Cisco Cybersecurity Essentials

Started on	Thursday, 16 November 2023, 9:51 PM
State	Finished
Completed on	Thursday, 16 November 2023, 10:08 PM
Time taken	16 mins 42 secs
Marks	38.00/38.00
Grade	**100.00** out of 100.00

Question **1**

Correct

Mark 2.00 out of 2.00

A breach occurs in a company that processes credit card information. Which industry specific law governs credit card data protection?

Select one:

- PCI DSS ✔
- SOX
- GLBA
- ECPA

Refer to curriculum topic: 8.2.2
The Payment Card Industry Data Security Standard (PCI DSS) governs how to protect credit card data as merchants and banks exchange transactions.

The correct answer is: PCI DSS

Question **2**

Correct

Mark 2.00 out of 2.00

A company has had several incidents involving users downloading unauthorized software, using unauthorized websites, and using personal USB devices. The CIO wants to put in place a scheme to manage the user threats. What three things might be put in place to manage the threats? (Choose three.)

Select one or more:

- Implement disciplinary action.
- Monitor all activity by the users.
- ✓ Use content filtering. ✔
- ✓ Disable CD and USB access. ✔
- ✓ Provide security awareness training. ✔
- Change to thin clients.

Refer to curriculum topic: 8.1.1
Users may be unaware of their actions if not educated in the reasons why their actions can cause a problem with the computer. By implementing several technical and nontechnical practices, the threat can be reduced.

The correct answers are: Disable CD and USB access., Use content filtering., Provide security awareness training.

Question **3**

Correct

Mark 2.00 out of 2.00

What are three disclosure exemptions that pertain to the FOIA? (Choose three.)

Select one or more:

- public information from financial institutions
- ✓ law enforcement records that implicate one of a set of enumerated concerns ✔
- ✓ national security and foreign policy information ✔
- information specifically non-exempt by statue
- non-geological information regarding wells
- ✓ confidential business information ✔

Refer to curriculum topic: 8.2.2
The nine Freedom of Information Act (FOIA) exemptions include the following:

1. National security and foreign policy information
2. Internal personnel rules and practices of an agency
3. Information specifically exempted by statute
4. Confidential business information
5. Inter- or intra-agency communication subject to deliberative process, litigation, and other privileges
6. Information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy
7. Law enforcement records that implicate one of a set of enumerated concerns
8. Agency information from financial institutions
9. Geological and geophysical information concerning wells

The correct answers are: national security and foreign policy information, confidential business information, law enforcement records that implicate one of a set of enumerated concerns

Question **4**

Correct

Mark 2.00 out of 2.00

As a security professional, there is a possibility to have access to sensitive data and assets. What is one item a security professional should understand in order to make informed ethical decisions?

Select one:

- cloud providers
- laws governing the data ✔
- potential bonus
- partnerships
- potential gain

Refer to curriculum topic: 8.2.1
Ethics in the security profession are extremely important because of the sensitivity of the data and assets. Compliance to government and state requirements is needed in order to make good judgments.

The correct answer is: laws governing the data

Question **5**

Correct

Mark 2.00 out of 2.00

A consultant is hired to make recommendations on managing device threats in a company. What are three general recommendations that can be made? (Choose three.)

Select one or more:

- Disable administrative rights for users. ✔
- Enable screen lockout. ✔
- Remove content filtering.
- Enable media devices.
- Enable automated antivirus scans. ✔
- Enforce strict HR policies.

Refer to curriculum topic: 8.1.2
Workstations can be hardened by removing unnecessary permissions, automating processes, and turning on security features.

The correct answers are: Disable administrative rights for users., Enable screen lockout., Enable automated antivirus scans.

Question **6**

Correct

Mark 2.00 out of 2.00

If a person knowingly accesses a government computer without permission, what federal act laws would the person be subject to?

Select one:

- CFAA ✔
- GLBA
- SOX
- ECPA

Refer to curriculum topic: 8.2.2
The Computer Fraud and Abuse Act (CFAA) provides the foundation for US laws criminalizing unauthorized access to computer systems.

