

Question 1: **Skipped**

What is the main purpose of regular newsletters and intranet postings in security awareness training?

☐ **To promote the company's products and services**

☐ **To inform employees about company policies and procedures** (Correct)

☐ **To provide entertainment during work hours**

☐ **To encourage employees to take longer breaks**

Explanation

The main purpose of regular newsletters and intranet postings in security awareness training is to inform employees about company policies and procedures related to information security and to keep them updated on new threats and risks.

Question 2: **Skipped**

Which plan is activated when both the Incident Response and Business Continuity plans fail?

☐ **None of the above**

☐ **Business Continuity plan**

☐ **Incident Response plan**

☐ **Disaster Recovery plan** (Correct)

Explanation

The Disaster Recovery plan is activated when both the Incident Response and Business Continuity plans fail.

Question 3: **Skipped**

In what situations is face-to-face training most effective?

☐ **When training a small group of employees**

☐ **When employees have different schedules**

☐ **When the training material is complex and requires interaction** (Correct)

☐ **When the organization has a limited budget for training**

Explanation

Face-to-face training is most effective when the training material is complex and requires interaction, as it allows for

immediate feedback and clarification of any confusion or questions.

Question 4: **Skipped**

Who are potential members of a typical incident response team?

☐ **Engineers and system administrators**

☐ **All of the above**

☐ **First responders and medical professionals**

☐ **Legal representatives and public**

**affairs/communications
representatives** (Correct)

Explanation

potential members of a typical incident response team include representatives of senior management, information security professionals, legal representatives, and public affairs/communications representatives.

Question 5: **Skipped**

In the context of disaster recovery, what does DRP stand for?

☐ **Disaster Response Plan**

☐ **Disaster Recovery
Plan** (Correct)



Disaster Relief Plan



Disaster Reduction Plan

Explanation

DRP stands for Disaster Recovery Plan.

Question 6: **Skipped**

A company experienced an event in which an unauthorized user accessed personally identifiable information. What term best describes this event?



Disaster recovery



Breach

(Correct)



Adverse event



Business continuity

Explanation

The event described is a breach, which involves unauthorized access to sensitive information.

Question 7: **Skipped**

What is the difference between business continuity planning and disaster recovery planning?

- **Business continuity planning is about preventing disasters from occurring, while disaster recovery planning is about responding to disasters.**

- ☐ **Business continuity planning is about maintaining critical business functions, while disaster recovery planning is about restoring IT and communications back to full operations after a disruption.** (Correct)

- ☐ **Business continuity planning is about restoring IT and communications back to full operations after a disruption, while disaster recovery planning**

is about maintaining critical business functions.



Business continuity planning and disaster recovery planning are the same things.

Explanation

the difference between business continuity planning and disaster recovery planning is that the former is about maintaining critical business functions, while the latter is about restoring IT and communications back to full operations after a disruption.

Question 8: **Skipped**

A hacker launches a specific attack to exploit a known system vulnerability. What term best describes this situation?

☐ **Intrusion**

☒ **Exploit** (Correct)

☐ **Event**

☐ **Breach**

Explanation

A hacker launching a specific attack to exploit a known system vulnerability is an example of an "Exploit" as per the paragraph.

Question 9: **Skipped**

A cybersecurity professional observes an unusual occurrence in the network or system. What term best describes this situation?

☐ **Exploit**

☐ **Intrusion**

☐ **Breach**

☐ **Event** **(Correct)**

Explanation

A cybersecurity professional observing an unusual occurrence in the network or system is an example of an "Event" as per the paragraph.

Question 10: **Skipped**

Which of the following is a common attack that relies on the recipient being unaware of the risk? (★)

☐ **Phishing** (Correct)

☐ **Denial-of-service attack**

☐ **Firewall breach**

☐ **Ransomware**

Explanation

Phishing is a common attack that relies on the recipient being unaware of the risk, as it involves sending an email that appears to be from a trustworthy source but actually contains a malicious link or attachment.

Question 11: **Skipped**

A new employee is being onboarded to a company's security team. What is the first component they should learn about in the incident response plan?

