Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

Time on Task:	Progress:
Unknown	100%

Report Generated: Monday, July 7, 2025 at 9:42 PM

Guided Exercises

Part 1: Research Incident Response Documentation

4. **Describe** the purposes of an incident response policy, incident response plan, and incident response procedures.

The purpose of an incident response policy, incident response plan, and incident response procedures are all important and are all tied together. If something were to happen, there should be steps that are planned ahead of time so everyone knows what they are doing and how they are supposed to do it. The policy includes the organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process. The plan includes the organization’s mission, strategies, and goals for incident response should help in determining the structure of its incident response capability. The incident response program structure should also be discussed within the plan. Lastly the procedures should be based on the incident response policy and plan. Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations. In addition, following standardized responses should minimize errors, particularly those that might be caused by stressful incident handling situations. SOPs should be tested to validate their accuracy and usefulness, then distributed to all team members. Training should be provided for SOP users; the SOP documents can be used as an instructional tool.

5. **Identify** which document type (policies, plans, and procedures) corresponds to which risk management layer and **provide** your justification.

Policy would be tier 1, organization. The policies would be set by higher ups and they guide how the whole company should deal with risk. Plan would be tier 2, mission/business processes. The plans explain how to follow the rules from the policies. They help people with what to do incase these incidents do happen. Lastly there is procedures, which is tier 3 information systems. These would be step by step things to do incase of an incident. It ensures that the workers do the right thing and guides them step by step.

9. **Identify** three examples of external information sharing during the Equifax timeline, including the date, details, and stakeholder.

March 7, 2017? Apache Struts Project Management Committee announces the CVE-2017-5638vulnerability affecting Apache Struts and releases the patch.
March 8, 2017? The United States Computer Emergency Readiness Team (US-CERT) sends Equifax analert to patch the particular vulnerability in Apache Struts software.
March 9, 2017? Equifax's Global Threat and Vulnerability Management (GTVM) team disseminates USCERT notification internally by email requesting responsible personnel apply the criticalpatch within 48 hours.5

11. **Describe** three team models.

Central Incident Response Team. A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.Distributed Incident Response Teams. The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility). However, the teams should be part of a single coordinated entity so that the incident response process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents.Coordinating Team. An incident response team provides advice to other teams without havingauthority over those teams—for example, a department-wide team may assist individual agencies' teams. This model can be thought of as a CSIRT for CSIRTs.

12. **Describe** three staffing models.

Employees. The organization performs all of its incident response work, with limited technical and administrative support from contractors. Partially Outsourced. The organization outsources portions of its incident response work. Section 2.4.2 discusses the major factors that should be considered with outsourcing. Although incident response duties can be divided among the organization and one or more outsourcers in many ways, a few arrangements have become commonplace:– The most prevalent arrangement is for the organization to outsource 24-hours-a-day, 7-days-aweek (24/7) monitoring of intrusion detection sensors, firewalls, and other security devices to an offsite managed security services provider (MSSP). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the organization’s incident response team.– Some organizations perform basic incident response work in-house and call on contractors to assist with handling incidents, particularly those that are more serious or widespread. Lastly is fully Outsourced. The organization completely outsources its incident response work, typically to an onsite contractor. This model is most likely to be used when the organization needs a full-time, onsite incident response team but does not have enough available, qualified employees. It is assumed that the organization will have employees supervising and overseeing the outsourcer’s work.

13. **Describe** eight groups within an organization that CIRT can turn to for their expertise, judgment, and abilities.

