 QUESTIONS

[**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q1)**.**   Ravila, a new CISO in a healthcare organization, is reviewing incident response records from the past several years. Ravila has determined that minor incidents were managed with too much rigor and complexity, while major incidents weren’t dealt with thoroughly enough. What might be the cause of this?

**A.**   Lack of training for incident responders

**B.**   Inconsistent levels of response to incidents

**C.**   Lack of a tiered incident response plan

**D.**   Improperly tuned SIEM use cases

[**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q2)**.**   Which of the following is *not* a valid objection for using incident response plan “templates” to serve as an organization’s security incident response plan?

**A.**   The templates will lack the specifics about business processes and technology.

**B.**   The templates will lack the specific regulations the organization is required to comply with.

**C.**   The templates will lack the names of specific departments and executives.

**D.**   The templates will not specifically call on the organization’s crisis response plan.

[**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q3)**.**   Why would an organization consider developing alerts on its security information and event management system, as opposed to using its existing daily log review procedure?

**A.**   More accurate and timely awareness of security issues requiring action

**B.**   Compliance with PCI 3.2 requirement 10.6

**C.**   Reduce costs associated with time-consuming log review

**D.**   Free up staff to perform more challenging and interesting tasks

[**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q4)**.**   The purpose of documenting the steps taken during the response to an actual security incident includes all of the following *except* which one?

**A.**   Helps the organization understand how to respond more effectively during future incidents

**B.**   Helps the organization understand whether incident responders followed incident response procedures

**C.**   Helps the organization understand whether the organization recovered from the incident

**D.**   Helps the organization understand whether the incident response was compliant with applicable laws

[**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q5)**.**   While responding to a security incident, the person acting as the incident commander is unable to notify a particular executive in an escalation procedure. What should the incident responder do next?

**A.**   Notify regulators that the organization is experiencing a cyber incident and requires assistance.

**B.**   Notify law enforcement that the organization is experiencing a cyber incident and requires assistance.

**C.**   Order incident responders to suspend their activities until the executive has been contacted.

**D.**   Notify the next highest executive in the escalation chain.

[**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q6)**.**   Why should incident responders participate in incident response tabletop exercises?

**A.**   Helps incident responders better understand incident response procedures

**B.**   Helps incident responders find mistakes in incident response procedures

**C.**   Helps incident responders understand how long it should take to respond to actual incidents

**D.**   Helps incident responders memorize incident response procedures so they can respond more quickly

[**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q7)**.**   Why should incident responders be asked to review incident response procedures?

**A.**   Helps incident responders memorize incident response procedures so they can respond more quickly

**B.**   Helps incident responders understand how long it should take to respond to actual incidents

**C.**   Helps incident responders better understand incident response procedures

**D.**   Helps incident responders find mistakes in incident response procedures

[**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q8)**.**   Why would PCI-DSS requirements require organizations to put emergency contact information for card brands in their incident response plans?

**A.**   An emergency is a poor time to start looking for emergency contact information for outside organizations.

**B.**   Card brands must be notified of an incident as soon as possible.

**C.**   Requirement 12.10.1 in PCI-DSS requires it.

**D.**   It reminds organizations to notify the card brands in the event of a breach.

[**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q9)**.**   The purpose of a post-incident review of a security incident includes all of the following *except* which one?

**A.**   Determine the root cause of the incident.

**B.**   Identify improvements in incident response procedures.

**C.**   Determine the motivation of the attacker.

**D.**   Identify improvements in cybersecurity defenses.

[**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q10)**.**   James, the CISO in an organization, has reviewed the organization’s incident response plans and disaster recovery plans and has determined that incident response plans do not include any provisions should a security incident occur during a declared disaster of the organization. What is James’s most appropriate response?

**A.**   Declare a security incident.

**B.**   Request that the next tabletop exercise take place at the emergency operations center.

**C.**   No response is required because security incident response plans are not required for DR sites.

**D.**   Request that incident response and disaster recovery teams update the IRP to include procedures during emergency operations mode.

[**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q11)**.**   Which term in security incident response represents the final activity that takes place during a response to an incident?

**A.**   Post-incident review

**B.**   Remediation

**C.**   Closure

**D.**   Containment

[**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q12)**.**   Which step in an incident response plan is associated with tabletop exercises?

**A.**   Remediation

**B.**   Detection

**C.**   Analysis

**D.**   Planning

[**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q13)**.**   Of what value is a business impact analysis (BIA) in security incident response planning?

**A.**   Identifies the business owners associated with information systems, and therefore the escalation path

**B.**   Identifies the systems that require forensic examination during an incident

**C.**   Indirectly identifies the most important information systems that require protection from threats

**D.**   Directly identifies the location of the most critical data

[**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q14)**.**   Which of the following criteria would likely *not* be used to classify a security incident?

**A.**   Data volume

**B.**   System location

**C.**   Data sensitivity

**D.**   Operational criticality

[**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q15)**.**   An incident response team is responding to a situation in which an intruder has successfully logged on to a system using stolen nonprivileged credentials. Which steps are most effective at containing this incident?

**A.**   Lock the compromised user account.

**B.**   Reset the password of the compromised user account.

**C.**   Kill all processes associated with the compromised user account.

**D.**   Blackhole the intruder’s originating IP address and lock the compromised user account.

[**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q16)**.**   In what circumstances should executive management be notified of a security incident?

**A.**   In no cases, other than monthly and quarterly metrics

**B.**   In all cases

**C.**   When its impact is material

**D.**   When regulators are required to be notified

[**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q17)**.**   Which of the following individuals should approve the release of notifications regarding cybersecurity incidents to affected parties who are private citizens?

**A.**   General counsel

**B.**   Chief marketing officer

**C.**   Chief information security officer

**D.**   Security incident response commander

[**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q18)**.**   What is the purpose of a write blocker in the context of security incident response?

**A.**   Protects forensic evidence against tampering

**B.**   Creates forensically identical copies of hard drives

**C.**   Assures that hard drives can be examined without being altered

**D.**   Assures that affected systems cannot be altered

[**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q19)**.**   An employee in an organization is suspected of storing illegal content on the workstation assigned to him. Human resources asked the security manager to log on to the workstation and examine its logs. The security manager has identified evidence in the workstation’s logs that supports the allegation. Which statement best describes this investigation?

**A.**   The investigation was performed properly, and the organization can proceed with disciplinary action.

**B.**   Because forensic tools were not used to preserve the state of the workstation, the veracity of the evidence identified in the investigation can be called into question.

**C.**   The investigation should enter a second phase in which forensic tools are used to specifically identify the disallowed behavior.

**D.**   The investigation cannot continue because the initial examination of the workstation was performed without a signed warrant.

[**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q20)**.**   Under the state of California’s data security and privacy law of 2002 (SB 1386), under what circumstances is an organization *not* required to notify affected parties of a breach of personally identifiable information (PII)?

**A.**   When the organization cannot identify affected parties

**B.**   When the PII is encrypted at rest

**C.**   When the number of compromised records is less than 20,000

**D.**   When the number of total records is less than 20,000

[**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q21)**.**   Which of the following is *not* considered a part of a security incident post-incident review?

**A.**   Motivations of perpetrators

**B.**   Effectiveness of response procedures

**C.**   Accuracy of response procedures

**D.**   Improvements of preventive controls

[**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q22)**.**   Which of the following is usually *not* included in a cost analysis of a security incident during post-incident review?

**A.**   Penalties and legal fees

**B.**   Notification to external parties

**C.**   Assistance by external parties

**D.**   Loss of market share

[**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q23)**.**   Which of the following describes the best practice for capturing login log data?

**A.**   Capture all unsuccessful login attempts. Capture user ID, password, IP address, and location.

**B.**   Capture all successful and unsuccessful login attempts. Capture user ID, password, IP address, and location.

**C.**   Capture all successful and unsuccessful login attempts. Capture user ID, IP address, and location.

**D.**   Capture all unsuccessful login attempts. Capture user ID, IP address, and location.

[**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q24)**.**   What is the best method for utilizing forensic investigation assistance in organizations too small to hire individuals with forensic investigation skills?

**A.**   Utilize interns from a nearby college or university that teaches cyberforensic investigations.

**B.**   Request assistance from law enforcement at the city, state/province, or national level.

**C.**   Obtain an incident response retainer from a cybersecurity firm that specializes in security incident response services.