☐ **Containment**

☐ **Detection and analysis**

☐ **Preparation** **(Correct)**

☐ **eradication**

Explanation

the first component of an incident response plan is preparation, which includes developing a policy approved by management, identifying critical data and systems, training staff on incident response, and implementing an incident response team.

Question 12: **Skipped**

Which component of the incident response plan involves identifying critical data and systems?

☐ **Preparation** (Correct)

☐ **eradication**

☐ **Detection and analysis**

☐ Containment

Explanation

one of the components of incident response planning is to identify critical data and systems as part of the preparation phase.

Question 13: **Skipped**

A company's web page is defaced by a hacker who leaves a message on the page. What type of event has occurred?

☐ Adverse event

☐ Exploit

☐ **Intrusion**

☐ **Security incident** (Correct)

Explanation

A security incident is an event in which an information system or the information it contains is threatened or compromised.

Question 14: **Skipped**

A large organization is planning to create a Disaster Recovery Plan. Which of the following is the BEST document to provide a high-level overview of the plan?

☐ **Executive summary** (Correct)

☐ **Full copies of the plan for critical disaster recovery team members**

☐ **Technical guides for IT personnel**

☐ **Department-specific plans**

Explanation

An executive summary provides a high-level overview of the plan and is intended for executives and other high-level stakeholders.

Question 15: **Skipped**

What is the importance of identifying roles and responsibilities in incident response planning?

☐ **To choose an appropriate containment strategy**

☐ **To ensure that everyone knows their job in the incident response process** (Correct)

☐ **To prevent incidents from happening**

☐ **To reduce the impact of the incident**

Explanation

one of the components of incident response planning is to identify roles and responsibilities to ensure that everyone knows their job in the incident response process.

Question 16: **Skipped**

An employee unintentionally shares confidential information with an unauthorized party. What term best describes this situation?

☐ **Intrusion**

☐ **Breach** **(Correct)**

☐ **Event**

☐ **Exploit**

Explanation

An employee unintentionally sharing confidential information with an unauthorized party is an example of a "Breach" as per the paragraph.

Question 17: **Skipped**

A company's IT system experienced a system crash that resulted in a loss of data. What term best describes this event?

☐ **Business continuity**

☐ **Incident** **(Correct)**

☐ **Adverse event**

☐ **Breach**

Explanation

An incident is an event that results in a loss of or damage to an organization's assets, including its information, services, and reputation.

Question 18: **Skipped**

Which of the following is a goal of security awareness training?

☐ **To educate
employees about
information**

(Correct)

security risks and policies

☐ **To encourage employees to work longer hours**

☐ **To promote employee well-being and job satisfaction**

☐ **To prevent employees from taking breaks during work hours**

Explanation

The primary goal of security awareness training is to educate employees about information security risks and policies, and

to teach them how to identify and avoid security threats.

Question 19: **Skipped**

A company's network has been infected with malware, and all its servers are down. What is the first step that the Disaster Recovery Team should take to restore the systems?

☐ **Conduct a risk assessment to determine the extent of the damage**

☐ **Contact law enforcement to investigate the cyberattack**



Disconnect the affected systems from the network (Correct)



Restore data from backup systems

Explanation

The first step that the Disaster Recovery Team should take to restore systems in the event of a malware infection is to disconnect the affected systems from the network to prevent further spread of the malware.

Question 20: **Skipped**

Which plan provides the team with immediate response procedures and checklists and guidance for management?

☒ **Incident Response plan** (Correct)

☐ **Business Continuity plan**

☐ **All of the above**

☐ **Disaster Recovery plan**

Explanation

The Incident Response plan provides the team with immediate response procedures and checklists and guidance for management.

Question 21: **Skipped**

Which of the following best describes the purpose of a business impact analysis?

- ☐ **To mitigate security violations and ensure that business operations can continue during a contingency**

☐ **To analyze an information system's requirements and functions in order to determine system contingency priorities** (Correct)

☐ **To document a predetermined set of instructions or procedures for restoring IT and communications services after a disruption**



To provide a high-level overview of the disaster recovery plan

Explanation

A business impact analysis is used to determine the potential effects of an interruption to critical business functions and to prioritize the recovery of those functions based on their criticality.

