Mississippi State UNIVERSITY

CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 3
Cyber Incident Response

The Incident Response Process

Chapter 7

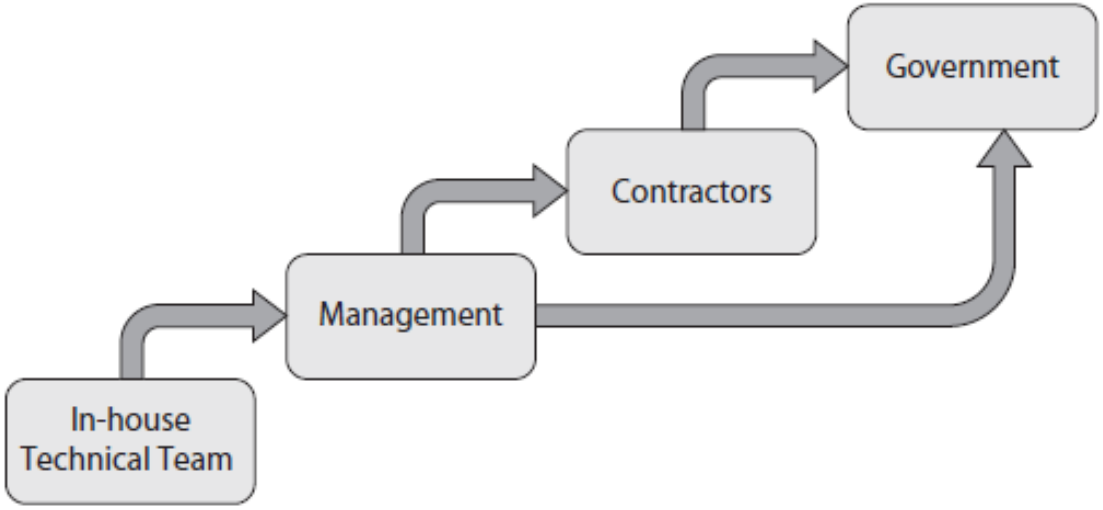
Outline

- A Cast of Characters
- Response Techniques
- Communication Processes
- Quiz

A Cast of Characters

- **Key roles in an incident response**
  - **Can be determined based on the established escalation thresholds**
    - **In-house technical team**
      - **Should always be involved in responding to an incident**
    - **Management**
      - **Should not be involved in routine incident responses such, as a failed phishing email attempt**
      - **Should be involved if there is a direct impact on the business such as rebooting a production server to eradicate malware in it**
    - **Contractors**
      - **Should be brought in if the in-house team is not capable of responding to the incident**
    - **Government**
      - **If the incident escalates, even more, the organization might need to involve the government such as law enforcement or the FBI**

[1]



Key Roles

The above figure is a typical role escalation model.

[1]

A Cast of Characters

- **Technical Staff**
  - **Also known as Incident Response (IR) Team**
  - **Those who respond to the incident depends on the incident itself**
    - **A single analyst might be the only person needed in some incidents**
    - **Several technical personal might be needed for many different departments for other incidents**
  - **Incident response plan**
    - **Should detail who is the person leading the response and who they delegate tasks to in each department**
    - **Ensure the tasks are delegated to personnel with the proper authority to be helpful in the event of an incident**

[1]

A Cast of Characters

- **Contractors**
  - **In the case, your technical team is not able to handle an incident, make sure your organization has a contract with an incident response firm**
  - **Have a plan in place for when you must call in the IR contractors**
    - **Step-by-step guide for how the IR contractors will enter the facility, what they have access to, and what systems are off-limits**
    - **Contractors should sign nondisclosure agreements (NDA)**
    - **IR contractors cannot train your organization's staff**
    - **Everyone in the organization should know what an IR contractor response looks like**

[1]

A Cast of Characters

- **Management**
  - **IR team should include key senior leaders from every business unit**
  - **Shapes the response process by**
    - **Minimizing disruptions**
    - **Addressing regulatory issues**
    - **Provide an interface with the personnel in the affected business unit**
- **Law Enforcement**
  - **Law enforcement agency(LEA)**
    - **If there are many incidents, your organization is required by law to involve the LEA**
    - **These laws sometimes have a timeline an organization must adhere to in responding to an incident**
  - **Ensure the possible engagement with the LEA is in your organization incident response plan**