**D.**   Use one of several cloud-based, automated forensic examination services.

[**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q25)**.**   Threat analysts in an organization have identified a potential malware threat in an advisory. Detection in production systems will necessitate configuration changes to antivirus systems on production servers. What approach is best for making these configuration changes?

**A.**   Make the changes as soon as possible on production servers to stop the threat.

**B.**   Test the changes on nonproduction servers and measure performance impact.

**C.**   Write a rule in intrusion detection systems to block the threat at the network layer.

**D.**   Update antivirus signature files to permit detection of the threat.

[**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q26)**.**   Which methods are used to test security incident response plans?

**A.**   Document review, tabletop simulation, actual incident

**B.**   Document review, walkthrough, parallel test, cutover test

**C.**   Document review, walkthrough, tabletop simulation, parallel test, cutover test

**D.**   Document review, walkthrough, tabletop simulation

[**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q27)**.**   In the European General Data Protection Regulation, how quickly must an organization report a security breach of PII to government authorities?

**A.**   72 hours

**B.**   48 hours

**C.**   24 hours

**D.**   4 hours

[**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q28)**.**   An organization that obtains a SIEM is hoping to improve which security incident response-related metric?

**A.**   Remediation time

**B.**   Dwell time

**C.**   Postmortem quality

**D.**   Damage assessment

[**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q29)**.**   Ravila, a new CISO in a healthcare organization, is reviewing incident response records from the past several years. Ravila has determined that minor incidents were managed inconsistently from one incident to the next. Staff turnover has not been an issue. What is the most likely cause of this?

**A.**   Insufficient capacity for storage of forensic evidence

**B.**   Excessive meddling by executive management

**C.**   Inattention to detail

**D.**   Lack of detailed incident response playbooks

[**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q30)**.**   Who are the best parties to develop an organization’s security incident response plan?

**A.**   Business leaders and the general counsel

**B.**   Security consultants from an outside firm

**C.**   Security specialists and technology subject matter experts

**D.**   Regulators and security incident response subject matter experts

[**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q31)**.**   An organization has developed DLP solutions on its endpoints and file servers, but an adversary was able to exfiltrate data nonetheless. What solution should the organization next consider to detect unauthorized data exfiltration?

**A.**   Network anomaly detection

**B.**   Advanced antimalware

**C.**   Endpoint firewalls

**D.**   DDoS mitigation

[**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q32)**.**   Which sequence correctly identifies the steps in security incident response?

**A.**   Detection, Analysis, Containment, Eradication, Recovery, Closure

**B.**   Analysis, Containment, Eradication, Recovery, Closure

**C.**   Detection, Containment, Closure, Recovery

**D.**   Detection, Analysis, Eradication, Closure, Recovery

[**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q33)**.**   At what point in security incident response should the general counsel be notified?

**A.**   During quarterly reporting of key risk indicators

**B.**   During the post-incident review

**C.**   When the incident is initially declared

**D.**   When notification of regulators or external parties is likely

[**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q34)**.**   Designated incident responders would be asked to attend planned incident tabletop exercises for all reasons *except* which one?

**A.**   Tabletop exercises serve as training for incident responders.

**B.**   Tabletop exercises are important for estimating the amount of time required to respond to security incidents.

**C.**   Tabletop exercises help incident responders become familiar with incident response procedures.

**D.**   Tabletop exercises help identify errors in incident response procedures.

[**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q35)**.**   What is the best time frequency for conducting tabletop exercises?

**A.**   When significant changes are made to the incident response plan

**B.**   Annually

**C.**   Annually, or when there are significant changes to the incident response plan

**D.**   Upon inception of the initial incident response plan

[**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q36)**.**   What should a security incident response plan utilize to ensure effective notifications of internal and external parties?

**A.**   Business continuity plan

**B.**   Crisis response plan

**C.**   Contact list

**D.**   Disaster recovery plan

[**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q37)**.**   An organization recently suffered a security attack in which the attacker gained a foothold in the organization through the exploit of a weakness in an Internet-facing system. The root cause analysis in the post-incident review indicated that the cause of the incident was the lack of a particular security patch on the system that was initially attacked. What can the security leader conclude from the root cause?

**A.**   System engineers need additional training in patch management.

**B.**   The firewall failed to block the attack.

**C.**   The vulnerability management process needs to be improved.

**D.**   The root cause analysis was not sufficient to identify the real root cause.

[**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q38)**.**   What compensating control is most appropriate for the absence of encryption of backup media?

**A.**   Store backup media in locked containers in a keycard-access controlled room.

**B.**   Backup sensitive data to encrypted zip archives, which are backed up to tape.

**C.**   Obfuscate the names of files backed up to backup media.

**D.**   Do not permit backup media to be removed from the processing center.

[**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q39)**.**   The practice of proactively searching for signs of unauthorized intrusions is known as what?

**A.**   Geolocation

**B.**   Password cracking

**C.**   Threat hunting

**D.**   Log correlation

[**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q40)**.**   Incident responders have been asked to review a newly developed incident response plan. Incident responders’ feedback suggests confusion regarding what is expected from them and others in the organization during an actual incident. What is the most likely cause of this?

**A.**   The incident response plan lacks definitions of roles and responsibilities.

**B.**   The incident response plan lacks a list of key contacts.

**C.**   The incident responders have not yet been trained in the use of the plan.

**D.**   Outsourced forensics services have not yet been defined.

[**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q41)**.**   A SaaS-based e-mail services provider backs up its customer data through replication of data from one storage system in the main processing center to another storage system in an alternative processing center. This data assurance architecture leaves the organization vulnerable to what type of an attack?

**A.**   LUN spoofing

**B.**   Supply chain

**C.**   Smurf

**D.**   Ransomware

[**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q42)**.**   A multinational organization that is developing its security incident response plan has created its matrix of severity levels based upon data sensitivity, operational criticality, and data location. Why is this severity level scheme feasible or infeasible?

**A.**   The scheme is feasible because it identifies basic characteristics of its data sets.

**B.**   The scheme is feasible because of its simplicity.

**C.**   The scheme is not feasible because of its complexity.

**D.**   The scheme is not feasible because it is not mapped to business function.

[**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q43)**.**   An organization’s SIEM has generated alerts suggesting a user’s workstation is being attacked by ransomware. What steps should be taken in an effort to contain the incident?

**A.**   Disconnect the user’s workstation from the network.

**B.**   Disconnect the user’s workstation from the network and lock the user’s account.

**C.**   Lock the user’s account and scan the network for other infected systems.

**D.**   Pay the ransom and obtain decryption keys to recover lost data.

[**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q44)**.**   What is the main purpose for including an escalation process in an incident response plan?

**A.**   Legal is notified only if regulators are required to be notified.

**B.**   Executives are notified only if the incident is severe enough to warrant their involvement.

**C.**   Legal is notified only if affected parties need to be notified.

**D.**   It provides an additional set of resources to help the incident response team.

[**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q45)**.**   What is the likely role of the chief marketing officer in an information security incident?

**A.**   Keep records of security incident proceedings

**B.**   Update marketing collateral to state that security is important to the organization

**C.**   Notify regulators of the incident

**D.**   Develop press releases that describe the incident and the organization’s response to it

[**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q46)**.**   An organization has determined that there are no resources who have experience with malware reverse engineering and analysis. What is the organization’s best short-term remedy for this deficiency?

**A.**   Employ log correlation and analysis on the SIEM.

**B.**   Obtain tools that perform malware reverse engineering.

**C.**   Obtain an incident response retainer from a qualified security consulting firm.

**D.**   Train incident responders in malware analysis.

[**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q47)**.**   Why should forensic analysis tools *not* be placed on incident responders’ daily-use workstations?

**A.**   Workstations would become too costly and be a theft risk.

**B.**   Incident responders will not be able to complete daily tasks during incident response.

**C.**   Daily-use workstations do not have sufficient RAM capacity.

**D.**   Daily-use activities may influence forensic tools and cast doubt on their integrity.

[**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q48)**.**   The entirety of a service provider contract on incident response states, “Customer is to be notified within 48 hours of a suspected breach.” Why is this statement sufficient or insufficient?

**A.**   The statement is insufficient because “suspected breach” is ambiguous.

**B.**   The statement is insufficient because 48 hours is too long an interval.

**C.**   The statement is sufficient because 48 hours is considered reasonable.

**D.**   The statement is sufficient because “suspected breach” is a well-known industry term.

[**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q49)**.**   A post-incident-review process addresses all of the following *except* which one?

