# CyberRookie CSX Fundamentals - Section 5: Incident Response

Quizlet

Study online at quizlet.com/_7r6gfm

| | |
|---|---|
| 1. **All organizations need to put significant effort into** | Protecting and preventing cyberattacks from causing harm or disruption |
| 2. **Security controls are not perfect and cannot completely eliminate all risk** | It is important that organizations prepare for, and are capable of detecting and managing, potential cybersecurity problems. |
| 3. **An event** | Is any change, error or interruption within an IT infrastructure such as a system crash, a disk error or a user forgetting their password. |
| 4. **The National Institute of Standards and Technology (NIST) defines an event as** | Any observable occurrence in a system or network. |
| 5. **NIST defines an incident as** | A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. |
| 6. **An incident is** | The attempted or successful unauthorized access, use, disclosure, modification or loss of information or interference with system or network operations. |
| 7. **An incident is** | The activity of a human threat agent. |
| 8. **An incident is** | Anything disruptive, including a court order for discovery of electronic information or disruption from a natural disaster. |
| 9. **Regardless of the exact definition used by a particular organization** | It is important to distinguish between events that are handled in the normal course of business and incidents |
| 10. **A cybersecurity incident** | Is an adverse event that negatively impacts the confidentiality, integrity and availability of data. |
| 11. **Cybersecurity incidents** | May be unintentional, such as someone forgetting to activate an access list in a router, or intentional, such as a targeted attack by a hacker |
| 12. **Technical incidents include** | Viruses, malware, denial-of-service (DoS) and system failure |
| 13. **Physical incidents** | May include social engineering and lost or stolen laptops or mobile devices |
| 14. **US-CERT provides the following categories of security incidents and reporting time frames used by federal agencies** | CAT1, CAT2, CAT3, CAT4, CAT5, CAT6 |
| 15. **CAT 1** | Unauthorized Access, An individual gains logical or physical access without permission to a network, system, application, data or other resource. Within 1 hour of discovery/detection |
| 16. **CAT2** | Denial-of-service (DoS), An attack that successfully prevents or impairs normal authorized functionality of networks, systems or applications by exhausting resources. Within 2 hours of discovery/ detection if the successful attack is still ongoing |
| 17. **CAT3** | Malicious Code, Successful installation of malicious software (e.g., virus, worm, Trojan horse or other code-based malicious entity) that infects an operating system or application. Daily; within 1 hour of discovery/detection if widespread |
| 18. **CAT4** | Improper Usage, A person violates acceptable computing use policies. Weekly |
| 19. **CAT5** | Scans/Probes/Attempted Access, Any activity that seeks to access or identify a computer, open ports, protocols, service or any combination. Monthly |
| 20. **CAT6** | Investigation, Unconfirmed incidents that are potentially malicious or anomalous activity. |
| 21. **Incident response** | Is a formal program that prepares an entity for an incident |
| 22. **Incident response generally includes** | Preparation, Detection and Analysis, Investigation, Mitigation and Recovery, Postincident Analysis |

