. **Incident Closure**

Incident Management

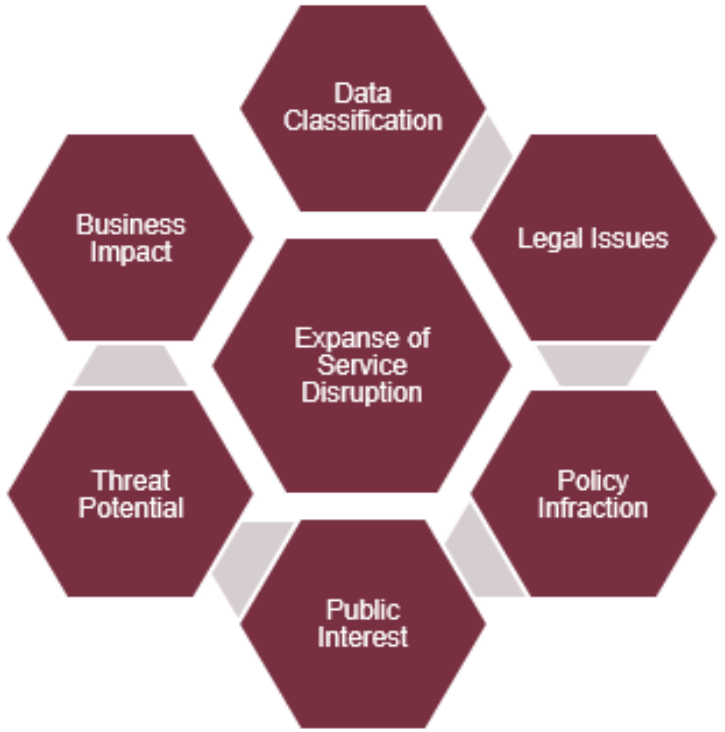
Activities in successful incident management



1. Incident Identification, Logging, and Categorization

- Incidents are identified through user reports, solution analyses, or manual identification.
- Once identified, the incident is logged and investigation and categorization can begin. Categorization is important to determining how incidents should be handled and for prioritizing response resources.

- The CSIRT will classify each incident as a Class A, Class B, or Class C incident based upon risk severity. The following criteria are used to determine incident classification:



Class A Incident: Low Severity

- A Class A incident is any incident that has a low impact to university information technology resources and is contained within the unit.
- The following criteria define **Class A** incidents:
  1. **Data classification:** Unauthorized disclosure of confidential information has not occurred.
  2. **Legal issues:** Lost or stolen hardware that has low monetary value or is not part of a mission critical system.
  3. **Business impact:** Incident does not involve mission critical services.
  4. **Expanse of service disruption:** Incident is within a single unit.
  5. **Threat potential:** Threat to other information technology resources is minimal.
  6. **Public interest:** Low potential for public interest.
  7. **Policy infraction:** Security policy violations determined by the university.

Class B Incident: Moderate Severity

- A Class B incident is any incident that has a moderate impact to university information technology resources and is contained within the unit.
- The following criteria define **Class B** incidents:
  1. **Data classification:** Unauthorized disclosure of confidential information has not been determined.
  2. **Legal issues:** Lost or stolen hardware with high monetary value or that is part of mission critical system.
  3. **Business impact:** Incident involves mission critical services.
  4. **Expanse of service disruption:** Incident affects multiple units within the university.
  5. **Threat potential:** Threat to other university information technology resources is possible.
  6. **Public interest:** There is the potential for public interest.
  7. **Policy infraction:** Security policy violations determined by the university.

Class C Incident: High Severity

- A Class C incident is any incident that has impacted or has the potential to impact other external information technology resources and/or events of public interest.

- The following criteria define **Class C** incidents:
  1. **Data classification:** Unauthorized disclosure of confidential information has occurred outside the university.
  2. **Legal issues:** Incident investigation and response is transferred to law enforcement.
  3. **Business impact:** Threat to other university information technology resources is high.
  4. **Expanse of service disruption:** Disruption is wide spread across the university and/or other entities.
  5. **Threat potential:** Incident has potential to become wide spread across the university and/or threatens external, third-party information technology resources.
  6. **Public interest:** There is active public interest in the incident.
  7. **Policy infraction:** Security policy violations determined by the university.