**A.**   Root cause analysis

**B.**   Selection of future incident response personnel

**C.**   Potential improvements in preventive and detective controls

**D.**   Potential improvements in security incident response procedures

[**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q50)**.**   Which of the following techniques best describes the impact of a security incident to management?

**A.**   Hard costs and soft costs

**B.**   Hard costs, soft costs, and qualitative impacts

**C.**   The total of all outsourced professional services

**D.**   The total of all hardware replacement for affected systems

[**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q51)**.**   For what reason(s) would an IT service desk incident ticketing system be inappropriate for storage of information related to security incidents?

**A.**   Automatic escalations would be timed incorrectly.

**B.**   A service desk incident ticketing system is designed for a different purpose.

**C.**   Sensitive information about an incident would be accessible to too few personnel.

**D.**   Sensitive information about an incident would be accessible to too many personnel.

[**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q52)**.**   At what point during security incident response should law enforcement be contacted?

**A.**   When root cause analysis during post-incident review identifies that a law has been broken

**B.**   When directed by the incident response plan and approved by the incident response commander

**C.**   When directed by the incident response plan and approved by the general counsel

**D.**   When the incident response commander determines a law has been broken

[**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q53)**.**   SOC operators and the incident response team have confirmed that an intruder has successfully compromised a web server and is logged in to it. The IR team wants to take steps to contain the incident but doesn’t want to disrupt operations unnecessarily. What approach should the IR team take?

**A.**   Test the proposed changes in a test environment first.

**B.**   Take containment steps as quickly as possible.

**C.**   Lock the user account and reboot the server.

**D.**   Turn on firewall debugging.

[**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q54)**.**   An organization has successfully completed training and walkthroughs of its incident response plan. What is the next best step?

**A.**   Repeat training at regular intervals.

**B.**   Conduct one or more tabletop exercises.

**C.**   Wait for an actual incident to prove the effectiveness of training and walkthroughs.

**D.**   Conduct a penetration test of production systems to measure response.

[**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q55)**.**   In a business-to-business service provider contract, which language is most reasonable for notification of a security incident?

**A.**   Notify customer within 1 hour of a breach

**B.**   Notify customer within 48 hours of a suspected breach

**C.**   Notify customer immediately after a breach

**D.**   Notify customer within 48 hours of a breach

[**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q56)**.**   All of the following are metrics for security incident response *except* which one?

**A.**   Dwell time

**B.**   Lag time

**C.**   Containment time

**D.**   Time to notify affected parties

QUICK ANSWER KEY

|  |  |  |
| --- | --- | --- |
| [**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa1)**.**   C  [**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa2)**.**   B  [**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa3)**.**   A  [**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa4)**.**   C  [**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa5)**.**   D  [**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa6)**.**   A  [**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa7)**.**   D  [**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa8)**.**   B  [**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa9)**.**   C  [**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa10)**.**   D  [**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa11)**.**   A  [**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa12)**.**   D  [**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa13)**.**   C  [**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa14)**.**   B  [**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa15)**.**   D  [**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa16)**.**   D  [**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa17)**.**   A  [**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa18)**.**   C  [**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa19)**.**   B  [**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa20)**.**   B | [**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa21)**.**   A  [**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa22)**.**   D  [**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa23)**.**   C  [**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa24)**.**   C  [**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa25)**.**   B  [**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa26)**.**   D  [**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa27)**.**   A  [**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa28)**.**   B  [**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa29)**.**   D  [**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa30)**.**   C  [**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa31)**.**   A  [**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa32)**.**   A  [**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa33)**.**   D  [**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa34)**.**   B  [**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa35)**.**   C  [**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa36)**.**   B  [**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa37)**.**   D  [**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa38)**.**   A  [**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa39)**.**   C  [**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa40)**.**   A | [**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa41)**.**   D  [**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa42)**.**   A  [**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa43)**.**   B  [**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa44)**.**   B  [**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa45)**.**   D  [**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa46)**.**   C  [**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa47)**.**   D  [**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa48)**.**   A  [**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa49)**.**   B  [**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa50)**.**   B  [**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa51)**.**   D  [**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa52)**.**   C  [**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa53)**.**   A  [**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa54)**.**   B  [**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa55)**.**   D  [**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5qa56)**.**   B |

A ANSWERS

[**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q1)**.**   Ravila, a new CISO in a healthcare organization, is reviewing incident response records from the past several years. Ravila has determined that minor incidents were managed with too much rigor and complexity, while major incidents weren’t dealt with thoroughly enough. What might be the cause of this?

**A.**   Lack of training for incident responders

**B.**   Inconsistent levels of response to incidents

**C.**   Lack of a tiered incident response plan

**D.**   Improperly tuned SIEM use cases

Images  **C**. This organization has an incident response plan that has one path of response for incidents of all severities. The result is this: incidents of high severity are treated too lightly, and incidents of low severity are treated with too much rigor.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because lack of training would more likely result in the response to all incidents being subpar. **B** is incorrect because this is another way of describing the question rather than a description of its cause. **D** is incorrect because SIEM use case tuning would not likely cause this phenomenon.

[**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q2)**.**   Which of the following is *not* a valid objection for using incident response plan “templates” to serve as an organization’s security incident response plan?

**A.**   The templates will lack the specifics about business processes and technology.

**B.**   The templates will lack the specific regulations the organization is required to comply with.

**C.**   The templates will lack the names of specific departments and executives.

**D.**   The templates will not specifically call on the organization’s crisis response plan.

Images  **B**. This objection, that the templates will lack the names of specific regulations that the organization is obligated to comply with, is the weakest objection to the use of templates and is therefore the correct answer.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because the lack of specifics about business processes and technologies in use is a valid objection to the use of a template. It is critical that an incident response plan be very specific about existing business processes so that the steps in an incident response plan will properly call out existing processes in the steps to respond to a security incident. Similarly, it is critical that an incident response plan have specific information about the technologies in use, as incident response plan steps will often direct responders to utilize technology in place for troubleshooting, isolation, and mitigation. **C** is incorrect because the lack of specific names of departments and executives is a valid objection to the use of such a template. The names of specific departments are needed so that incident responders understand which departments to work with during various stages of incident response. The names of executives are also useful, as executives do need to be informed about an incident in progress. **D** is incorrect because the lack of specific references to an organization’s crisis response plan is a valid objection to such a template. A security incident response plan certainly needs to call out the organization’s crisis response plan, as a highly severe security incident may need to trigger an organization’s crisis response plan.

[**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q3)**.**   Why would an organization consider developing alerts on its security information and event management system, as opposed to using its existing daily log review procedure?

**A.**   More accurate and timely awareness of security issues requiring action

**B.**   Compliance with PCI 3.2 requirement 10.6

**C.**   Reduce costs associated with time-consuming log review

**D.**   Free up staff to perform more challenging and interesting tasks

Images  **A**. The best reason for developing alerts in a security information and event management system (SIEM) is the near-instantaneous alerting of personnel of a security matter requiring investigation and potential remediation. Daily log review is time consuming and infeasible in all but the smallest organizations due to the high volume of log data that is produced in information systems.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because PCI requirement 10.6 does not specifically require that an organization employ a SIEM with alerts, although it is suggested as a more effective approach for daily log review. **C** is incorrect because cost reduction is not the best reason to generate security alerts. **D** is incorrect because providing staff with professional challenges is not the best answer to this question.

[**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q4)**.**   The purpose of documenting the steps taken during the response to an actual security incident includes all of the following *except* which one?

**A.**   Helps the organization understand how to respond more effectively during future incidents

**B.**   Helps the organization understand whether incident responders followed incident response procedures

**C.**   Helps the organization understand whether the organization recovered from the incident

**D.**   Helps the organization understand whether the incident response was compliant with applicable laws

Images  **C**. Documenting the steps followed during response to an actual incident probably does little to help the organization understand whether it actually recovered from the incident. Key personnel in the organization will know whether recovery was complete and successful and whether response steps were recorded or not.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because a review of steps taken during response to an actual incident can help incident responders better understand whether they acted effectively. **B** is incorrect because documentation of the steps taken during response to an actual incident will help responders know whether the proper steps were taken. **D** is incorrect because knowing what steps were taken during an actual incident will help incident responders better understand whether their actions were compliant with applicable laws—for instance, whether evidence was properly collected and protected and whether appropriate parties were notified.

[**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q5)**.**   While responding to a security incident, the person acting as the incident commander is unable to notify a particular executive in an escalation procedure. What should the incident responder do next?