Question 22: **Skipped**

An organization develops a set of procedures to restore critical business processes after a significant disruption. What type of plan is this?



Security operations plan

☐ **Disaster recovery plan**

☐ **Business continuity plan** (Correct)

☐ **Incident response plan**

Explanation

Business continuity plans are designed to help organizations continue operating during and after a significant disruption.

Question 23: **Skipped**

Which of the following is an example of a security awareness training material? (★)

☐ **A map of the office building**

☐ **A guide to employee benefits**

☐ **A list of company products**

☐ **A training video on phishing attacks** **(Correct)**

Explanation

A training video on phishing attacks is an example of a security awareness training material as it educates employees

on how to identify and avoid phishing attacks which are a common method used by cybercriminals to steal sensitive information.

Question 24: **Skipped**

A company experiences a major IT outage and cannot perform its critical business functions. What type of plan will help the company recover from this event?

☐ **Incident response plan**

☐ **Disaster recovery plan** (Correct)

☐ **Business continuity plan**

☐ **Zero day plan**

Explanation

A disaster recovery plan is designed to help a company recover from a significant disruption to its IT infrastructure, such as a major IT outage.

Question 25: **Skipped**

An unauthorized user gains access to a company's internal network and begins to download sensitive data. What type of incident has occurred?

☐ **Adverse event**

☐ **Breach** **(Correct)**

☐ **Intrusion**

☐ **Exploit**

Explanation

A breach is an incident in which an unauthorized user gains access to sensitive information.

Question 26: **Skipped**

Which of the following is a potential target of security awareness training?

☐ **Competitors**

☐ **Vendors**

☐ **Customers**

☒ **Employees** **(Correct)**

Explanation

Employees are a potential target of security awareness training, as they play a critical role in preventing security breaches by identifying and avoiding potential security threats.

Question 27: **Skipped**

What is the primary goal of incident management?

☐ **To reduce the impact of an incident**

☐ **To resume interrupted operations as soon as possible**

☐ **To prepare for any incident** (Correct)

☐ **To protect life, health and safety**

Explanation

the primary goal of incident management is to be prepared. Preparation requires having a policy and a response plan that will lead the organization through the crisis.

Question 28: **Skipped**

Why is the recovery of IT often crucial to the recovery and sustainment of business operations?

☐ **IT is not important to business operations.**

☐ **Many businesses rely heavily on IT for their operations.** **(Correct)**

☐ **IT is often the cause of the disaster.**



**IT can be easily recovered
without any impact on
business operations.**

Explanation

the recovery of IT is often crucial to the recovery and sustainment of business operations because many businesses rely heavily on IT for their operations.

Question 29: **Skipped**

A company experiences a power outage that causes a major disruption in its operations. What type of plan will help the company restore operations? (★)



**Business
continuity plan**

(Correct)

☐ **Security operations plan**

☐ **Incident response plan**

☐ **Disaster recovery plan**

Explanation

A business continuity plan is designed to help a company continue its critical business functions during and after a significant disruption, such as a power outage.

Question 30: **Skipped**

What is the first step in incident response planning?

☐ **Identify critical data and systems**

☐ **Train staff on incident response**

☐ **Implement an incident response team**

☐ **Develop a policy approved by management** **(Correct)**

Explanation

the first step in incident response planning is to develop a policy approved by management.

Question 31: **Skipped**

What does the term "business" in business continuity planning refer to?

☐ **The technical systems of the organization**

☐ **The operational aspects of the organization** (Correct)

☐ **The physical infrastructure of the organization**



**The financial performance
of the organization**

Explanation

the term "business" in business continuity planning refers to the operational aspects of the organization.

Question 32: **Skipped**

A cybersecurity professional detects an unknown system vulnerability that can be exploited without risk of detection or prevention. What term best describes this situation?