[1]

A Cast of Characters

- **Stakeholders**
  - **IR stakeholders**
    - **Individuals or team that are part of the organization**
    - **These individuals play a role in the incident response plan**
    - **Extra care must be taken to ensure they know how to play their role when a major incident happens**
- **Human Resources (HR)**
  - **If any of the members in the organization have been involved in an incident HR must be informed**
  - **If disciplinary actions are required, HR also must be involved**
  - **Should be a part of the IR team the IR planning process**

[1]

A Cast of Characters

- **Legal Team**
  - **Legal counsel is needed**
    - **If the LEA is ever involved**
    - **If your organization handles public health information (PHI)**
  - **It is best to already have a legal team that your organization is familiar with before an incident takes place**
- **Marketing Team**
  - **This is the group that manages communication with customers and investors**
    - **Their goal is to mitigate damage to the trust customers or investors have in the organization**
  - **Can be any part of the organization the communicates directly with the general public**
  - **Should be part of IR planning**

[1]

A Cast of Characters

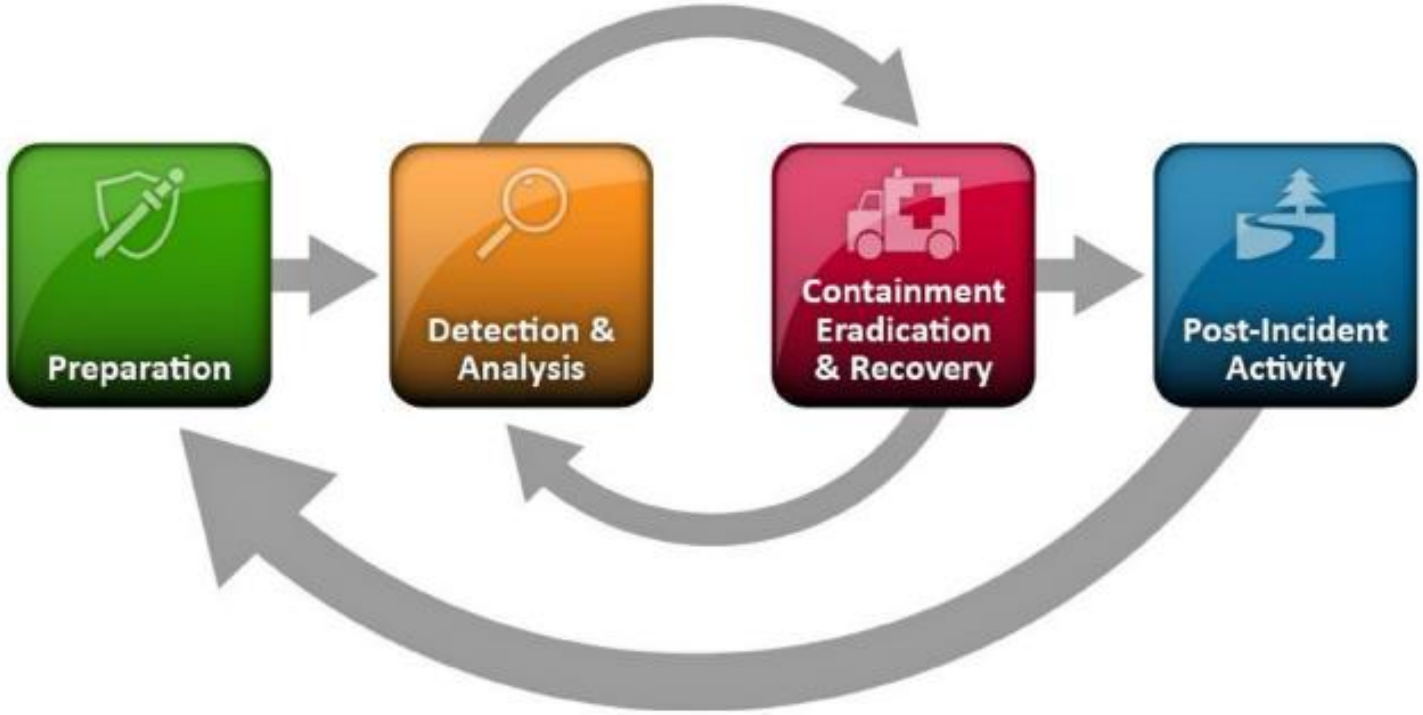
- **Uninvolved Management**
  - **Senior management is not likely to be involved in IR; unless it's a very serious incident**
  - **It is important that they know what the IR plan is and to keep them up to date**
  - **Can be vital in getting needed resources for an IR plan and during an IR**

