Exam Report: 9.1.6 Practice Questions

Date: 1/28/2020 9:51:41 am
Time Spent: 9:42

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

When you dispose of a computer or sell used hardware and 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?

○ Reformat all the hard disks in the computer.

○ Encrypt all the data on the hard disks.

➡ ● Damage the hard disks so badly that all data remanence is gone.

○ Delete all files from all the hard disks in the computer.

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 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

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_04]

Question 2: Incorrect

The government and military use the following information classification system:

- Unclassified
- Sensitive but unclassified
- Confidential
- Secret
- Top secret

Drag the 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.

~~Secret~~ Top secret

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

✓ Unclassified

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

✓ Sensitive but unclassified

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

~~Top secret~~ 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 of information 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

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_02]

Question 3: Incorrect

Many organizations use the Information Security Classification Framework, which uses the following classifications:

- High
- Medium
- Low

Drag the sensitivity classification on the left to the appropriate description on the right. (Classifications may be used once, more than once, or not at all.)

Could cause personal hardship or embarrassment.

✓ Medium

Could cause personal embarrassment or inconvenience.

✓ Low

Could cause loss of life or social hardship.

✓ High

Could cause operational harm such as loss of control or loss of public trust.

~~Medium~~ High

Could cause operational harm such as loss of confidence or damage to reputation.

~~Low~~ Medium

Explanation

Many organizations use the Information Security Classification Framework, which has the following sensitivity classifications:

- **High**: could cause extremely serious personal or organizational injury, including:
  - Extreme financial loss
  - Extreme operational harm, such as loss of control or loss of public trust
  - Extreme personal harm, such as loss of life or social hardship
- **Medium**: could cause serious personal or organizational injury, including:

- Significant financial loss
- Significant operational harm, such as loss of confidence or damage to reputation
- Significant personal harm, such as personal hardship or embarrassment

- **Low**: could cause limited or no injury to individuals or the organization, including:
  - Limited financial loss
  - Limited operational harm, such as reduced organizational effectiveness or loss of morale
  - Limited personal harm, such as embarrassment or inconvenience

References

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_01]

▼ Question 4: Correct

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

○ ACA

○ FISMA

○ FACTA

➡ ● HIPAA

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**, the Fair and Accurate Credit Transactions Act, was created to protect against identity theft. It 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**, the 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

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_06]

▼ Question 5: Correct

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

○ Degaussing

➡ ● Pulverizing

○ Pulping

○ Purging

○ 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

- **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**: this technique is 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. It also ruins the motors inside the drive.
- **Purging**: the removal of sensitive data, ensuring that the data cannot be reconstructed by any known technique.
- **Wiping**: is 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 zeros and ones to overwrite data onto all sectors of the device. The data is rendered unrecoverable and achieves data sanitization.

References

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_05]

▼ **Question 6:** Incorrect

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?

○ Proprietary information

● ~~Private internal information~~

➡ ○ Personally identifiable information

○ Private restricted 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, or to identify an individual in context. This includes:

- Full name (if not common)
- Home address
- Email address (if private from an association/club membership, et cetera)
- 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

LabSim for Security Pro, Section 9.1
[All Questions SecPro2017_v6.exm DATA_MAN_03]