Exploit



Breach

☐ **Event**

☐ **Zero Day** **(Correct)**

Explanation

A cybersecurity professional detecting an unknown system vulnerability that can be exploited without risk of detection or prevention is an example of a "Zero Day" as per the paragraph.

Question 33: **Skipped**

A company's security team detects a cyber attack against its information systems and activates a set of procedures to mitigate the attack. What type of plan is this?

☐ **Business continuity plan**

☐ **Disaster recovery plan**

☐ **Security operations plan**

☐ **Incident response plan** (Correct)

Explanation

An incident response plan provides guidance and procedures for detecting, responding to, and mitigating a security incident.

Question 34: **Skipped**

When is the Business Continuity plan enacted?

☐ **Either when there is a security incident or when there is a natural disaster** (Correct)

☐ **When there is a natural disaster**

☐ **When there is a loss of business operations**

☐ **When there is a security incident**

Explanation

The Business Continuity plan is enacted when there is a security incident or a natural disaster that results in a loss of business operations.

Question 35: **Skipped**

A company's primary data center goes down due to a hardware failure causing a major disruption to the IT and communications systems. What is the focus of disaster recovery planning in this scenario?

☐ **Maintaining critical business functions during the disruption**

☐ **Guiding the actions of emergency response personnel during the disruption**

☐ **Restoring IT and communications back to full operations after the disruption** (Correct)

☐ **Fixing the hardware failure**

Explanation

the focus of disaster recovery planning is on restoring IT and communications back to full operations after a disruption.

Question 36: **Skipped**

An organization experiences a security event that potentially jeopardizes the confidentiality, integrity, or availability of its information system. What term best describes this situation?

☐ **Event**

☐ **Breach**

☐ **Exploit**

☒ **Incident** **(Correct)**

Explanation

An organization experiencing a security event that potentially jeopardizes the confidentiality, integrity, or availability of its information system is an example of an "Incident" as per the paragraph.

Question 37: **Skipped**

A cybersecurity professional discovers a system vulnerability that can be exploited by a threat source. What term best describes this situation?

☒ **Vulnerability** (Correct)

☐ **Breach**

☐ **Event**

☐ **Exploit**

Explanation

A cybersecurity professional discovering a system vulnerability that can be exploited by a threat source is an example of a "Vulnerability" as per the paragraph.

Question 38: **Skipped**

How do IT professionals differentiate between typical IT problems and security incidents?

☐ **By receiving specific training on incident response** (Correct)

☐ **By participating in remediation and lessons learned stages**

☐ **By collecting evidence and reporting the incident**



By providing medical assistance at accident scenes

Explanation

IT professionals need specific training on incident response to determine the difference between a typical IT problem and a security incident.

Question 39: **Skipped**

What is the purpose of the containment, eradication, and recovery phase of incident response?



To document lessons learned and improve future incident

(Correct)

response effectiveness

☐ **To detect and analyze incidents**

☐ **To contain and eradicate incidents**

☐ **To prepare for future incidents**

Explanation

the purpose of the post-incident activity phase of incident response is to document lessons learned and improve future incident response effectiveness.

Question 40: **Skipped**

A company's mission-critical functions were disrupted due to a system outage. What plan should the organization have in place to sustain these operations during and after a significant disruption?

☐ **Intrusion detection plan**

☐ **Disaster recovery plan**

☐ **Incident response plan**

☐ **Business continuity plan** **(Correct)**

Explanation

The organization should have a Business Continuity plan in place to sustain mission-critical functions during and after a significant disruption.

Question 41: **Skipped**

Which of the following is an effective way to provide security awareness training to a large number of people?

☐ **Posting security posters in the break room**

☒ **Online training** (Correct)

☐ **Sending emails to employees**



Face-to-face training

Explanation

Online training is an effective way to provide security awareness training to a large number of people, as it can be accessed from anywhere at any time and allows employees to complete training at their own pace.