| | |
|---|---|
| 23. **Preparation** | To establish roles, responsibilities and plans for how an incident will be handled |
| 24. **Detection and Analysis** | Capabilities to identify incidents as early as possible and effectively assess the nature of the incident |
| 25. **Investigation** | Capability if identifying an adversary is required |
| 26. **Mitigation and Recovery** | Procedures to contain the incident, reduce losses and return operations to normal |
| 27. **Postincident Analysis** | To determine corrective actions to prevent similar incidents in the future |
| 28. **Waiting until an incident occurs to figure out what to do** | Is a recipe for disaster. |
| 29. **Adequate incident response planning and implementation allows** | An organization to respond to an incident in a systematic manner that is more effective and timely |
| 30. **Organizations that do not plan for a cybersecurity incident** | Will suffer greater losses for a more extended period of time |
| 31. **The current trend shows** | An increase in incident occurrences. These attacks are becoming more sophisticated and are resulting in escalating losses. |
| 32. **Many national regulations and international standards require** | The development of incident response capabilities |
| 33. **Compliance regulations such as Payment Card Industry (PCI) and Federal Deposit Insurance Corporation (FDIC)** | Provide strict requirements for security policies and incident response planning |
| 34. **The model proposed by Schultz, Brown and Longstaff presents the six-phase model of incident response including** | Preparation, identification, containment, eradication, restoration and follow-up |
| 35. **Preparation** | This phase prepares an organization to develop an incident response plan prior to an incident. Sufficient preparation facilitates smooth execution |
| 36. **Identification** | This phase aims to verify if an incident has happened and find out more details about the incident. Reports on possible incidents may come from information systems, end users or other organizations. |
| 37. **Containment** | After an incident has been identified and confirmed, the IMT is activated and information from the incident handler is shared. The team will conduct a detailed assessment and contact the system owner or business manager of the affected information systems/assets to coordinate further action |
| 38. **Eradication** | When containment measures have been deployed, it is time to determine the root cause of the incident and eradicate it restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause |
| 39. **Recovery** | This phase ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDO) or business continuity plan (BCP). The time constraint up to this phase is documented in the RTO |
| 40. **Lessons learned** | At the end of the incident response process, a report should always be developed to share what occurred, what measures were taken and the results after the plan was executed. Part of the report should contain lessons learned that provide the IMT and other stakeholders valuable learning points of what could have been done better |
| 41. **In order to prepare for and identify an incident** | Organizations use a myriad of security tools, such as vulnerability assessments, firewalls and intrusion detection systems (IDSs), that collect a high volume of data. |
| 42. **Security teams** | Have to analyze and interpret this overwhelming amount of data, referred to as log data overload |

| | |
|---|---|
| 43. **An emerging solution to the problem of analyzing and interpreting this overwhelming amount of data, referred to as log data overload is** | Security event management (SEM) |
| 44. **SEM systems** | Automatically aggregate and correlate security event log data across multiple security devices. This allows security analysts to focus on a manageable list of critical events. |
| 45. **Security incidents are** | Often made up of a series of events that occur throughout a network |
| 46. **By correlating data, the SEM can** | Take many isolated events and combine them to create one single relevant security incident |
| 47. **SEM's can use either** | Rule-based or statistical correlation |
| 48. **Rule-based correlations** | Create situation-specific rules that establish a pattern of events |
| 49. **Statistical correlation** | Uses algorithms to calculate threat levels incurred by relevant events on various IT assets. |
| 50. **Security incident and event management (SIEM) systems** | Take the SEM capabilities and combine them with the historical analysis and reporting features of security information management (SIM) systems. |
| 51. **Information security teams should** | Periodically analyze the trends found from SEM or SIEM systems, such as attempted attack types or most frequently targeted resources. This allows the organization to investigate incidents as well as allocate appropriate resources to prevent future incidents. |
| 52. **Cybersecurity incident investigations include** | The collection and analysis of evidence with the goal of identifying the perpetrator of an attack or unauthorized use or access. May overlap the technical analysis used in incident response where the objective is to understand the nature of the attack, what happened and how it occurred |
| 53. **The goals of an investigation can conflict** | With the goals of incident response. |
| 54. **Investigations may require** | The attack or unauthorized access to continue while it is analyzed and evidence is collected, whereas remediation may destroy evidence or preclude further investigation |
| 55. **The organization's management must** | Be an integral part of making decisions between investigating and remediation. |
| 56. **Investigations may be conducted for** | Criminal activity (as defined by governmental statutes and legislation), violations of contracts or violations of an organization's policies. |
| 57. **Cybersecurity investigators may also assist** | In other types of investigations where computers or networks were used in the commission of other crimes, such as harassment where email was used. |
| 58. **An investigation may take place entirely** | In-house, or may be conducted by a combination of in-house personnel, service providers and law enforcement or regulators. |
| 59. **It is very important to preserve** | Evidence in any situation |
| 60. **Most organizations are not well equipped to deal with** | Intrusions and electronic crimes from an operational and procedural perspective, and they respond to it only when the intrusion has occurred and the risk is realized |
| 61. **The evidence loses its** | Integrity and value in legal proceedings if it has not been preserved and subject to a documented chain of custody. This happens when the incident is inappropriately managed and responded to in an ad hoc manner. |
| 62. **For evidence to be admissible in a court of law** | The chain of custody needs to be maintained accurately and chronologically. |
| 63. **The chain of evidence essentially contains information regarding:** | Who had access to the evidence, The procedures followed in working with the evidence, Proof that the analysis is based on copies that are identical to the original evidence |
| 64. **The evidence of a computer crime exists in the form of** | Log files, file time stamps, contents of memory, etc |