**A.**   Notify regulators that the organization is experiencing a cyber incident and requires assistance.

**B.**   Notify law enforcement that the organization is experiencing a cyber incident and requires assistance.

**C.**   Order incident responders to suspend their activities until the executive has been contacted.

**D.**   Notify the next highest executive in the escalation chain.

Images  **D**. The best choice among those available here is for the incident commander to notify the next highest executive in the escalation chain. This is not an ideal situation, but security incident response does not always proceed as expected.

Images  **A**, **B**, and **C**are incorrect. **A** and **B** are incorrect because notification of outside authorities is not an appropriate alternative action to the inability to contact an executive. **C** is incorrect because suspension of security incident response activities may permit attackers to continue inflicting damage to the organization.

[**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q6)**.**   Why should incident responders participate in incident response tabletop exercises?

**A.**   Helps incident responders better understand incident response procedures

**B.**   Helps incident responders find mistakes in incident response procedures

**C.**   Helps incident responders understand how long it should take to respond to actual incidents

**D.**   Helps incident responders memorize incident response procedures so they can respond more quickly

Images  **A**. Participation in incident response tabletop exercises helps incident responders become more familiar with incident response procedures. Talking through a simulated incident and thinking about each step in incident response helps responders better understand each step—how to perform it and why it is needed.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because the identification of mistakes is not the primary purpose of an incident response tabletop exercise, although it does sometimes occur. **C** is incorrect because knowing the length of time required to respond to an incident is not a primary purpose of tabletop exercises. **D** is incorrect because memorization of response procedures is not an objective of tabletop exercises.

[**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q7)**.**   Why should incident responders be asked to review incident response procedures?

**A.**   Helps incident responders memorize incident response procedures so they can respond more quickly

**B.**   Helps incident responders understand how long it should take to respond to actual incidents

**C.**   Helps incident responders better understand incident response procedures

**D.**   Helps incident responders find mistakes in incident response procedures

Images  **D**. A primary purpose of incident response plan document review is to identify errors in response plans so that they can be corrected prior to an actual incident occurring.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because memorization of response procedures is not an objective of a document review of an incident response plan. **B** is incorrect because gaining an understanding of the length of time required to respond to an incident is not an objective of a review of incident response documents. **C** is incorrect because the primary objective of a document review is not to help incident responders be more familiar with incident response procedures. That said, improved familiarity is a valuable by-product of such a review.

[**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q8)**.**   Why would PCI-DSS requirements require organizations to put emergency contact information for card brands in their incident response plans?

**A.**   An emergency is a poor time to start looking for emergency contact information for outside organizations.

**B.**   Card brands must be notified of an incident as soon as possible.

**C.**   Requirement 12.10.1 in PCI-DSS requires it.

**D.**   It reminds organizations to notify the card brands in the event of a breach.

Images  **B**. According to PCI-DSS requirement 12.10.1, card brands’ emergency contact information should be included in organizations’ security incident response plans because the card brands should be notified as soon as possible after knowledge of a breach of credit card data.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because, although it is true that an emergency is a poor time to start looking around for emergency contact information, this is not the best answer. **C** is incorrect because this answer is circular; there is a reason for the requirement, and answer B offers the reason. **D** is incorrect because the presence of contact information does not serve as a reminder; instead, security incident response procedures should explicitly specify when, and under what conditions, an organization is required to notify one or more of the card brands.

[**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q9)**.**   The purpose of a post-incident review of a security incident includes all of the following *except* which one?

**A.**   Determine the root cause of the incident.

**B.**   Identify improvements in incident response procedures.

**C.**   Determine the motivation of the attacker.

**D.**   Identify improvements in cybersecurity defenses.

Images  **C**. Determination of the motivation of an attacker is not one of the objectives of a review of the response to a security incident.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because determination of the root cause of a security incident *is* one of the main reasons for conducting a post-incident review. **B** is incorrect because identification of improvements in incident response procedures *is* one of the reasons for conducting a post-incident review. **D** is incorrect because the identification of improvements in defenses *is* one of the objectives of a post-incident review.

[**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q10)**.**   James, the CISO in an organization, has reviewed the organization’s incident response plans and disaster recovery plans and has determined that incident response plans do not include any provisions should a security incident occur during a declared disaster of the organization. What is James’s most appropriate response?

**A.**   Declare a security incident.

**B.**   Request that the next tabletop exercise take place at the emergency operations center.

**C.**   No response is required because security incident response plans are not required for DR sites.

**D.**   Request that incident response and disaster recovery teams update the IRP to include procedures during emergency operations mode.

Images  **D**. The organization’s incident response plan needs to be updated to include procedures, contact information, and other relevant information to assist incident responders to respond to a security incident properly should one occur while the organization is in emergency operations mode.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because declaration of an incident is inappropriate; there is no incident happening here. **B** is incorrect because a tabletop exercise in the context of an emergency operations center, while potentially valuable, will be at least somewhat ineffective because there are no security incident response procedures to be followed should a security incident occur while in emergency operations mode. **C** is incorrect because security incidents certainly must be declared should an incident occur at a DR site.

[**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q11)**.**   Which term in security incident response represents the final activity that takes place during a response to an incident?

**A.**   Post-incident review

**B.**   Remediation

**C.**   Closure

**D.**   Containment

Images  **A**. A post-incident review, sometimes casually called a postmortem, is a review of the entire incident intended to help reviewers understand the incident’s cause, the role of preventive and detective capabilities, and the effectiveness of incident responders. The purpose of the after-action review is to identify improvements in defenses and response procedures to reduce the probability and/or impact of a similar future incident and to ensure more effective response should one occur.

Images  **B**, **C**, and **D**are incorrect. These are all steps that take place after containment, mitigation, and recovery. Typically, the steps in security incident response are planning, detection, initiation, analysis, containment, eradication, recovery, remediation, closure, and post-incident review. Evidence is retained after an incident for an unspecific period of time.

[**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q12)**.**   Which step in an incident response plan is associated with tabletop exercises?

**A.**   Remediation

**B.**   Detection

**C.**   Analysis

**D.**   Planning

Images  **D**. Security incident response tabletop exercises are a part of planning. The actual exercise itself will include most of the steps of an actual incident so that responders will be more familiar with response procedures.

Images  **A**, **B**, and **C**are incorrect. Tabletop exercises are not limited to remediation, detection, or analysis, but are concerned with the entire lifecycle of incident response.

[**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q13)**.**   Of what value is a business impact analysis (BIA) in security incident response planning?

**A.**   Identifies the business owners associated with information systems, and therefore the escalation path

**B.**   Identifies the systems that require forensic examination during an incident

**C.**   Indirectly identifies the most important information systems that require protection from threats

**D.**   Directly identifies the location of the most critical data

Images  **C**. The business impact analysis (BIA) is a discovery and analysis activity that identifies the most critical business processes in an organization. The BIA also identifies information systems, service providers, and suppliers that support those business processes. In information security and security incident response, the BIA helps to identify an organization’s most important information systems.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because the identification of business owners is a secondary benefit from the BIA. **B** is incorrect because the BIA does not determine the need for forensic examination. **D** is incorrect because the location of critical data is a by-product of the BIA, but is not necessarily critical for incident response.

[**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q14)**.**   Which of the following criteria would likely *not* be used to classify a security incident?

**A.**   Data volume

**B.**   System location

**C.**   Data sensitivity

**D.**   Operational criticality

Images  **B**. The location of a system is the least likely factor to be used to classify a security incident, unless the incident constitutes a breach of privacy of individuals, in which case there may be applicable laws such as GDPR or CCPA. Further, one influence of the location of a system might be the selection of personnel to respond to an incident, but this is not a part of incident classification.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because the volume of data involved in an incident is likely to influence the incident’s classification, particularly if the data is sensitive. **C** is incorrect because the sensitivity of data involved in an incident is highly likely to influence the incident’s classification because of the possibility that regulators, law enforcement, or affected parties may need to be notified. **D** is incorrect because operational criticality of a system is likely to influence the incident’s classification.

[**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q15)**.**   An incident response team is responding to a situation in which an intruder has successfully logged on to a system using stolen nonprivileged credentials. Which steps are most effective at containing this incident?

**A.**   Lock the compromised user account.

**B.**   Reset the password of the compromised user account.

**C.**   Kill all processes associated with the compromised user account.

**D.**   Blackhole the intruder’s originating IP address and lock the compromised user account.

Images  **D**. Locking the compromised user account and blocking access from the intruder’s originating IP address are the best available steps here. Other steps should also be taken, including killing all processes running under the compromised user account.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because locking the compromised user account may be ineffective, as the intruder may have compromised other accounts. **B** is incorrect because resetting the password will not stop the attack in progress unless the intruder needs to log in again. **C** is incorrect because killing processes alone will not necessarily prevent the intruder from logging in again. None of these choices are completely effective.