[1]

Response Techniques

- **Event**
  - Any occurrence that can be observed, verified and documented
- **Incident**
  - One or more related events that compromise the organization's security posture
- **Incident Response**
  - The process of negating the effects of the incident on an information system
- **Recovery**
  - The part of the process that restores the functionality of an information system to its pre-incident state

[1]



Response Techniques

The above figure shows the incident response lifecycle from the NIST Special Publication 800-61 (Revision 2).

[1]

Interactive Exercise: 1

What is IR?	
Name the 9 key groups involved in IR	
Which NIST Special Publication describes the entire IR process?	

[2]

Interactive Exercise Ans: 1

What is IR?	**"IR," or "Incident Response," is the process of negating the effects of an incident on an information system.**
Name the 9 key groups involved in IR	1. Technical staff or team, 2. Contractors, 3. Law enforcement, 4. Management, 5. Stakeholders, 6. Human Resources, 7. Legal, 8. Marketing Department, and 9. Un-involved management
Which NIST Special Publication describes the entire IR process?	NIST SP 800-61 revision 2.

[2]

Response Techniques

- **Containment**
  - **The set of actions that attempts to deny the threat agent from causing more damage**
  - **Proper containment process gives the IR team more time to respond to the incident**
  - **Proactive containment approach example**
    - **Disconnect the affected system from the network**
  - **Reactive containment approach example**
    - **Cause a denial of service or limit functionality of critical systems**
  - **Persevering evidence is an important part of a containment**

[1]

Response Techniques

- **Segmentation**
  - **Provides an important layer of defense by breaking apart the network into subnetworks**
    - **The goal is to prevent hosts in different subnets from directly communicating with one another**
    - **During an incident having the network segmented will help contain the incident**
- **Isolation**
  - **Isolation VLAN**
    - **Suspicious or compromised hosts can be moved to this isolated part of the network**
    - **Does not have any connectivity to the rest of the network**
    - **Prevents the spread of malware affecting the host**
    - **Prevents malware from talking to an external host such as command-and-control (C2) nodes**
  - **Can be used to analyze malware and create indicators of compromises (IOCs) for others such as the Computer Emergency Readiness Team(CERT) or Information Sharing and Analysis Center (ISAC)**

[1]

Response Techniques

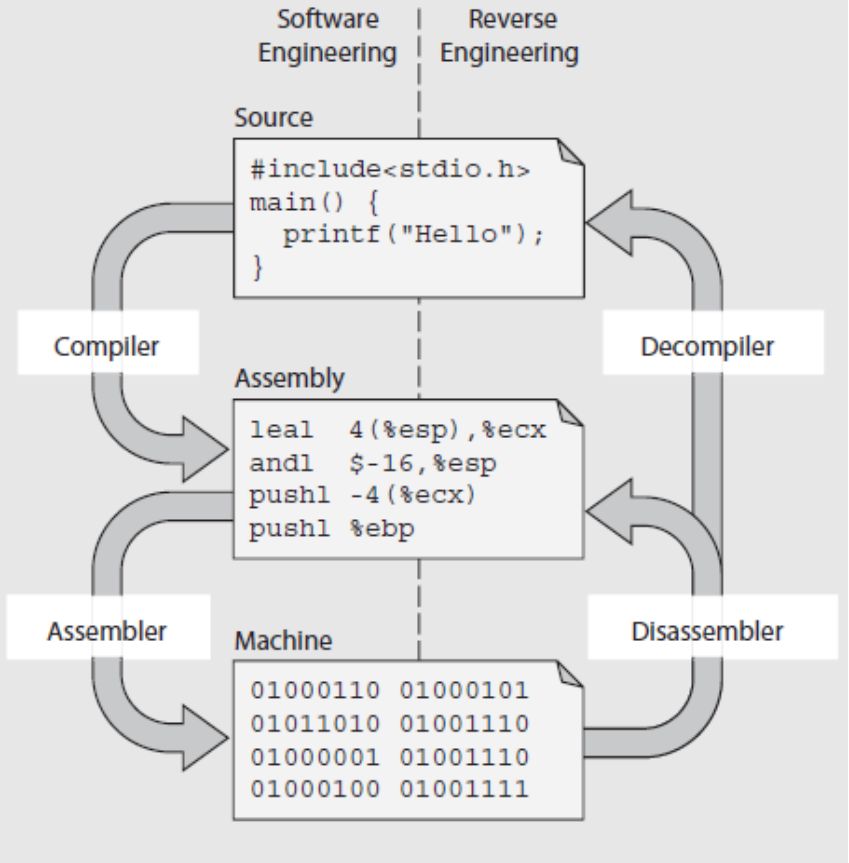
- **Removal**
  - **Complete removal of compromised systems from the network**
  - **Options to consider once a host is removed from the network**
    - **Should you keep the host powered on?**
    - **Should you shut the host down and preserve it?**
    - **Should you rebuild the host?**
- **Factors to consider in answering those questions**
  - **Threat intelligence value**
    - **If your organization has threat intelligence capabilities, then you might be able to gain more insight on the compromised host if it was kept running.**
  - **Crime scene evidence**
    - **If your organization has the required resources, it would be best to capture an image of the compromised host for a possible forensic investigation.**
  - **Ability to restore**
    - **If your organization had critical business information only on the compromised host, then it would be vital for the host to be imaged.**
- **The removal of a compromised host should be well documented**