| | |
|---|---|
| 65. **Rebooting the system or accessing files could** | Result in such evidence being lost, corrupted or overwritten |
| 66. **one of the first steps taken in Evidence Preservation should be** | Copying one or more images of the attacked system |
| 67. **Memory content should also be** | Dumped to a file before rebooting the system. |
| 68. **Any further analysis must be performed** | On an image of the system and on copies of the memory dumped—not on the original system in question |
| 69. **In addition to protecting the evidence, it is also important to preserve** | The chain of custody |
| 70. **Chain of custody** | Is a term that refers to documenting, in detail, how evidence is handled and maintained, including its ownership, transfer and modification |
| 71. **Chain of custody is necessary to satisfy** | Legal requirements that mandate a high level of confidence regarding the integrity of evidence |
| 72. **Investigations have clearly defined** | Legal requirements and these vary from country to country |
| 73. **Only trained investigators working with legal counsel should** | Undertake investigations |
| 74. **Some of the legal issues that may be applicable include** | Evidence collection and storage, Chain of custody of evidence, Searching or monitoring communications, Interviews or interrogations, Licensing requirements, Law enforcement involvement, Labor, union and privacy regulation |
| 75. **Failure to perform an investigation in compliance with the appropriate legal requirements may create** | Criminal or civil liabilities for the investigator and organization or may result in an inability to pursue legal remedies. |
| 76. **Many attacks are** | International in scope, and navigating the different (and sometimes conflicting) legal issues can be challenging, adding complexity to cybersecurity investigations. |
| 77. **In some countries, private individuals and organizations are not permitted to** | Carry out investigations and require law enforcement |
| 78. **Digital forensics** | Is the "process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law) |
| 79. **Computer forensics includes activities that** | Involve the exploration and application of methods to gather, process, interpret and use digital evidence<br>that help to substantiate whether an incident happened |
| 80. **Computer forensics includes activities such as** | Providing validation that an attack actually occurred, Gathering digital evidence that can later be used in judicial proceedings |
| 81. **Any electronic document or data can be used as** | Digital evidence, provided there is sufficient manual or<br>electronic proof that the contents of digital evidence are in their original state and have not been tampered with<br>or modified during the process of collection and analysis. |
| 82. **It is important to use industry-specified best practices, proven tools and due diligence** | To provide reasonable assurance of the quality of evidence |
| 83. **It is also important to demonstrate integrity and reliability of evidence** | For it to be acceptable to law enforcement authorities |