[**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q16)**.**   In what circumstances should executive management be notified of a security incident?

**A.**   In no cases, other than monthly and quarterly metrics

**B.**   In all cases

**C.**   When its impact is material

**D.**   When regulators are required to be notified

Images  **D**. Executive management should be notified of a cyber incident when it has been determined that regulators must be notified. This is not the only circumstance in which executives should be notified; others include incidents that disrupt business operations as well as large-scale incidents involving the compromise of sensitive information.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because executives should be notified of serious incidents. **B** is incorrect because it is not necessary to notify executives of small-scale incidents. **C** is incorrect because it is not as good an answer as D.

[**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q17)**.**   Which of the following individuals should approve the release of notifications regarding cybersecurity incidents to affected parties who are private citizens?

**A.**   General counsel

**B.**   Chief marketing officer

**C.**   Chief information security officer

**D.**   Security incident response commander

Images  **A**. The general counsel—the top-ranking attorney—should be the person who approves the release of notifications to affected parties. An attorney has expertise in interpretation of applicable laws, and it is these laws that stipulate notifications to outside parties.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because the marketing executive generally does not have expertise in the law to decide when to perform a required notification. The marketing executive may, however, assist in the process of notifying those parties. **C** is incorrect because the CISO is generally not the leading expert in the law to determine if and when notification of outside parties is required. Further, because the CISO is generally responsible for security incident response, the CISO, the general counsel, and others function as an executive team responsible for high-level decisions, which is preferable over a single individual who makes all of the strategic decisions. **D** is incorrect because the incident commander is a lower level person who is responsible for response logistics, but not for making high-level decisions such as notification of external affected parties.

[**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q18)**.**   What is the purpose of a write blocker in the context of security incident response?

**A.**   Protects forensic evidence against tampering

**B.**   Creates forensically identical copies of hard drives

**C.**   Assures that hard drives can be examined without being altered

**D.**   Assures that affected systems cannot be altered

Images  **C**. A write blocker is used to connect a hard drive that is the subject of forensic analysis to a computer. The write blocker permits the computer to read from the subject hard drive but does not permit any updates to the hard drive. This serves as an important control in a forensic investigation by preserving the integrity of subject hard drives.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because a write blocker does not protect forensic evidence against tampering. **B** is incorrect because a write blocker is not used to create copies of hard drives; however, a write blocker is a supporting tool that ensures that copies of subject hard drives can be made without affecting the subject hard drives. **D** is incorrect because write blockers are not used to protect systems from being altered.

[**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q19)**.**   An employee in an organization is suspected of storing illegal content on the workstation assigned to him. Human resources asked the security manager to log on to the workstation and examine its logs. The security manager has identified evidence in the workstation’s logs that supports the allegation. Which statement best describes this investigation?

**A.**   The investigation was performed properly, and the organization can proceed with disciplinary action.

**B.**   Because forensic tools were not used to preserve the state of the workstation, the veracity of the evidence identified in the investigation can be called into question.

**C.**   The investigation should enter a second phase in which forensic tools are used to specifically identify the disallowed behavior.

**D.**   The investigation cannot continue because the initial examination of the workstation was performed without a signed warrant.

Images  **B**. Because the security manager logged in to the subject’s workstation without first taking steps to preserve a forensic copy of the workstation, the security manager could be accused of planting evidence on the workstation, and this allegation would be difficult to refute. The security manager should have first taken a forensic image of the workstation’s hard drive before examining its contents.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because the investigation was not performed properly: the security manager could potentially have tampered with the workstation’s hard drive and even planted evidence. If the disciplined employee brings a legal challenge to the organization, the challenge would cast doubt on the security manager’s actions. **C** is incorrect because the damage has already been done: the security manager’s initial examination of the hard drive has tainted the integrity of the hard drive; this cannot be undone. **D** is incorrect because a warrant is not required for an organization to conduct an examination and analyze its own property—in this case, a workstation.

[**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q20)**.**   Under the state of California’s data security and privacy law of 2002 (SB 1386), under what circumstances is an organization *not* required to notify affected parties of a breach of personally identifiable information (PII)?

**A.**   When the organization cannot identify affected parties

**B.**   When the PII is encrypted at rest

**C.**   When the number of compromised records is less than 20,000

**D.**   When the number of total records is less than 20,000

Images  **B**. Under the 2002 state of California’s security and privacy law (SB 1386), organizations are not required to notify affected parties of the breach of security if the information was encrypted at rest.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect, because even when an organization is unable to identify all of the specific parties affected by a security breach, the organization is required to publicly announce the breach. **C** is incorrect because there is no lower limit on the number of compromised records. **D** is incorrect because there is no limit on the size of a compromised database.

[**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q21)**.**   Which of the following is *not* considered a part of a security incident post-incident review?

**A.**   Motivations of perpetrators

**B.**   Effectiveness of response procedures

**C.**   Accuracy of response procedures

**D.**   Improvements of preventive controls

Images  **A**. The motivation of the perpetrators is generally not a part of a security incident post-incident review. Of the available answers, this is the least likely to be a part of a post-incident review.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because the effectiveness of response procedures is a key focus area on a post-incident review; it helps ensure that similar incidents in the future can be handled more effectively. **C** is incorrect because the accuracy of response procedures is considered; it helps ensure that organizations will handle similar future incidents more accurately. **D** is incorrect because a review of preventive (also detective and administrative) controls is a key focus of a post-incident review; it helps ensure that opportunities for improvements in relevant controls can help reduce the probability and/or impact of future events.

[**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q22)**.**   Which of the following is usually *not* included in a cost analysis of a security incident during post-incident review?

**A.**   Penalties and legal fees

**B.**   Notification to external parties

**C.**   Assistance by external parties

**D.**   Loss of market share

Images  **D**. Market share is generally *not* included in a cost analysis of a security event, because changes in market share may be more long term and potentially unknown for several months, quarters, or more. Changes in market share are also more difficult to attribute, as many other forces contribute to these changes.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because penalties (from regulators, customers, and others) and legal fees are generally included in the overall cost of a security breach. **B** is incorrect as the cost of notification to affected parties is generally included among costs of a security breach. **C** is incorrect because professional services fees and other costs from outside parties in support of the investigation, forensics, analysis, and other activities is generally included.

[**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q23)**.**   Which of the following describes the best practice for capturing login log data?

**A.**   Capture all unsuccessful login attempts. Capture user ID, password, IP address, and location.

**B.**   Capture all successful and unsuccessful login attempts. Capture user ID, password, IP address, and location.

**C.**   Capture all successful and unsuccessful login attempts. Capture user ID, IP address, and location.

**D.**   Capture all unsuccessful login attempts. Capture user ID, IP address, and location.

Images  **C**. The best practice for logging authentication events is the capture of all successful and unsuccessful login attempts and to capture the user ID, IP address, and location (if known).

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because successful login attempts should also be captured, and passwords should not be captured. **B** is incorrect because passwords should not be captured. **D** is incorrect because successful logins should also be captured.

[**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q24)**.**   What is the best method for utilizing forensic investigation assistance in organizations too small to hire individuals with forensic investigation skills?

**A.**   Utilize interns from a nearby college or university that teaches cyberforensic investigations.

**B.**   Request assistance from law enforcement at the city, state/province, or national level.

**C.**   Obtain an incident response retainer from a cybersecurity firm that specializes in security incident response services.

**D.**   Use one of several cloud-based, automated forensic examination services.

Images  **C**. Most organizations cannot justify hiring a cybersecurity specialist who has computer and network forensic investigations skills and experience. Such organizations should obtain an incident response retainer from a qualified cybersecurity professional services firm that will render assistance if and when a security incident occurs.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because interns will generally not have sufficient experience to be able to complete a forensic investigation and create a chain of custody. **B** is incorrect because law enforcement agencies, most of which have insufficient computer forensics resources, are generally not available to perform computer or network forensic analysis unless it is associated with a major crime. **D** is incorrect because there are no cloud-based forensic examination services (at the time of this writing).

[**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q25)**.**   Threat analysts in an organization have identified a potential malware threat in an advisory. Detection in production systems will necessitate configuration changes to antivirus systems on production servers. What approach is best for making these configuration changes?