[1]

Response Techniques

- **Reverse Engineering (RE)**
  - **The detailed examination of a product to figure out its features and how it was made**
  - **Dynamic analysis**
    - **Malware is analyzed in a sandbox**
    - **Shows what the malware does when executed**
      - **Malware sometimes detects that it is in a sandbox and will not execute**
  - **Static code analysis**
    - **Decompile or disassemble the binary code to analyze the assembly code**
    - **This will allow analysis to see all possible functions of the malware, not just what is displayed in a sandbox**
    - **This analysis can be used to find evidence of malware on other hosts**

[1]



Engineering and Reversing Software

- The figure above depicts
  - The compilation of source code to assembly, to assembled machine language.
  - The disassembling of machine language to assembly, and back to decompiled source code.

[1]

Interactive Exercise: 2

Name the 4 ways discussed in which we can contain an incident.	
The first step of IR is "Containment." What does this entail?	
How can you use segmentation to contain an incident?	
How can we use isolation to contain an incident?	
How can removal help contain an incident?	
If you have to remove an infected device off the network. What 3 factors must you consider?	
How can reverse engineering help contain an incident?	
What are two approaches to reverse engineering malware?	

[2]

Interactive Exercise Ans: 2

Name the 4 ways discussed in which we can contain an incident.	**1.Segmentation, 2. Isolation, 3. Removal, and 4. Reverse Engineering**
The first step of IR is "Containment." What does this entail?	"Containment" is a set of actions that attempts to deny the threat agent the ability or means to cause further damage. The goal is to prevent or reduce the spread of this incident while you strive to eradicate it.
How can you use segmentation to contain an incident?	You can segment your network by physically wiring separate networks or logically assigning devices to separate VLANs. In either case ,traffic between network segments must go through some sort of gateway device, which is often times a router with the appropriate ACLs.
How can we use isolation to contain an incident?	The isolation VLAN would have no connectivity to the rest of the network, which would prevent the spread of any malware. While a host is in isolation, the response team is able to safely observe its behaviors to gain information about the nature of the incident
How can removal help contain an incident?	The compromised hosts will come off the network permanently. When you remove a host from the network, you need to decide whether you will keep it powered on, shut it down and preserve it, or simply rebuild it.
If you have to remove an infected device off the network. What 3 factors must you consider?	1) Threat intelligence value: 2) Crime scene evidence: 3) Ability to restore
How can reverse engineering help contain an incident?	The idea to analyze the binary code to find the techniques it employs to achieve permanence in an infected host, or to identify a unique characteristic that could be used as a signature for the malware.
What are two approaches to reverse engineering malware?	1) Dynamic Analysis 2) Static Code Analysis

[2]

