Contents

Topic 1: Scenario

Scenario: Southern TelcoSol's DEA Encounter

Digital Evidence Controls and Crime Processing
CSEC650—Module 3

Southern TelcoSol's DEA Encounter
Timothy Sullivan, Chief Information Officer (CIO) of Southern TelcoSol, is engrossed in his work one afternoon when he receives a phone call from Drug Enforcement Administration (DEA) Special Agent Jennifer O'Hare. The phone call catches him off guard; Timothy is not aware of any dealings with the DEA, although some people in his information security team are members of the local chapter of InfraGard. The agent requests a meeting with Timothy in relation to an ongoing investigation into drug dealing. Timothy immediately has a hunch about what the DEA agent is referring to. However, all he says is that he will consult his colleagues and schedule the meeting shortly.

Scenario
Timothy, Southern TelcoSol's CIO, has been contacted by a DEA agent about an investigation into drug dealing. Timothy believes that the agent may be investigating Alana Blank, vice president of marketing at Southern TelcoSol.

Alana is suspected of communicating with a local drug dealer. Immediately after he receives the call from the DEA agent, Timothy calls his company's Chief Information Security Officer (CISO), Nelson Gomez, and Chief Executive Officer (CEO), Brad Timberlake, for an urgent meeting.

Here is a transcript of the conversation among Timothy, Nelson, and Brad.

Timothy: It seems we had valid suspicions about Alana Blank after all. I just got a call from the DEA requesting a meeting to discuss an ongoing drug-dealing investigation.

Brad: Did you mention Alana to her?

Timothy: No, I haven't brought that up yet. I wanted to discuss the matter with you first. Nelson, how much information do we have on this so far?

Nelson: We believe that Alana has been communicating with the leader of a local cocaine ring via e-mail and through an instant messaging feature on the professional networking site Plugg-In.

Brad: You discovered this last week, right?

Nelson: Yes, we discovered it last week during our internal IT audit. We were monitoring network traffic from external sites to detect malware when I noticed that Alana was communicating with Taylor Anthony.

Nelson: Taylor Anthony was recently in the news for his alleged involvement in international drug trafficking. This is a serious matter, and we need to decide how to handle it.

Brad: Let's take a call on it right now. We could allow Nelson to help the DEA agent gather any digital evidence she might need.

Brad: Alternatively, we could take a more passive approach by providing the DEA with supervised access to any computer systems that they request.

Timothy: Some organizations decide not to actively support investigations unless they're legally bound to do so under a search warrant or affidavit.

Analysis

Analyzing the Choices

Consider the scenario and the three distinct approaches that Southern TelcoSol can adopt to handle the investigation of Alana. Which approach do you think would be the most appropriate? In your opinion, are any of these approaches right or wrong?

Complete Cooperation

As Brad says in the scenario, Southern TelcoSol could have its CISO help the DEA gather any digital evidence required. By proactively helping law enforcement in an investigation, the organization would be acting as a good corporate citizen.

Supervised Access

Brad’s second option involves providing the DEA with supervised access to computer systems, and does not entail complete proactive cooperation. However, this approach still helps law enforcement to the extent that help is requested.

Minimal Cooperation

By offering minimal cooperation, an organization supports investigations only to the extent mandated by law. Most organizations take the approach of requesting the involvement of law enforcement only if they believe that the case involves a serious criminal matter, has an international dimension to it, or is related to cyberterrorism.

Topic 2: Module Introduction

When investigating computer crime, the digital trail of evidence involves complex technologies. A digital trail of evidence is harder to trace than a traditional one. Computer forensic investigators find it helpful to think like criminals. Adopting this mindset helps in the identification of relevant computer evidence.

There is a diverse range of computer crimes today, and computer criminals are normally ahead of the forensic technology curve. This module provides an overview of the various types of computer crime. It then discusses the relevance of computer evidence. The module explores the final steps in the chain-of-custody process—controlling digital evidence after it is acquired. Finally, the module examines differing approaches to sharing evidence with government agencies, including law enforcement.

Topic 3: Types of Computer Crime

Crimes Against Individuals

Computer Crimes

Computer crimes can be committed against individuals, as well as against private- and public-sector organizations.

Computer crimes commonly committed against individuals include:

- Cyberstalking
- Harassment
- Cyberbullying
- Identity theft
- Phishing
- Theft of personal information
- Extortion
- Spam

Analyzing Scenarios

Victim 1: Natalie James
Natalie's friend, John, had asked her out on a date, but she refused to go out with him. A few days later, she received an obscene e-mail at work from an unknown sender who claimed that he knew her office address. When she ignored the e-mail, she started receiving frequent text messages from an unknown number making references to her whereabouts. Natalie is now afraid and has approached the local police for help.