**A.**   Make the changes as soon as possible on production servers to stop the threat.

**B.**   Test the changes on nonproduction servers and measure performance impact.

**C.**   Write a rule in intrusion detection systems to block the threat at the network layer.

**D.**   Update antivirus signature files to permit detection of the threat.

Images  **B**. Testing configuration changes in a nonproduction environment is the best first step to ensure that the configuration changes will not adversely affect production systems, both in terms of transaction capacity and correct function.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because there may be unintended consequences to the configuration change that may affect server availability. **C** is incorrect because intrusion detection systems cannot block intrusions. **D** is incorrect because threat analysts have already determined that a configuration change is necessary (perhaps activating real-time file access detection that might be normally turned off).

[**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q26)**.**   Which methods are used to test security incident response plans?

**A.**   Document review, tabletop simulation, actual incident

**B.**   Document review, walkthrough, parallel test, cutover test

**C.**   Document review, walkthrough, tabletop simulation, parallel test, cutover test

**D.**   Document review, walkthrough, tabletop simulation

Images  **D**. The types of tests that can be performed for security incident response are document review (where one or more individuals review the document on their own), walkthrough (where two or more individuals discuss the steps in the security incident response procedure), and tabletop simulation (where an expert moderator progressively reveals a realistic security incident scenario, and incident responders and others discuss their response activities and the challenges encountered).

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because an actual incident is not considered a purposeful test of an incident response plan. **B** and **C** are incorrect because a parallel test and cutover test are used in disaster recovery planning.

[**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q27)**.**   In the European General Data Protection Regulation, how quickly must an organization report a security breach of PII to government authorities?

**A.**   72 hours

**B.**   48 hours

**C.**   24 hours

**D.**   4 hours

Images  **A**. The European GDPR requires that organizations report breaches of PII to authorities within 72 hours. If the organization takes more than 72 hours to notify authorities, an explanation for the delay must accompany the notification.

Images  **B**, **C**, and **D**are incorrect. All are incorrect because organizations are required to notify authorities of a PII breach within 72 hours, not 48, 24, or 4 hours.

[**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q28)**.**   An organization that obtains a SIEM is hoping to improve which security incident response-related metric?

**A.**   Remediation time

**B.**   Dwell time

**C.**   Postmortem quality

**D.**   Damage assessment

Images  **B**. Dwell time, or the time that elapses from the start of an incident to realization that the incident has occurred (or is still occurring), can be improved through the use of a SIEM. Collecting log data from systems in the organization, a SIEM correlates log events and produces alerts when actionable incidents are discovered.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because a SIEM will have negligible impact on dwell time. **C** is incorrect because a SIEM will have little or no impact on postmortem quality. **D** is incorrect because a SIEM will have only minor impact on damage assessment.

[**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q29)**.**   Ravila, a new CISO in a healthcare organization, is reviewing incident response records from the past several years. Ravila has determined that minor incidents were managed inconsistently from one incident to the next. Staff turnover has not been an issue. What is the most likely cause of this?

**A.**   Insufficient capacity for storage of forensic evidence

**B.**   Excessive meddling by executive management

**C.**   Inattention to detail

**D.**   Lack of detailed incident response playbooks

Images  **D**. Of the available choices, the most likely cause of inconsistent response to security incidents is the lack of detailed procedural documentation in the organization’s security incident response plan. These detailed procedures are commonly known as playbooks.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because insufficient storage capacity for forensic evidence is not a likely cause of inconsistent responses to incidents. **B** is incorrect because meddling by executives is not a likely cause for inconsistent response. **C** is incorrect because inattention to detail is not the most likely cause.

[**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q30)**.**   Who are the best parties to develop an organization’s security incident response plan?

**A.**   Business leaders and the general counsel

**B.**   Security consultants from an outside firm

**C.**   Security specialists and technology subject matter experts

**D.**   Regulators and security incident response subject matter experts

Images  **C**. The best parties to develop a security incident response plan are security specialists and experts in relevant information technology.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because business leaders and general counsel, though essential personnel to participate in the response to a breach, are not the best parties to develop an organization’s security incident response plan. **B** is incorrect because, although outside experts may be qualified to write a general-purpose plan, those consultants won’t be familiar with the organization’s business processes and uses of information technology. **D** is incorrect because regulators do not develop security incident response plans for organizations they regulate.

[**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q31)**.**   An organization has developed DLP solutions on its endpoints and file servers, but an adversary was able to exfiltrate data nonetheless. What solution should the organization next consider to detect unauthorized data exfiltration?

**A.**   Network anomaly detection

**B.**   Advanced antimalware

**C.**   Endpoint firewalls

**D.**   DDoS mitigation

Images  **A**. Network anomaly detection, including Netflow technology, is designed to baseline normal network behavior and report on anomalous network traffic.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because advanced antimalware is not designed to detect data exfiltration. **C** is incorrect because endpoint firewalls will not appreciably add to endpoint-based DLP in terms of detecting data exfiltration. **D** is incorrect because DDoS mitigation will not help with the detection of data exfiltration.

[**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q32)**.**   Which sequence correctly identifies the steps in security incident response?

**A.**   Detection, Analysis, Containment, Eradication, Recovery, Closure

**B.**   Analysis, Containment, Eradication, Recovery, Closure

**C.**   Detection, Containment, Closure, Recovery

**D.**   Detection, Analysis, Eradication, Closure, Recovery

Images  **A**. Of the choices available here, the correct sequence of steps in security incident response are Detection, Analysis, Containment, Eradication, Recovery, and Closure.

Images  **B**, **C**, and **D**are incorrect. None of these represents the correct sequence of steps in security incident response.

[**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q33)**.**   At what point in security incident response should the general counsel be notified?

**A.**   During quarterly reporting of key risk indicators

**B.**   During the post-incident review

**C.**   When the incident is initially declared

**D.**   When notification of regulators or external parties is likely

Images  **D**. The general counsel, sometimes known as the chief legal officer, should be notified when it is determined that there may be a need to report the incident to regulators or other affected parties. The general counsel is responsible for the interpretation of applicable laws and other legal obligations (such as private contracts between organizations) and for making decisions regarding actions required by those laws and contracts.

Images  **A**, **B**, and **C**are incorrect. **A** and **B** are incorrect because the general counsel should be notified during serious incidents, not after they have concluded. **C** is incorrect because the general counsel does not need to be informed of minor incidents.

[**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q34)**.**   Designated incident responders would be asked to attend planned incident tabletop exercises for all reasons *except* which one?

**A.**   Tabletop exercises serve as training for incident responders.

**B.**   Tabletop exercises are important for estimating the amount of time required to respond to security incidents.

**C.**   Tabletop exercises help incident responders become familiar with incident response procedures.

**D.**   Tabletop exercises help identify errors in incident response procedures.

Images  **B**. Tabletop exercises are generally not a suitable opportunity to determine the length of time to respond to an incident. Rather, incident response tabletop exercises are designed to help incident responders become more familiar with incident response procedures.

Images  **A**, **C**, and **D**are incorrect. These are all valid reasons for asking incident responders to attend tabletop exercises.

[**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q35)**.**   What is the best time frequency for conducting tabletop exercises?

**A.**   When significant changes are made to the incident response plan

**B.**   Annually

**C.**   Annually, or when there are significant changes to the incident response plan

**D.**   Upon inception of the initial incident response plan

Images  **C**. Incident response tabletop exercises should be performed at least annually, as well as when significant changes are made to incident response plans. The hiring of new incident responders would present another opportunity to conduct tabletop exercises.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because tabletop exercises should be conducted at least annually. If no changes are made to the incident response plan, significant time could elapse between exercises. **B** is incorrect because annual tabletop exercises are insufficient if significant changes are made to the security incident response plan. **D** is incorrect because an incident response plan should be exercised at least annually and when significant changes are made to the plan.

[**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q36)**.**   What should a security incident response plan utilize to ensure effective notifications of internal and external parties?

**A.**   Business continuity plan

**B.**   Crisis response plan

**C.**   Contact list

**D.**   Disaster recovery plan

Images  **B**. A crisis response plan typically contains contact information for parties to be contacted in various business emergency scenarios, including security incidents and breaches.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because a business continuity plan does not generally contain detailed information regarding the notification of internal and external parties. **C** is incorrect because a contact list does not, by itself, define which parties are contacted, at what times, and in what circumstances. **D** is incorrect because a disaster recovery plan does not generally contain detailed information regarding the notification of other parties.