Response Techniques

- **Eradication**
  - **Return all systems to a known good state**
    - **Should have baseline restore point for all information systems**
  - **Gather and log all evidence before recovering systems**
  - **Systems should be rebuilt to make them trustworthy again after being compromised**
- **Sanitization**
  - **The idea is to make it impossible to access data on a given medium**

[1]

Sanitization Techniques

- **Four techniques listed in increasing level of effectiveness**
  - **Overwriting**
    - Replacing the ones and zeros that represent storage media with random or fixed patterns of ones and zeros
    - Renders the original data unrecoverable
  - **Encryption**
    - Data on a given device is rendered unusable unless it is unencrypted with an encryption key
    - If the encryption key is deleted, the data on the device will be unrecoverable
  - **Degaussing**
    - Wipes the data from the device by applying a powerful magnetic force to the device
    - Renders the device unusable
  - **Physical destruction**
    - Physically destroying the media such as shredding, incinerating, or exposing the device to corrosive chemicals

[1]

Response Techniques

- **Reconstruction**
  - **Gold masters**
    - **Known-good hardened image of various standard configurations**
    - **Used to reconstruct or rebuild newly sanitized hosts**
  - **Without a gold master, reconstruction is difficult**
  - **Restoring data to the host is part of the reconstruction**
    - **If data is not backed up, regularly or at all then there is not an easy way of restoring data**
    - **The organization itself should enforce centrally managed backups of all systems**
    - **Do not leave the responsibility to backup data to the individual employee**

[1]

Response Techniques

- **Secure Disposal**
  - **All media should be sanitized before disposal with one of the sanitization methods discussed earlier**

[1]

Interactive Exercise: 3

The second step in IR is eradication. What does this entail?	
Name the 3 ways discussed in which we can eradicate an incident.	
How can sanitization help eradicate an incident?	
Name 4 methods of sanitization discussed.	
How can reconstruction help eradicate an incident?	
What are Gold Masters?	
How can secure disposal help eradicate an incident?	

[2]

Interactive Exercise ANS: 3

The second step in IR is eradication. What does this entail?	process, in which we return all systems to a known-good state. Once all evidence is captured, we fix all that was broken. The aim is to restore full, trustworthy functionality, to the organization for hosts that were compromised.
Name the 3 ways discussed in which we can eradicate an incident.	1.Sanitization, 2. Reconstruction, and 3. Secure disposal
How can sanitization help eradicate an incident?	"sanitization" refers to the process by which access to data on a given medium is made infeasible for a given level of effort.
Name 4 methods of sanitization discussed.	1) "Overwriting" 2) "Encryption:". 3) "Degassing" 4) "Physical destruction"
How can reconstruction help eradicate an incident?	Process to rebuild the host to its pristine state. The best approach to doing this it to ensure that you have created known-good, "Gold Masters" and facilitate the process of rebuilding a compromised host/host data
What are Gold Masters?	Gold Masters are images of system and their correct configuration settings.
How can secure disposal help eradicate an incident?	When you're disposing media or devices as a result of an IR, any of the 4 techniques covered. 1) Overwriting is only feasible with regard to HDDs and might not be available for SSDs 2) Encryption-based purging can be found in multiple workstations, servers, and mobile OSs, but not in all 3) Degaussing only works on magnetic media, and some advanced magnetic drives use stronger fields to store data and may render older degaussers inadequate 4) In the end, the only way to securely dispose of these devices is by physically destroying them using an accredited process or service provider.

[2]

Response Techniques

- **Validation**
  - **Within the realm of incident response validation is**
    - **Ensuring all attack vectors have been identified**
    - **Ensuring effective countermeasures have been implemented for those attack vectors**
  - **This analysis is performed after an attack or during the response to an incident**

[1]

Response Techniques

- **Patching**
  - **Is the process of updating vulnerable software**
  - **Some of the most damaging incidents are due to unpatched software**
    - **Reasons for software being unpatched**
      - **Failure to update software for a known vulnerability**
      - **The existence of a "Zero Day" vulnerability**
  - **Network Access Control (NAC)**
    - **Can be used to protect your network against a "bring your own device" (BYOD) environment**
    - **Test any device trying to connect to the network, for needed patches, updates, anti-malware, and other enforced policies**
    - **Failed tests will result in the device being placed in a quarantine network to prevent a possible spread of malware**

