Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/28/2022 9:11:21 am • Time spent: 02:21

Score: 70%

Passing Score: 80%

Question 1: ✔ Correct

Your organization has discovered that an overseas company has reverse-engineered and copied your main product and is now selling a counterfeit version.

Which of the following BEST describes the type of consequence your organization has suffered?

- Fines
- Escalation
- IP theft
- Reputation damage

EXPLANATION

Intellectual property (IP) is the lifeblood of companies. When their IP is stolen, they lose competitive advantage. The internet has made the world smaller, and companies are now competing with others from around the globe. When IP is stolen through a data breach, it is often sold to competing companies. Many of the companies are overseas and not subject to laws in the United States, making them difficult to prosecute. This allows reverse-engineering or direct copying of IP and gives thieves an undeserved revenue source. This also floods the market with counterfeit goods.

A company's reputation determines if people invest, if consumers buy a product or service, or if foreign governments even allow a certain company to do business in their jurisdiction. This scenario does not describe this.

Fines can be levied against an organization as a result of a data breach. This scenario does not describe this.

Escalation can be separated into two categories, which are internal escalation and external escalation. Internal escalation is part of a company's incident-response plan. External escalation is when experts need to be brought in from the outside to investigate, provide legal counsel, or even enforce laws.

REFERENCES

14.3.2 Consequences of Breaches Facts

q_breaches_iptheft_secp7.question.fex

Question 2: ✔ Correct

Your organization has suffered a data breach, and it was made public. As a result, stock prices have fallen, as consumers no longer trust the organization.

Which of the following BEST describes the type of consequence your organization has suffered due to the breach?

- Notifications
- IP theft
- Identity theft
- Reputation damage

EXPLANATION

This scenario best describes an organization's reputation damage from a data breach. A company's reputation determines if people invest, if consumers buy a product or service, or if foreign governments even allow a certain company to do business in their jurisdiction. A company lives or dies by its revenues and investments, so a breach that exposes client data directly affects the way consumers and investors spend their money. A data breach can cause stock prices to fall, and falling stock prices lead to selloffs and permanent damage.

Notifications are usually sent out following a data breach. This scenario does not describe this.

Intellectual property (IP) is the lifeblood of companies. When their IP is stolen, they lose competitive advantage. This scenario does not describe this.

Identity theft is when a breach occurs and personal information is stolen. The affected individual or entity is forced to do hours of work to correct someone else's mistake.

REFERENCES

14.3.2 Consequences of Breaches Facts

q_breaches_reputation_secp7.question.fex

Question 3: ✔ Correct

If you lose your wallet or purse and it ends up in the wrong hands, several pieces of information could be used to do personal harm to you. These pieces of information include the following:

- Name and address
- Driver license number
- Credit card numbers
- Date of birth

Which of the following classifications does this information fall into?

- Private internal information
- ➡ Personally identifiable information (PII)
- Private restricted information
- Proprietary information

EXPLANATION

Personally identifiable information (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person. This information includes:

- Full name (if not common)
- Home address
- Email address (if private from an association/club membership, etc.)
- National identification number
- Passport number
- IP address (when linked, but it is not PII by itself in US)
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Telephone number
- Login name, screen name, nickname, or handle

Proprietary information is information that a company wishes to keep confidential. Private internal information is restricted to individuals within the organization and can include personnel records, financial records, and customer lists. Private restricted information is restricted to limited authorized personnel within the organization and can include trade secrets, strategic information, and highly sensitive information.

REFERENCES

14.3.4 Information Classification Facts

q_info_class_pii_secp7.question.fex

Question 4: ✕ Incorrect

The government and military use the following information classification system:

- Unclassified
- Sensitive But Unclassified
- Confidential
- Secret
- Top Secret

Drag each classification on the left to the appropriate description on the right.

The lowest level of classified information used by the military. Release of this information could cause damage to military efforts.

✓ Confidential

If this information is released, it poses grave consequences to national security.

✓ Top Secret

This information can be accessed by the public and poses no security threat.

~~Sensitive But Unclassified~~ Unclassified

If this information is disclosed, it could cause some harm, but not a national disaster.

~~Unclassified~~ Sensitive But Unclassified

If this information is disclosed, it could cause severe and permanent damage to military actions.

✓ Secret

EXPLANATION

The government and military use the following information classification system:

- Unclassified: information that can be accessed by the public and poses no security threat.
- Sensitive But Unclassified: information that, if disclosed, could cause some harm but not a national disaster.
- Confidential: information that is the lowest level of classified information used by the military. It allows restriction of release under the Freedom of Information Act. Release of this information could cause damage to military efforts.
- Secret: information that, if disclosed, could cause severe and permanent damage to military actions.
- Top Secret: information that is the highest level of classified information used by the military. If Top Secret information is released, it poses a grave threat to national security.

REFERENCES

14.3.4 Information Classification Facts

q_info_class_types_secp7.question.fex

Question 5: ✔ Correct

Which of the following laws was designed to protect a child's information on the internet?

- GDPR
- COPPA
- CCPA
- GLBA

EXPLANATION

The Children's Online Privacy Protection Act of 1998 (COPPA) requires organizations that provide online services designed for kids below the age of 13 (such as websites and gaming sites) to obtain parental consent prior to collecting a child's personal information and using it. This includes such actions as displaying the information on the website, selling it to a marketing company, and so on.