The correct answer is: CFAA

Question **7**

Correct

Mark 2.00 out of 2.00

An auditor is asked to assess the LAN of a company for potential threats. What are three potential threats the auditor may point out? (Choose three.)

Select one or more:

- the acceptable use policy
- a misconfigured firewall ✔
- complex passwords
- locked systems
- unlocked access to network equipment ✔
- unauthorized port scanning and network probing ✔

Refer to curriculum topic: 8.1.3
The LAN can have many endpoint devices connected. Analyzing both the network devices and the endpoints connected is important in determining threats.

The correct answers are: unlocked access to network equipment, unauthorized port scanning and network probing, a misconfigured firewall

Question **8**

Correct

Mark 2.00 out of 2.00

As part of HR policy in a company, an individual may opt-out of having information shared with any third party other than the employer. Which law protects the privacy of personal shared information?

Select one:

- SOX
- PCI
- GLBA ✔
- FIRPA

Refer to curriculum topic: 8.2.2
The Gramm-Leach-Bliley Act (GLBA) includes privacy provisions for individuals and provides opt-out methods to restrict information sharing with third-party firms.

The correct answer is: GLBA

Question **9**

Correct

Mark 2.00 out of 2.00

An organization has implemented a private cloud infrastructure. The security administrator is asked to secure the infrastructure from potential threats. What three tactics can be implemented to protect the private cloud? (Choose three.)

Select one or more:

- Disable firewalls.
- ✓ Update devices with security fixes and patches. ✔
- Grant administrative rights.
- ✓ Disable ping, probing, and port scanning. ✔
- Hire a consultant.
- ✓ Test inbound and outbound traffic. ✔

Refer to curriculum topic: 8.1.4
Organizations can manage threats to the private cloud using the following methods:

- Disable ping, probing, and port scanning.
- Implement intrusion detection and prevention systems.
- Monitor inbound IP traffic anomalies.
- Update devices with security fixes and patches.
- Conduct penetration tests post configuration.
- Test inbound and outbound traffic.
- Implement a data classification standard.
- Implement file transfer monitoring and scanning for unknown file type.

The correct answers are: Disable ping, probing, and port scanning., Test inbound and outbound traffic., Update devices with security fixes and patches.

Question **10**

Correct

Mark 2.00 out of 2.00

A company is attempting to lower the cost in deploying commercial software and is considering a cloud based service. Which cloud based service would be best to host the software?

Select one:

- RaaS
- SaaS ✔
- IaaS
- PaaS

Refer to curriculum topic: 8.1.5
Software as a service (SaaS) provides access to software that is centrally hosted and accessed by users via a web browser on the cloud.

The correct answer is: SaaS

Question **11**

Correct

Mark 2.00 out of 2.00

Why is Kali Linux a popular choice in testing the network security of an organization?

Select one:

- It is an open source Linux security distribution and contains over 300 tools. ✔
- It can be used to intercept and log network traffic.
- It can be used to test weaknesses by using only malicious software.
- It is a network scanning tool that prioritizes security risks.

Refer to curriculum topic: 8.2.4
Kali is an open source Linux security distribution that is commonly used by IT professionals to test the security of networks.

The correct answer is: It is an open source Linux security distribution and contains over 300 tools.

Question **12**

Correct

Mark 2.00 out of 2.00

What are the three broad categories for information security positions? (Choose three.)

Select one or more:

- seekers
- ✓ definers ✔
- doers
- ✓ builders ✔
- creators
- ✓ monitors ✔

Refer to curriculum topic: 8.3.1
Information security positions can be categorized as::

- definers
- builders
- monitors

The correct answers are: definers, builders, monitors

Question **13**

Correct

Mark 2.00 out of 2.00

A school administrator is concerned with the disclosure of student information due to a breach. Under which act is student information protected?

Select one:

- HIPPA
- FERPA ✔
- CIPA
- COPPA

Refer to curriculum topic: 8.2.2
The Family Education Records and Privacy Act (FERPA) prohibits the improper disclosure of personal education records.