[**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q37)**.**   An organization recently suffered a security attack in which the attacker gained a foothold in the organization through the exploit of a weakness in an Internet-facing system. The root cause analysis in the post-incident review indicated that the cause of the incident was the lack of a particular security patch on the system that was initially attacked. What can the security leader conclude from the root cause?

**A.**   System engineers need additional training in patch management.

**B.**   The firewall failed to block the attack.

**C.**   The vulnerability management process needs to be improved.

**D.**   The root cause analysis was not sufficient to identify the real root cause.

Images  **D**. The root cause analysis of this security incident is insufficient. It is not appropriate to conclude that the breach occurred because of the lack of a patch. Proper root cause analysis would further ask the following: Why was the patch missing? Why wasn’t this server a part of the patch management process? Why did the server get implemented without being included in the patch management process? Why did the monthly review of patched systems miss this new server? And why did an underqualified person perform the monthly review? In this example string of questions, root cause analysis keeps asking why until no more information is available.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because this conclusion cannot be reasonably reached based upon a missing patch. **B** is incorrect because there is not enough information to conclude that a firewall rule failure was the cause of the incident. **C** is incorrect because there is not enough information to say which portion of the vulnerability management process requires improvement.

[**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q38)**.**   What compensating control is most appropriate for the absence of encryption of backup media?

**A.**   Store backup media in locked containers in a keycard-access controlled room.

**B.**   Backup sensitive data to encrypted zip archives, which are backed up to tape.

**C.**   Obfuscate the names of files backed up to backup media.

**D.**   Do not permit backup media to be removed from the processing center.

Images  **A**. Improving the security of unencrypted backup media is the most feasible compensating control. Many organizations still utilize mainframe and midrange computer systems that do not have the capability of encrypting backup media. But organizations, even when using newer hardware, sometimes do not encrypt backup media for a variety of valid reasons.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because there may be insufficient resources to zip archive very large data sets. **C** is incorrect because obfuscating filenames does little to protect the information contained therein. **D** is incorrect because retaining backup media in the processing center eliminates data assurance in certain disaster scenarios in which systems and media are damaged in the data center—for instance, in case of flood or fire.

[**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q39)**.**   The practice of proactively searching for signs of unauthorized intrusions is known as what?

**A.**   Geolocation

**B.**   Password cracking

**C.**   Threat hunting

**D.**   Log correlation

Images  **C**. “Threat hunting” is the term used to describe the activity by which analysts use advanced tools to search for signs of possible intrusions into systems. An example case of threat hunting involves the search for a specific operating system file that has a particular checksum, indicating that it has been altered with a specific emerging form of malware.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because geolocation is concerned with the identification of the geographic location of a subject. **B** is incorrect because password cracking is used to derive passwords from a hashed or encrypted password archive. **D** is incorrect because log correlation is an activity performed by a SIEM to identify potential intrusions or other unauthorized activity.

[**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q40)**.**   Incident responders have been asked to review a newly developed incident response plan. Incident responders’ feedback suggests confusion regarding what is expected from them and others in the organization during an actual incident. What is the most likely cause of this?

**A.**   The incident response plan lacks definitions of roles and responsibilities.

**B.**   The incident response plan lacks a list of key contacts.

**C.**   The incident responders have not yet been trained in the use of the plan.

**D.**   Outsourced forensics services have not yet been defined.

Images  **A**. The incident responders are confused because roles and responsibilities are undefined. This is a critical deficiency in an IRP because there will be confusion when important decisions need to be made, including declaration of an incident, escalation, and notification of regulators, affected parties, and law enforcement.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because the absence of key contacts is not likely to produce this type of confusion. **C** is incorrect because the lack of training is unlikely to result in incident responders not knowing who is responsible for carrying out specific activities during an incident. **D** is incorrect because the absence of a forensic analysis firm is not likely to produce this apparently wider confusion.

[**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q41)**.**   A SaaS-based e-mail services provider backs up its customer data through replication of data from one storage system in the main processing center to another storage system in an alternative processing center. This data assurance architecture leaves the organization vulnerable to what type of an attack?

**A.**   LUN spoofing

**B.**   Supply chain

**C.**   Smurf

**D.**   Ransomware

Images  **D**. An organization that replicates data from one storage system to another is likely to be vulnerable to ransomware: storage systems will likely replicate the destructive encryption from the main storage system to other storage systems. This would result in no source of undamaged files from which to recover.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because LUN spoofing is a fictitious term. **B** is incorrect because a supply chain attack is an attack on a manufacturing company in an attempt to alter or substitute components in a manufactured product (which can include software) for malicious reasons. **C** is incorrect because a Smurf attack is an attack in which large numbers of ICMP packets with the intended target source IP are broadcast to a network using an IP broadcast address.

[**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q42)**.**   A multinational organization that is developing its security incident response plan has created its matrix of severity levels based upon data sensitivity, operational criticality, and data location. Why is this severity level scheme feasible or infeasible?

**A.**   The scheme is feasible because it identifies basic characteristics of its data sets.

**B.**   The scheme is feasible because of its simplicity.

**C.**   The scheme is not feasible because of its complexity.

**D.**   The scheme is not feasible because it is not mapped to business function.

Images  **A**. This scheme, while a bit complex, appears reasonable because it addresses primary characteristics of data sets. The sensitivity of data is an indication of whether it is protected by regulation or private obligations; the operational criticality of data associates the data to revenue or organizational reputation; the location of data indicates local regulation or perhaps the identity of a local incident response team. Surely, simpler schemes are more common, but this is a multinational organization, which introduces potentially several operational complications.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because this scheme is not as simple as most. **C** is incorrect because this scheme, while somewhat complex, can be workable. **D** is incorrect because there is insufficient information to reach this conclusion.

[**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q43)**.**   An organization’s SIEM has generated alerts suggesting a user’s workstation is being attacked by ransomware. What steps should be taken in an effort to contain the incident?

**A.**   Disconnect the user’s workstation from the network.

**B.**   Disconnect the user’s workstation from the network and lock the user’s account.

**C.**   Lock the user’s account and scan the network for other infected systems.

**D.**   Pay the ransom and obtain decryption keys to recover lost data.

Images  **B**. Disconnecting the user’s workstation and locking the user’s account are the best first steps for containment. If the malware is running on the workstation, disconnecting it should prevention the loss of data on file shares that the user is permitted to access. Locking the user’s account will help to slow down instances of malware that may be present on other systems.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because there may be other instances of malware running under the user’s account on other systems. **C** is incorrect because although the user’s account should be locked right away, scanning for other infected systems is a reasonable step later in the containment phase. **D** is incorrect because paying a ransom does not facilitate data recovery in about half of all ransomware cases.

[**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q44)**.**   What is the main purpose for including an escalation process in an incident response plan?

**A.**   Legal is notified only if regulators are required to be notified.

**B.**   Executives are notified only if the incident is severe enough to warrant their involvement.

**C.**   Legal is notified only if affected parties need to be notified.

**D.**   It provides an additional set of resources to help the incident response team.

Images  **B**. The primary reason for escalation in an incident response plan is to provide a structured way for specific executives to be notified during a serious incident. A structured incident response plan will include incident severity levels that can be objectively identified; severity levels will have varying frequencies of communicated updates, named resources to assist, and executives to notify. Executives need to be aware of a serious incident because it is more likely to have long-term operational and reputational impacts on the organization.

Images  **A**, **C**, and **D**are incorrect. **A** and **C** are incorrect because notification of regulators, legal staff, and affected parties is but a narrow aspect of the need for escalation. **D** is incorrect because escalation, while it may indeed provide additional resources, is a function of the severity of the incident, not the desire for additional help.

[**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q45)**.**   What is the likely role of the chief marketing officer in an information security incident?

**A.**   Keep records of security incident proceedings

**B.**   Update marketing collateral to state that security is important to the organization

**C.**   Notify regulators of the incident

**D.**   Develop press releases that describe the incident and the organization’s response to it

Images  **D**. One activity that the chief marketing officer will perform is the development and distribution of press releases that describe the incident and the steps that the organization is taking to contain it and recover from it. Ideally, general versions of these press releases are written during incident response plan development.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because a marketing person is an unlikely choice to serve as the incident response team’s scribe. **B** is incorrect because such collateral updates are not a part of incident response, but activities that take place whenever the organization wishes to update its marketing messaging. **C** is incorrect because it is more likely that senior executives or the general counsel will be notifying regulators.