Question 42: **Skipped**

Who should participate in creating a business continuity plan (BCP)? (★)



**Only members from the
management team**

☐ **Only members from the
finance department**

☐ **Only members from the IT
department**

☐ **Members from
across the organization** **(Correct)**

Explanation

members from across the organization should participate in creating the BCP to ensure all systems, processes, and operations are accounted for in the plan.

Question 43: **Skipped**

A company's data center experiences a fire causing extensive damage to the IT and communications systems. What is the goal of disaster recovery planning in this scenario?

☐ To prevent the fire from occurring again

☐ To guide the actions of emergency response personnel during the disruption

☐ To restore IT and communications back to full operations after the disruption **(Correct)**



To maintain critical business functions during the disruption

Explanation

the goal of disaster recovery planning is to restore IT and communications back to full operations after a disruption.

Question 44: **Skipped**

What is the priority of incident response in the context of incident management?



Reduce the impact of the incident



**Protect life, health
and safety**

(Correct)



**Protect the organization's
mission and objectives**



**Resume interrupted
operations as soon as
possible**

Explanation

the priority of any incident response is to protect life, health and safety.

Question 45: **Skipped**

What term is used to describe the process of incident management in some organizations?

☐ **Business continuity management**

☐ **Event management**

☐ **Incident response planning**

☐ **Crisis management** **(Correct)**

Explanation

some organizations use the term "crisis management" to describe the process of incident management.

Question 46: **Skipped**

An organization experiences a security event that does not affect the confidentiality, integrity, or availability of its information system. What term best describes this situation?



Event

(Correct)



Exploit



Incident



Breach

Explanation

An organization experiencing a security event that does not affect the confidentiality, integrity, or availability of its information system is an example of an "Event" as per the paragraph.

Question 47: **Skipped**

A company's security team monitors, detects, and analyzes events on the network to prevent and resolve issues before they result in business disruptions. What is this team called?



Incident response team



Business continuity team



SOC team

(Correct)



Disaster recovery team

Explanation

The team described in the question is most likely called a Security Operations Center (SOC), which is responsible for monitoring, detecting, and responding to security incidents on a company's network. While the other teams listed may also be involved in addressing security issues, they have more specific focuses.

Question 48: **Skipped**

A previously unknown vulnerability is discovered in a software program that could allow a hacker to gain access to sensitive data. What is this called?



Zero day

(Correct)

☐ **Business continuity**

☐ **Disaster recovery**

☐ **Security incident**

Explanation

A zero day vulnerability is a previously unknown vulnerability that could be exploited by a hacker before a patch or fix is available.

Question 49: **Skipped**

A company performs an analysis of its information system's requirements functions and interdependencies in order to prioritize contingency requirements. What is this process called?

☐ **Business continuity plan**

☐ **Incident response plan**

☐ **Disaster recovery plan**

☐ **Business impact analysis** (Correct)

Explanation

Business impact analysis is a process used to identify the impact of a disruption on an organization's operations and prioritize contingency plans.

Question 50: **Skipped**

What is the purpose of immediate response procedures and checklists in a business continuity plan?

☐ **To safeguard the confidentiality, integrity, and availability of information**

☐ **To ensure business operations are accounted for in the plan**

☐ **To provide guidance for management**



**To notify
personnel that
the BCP is being
enacted**

(Correct)

Explanation

immediate response procedures and checklists are included in the BCP to alert personnel that the plan is being enacted.

Question 51: **Skipped**

What are the primary responsibilities of a computer incident response team (CIRT) during an incident?

☐ **To assess the amount and scope of damage caused by the incident** (Correct)

☐ **To troubleshoot network and system issues**

☐ **To provide medical assistance at accident scenes**

☐ **To determine the difference between minor and major injuries**

Explanation

the primary responsibilities of a CIRT during an incident are to determine the amount and scope of damage caused by the incident, determine whether any confidential information was compromised, implement necessary recovery procedures, and supervise implementation of additional security measures.

Question 52: **Skipped**

What is the definition of an intrusion in the context of cybersecurity?