The correct answer is: FERPA

Question **14**

Correct

Mark 2.00 out of 2.00

A security professional is asked to perform an analysis of the current state of a company network. What tool would the security professional use to scan the network only for security risks?

Select one:

- vulnerability scanner ✔
- pentest
- packet analyzer
- malware

Refer to curriculum topic: 8.2.4
Vulnerability scanners are commonly used to scan for the following vulnerabilities:

- Use of default passwords or common passwords
- Missing patches
- Open ports
- Misconfiguration of operating systems and software
- Active IP addresses

The correct answer is: vulnerability scanner

Question **15**

Correct

Mark 2.00 out of 2.00

What are two potential threats to applications? (Choose two.)

Select one or more:

- unauthorized access ✔
- data loss ✔
- power interruptions
- social engineering

Refer to curriculum topic: 8.1.7
Threats to applications can include the following:

- Unauthorized access to data centers, computer rooms, and wiring closets
- Server downtime for maintenance purposes
- Network operating system software vulnerability
- Unauthorized access to systems
- Data loss
- Downtime of IT systems for an extended period
- Client/server or web application development vulnerabilities

The correct answers are: data loss, unauthorized access

Question **16**

Correct

Mark 2.00 out of 2.00

What three services does CERT provide? (Choose three.)

Select one or more:

- develop tools, products, and methods to analyze vulnerabilities ✔
- develop tools, products, and methods to conduct forensic examinations ✔
- develop attack tools
- create malware tools
- enforce software standards
- resolve software vulnerabilities ✔

Refer to curriculum topic: 8.2.3
CERT provides multiple services, including:

- helps to resolve software vulnerabilities
- develops tools, products, and methods to conduct forensic examinations
- develops tools, products, and methods to analyze vulnerabilities
- develops tools, products, and methods to monitor large networks
- helps organizations determine how effective their security-related practices are

The correct answers are: resolve software vulnerabilities, develop tools, products, and methods to analyze vulnerabilities, develop tools, products, and methods to conduct forensic examinations

Question **17**

Correct

Mark 2.00 out of 2.00

What can be used to rate threats by an impact score to emphasize important vulnerabilities?

Select one:

- ACSC
- ISC
- NVD ✔
- CERT

Refer to curriculum topic: 8.2.3
The National Vulnerability Database (NVD) is used to assess the impact of vulnerabilities and can assist an organization in ranking the severity of vulnerabilities found within a network.

The correct answer is: NVD

Question **18**

Correct

Mark 2.00 out of 2.00

Unauthorized visitors have entered a company office and are walking around the building. What two measures can be implemented to prevent unauthorized visitor access to the building? (Choose two.)

Select one or more:

- Lock cabinets.
- Prohibit exiting the building during working hours.
- Establish policies and procedures for guests visiting the building. ✔
- Conduct security awareness training regularly. ✔

Refer to curriculum topic: 8.1.6
Any unauthorized individual that accesses a facility may pose a potential threat. Common measures to increase physical security include the following:

- Implement access control and closed-circuit TV (CCTV) coverage at all entrances.
- Establish policies and procedures for guests visiting the facility.
- Test building security using physical means to covertly gain access.
- Implement badge encryption for entry access.
- Conduct security awareness training regularly.
- Implement an asset tagging system.

The correct answers are: Establish policies and procedures for guests visiting the building., Conduct security awareness training regularly.

Question **19**

Correct

Mark 2.00 out of 2.00

What are two items that can be found on the Internet Storm Center website? (Choose two.)

Select one or more:

- InfoSec job postings ✔
- current laws
- InfoSec reports ✔
- historical information

Refer to curriculum topic: 8.2.3
The Internet Storm Center website has a daily InfoSec blog, InfoSec tools, and news among other InfoSec information.

The correct answers are: InfoSec reports, InfoSec job postings

◀ Launch Chapter 8

Jump to...

Final Quiz ▶