[**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q46)**.**   An organization has determined that there are no resources who have experience with malware reverse engineering and analysis. What is the organization’s best short-term remedy for this deficiency?

**A.**   Employ log correlation and analysis on the SIEM.

**B.**   Obtain tools that perform malware reverse engineering.

**C.**   Obtain an incident response retainer from a qualified security consulting firm.

**D.**   Train incident responders in malware analysis.

Images  **C**. The best short-term solution is to obtain a retainer from a security incident response firm that has staff and tooling available for this purpose. A viable long-term remedy may include training of in-house staff and acquisition of malware analysis tools.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because log correlation and analysis on a SIEM will not contribute to the cause of malware analysis. **B** is incorrect because malware analysis tools are not helpful if personnel are not trained in their use. **D** is incorrect because training is not a viable short-term remedy.

[**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q47)**.**   Why should forensic analysis tools *not* be placed on incident responders’ daily-use workstations?

**A.**   Workstations would become too costly and be a theft risk.

**B.**   Incident responders will not be able to complete daily tasks during incident response.

**C.**   Daily-use workstations do not have sufficient RAM capacity.

**D.**   Daily-use activities may influence forensic tools and cast doubt on their integrity.

Images  **D**. The rule of forensic analysis tools is that they must be run on dedicated, isolated systems that are used for no other purpose. Only this will instill confidence that other activities cannot influence the outcome of forensic investigations.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because theft risk is not a significant risk; still, it can be mitigated through secure storage of forensic computers. **B** is incorrect because this does not address the need for system isolation. **C** is incorrect because RAM capacity does not address the need for the forensic analysis system to be isolated from other activities.

[**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q48)**.**   The entirety of a service provider contract on incident response states, “Customer is to be notified within 48 hours of a suspected breach.” Why is this statement sufficient or insufficient?

**A.**   The statement is insufficient because “suspected breach” is ambiguous.

**B.**   The statement is insufficient because 48 hours is too long an interval.

**C.**   The statement is sufficient because 48 hours is considered reasonable.

**D.**   The statement is sufficient because “suspected breach” is a well-known industry term.

Images  **A**. The term “suspected breach” is ambiguous and should be defined more specifically. Otherwise, it would be too easy for an organization to consider nearly every activity a “suspected breach.”

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because 48 hours is a reasonable and standard interval for breach notification. **C** is incorrect because, even though 48 hours is a reasonable and standard interval for breach notification, the term “suspected breach” is ambiguous, so the statement is insufficient. **D** is incorrect because “suspected breach” is not a term that is interpreted consistently.

[**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q49)**.**   A post-incident-review process addresses all of the following *except* which one?

**A.**   Root cause analysis

**B.**   Selection of future incident response personnel

**C.**   Potential improvements in preventive and detective controls

**D.**   Potential improvements in security incident response procedures

Images  **B**. The selection of future incident response personnel is not likely to be included in a post-incident review. But on the topic of incident response personnel, issues of their training and knowledge may be discussed if there is a need for improvement.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because a sound incident response post-incident review will include root cause analysis to identify the root cause of the incident. **C** is incorrect because post-incident review will strive to identify improvements in controls to increase awareness of an incident and to reduce its impact and probability of occurrence. **D** is incorrect because a post-incident review attempts to find improvement opportunities in the incident review process itself.

[**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q50)**.**   Which of the following techniques best describes the impact of a security incident to management?

**A.**   Hard costs and soft costs

**B.**   Hard costs, soft costs, and qualitative impacts

**C.**   The total of all outsourced professional services

**D.**   The total of all hardware replacement for affected systems

Images  **B**. Because the costs and impact of a security incident can vary, the best approach is to report on specific hard costs, including professional services, tooling, and equipment, as well as soft costs, including the labor hours by in-house staff, together with qualitative impact such as market share or reputation damage that are difficult to quantify.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because hard costs and soft costs ignore qualitative impact such as loss of market share and reputational damage. **C** is incorrect because the cost of outsourced services probably does not represent the totality of hard costs, and it does not represent qualitative impact such as reputation. **D** is incorrect because hardware replacement, when it is needed at all, is probably a small portion of the total cost of an incident.

[**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q51)**.**   For what reason(s) would an IT service desk incident ticketing system be inappropriate for storage of information related to security incidents?

**A.**   Automatic escalations would be timed incorrectly.

**B.**   A service desk incident ticketing system is designed for a different purpose.

**C.**   Sensitive information about an incident would be accessible to too few personnel.

**D.**   Sensitive information about an incident would be accessible to too many personnel.

Images  **D**. The primary reason why an IT service desk incident ticketing system would not be used for security incidents is the potential for highly sensitive information in the ticketing system being available to all service desk and other IT personnel. A potential compromise is to record all incidents in the service desk ticketing system but store the most sensitive information (such as suspected personnel in an insider event or details about sensitive affected data or sensitive exploit information) elsewhere and reference it in the ticketing system.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because escalations can often be customized for incidents of various types and severities. **B** is incorrect because an IT service desk incident ticketing system is an appropriate system for tracking security incidents. **C** is incorrect because details about a security incident should not be widely available.

[**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q52)**.**   At what point during security incident response should law enforcement be contacted?

**A.**   When root cause analysis during post-incident review identifies that a law has been broken

**B.**   When directed by the incident response plan and approved by the incident response commander

**C.**   When directed by the incident response plan and approved by the general counsel

**D.**   When the incident response commander determines a law has been broken

Images  **C**. Law enforcement should be contacted when the incident response plan suggests such contact and when the general counsel has specifically approved it.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because post-incident review is generally far too late to notify law enforcement. **B** and **D** are incorrect because the incident commander is not the appropriate party to approve contact of law enforcement.

[**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q53)**.**   SOC operators and the incident response team have confirmed that an intruder has successfully compromised a web server and is logged in to it. The IR team wants to take steps to contain the incident but doesn’t want to disrupt operations unnecessarily. What approach should the IR team take?

**A.**   Test the proposed changes in a test environment first.

**B.**   Take containment steps as quickly as possible.

**C.**   Lock the user account and reboot the server.

**D.**   Turn on firewall debugging.

Images  **A**. When an incident response team is attempting to remove an intruder from a live system, it is often best first to test any changes in a test environment to understand the actual impact of such removal.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because hastily made containment steps may disrupt operations of the system. **C** is incorrect because rebooting the server may have significant impact on operations (it is not revealed whether the affected server has no counterparts or is part of a server farm). **D** is incorrect because firewall debugging is not likely to help in incident containment.

[**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q54)**.**   An organization has successfully completed training and walkthroughs of its incident response plan. What is the next best step?

**A.**   Repeat training at regular intervals.

**B.**   Conduct one or more tabletop exercises.

**C.**   Wait for an actual incident to prove the effectiveness of training and walkthroughs.

**D.**   Conduct a penetration test of production systems to measure response.

Images  **B**. After successfully completing training of incident response personnel and a walkthrough of the incident response plan, the next activity that should take place is a tabletop exercise, which is a facilitated simulation of an actual incident to help the organization better understand whether its incident response plan is effective.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because repeating training, while it may be useful, is not the next best step. **C** is incorrect because there are other preparatory activities that should take place, particularly tabletop exercises. **D** is incorrect because the main purpose of a penetration test is the identification of vulnerabilities, not a test of an organization’s incident response capabilities.

[**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q55)**.**   In a business-to-business service provider contract, which language is most reasonable for notification of a security incident?

**A.**   Notify customer within 1 hour of a breach

**B.**   Notify customer within 48 hours of a suspected breach

**C.**   Notify customer immediately after a breach

**D.**   Notify customer within 48 hours of a breach

Images  **D**. Notification of a customer within 48 hours of a breach is the most reasonable language. The term “breach” will need to be clearly defined elsewhere in the contract.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because notification within 1 hour is unreasonably fast for notification. **B** is incorrect because the term “suspected breach” is a potentially wide loophole. **C** is incorrect, as “immediately” is ambiguous and unreasonable.

[**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch5.xhtml#ch5q56)**.**   All of the following are metrics for security incident response *except* which one?

**A.**   Dwell time

**B.**   Lag time

**C.**   Containment time

**D.**   Time to notify affected parties

Images  **B**. “Lag time” is not a common term in information security metrics and is not likely to be reported.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because dwell time, or the time that elapses between the start of an incident and the organization’s awareness of the incident, is a common and meaningful metric. **C** is incorrect because containment time is a common and meaningful metric. **D** is incorrect because the time to notify affected parties is a common and meaningful metric.