| | | |
|---|---|---|
| 84. | **if the IS auditor "boots" a computer suspected of containing stored information that might represent evidence in a court case** | The auditor cannot later deny that they wrote data to the hard drive because the boot sequence writes a record to the drive. This is the reason specialist tools are used to take a true copy of the drive, which is then used in the investigation. |
| 85. | **There are four major considerations in the chain of events in regards to evidence in digital forensics** | Identify, Preserve, Analyze, Present |
| 86. | **Forensic Chain of Events: Identify** | Refers to the identification of information that is available and might form the evidence of an incident |
| 87. | **Forensic Chain of Events: Preserve** | Retrieving identified information and preserving it as evidence, the imaging of original media in presence of an independent third party, requires being able to document chain-of-custody so that it can be established in a court of law. |
| 88. | **Forensic Chain of Events: Analyze** | Extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format requires an in-depth knowledge of how different pieces of evidence may fit together. performed using an image of media and not the original |
| 89. | **Forensic Chain of Events: Present** | Involves a presentation to the various audiences such as management, attorneys, court, etc |
| 90. | **Acceptance of the evidence depends upon** | The manner of presentation (as it should be convincing),<br>qualifications of the presenter, and credibility of the process used to preserve and analyze the evidence |
| 91. | **The assurance professional should** | Give consideration to key elements of computer forensics during audit planning |
| 92. | **Key elements of computer forensics during audit planning** | Data Protection, Data Acquisition, Imaging, Extraction, Interrogation, Ingestion/Normalization, Reporting, Network Traffic Analysis, Log File Analysis, Time Lines, Anti-forensics |
| 93. | **Data Protection** | To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocols to inform appropriate parties that electronic evidence will be sought and to not destroy it by any means |
| 94. | **Infrastructure and processes for incident response and handling** | Should be in place to permit an effective response and forensic investigation if an event or incident occurs. |
| 95. | **Data Acquisition** | All information and data required should be transferred into a controlled location; this includes all types of<br>electronic media such as fixed disk drives and removable media. |
| 96. | **Each device must be checked to ensure** | That it is write-protected by using a device known as a write-blocker. |
| 97. | **It is also possible to get data and information from witnesses or related parties by** | Recorded statements. |
| 98. | **By volatile data, investigators can determine** | What is currently happening on a system. This kind of data includes open ports, open files, active processes, user logons and other data present in RAM |
| 99. | **Volatile data is lost** | When the computer is shut down. |
| 100. | **Imaging** | Is a process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed |
| 101. | **The imaging process** | Is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis |
| 102. | **Imaging duplicates the disk surface** | Sector by sector |

| | | |
|---|---|---|
| 103. | **It is sometimes possible to recover destroyed information** | (erased even by reformatting) from the disk's surface |
| 104. | **Extraction** | Consists of identification and selection of data from the imaged data set |
| 105. | **The extraction process should include** | Standards of quality, integrity and reliability |
| 106. | **The extraction process includes** | Software used and media where an image was made |
| 107. | **The extraction process could include** | Different sources such as system logs, firewall logs, IDS logs, audit trails and network management information. |
| 108. | **Interrogation** | Is used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data |
| 109. | **Ingestion/Normalization** | Process converts the information extracted to a format that can be understood by investigators |
| 110. | **Ingestion/Normalization** | It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tools |
| 111. | **It is possible to create relationships from data by extrapolation** | Using techniques such as fusion, correlation, graphing, mapping or time lining, which could be used in the construction of the investigation's hypothesis |
| 112. | **The information obtained from digital forensics has** | Limited value when it is not collected and reported in the proper way |
| 113. | **A digital forensics report must state** | Why the system was reviewed, how the computer data were reviewed and what conclusions were made from this analysis. |
| 114. | **The digital forensics report should achieve the following goals** | Accurately describe the details of an incident, Be understandable to decision makers, Be able to withstand a barrage of legal scrutiny, Be unambiguous and not open to misinterpretation, Be easily referenced, Contain all information required to explain conclusions reached, Offer valid conclusions, opinions or recommendations when needed, Be created in a timely manner |
| 115. | **The digital forensics report should also identify** | The organization, sample reports and restrictions on circulation (if any) and include any reservations or qualifications that the assurance professional has with respect to the assignment |
| 116. | **Network traffic analysis** | Identifies patterns in network communications |
| 117. | **Traffic analysis does not need to have** | The actual content of the communication but analyzes where traffic is taking place, when and for how long communications occur, and the size of information transferred. |
| 118. | **Traffic analysis can be used proactively to** | Identify potential anomalies in communications or during incident response to develop footprints that identify different attacks or the activities of different individuals |
| 119. | **Audit trail software** | Can create large files, which can be extremely difficult to analyze manually. |
| 120. | **The use of automated tools is likely to be** | The difference between unused audit trail data and an effective review. |
| 121. | **Some of the types of logging tools include** | Audit reduction tools, Trend/variance-detection tools, Attack-signature-detection tools |
| 122. | **Audit reduction tools** | These are preprocessors designed to reduce the volume of audit records to facilitate manual review. these tools can remove many audit records known to have little security significance and remove records generated by specified classes of events |
| 123. | **Trend/variance-detection tools** | These look for anomalies in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major variations |
| 124. | **Attack-signature-detection tools** | These look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed logon attempts. |
| 125. | **Timelines** | Are chronological graphs where events related to an incident can be mapped to look for relationships in complex cases |
| 126. | **Timelines can provide** | Simplified visualization for presentation to management and other nontechnical audiences. |