The General Data Protection Regulation (GDPR) is a data-compliance regulation that started in 2018. GDPR provides sweeping changes to the way customer data is treated in the European Union.

The California Consumer Privacy Act (CCPA) was passed in 2020 and was one of the first data privacy acts in the United States.

The Gramm-Leach-Bliley Act (GLBA) is designed to protect private data held at financial institutions.

REFERENCES

14.3.6 Privacy and Responsibility of Data

q_priv_data_resp_coppa_secp7.question.fex

Question 6: ✔ Correct

Which of the following government acts protects medical records and personal health information?

- ACA
- HIPAA
- FACTA
- FISMA

EXPLANATION

In the US, you must follow laws dictated by three government acts:

- HIPAA stands for Health Insurance Portability and Accountability Act. HIPAA protects medical records and personal health information. Companies that provide healthcare insurance handle HIPAA-protected information. And, of course, companies that provide health-related services also handle HIPAA-protected information.
- FACTA (Fair and Accurate Credit Transactions Act) was created to protect against identity theft. The act applies to the disposal of consumer reports and related information. FACTA includes credit reports, credit scores, employment history information, check writing history, insurance claims, residential or tenant history, and medical history. Every business handles FACTA-protected information, and every business must comply with FACTA laws.
- FISMA (Federal Information Security Management Act) protects government information. It is primarily concerned with proper data destruction and has detailed disposal requirements.
- ACA is the Affordable Care Act, often referred to as Obamacare.

REFERENCES

14.3.6 Privacy and Responsibility of Data

q_priv_data_resp_hipaa_01_secp7.question.fex

Question 7: ✔ Correct

HIPAA is a set of federal regulations that define security guidelines. What do HIPAA guidelines protect?

- Non-repudiation
- Privacy
- Integrity
- Availability

EXPLANATION

HIPAA is a set of federal regulations that enforce the protection of privacy. Specifically, HIPAA protects the privacy of medical records.

REFERENCES

14.3.6 Privacy and Responsibility of Data

q_priv_data_resp_hipaa_02_secp7.question.fex

Question 8: ✕ Incorrect

Which of the following is the LEAST reliable means of cleaning or purging media?

- OS low-level formatting
- ~~Drive controller hardware-level formatting~~
- Overwriting every sector with alternating 1s and 0s
- Degaussing

EXPLANATION

The least reliable means to clean or purge media is degaussing. Degaussing is the use of strong magnetic fields to remove stored information from a drive. Unfortunately, user error and equipment failure often results in only partially cleaned media.

Various forms of formatting (such as OS low-level formatting and drive controller hardware-level formatting) are not perfect, but they are often more reliable than degaussing. Overwriting every sector with alternating 1s and 0s can be effective if performed multiple times (such as 60 or more).

REFERENCES

14.3.8 Data Destruction Facts

q_data_destroy_facts_degaus_secp7.question.fex

Question 9: ✕ Incorrect

When you dispose of a computer or sell used hardware, it is crucial that none of the data on the hard disks can be recovered.

Which of the following actions can you take to ensure that no data is recoverable?

- Delete all files from all the hard disks in the computer.
- Encrypt all data on the hard disks.
- ~~Reformat all the hard disks in the computer.~~
- Damage the hard disks so badly that all data remanence is gone.

EXPLANATION

When you dispose of a computer, sell used hardware, or erase important information, it's crucial to destroy all of the data on a device. It's not enough to delete the data. Reformatting the hard drive is also not sufficient. If other people can access the computer, they can use data remanence (the residual representation of erased data) to recover information. You must damage the hardware so badly that the remanence is gone.

REFERENCES

14.3.8 Data Destruction Facts

q_data_destroy_facts_pulv_01_secp7.question.fex

Question 10: ✔ Correct

Which of the following data destruction techniques uses a punch press or hammer system to crush a hard disk?

- Purging
- Pulping
- Pulverizing
- Degaussing
- Shredding

EXPLANATION

The following are various ways to destroy data:

- Burning: the method of building a small fire somewhere legal and safe. Use metal tongs to burn your documents one by one or a few at a time. It's important to ensure that each document is turned into ash. If sensitive information escapes the flames and flies away, it might fall into the wrong hands.
- Shredding: running a hard disk through a disk shredder, physically destroying the drive.
- Pulping: a way of removing all traces of ink from paper by using chemicals and then mashing the paper into pulp. Since these chemicals can ruin carpet and clothing, you should perform this process outside and use protective gloves.
- Pulverizing: like shredding except that it uses a punch press or hammer system to crush a hard disk into a pile of metal confetti.
- Degaussing: purges the hard disk by exposing it to a high magnetic pulse that destroys all of the data on the disk. This also ruins the motors inside the drive.
- Purging: the removal of sensitive data, ensuring that it cannot be reconstructed by any known technique.
- Wiping: a software-based method of overwriting data to completely destroy all electronic data residing on a hard disk drive or other digital media. Wiping uses 0s and 1s to overwrite data onto all sectors of the device. The data is rendered unrecoverable and achieves data sanitization.

REFERENCES

14.3.8 Data Destruction Facts

q_data_destroy_facts_pulv_02_secp7.question.fex