2. Incident Notification & Escalation

- **Incident alerting takes place in this step although the timing may vary according to how incidents are identified or categorized.**
- Additionally, **if incidents are minor, details may be logged or notifications sent without an official alert.**
- Escalation is based on the categorization assigned to an incident and who is responsible for response procedures. If incidents can be automatically managed, escalation can occur transparently.
- This includes notifying any relevant staff, customers, or authorities about the incident and any expected disruption of services.

3. Investigation and Diagnosis

- Once incident tasks are assigned, **staff can begin investigating the type, cause, and possible solutions for an incident.** After an incident is diagnosed, **you can determine the appropriate remediation steps.**

4. Resolution and Recovery

- Resolution and recovery involve **eliminating threats or root causes of issues and restoring systems to full functioning.**
- Depending on incident type or severity, this may require multiple stages to ensure that incidents don’t reoccur.
- For example, if the incident involves a malware infection, you often cannot simply delete the malicious files and continue operations.
- Instead, you need to create a clean copy of your infected systems, isolate the infected components, and fully replace systems to ensure that the infection doesn’t spread.

5. Incident Closure

- Closing incidents typically involves finalizing documentation and evaluating the steps taken during response.
- This evaluation helps teams identify areas of improvement and proactive measures that can help prevent future incidents.
- Incident closure may also involve providing a report or retrospective to administrative teams, board members, or customers.
- This information can help rebuild any trust that may have been lost and creates transparency regarding your operations.

Ways of Improving Your Incident Management Process

- When defining your incident management processes, the following tips can help you ensure that your processes are effective.
- These tips can also help ensure that your team is able to adopt processes reliably.

a) Train and Support Employees

- Properly training employees at all levels of your organization can significantly benefit incident management processes.
- When non-IT staff are aware of how to identify and report incidents, your IT teams can respond faster and need to spend less time interpreting reports.
- When IT staff are properly trained, they are more effective at working together and can use tools more efficiently.

b) Set Alerts That Matter

- Avoiding alert overload is one of the most important aspects of incident management. If your teams are drowning in alerts, incidents are likely to be overlooked and response times are longer.
- To avoid this, you should carefully plan how events are categorized and what those categories mean for alerts.
- When defining incident alerts you may find it helpful to start by defining your service level indicators.
- You can use these indicators to determine a hierarchy of functioning that prioritizes root causes over surface-level symptoms. An alert informing teams that a server went down is more useful and effective than 30 alerts, one for each service on that server.

c) Prepare Your Team for On-Call

- With alert priorities determined, you also need to account for who is responding to those alerts.
- Defining an on-call schedule helps you ensure that a responder with the appropriate skills and permissions is always available. On-call procedures can also help you ensure that alerts are properly escalated.
- After each shift, consider adjusting on-call duties according to the amount of effort that individual staff made.
- This can ensure your team members aren’t getting overwhelmed.
- For example, if one team member responds to multiple high-priority incidents in a shift, they should get more time off-call than someone who didn’t have to respond.

d) Establishing Communication Guidelines

- Establishing effective communication is critical to team collaboration and effectiveness.
- One way to protect and ensure communication is to create guidelines. These guidelines can specify **what channels staff should use, what content is expected in those channels and how communications should be documented.**
- Clear guidelines can help diffuse tension and blame during stressful response periods by presenting a standard for how employees are expected to interact.
- Additionally, when communications are documented, teams can refer back to verify content and more easily pass on information without losing detail. This can reduce frustration overall, including the chance of misdirected stress.

e) Update Change Processes

- Depending on the systems you are using and your responders' expertise, you may need to verify or confirm changes required for response.
- You want to prevent responders from enacting harmful changes or from getting stuck waiting for unnecessary approval.
- One option is to clearly identify what levels or types of changes individual staff can make and who they can go to for approval when needed.
- If your system requires all changes to be approved by a **change advisory board (CAB)** you need to ensure that the board is readily available.
- If board members cannot give the same availability as your responders, you need to put emergency override procedures in place to prevent excess damage.

f) Improve Systems With Lessons Learned

- Reviews should evaluate the reason for the incident and work to identify if any preventative measures can be taken against future incidents.
- If so, teams need to define and assign tasks to take those measures immediately.
- Additionally, reviews can help ensure that any remaining incident documentation is completed. This is necessary for liability and compliance auditing.

- Thank you