| | | |
|---|---|---|
| 127. | **Programmers develop anti-forensics tools to** | Make it difficult or impossible for investigators to retrieve information during an investigation |
| 128. | **Anti-forensics tactics, techniques and procedures (TTPs) include, but are not limited to:** | Securely deleting data, Overwriting metadata, Preventing data creation, Encrypting data, Encrypting network protocols, Hiding data in slack space or other unallocated locations, Hiding data or a file within another file (steganography) |
| 129. | **When incident response plans fail to control an incident** | The incident could escalate into a disaster |
| 130. | **Disasters** | Are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting organizational operations |
| 131. | **The disruption could be a few minutes to several months** | Depending on the extent of damage to the information resource |
| 132. | **Most important, disasters require** | Recovery efforts to restore operational status. |
| 133. | **A disaster may be caused by** | Natural calamities, such as earthquakes, floods, tornadoes and fire, or a disaster may be caused by events precipitated by humans such as terrorist attacks, hacker attacks, viruses or human error |
| 134. | **Many disruptions start** | As mere incidents |
| 135. | **If the organization has a help desk or service desk** | It would act as the early warning system to recognize the first signs of an upcoming disruption |
| 136. | **Until these "creeping disasters" strike (the database halts)** | They cause only infrequent user complaints |
| 137. | **A cybersecurity-related disaster may occur when** | A disruption in service is caused by system malfunctions, accidental file deletions, untested application releases, loss of backup, network DoS attacks, intrusions or viruses. |
| 138. | **These events may require** | Action to recover operational status in order to resume service. Such actions may necessitate restoration of hardware, software or data files. |
| 139. | **The purpose of business continuity planning (BCP)/disaster recovery planning (DRP) is to** | Enable a business to continue offering critical services in the event of a disruption and to survive a disastrous interruption to activities. |
| 140. | **Rigorous planning and commitment of resources** | Are necessary to adequately plan for such an event. |
| 141. | **BCP takes into consideration** | Those critical operations that are necessary to the survival of the organization, The human/material resources supporting them, Predisaster readiness covering incident response management to address all relevant incidents affecting business processes, Evacuation procedures, Procedures for declaring a disaster (escalation procedures) |
| 142. | **BCP takes into consideration** | Circumstances under which a disaster should be declared. All interruptions are not disasters, but a small incident not addressed in a timely or proper manner may lead to a disaster, The clear identification of the responsibilities in the plan, of the persons responsible for each function in the plan, of contract information, The step-by-step explanation of the recovery process, The clear identification of the various resources required for recovery and continued operation of the organization |
| 143. | **BCP is primarily the responsibility of** | Senior management, because they are entrusted with safeguarding the assets and the viability of the organization, as defined in the BCP/DRP policy |
| 144. | **The BCP is generally followed by** | The business and supporting units, to provide a reduced but sufficient level of functionality in the business operations immediately after encountering an interruption, while recovery is taking place |
| 145. | **Depending on the complexity of the organization** | There could be one or more plans to address the various aspects of BCP and DRP. However, each has to be consistent with other plans to have a viable BCP strategy. |