First is management. Management establishes incident response policy, budget, and staffing. Ultimately, management is held responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting to Congress, OMB, the General Accounting Office (GAO), andother parties. Next is information Assurance. Information security staff members may be needed during certain stages of incident handling (prevention, containment, eradication, and recovery)—for example, to alter network security controls (e.g., firewall rulesets).Then is IT Support. IT technical experts (e.g., system and network administrators) not only have the needed skills to assist but also usually have the best understanding of the technology they manage on a daily basis. This understanding can ensure that the appropriate actions are taken for the affected system, such as whether to disconnect an attacked system. The legal Department. Legal experts should review incident response plans, policies, and procedures toensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.Next is Public Affairs and Media Relations. Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public.There is also Human Resources. If an employee is suspected of causing an incident, the human resources department may be involved—for example, in assisting with disciplinary proceedings. Then, Business Continuity Planning. Organizations should ensure that incident response policies and procedures and business continuity processes are in sync. Computer security incidents undermine the business resilience of an organization. Business continuity planning professionals should be made aware of incidents and their impacts so they can fine-tune business impact assessments, risk assessments, and continuity of operations plans. Further, because business continuity planners have extensive expertise in minimizing operational disruption during severe circumstances, they may be valuable in planning responses to certain situations, such as denial of service (DoS) conditions.Lastly there is Physical Security and Facilities Management. Some computer security incidents occur through breaches of physical security or involve coordinated logical and physical attacks. The incident response team also may need access to facilities during incident handling—for example, to acquire a compromised workstation from a locked office.

14. **Describe** four services that a CIRT can provide.

They offer intrusion Detection. The first tier of an incident response team often assumes responsibility for intrusion detection The team generally benefits because it should be poised to analyze incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies.They also have advisory Distribution. A team may issue advisories within the organization regarding new vulnerabilities and threats.18 Automated methods should be used whenever appropriate to disseminate information; for example, the National Vulnerability Database (NVD) provides information via XML and RSS feeds when new vulnerabilities are added to it. Advisories are often most necessary when new threats are emerging, such as a high-profile social or political event (e.g., celebrity wedding) thatattackers are likely to leverage in their social engineering. Only one group within the organization should distribute computer security advisories to avoid duplicated effort and conflicting information. Another service is Education and Awareness. Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team. This information can be communicated through many means: workshops, websites, newsletters, posters, and even stickers on monitors and laptops. Lastly there is Information Sharing. Incident response teams often participate in information sharing groups, such as ISACs or regional partnerships. Accordingly, incident response teams often manage the organization's incident information sharing efforts, such as aggregating information related to incidents and effectively sharing that information with other organizations, as well as ensuring that pertinent information is shared within the enterprise.

Part 2: Research the Incident Response Life Cycle

2. **Describe** two preparation actions within the incident response life cycle.

One preparation is On-call information for other teams within the organization, including escalation information.Incident reporting mechanisms, such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously

4. **Describe** the relationship between risk assessment and incident response.

Risk assessment helps an organization identify its most valuable assets and the threats they face. Incident response uses that information to prepare for, detect, and respond to attacks that target those risks.

6. **Describe** an attack vector that is not listed in Section 3.2.1.

Social Engineering is an attack vector not listed. It happens when an attacker tricks someone into giving up information or access, like pretending to be tech support to steal a password.

7. **Identify** two early warning signs or indicators of incidents.

A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server. Antivirus software alerts when it detects that a host is infected with malware.

8. **Describe** two methods of incident analysis.

Profile Networks and Systems. Profiling is measuring the characteristics of expected activity so that changes to it can be more easily identified. Examples of profiling are running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. In practice, it is difficult to detect incidents accurately using most profiling techniques; organizations should use profiling as one of several detection and analysis techniques.Understand Normal Behaviors. Incident response team members should study networks, systems, and applications to understand what their normal behavior is so that abnormal behavior can be recognized more easily. No incident handler will have a comprehensive knowledge of all behavior throughout the environment, but handlers should know which experts could fill in the gaps. One way to gain this knowledge is through reviewing log entries and security alerts. This may be tedious iffiltering is not used to condense the logs to a reasonable size. As handlers become more familiar withthe logs and alerts, they should be able to focus on unexplained entries, which are usually moreimportant to investigate. Conducting frequent log reviews should keep the knowledge fresh, and theanalyst should be able to notice trends and changes over time. The reviews also give the analyst anindication of the reliability of each source.

9. **Identify** three examples of incident documentation.