[1]

Response Techniques

- **Permissions**
  - **After an incident response**
    - **Analyze possible inappropriate evaluated permissions**
  - **Your organization should have a least privilege policy**
    - **Prevents users from having excessive privileges**
  - **Many incidents have happed due to**
    - **An adversary escalating privileges**
    - **An adversary taking control over an admin account**
- **Scanning**
  - **Identifies and logs all systems on a network and then scans each system for known vulnerabilities.**
  - **Prevent an incident from recurring by**
    - **Determining what caused the incident**
    - **Scanning other systems for related vulnerabilities**
    - **Implementing controls to prevent the incident from happening again**

[1]

Response Techniques

- **Monitoring**
  - **Incorporate IOCs in the organization monitoring plan by**
    - **Adding the IOCs to rules in an IDS or IPS**
    - **Providing the IOCs to organizations such as US-CERT or ISACs**

[1]

Interactive Exercise: 4

Validation is the third step in the IR process. What does this entail?	
Name the 4 methods of validation discussed?	
How can validating patching help in the IR process?	
How can validating permissions help in the incident response process?	
How can scanning help with validation?	
How can monitoring help with validation?	

[2]

Interactive Exercise ANS: 4

Validation is the third step in the IR process. What does this entail?	**The "validation" process in IR is focused on ensuring that we have identified the corresponding attack vectors and implemented effective countermeasures against them.**
Name the 4 methods of validation discussed?	1. Patching, 2. Permissions, 3. Scanning, 4. Monitoring
How can validating patching help in the IR process?	Many of the most damaging incidents are the result of an unpatched software flaw. Is it a known or unknown vulnerability (zero day). Part of the response would then be to identify the failure, correct it, and then validate that the fix is effective at preventing a repeated incident in the future.
How can validating permissions help in the incident response process?	You need to validate permissions in an IR to find any elevated permissions that may have caused the incident.
How can scanning help with validation?	After recovering from an Incident, you would want to scan your systems for other instances of that same (or related) vulnerability.
How can monitoring help with validation?	By adding the IOCs to rules in an IDS or IPS. Also providing the IOCs to organizations such as US-CERT or ISACs

[2]

Response Techniques

- **Corrective Actions**
  - **Is the phase of an incident response that allows the organization to learn from the incident**
  - **Improving the organization's posture by applying lessons learned and using information gained**

[1]

Response Techniques

- **Lessons-Learned Report**
  - **Hotwash**
    - A quick meeting to discuss what happened
  - **After Action Review (AAR)**
    - Formally document issues and recommendations
    - Every participant input is collected before AAR
  - **A general report format for each incident participant**
    - Issue
      - A brief single sentence from the participants perspective of the issue that accrued
    - Discussion
      - A paragraph-long description of what happened and what can be learned from it
    - Recommendation
      - Was the team's response effective or ineffective
      - Recommendation on how to sustain or improve response

[1]

Response Techniques

- **Change Control Process**
  - **Designed to prevent any major changes being made without careful consideration by all possibly affected parties**
- **Change Control Board (CCB)**
  - **Review the IR team's important change recommendations**
  - **The board consists typically of**
    - **Various business unit representatives**
    - **Relevant stakeholders**

[1]

Response Techniques

- **Updates to Response Plan**
  - **The IR plan should be reviewed and updated if needed**
  - **IR team has more control over the IR plan than implanting organization-wide changes**
- **Summary Report**
  - **Depending on the severity and impact of the incident, the report can be short or long**
  - **Consider the purpose of the report such as,**
    - **Ensuring future IR team members are taught the lessons-learned from the incident**

[1]

Communication Processes

- **Important Note**
  - **It is vital to maintain effective communication among all team members and stakeholders during an incident response**
- **Internal Communications**
  - **War Room**
    - **Either virtual or physical room that internal parties can meet and discuss response activities**
  - **Establish a secure communication channel such as group-text or email to keep key personal up-to-date during an incident**

[1]

Communication Processes

- **External Communications**
  - **Designate a trained professional to the role of external communication**
    - **Sensible reports can be turned into damaging sound bites if not careful**
  - **The legal team must be involved if the organization is required to communicate with government entities**
  - **The media relations team should be utilized to support the organization's perceived transparency and trustworthiness**
  - **Communication with key partners such as investors or business collaborators**
    - **Prevent the price of the company's stoke from drop by communicating to key partners plans to midgait losses and risks**

[1]

Final Interaction Exercise

Corrective actions is the fourth step in IR. What does this entail?	
Name the 4 methods of corrective actions discussed	
How can a lessons-learned report implement corrective actions?	
How can the change control process implement corrective actions?	
How can updating your response plans implement corrective actions?	
How can Summary reports implement corrective actions?	
The two types of communication during the IR process. What are they?	