| | | |
|---|---|---|
| 146. | **Even if similar processes of the same organization are handled at a different geographic location** | The BCP and DRP solutions may be different for different scenarios |
| 147. | **BCP and DRP solutions may be different due to** | Contractual requirements |
| 148. | **A BCP solution for the online service** | Will be significantly different than one for the back office processing. |
| 149. | **The first step in preparing a new BCP** | Is to identify the business processes of strategic importance—those key processes that are responsible for both the permanent growth of the business and for the fulfillment of the business goals |
| 150. | **Ideally, the BCP/DRP should be supported by** | A formal executive policy that states the organization's overall target for recovery and empowers those people involved in developing, testing and maintaining the plans. |
| 151. | **Based on the key processes, a business impact analysis (BIA) process should** | Begin to determine time frames, priorities, resources and interdependencies that support the key processes |
| 152. | **Business risk is directly proportional to** | The impact on the organization and the probability of occurrence of the perceived threat |
| 153. | **The result of the BIA should be the identification of the following** | The human resources, data, infrastructure elements and other resources that support the key processes, A list of potential vulnerabilities—the dangers or threats to the organization, The estimated probability of the occurrence of these threats, The efficiency and effectiveness of existing risk mitigation controls (risk countermeasures) |
| 154. | **Information is collected for the BIA from** | Different parts of the organization which own key processes/applications. |
| 155. | **To evaluate the impact of downtime for a particular process/application** | The impact bands are developed (i.e., high, medium, low) and, for each process, the impact is estimated in time (hours, days, weeks). The same approach is used when estimating the impact of data loss. |
| 156. | **The financial impact may be estimated using** | The same techniques, assigning the financial value to the particular impact band |
| 157. | **Data for the BIA** | May be collected on the time frames needed to supply vital resources—how long the organization may run if a supply is broken or when the replacement has arrived. |
| 158. | **The BIA should answer three important questions:** | What are the different business processes?, What are the critical information resources related to an organization's critical business processes? What is the critical recovery time period for information resources in which business processing must be resumed before significant or unacceptable losses are suffered? |
| 159. | **RTO is defined as the** | RTO is defined as the |
| 160. | **The RTO is usually determined based on the** | Point where the ongoing cost of the loss is equal to the cost of recovery. |
| 161. | **RPO is defined as the** | Acceptable data loss in case of a disruption of operations |
| 162. | **The RTO indicates** | The earliest point in time to which it is acceptable to recover data. In other words, it is the last known point of good data. |
| 163. | **To ensure an effective incident management plan or disaster recovery plan** | The RTO and RPO must be closely linked. A short RTO may be difficult to achieve if there is a large amount of data to be restored (RPO). |
| 164. | **In the case of IS BCP, the approach is the same as in BCP with the exception being** | That the continuity of IS processing is threatened |

| | | |
|---|---|---|
| 165. | **IS processing is of strategic importance** | It is a critical component since most key business processes depend on the availability of key systems, infrastructure components and data. |
| 166. | **The IS BCP should be** | Aligned with the strategy of the organization |
| 167. | **The criticality of the various application systems deployed in the organization depends on** | The nature of the business as well as the value of each application to the business. |
| 168. | **The value of each application to the business is** | Directly proportional to the role of the information system in supporting the strategy of the organization |
| 169. | **The components of the information system** | Are then matched to the applications |
| 170. | **The information system BCP/DRP** | Is a major component of an organization's overall business continuity and disaster recovery strategy. |
| 171. | **If the IS plan is a separate plan** | It must be consistent with and support the corporate BCP. |
| 172. | **Data recovery** | Is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible for any reason |
| 173. | **Recovery processes vary depending on** | The type and amount of data lost, the backup method employed and the backup media |
| 174. | **An organization's DRP must** | Provide the strategy for how data will be recovered and assign recovery responsibilities. |
| 175. | **Backup procedures** | Are used to copy files to a second medium such as a disk, tape or the cloud. |
| 176. | **Backup files should be kept** | At an offsite location |
| 177. | **Backups are usually automated using** | Operating system commands or backup utility programs |
| 178. | **Most backup programs compress the data** | So that the backups require fewer media |
| 179. | **There are three types of data backups** | Full, incremental and differential |
| 180. | **Full backups** | Provide a complete copy of every selected file on the system, regardless of whether it was backed up recently. This is the slowest backup method but the fastest method for restoring data |
| 181. | **Incremental backups** | Copy all files that have changed since the last backup was made, regardless of whether the last backup was a full or incremental backup. This is the fastest backup method but the slowest method for restoring data |
| 182. | **Differential backups** | Copy only the files that have changed since the last full backup. The file grows until the next full backup is performed |