Impact assessments related to the incident.Contact information for other involved parties (e.g., system owners, system administrators).A list of evidence gathered during the incident investigation.

10. **Identify** three factors for incident prioritization.

Functional Impact of the Incident. Incidents targeting IT systems typically impact the businessfunctionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existingfunctionality of the affected systems. Incident handlers should consider not only the currentfunctional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained. Information Impact of the Incident. Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization. Recoverability from the Incident. The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on anelongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

13. **Identify** two instances of incident notification in the Equifax timeline involving top-level management.

March 8 - The United States Computer Emergency Readiness Team sends Equifax an alert to patch the particular vulnerability in Apache Struts software. March 15 - Equifax's Security team runs scans to identify any systems containing the Apache Struts vulnerability

15. **Summarize** four actions performed in the third phase of incident response.

Evidence collection and management, identification of affected hosts, restoring systems to normal operation, containment to isolate incident location and prevent spread

16. **Describe** an example of the two-way communication between the second and third phases of incident response.

As containment efforts are underway and they may be redirected, it is important that analysis continues to ensure that all threats are documented. This also feeds back into evidence gathering because it may present additional evidence of the problem at hand and further assist with recovery efforts in the long run if supplementary analysis is conducted.

18. **Summarize** three actions performed in the fourth phase of incident response.

Exactly what happened, and at what times?How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?What information was needed sooner?

19. **Describe** the purpose of the feedback mechanism between the fourth phase to the first phase.

The post-incident can be a learning lesson for the company. If there was something that could have went better, they will change it, which would be part of the preparation cycle.

Challenge Exercise

- What type of team/staffing model could be adopted at Acme based on the given information? Why?

Acme should use a hybrid team model. It combines in-house staff with outside security experts. This works well because Acme is small and doesn't have full-time cybersecurity staff.

- Assume that the Acme Corporation had a comprehensive set of incident response procedures. What procedure would apply to the incident described above? Why?

Insider threat. This would be possible because the attacker was an Acme employee who admitted to the breach.

- Think about the external entities that Acme should contact about the incident. Identify one entity and provide your justification. Identify one external entity that should not be contacted and provide your justification.

One entity they should contact is the FBI. What happened was a crime and the authorities should be alerted so they can deal with it. A proper investigation would occur as well as legal action. One entity that shouldn't be contacted right away is the media. Publicly disclosing the breach without proper coordination could damage the company’s reputation and cause unnecessary panic

- Which internal stakeholders should the CIRT contact and why?

The CIO and CEO should be notified first so they can be aware and can properly allocate resources. HR should be notified so they take proper access management against the employee. Lastly the IT team should be notified so they can contain it

- After recovering from this incident, which services should the CIRT provide to Acme? Why?

They should provide post-incident analysis to identify the cause and weakness of the attack. Training should be done for employees and they should review the polices and procedures so everyone is aware

- Acme had not made preparations for cyber incidents, including this incident. Identify two preparation actions that could have prevented or mitigated the effects of this incident and provide your justification.

Regular patch management and vulnerability assessments could have prevented the exploitation. Keeping systems up-to-date would have closed the vulnerability before it could be exploited. There is also employee training and insider threat monitoring. Having these two things could have mitigated the effects. Making sure that employees are educated and aware could have prevented it, as well as monitoring for unusual behavior.

- What was the attack vector for this incident?

It was a known SMB vulnerability (CVE-2017-0143).

- What were the early warning signs and indicators of the incident?

There could have been renamed files and suspicious activity on the domain controller.

- Identify two criteria for determining the appropriate strategy that should be adopted in the containment phase and provide your justification.

The type of threat and the scope of the attack. Knowing how many systems are affected can help make the decision on how much containment is necessary. Understanding the type of threat is important to how they procede.

- Identify two types of post-incident activities that should be performed and provide your justification.

Have a post incident meeting on what went well and what can change. If there are things that went bad, update the policies and procedures. Then next time something occurs they can be better prepared based on past experiences.