[2]

Final Interaction Exercise Ans

Corrective actions is the fourth step in IR. What does this entail?	we apply the lessons learned and information gained from the process in order to improve our posture in the future.
Name the 4 methods of corrective actions discussed	1. Lessons-Learned Reports, 2. Change Control process, 3. Updating response plans, and 4. Summary Reports.
How can a lessons-learned report implement corrective actions?	1) Issue: a brief (usually single sentenced) label for an important (from the participant's perspective) issues that arose during the operation. 2) Discussion: A (usually paragraph long) description of what was observed and why it's important to remember or learn from it for the future. 3) Recommendation: Usually starts with a "sustain" or "improve" label if the contributor felt the team's response was effective or ineffective. 4) Every participant's input is collected and organized before the "After Action Review (ARR)." Usually all inputs are discussed during the review session.
How can the change control process implement corrective actions?	During the ARR, the teams will document recommendations for changes. These change requests will go to the Change Control Board (CCB).
How can updating your response plans implement corrective actions?	The IR plan should be reviewed, and if appropriate updated. If we can better prepare for future incidents
How can Summary reports implement corrective actions?	The post-incident report can be very short one-pager or a lengthy treatise; it all depends on the severity of the impact of the incident. Whatever the case, consider who will read the report and shape it in a way in which they can interpret it.
The two types of communication during the IR process. What are they?	1. "Internal Communications:" 2. "External Communications:"

[2]

Quiz

Chapter 7

Question #1

- **1. When decisions are made that involve significate funding requests or reaching out to law enforcement organizations, which of the following parties will be notified?**
  - **A. Contractors**
  - **B. Public relations staff**
  - **C. Senior leaders**
  - **D. Technical staff**

[1]

Answer #1

- C
  - Decisions to reach out to external law enforcement bodies or employ changes that will incur significant cost will likely require organizational leadership involvement
  - They will provide guidance to company priorities, assist in addressing regulatory issues, and provide the support necessary to get through the IR process

[1]

Question #2

- **2. The process of dissecting a sample of malicious software to determine its purpose is referred to as what?**
  - **A. Segmentation**
  - **B. Frequency analysis**
  - **C. Traffic analysis**
  - **D. Reverse engineering**

[1]

Answer #2

- **D**
  - **Reverse engineering malware is the process of decomposing malware to understand what it does and how it works**

[1]

Question #3

- **3. When would you consult your legal department in the conduct of an incident response?**
  - **A. Immediately after the discovery of the incident**
  - **B. When business processes are at risk because of a failed recovery operation**
  - **C. In cases of compromise of sensitive information such as PHI**
  - **D. In the case of a loss of more than 1 terabyte of data**

[1]

Answer #3

- **C**
  - **There are regulatory reporting requirements when dealing with compromises of sensitive data such as protected health information.**
  - **Since these can lead to civil penalties or even criminal charges, it is important to consult legal counsel**

[1]

Question #4

- **4. During the IR process, when is it a good time to perform a vulnerability scan to determine the effectiveness of corrective actions?**
  - **A. Change control process**
  - **B. Reverse engineering**
  - **C. Removal**
  - **D. Validation**

[1]

Answer #4

- **D**
  - **Additional scanning should be performed during validation to ensure that no additional vulnerabilities exist after remediation**

[1]

Question #5

- **5. What is the term for members of your organization who have a role in helping with some aspects of some incident response?**
  - **A. Shareholders**
  - **B. Stakeholders**
  - **C. Insiders**
  - **D. Public relations**

[1]

Answer #5

- **B**
  - **Stakeholders are those individuals and teams who are part of your organization and have a role in helping with some aspects of some incident response**