☐ **A particular attack that exploits system vulnerabilities**

☐ **A weakness in system security procedures or internal controls**

☐ **An observable occurrence
in a network or system**

☐ **A deliberate
security incident
in which an
intruder gains
access to a
system or system
resource without
authorization**

(Correct)

Explanation

an "Intrusion" is defined as a security event or combination of events that constitutes a deliberate security incident in which an intruder gains or attempts to gain access to a system or system resource without authorization.

Question 53: **Skipped**

A hacker gains access to a company's email server and sends out malicious emails from a legitimate email address, What type of incident has occurred?

☐ **Zero day exploit**

☐ **Data breach**

☐ **Security event** **(Correct)**

☐ **Adverse event**

Explanation

A security event refers to any occurrence that could potentially compromise the confidentiality, integrity, or availability of an organization's information assets. In this case, the hacker has gained unauthorized access to the email server and is using it to send out malicious emails, which is a security event.

Question 54: **Skipped**

What is the definition of an exploit in the context of IT security?

☐ **The documentation of a predetermined set of instructions or procedures for detecting, responding to, and limiting the consequences of a malicious cyberattack**

☐ **A security event in which an intruder gains**

**unauthorized access to a
system or resource**

- ☐ **A particular type of attack that exploits system vulnerabilities** (Correct)

- ☐ **The activities necessary to restore IT and communications services to an organization during and after an outage, disruption, or disturbance of any kind or scale**

Explanation

An exploit is a type of attack that takes advantage of a weakness in an information system or system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Question 55: **Skipped**

What does the term "zero day" refer to in the context of cybersecurity? (★)

☐ **A deliberate security incident**

☐ **A previously unknown system vulnerability** (Correct)

☐ **A weakness in system security procedures or internal controls**

☐ **An observable occurrence in a network or system**

Explanation

"Zero Day" refers to a previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures, or methods.

Question 56: **Skipped**

What does a breach refer to in the context of cybersecurity?

☐ **Any observable occurrence
in a network or system**

☐ **A previously unknown
system vulnerability**

☐ **An unauthorized
access to a
system or system
resource** (Correct)

☐ **A deliberate security
incident**

Explanation

a "Breach" refers to the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information.

Question 57: **Skipped**

A hacker gains access to an organization's system without authorization and steals confidential data. What term best describes this situation?

☐ **Breach**

☐ **Intrusion** **(Correct)**

☐ **Exploit**

☐ **Event**

Explanation

A hacker gaining access to an organization's system without authorization is an example of an "Intrusion" as per the paragraph.

Question 58: **Skipped**

A company's network experiences a sudden flood of network packets that causes a major slowdown in internet traffic. What type of event is this?

☐ **Business impact analysis**

☐ **Natural disaster**



Adverse event



Security incident (Correct)

Explanation

A security incident is any event that could potentially compromise the confidentiality, integrity, or availability of an organization's information assets. In this case, the sudden flood of network packets is likely caused by a distributed denial-of-service (DDoS) attack, which is a common type of cyber attack aimed at disrupting internet traffic and making online services unavailable.

Question 59: **Skipped**

A company's data center has been breached by hackers, and all its systems have been taken down. What is the main objective of the Disaster Recovery Plan (DRP) in such a scenario?

☐ **To relocate the data center to another location**

☐ **To restore the IT systems to their last known state** (Correct)

☐ **To ensure the physical safety of employees in the data center**

☐ **To investigate and prosecute the hackers responsible for the attack**

Explanation

The main objective of the Disaster Recovery Plan (DRP) in a scenario where a company's data center has been breached by hackers and all its systems have been taken down is to restore the IT systems to their last known state.

Question 60: **Skipped**

What is an incident in the context of cybersecurity?

☐ **An event that actually or potentially jeopardizes the confidentiality integrity or availability of an information system or the information the system processes stores or transmits.** (Correct)

☐ **A deliberate security incident in which an intruder gains access to a system or system resource without authorization**

☐ **A particular attack that exploits system vulnerabilities**

☐ **Any observable occurrence in a network or system**

Explanation

an "Incident" is defined as an event that actually or potentially jeopardizes the confidentiality integrity or availability of an information system or the information the system processes stores or transmits.