[1]

Question #6

- **6. What process during an IR is as important in terms of expectation management and reporting as the application of technical controls?**
  - **A. Management process**
  - **B. Change control process**
  - **C. Communications process**
  - **D. Monitoring process**

[1]

Answer #6

- **C**
  - **The communications process is a vital part of the IR process and will allow for an efficient recovery from an incident**

[1]

Scenario for Questions 7-12

- **You receive an alert about a compromised device on your network. Users are reporting that they are receiving strange messages in their inboxes and having problems sending e-mails. Your technical team reports unusual network traffic from the mail server. The team has analyzed the associated logs and confirmed that a mail server has been infected with malware**

Question #7

- **7. You immediately remove the server from the network and route all traffic to a backup server. What stage are you currently operating in?**
  - **A. Preparation**
  - **B. Containment**
  - **C. Eradication**
  - **D. Validation**

[1]

Answer #7

- **B**
  - **Containment is the set of actions that attempts to deny the threat agent the ability or means to cause further damage**

[1]

Question #8

- **8. Now that the device is no longer on the production network, you want to restore services. Before you rebuild the original server to a known-good condition, you want to preserve the current condition of the server for later inspection. What is the first step you want to take?**
  - **A. Format the hard drive**
  - **B. Reinstall the latest operating systems and patches**
  - **C. Make a forensic image of all connected media**
  - **D. Update the antivirus definitions on the server and save all configurations**

[1]

Answer #8

- **C**
  - **Since unauthorized access of computer systems is a criminal act in many areas, it may be useful to take a snapshot of the device in its current state using forensic tools to preserve evidence**

[1]

Question #9

- **9. What is the most appropriate course of action regarding communications with organizational leadership?**
  - **A. Provide updates on progress and estimate time of service restoration**
  - **B. Forward the full technical details on the affected server(s)**
  - **C. Provide details until after law enforcement is notified**
  - **D. Provide details only is unable to restore services**

[1]

Answer #9

- **A**
  - **Organizational leadership should be given enough information to provide guidance and support.**
  - **Management needs to be closely involved in critical decision-making points.**

[1]

Question #10

- **10. Your team has identified the strain of malware that took advantage of a bug in your mail server version to gain elevated privileges. Because you cannot be sure what else was affected on that server, what is your best course of action?**
  - **A. Immediately update the mail server software**
  - **B. Reimage the server's hard drive**
  - **C. Write additional firewall rules to allow only e-mail-related traffic to reach the server**
  - **D. Submit a request for a next-generation antivirus for the mail server**

[1]

Answer #10

- **B**
  - **Generally, the most effective means of disposing of an infected system is a complete reimaging of a system's storage to ensure that any malicious content was removed and to prevent reinfection**

[1]

Question #11

- **11. Your team believes it has eradicated the malware from the primary server. You attempt to bring affected systems back into the production environment in a responsible manner. Which of the following tasks will not be a part of this phase?**
  - **A. Applying the latest patches to server software**
  - **B. Monitoring network traffic on the server for signs of compromise**
  - **C. Determining the best time to phase in the primary server into operations**
  - **D. Using a newer operating system with different server software**

[1]

Answer #11

- **D**
  - **The goal of the IR process is to get services back to normal operations as quickly and safely as possible**
  - **Introducing completely new and untested software may introduce significant challenges to this goal**

[1]

Question #12

- **12. Your team has successfully restored services on the original server and verified that it is free from malware. What activity should be performed as soon as practical?**
  - **A. Preparing the lessons-learned report**
  - **B. Notifying law enforcement to press charges**
  - **C. Notifying industry partners about the incident**
  - **D. Notifying the press about the incident**

[1]

Answer #12

- **A**
  - **Preparing the lessons-learned report is a vital stage in the process after recovery**
  - **Should be performed as soon as possible after the incident to record as much information and complete any documentation that might be useful for the prosecution of the incident and to prevent future incidents from occurring**

[1]

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.
2. friedaj friedaj, “cysa-chapter-7-the-incident-response-process-flash-cards,” *Quizlet*, 17-Dec-2017. [Online]. Available: https://quizlet.com/296891011/cysa-chapter-7-the-incident-response-process-flash-cards/. [Accessed: 30-Nov-2020].