Question: Which computer crime do you think the e-mail and text messages constitute?
a. Harassment
b. Cyberstalking

Correct Answer: Option b

Feedback:
Using technology such as a cell phone or e-mail to monitor another person constitutes cyberstalking.

Harassment includes sending threatening or annoying materials to another person targeted because of gender, sexual orientation, race, or religion. For instance, a female manager who sends out anti-male jokes to the men in her department is engaging in harassment.

Victim 2: Jeanette Lewis
Jeanette Lewis is the CEO of a midsized IT company and the mother of two young girls. Over the past week, she has received a number of e-mails from unknown addresses, containing threats to kidnap her daughters unless she transfers $500,000 to a bank account in the Cayman Islands.

Question: Which computer crime do you think these e-mails constitute?

a. Extortion
b. Cyberbullying

Correct Answer: Option a

Feedback:
Threatening or coercing another person with the objective of achieving financial or other gain is extortion.

Cyberbullying involves using Internet technologies to intimidate or threaten another person. For instance, a young boy, Tommy, does not like another boy, Steve, because of Steve's religion. Tommy sends abusive e-mails and text messages insulting Steve's religion and threatening Steve with physical assault.

Victim 3: Alistair Chan
One of Alistair Chan's co-workers noticed that he was using a popular tax-preparation software program on his work computer. When Alistair left his computer unlocked during a coffee break, the co-worker used the computer to print a copy of Alistair's personal tax return.

Question: Which computer crime do you think this action constitutes?

a. Theft of personal information
b. Identity theft

Correct Answer: Option a

Feedback:
Stealing personal information, such as a person's Social Security number or medical or tax records, constitutes theft of personal information.

Identity theft involves stealing someone's identity and using it for malicious purposes. For instance, stealing someone's mail to get his or her credit card number and bank account information, and then withdrawing funds or making purchases in that person's name, is identity theft.

Victim 4: Jane Balfour
Jane Balfour is a senior citizen who mostly uses her computer to stay in touch with her friends and relatives over e-mail. One day, she receives an e-mail that appears to be from her bank. The e-mail asks her to update her account details and verify the credit card information that the bank has on file. She updates the information as requested and soon finds that her credit card has been misused to make expensive purchases online.

Question: Which computer crime do you think this constitutes?

a. Spam
b. Phishing

Correct Answer: Option b

Feedback:
Sending an e-mail that plausibly claims to be from a legitimate source, and which requests personal information like credit card numbers or bank account details, constitutes phishing.

Spam, also known as unsolicited commercial e-mail, often seeks to have computer users buy products. Some spam may also infect recipients' systems with malware. For instance, a virus writer develops a new worm that will serve as the basis of a rootkit and e-mails it to thousands of individuals, with the e-mail's subject line mentioning the name of a beautiful movie actress. When the recipient opens an attachment that appears to be a photo of the actress, the recipient's computer is immediately infected with the worm.

More Information

- In computer forensics, it is important to understand that computers and related equipment can be the source, vector, or target of a crime. For instance, computer malware makes a computer the target of a crime. In a Denial of Service (DoS) attack, a computer is the source of the crime.
- In the context of computer crimes, the word hacker is often used in a pejorative sense. A hacker is a highly proficient professional who delights in gaining knowledge about computer technologies. If a hacker breaks into systems, it is not necessarily to cause damage or steal data. It may be to determine and disclose the vulnerabilities in a particular system or software and even to help mitigate the vulnerabilities. The term hacker therefore has positive and negative connotations. On the other hand, the term cracker is used to describe a malicious hacker who uses his or her technological proficiency for personal gain or to damage systems.

Topic 3: Types of Computer Crime

Commercial and Government Crime

Forensic Frontiers is a weekly television show on forensic investigation. The show is hosted by Joanne Sebastian, an expert in computer forensics. This episode examines electronic crime against commercial enterprises and government agencies.

Segment 1

Here is a transcript of the conversation between Joanne and Vikram.

Joanne: Welcome to *Forensic Frontiers*. I'm Joanne Sebastian. In today's episode, we'll discuss electronic crime against commercial enterprises and government agencies.

Joanne: Joining me in the studio is another forensic expert who specializes in computer crime against corporate entities. Welcome to the show, Vikram Chandra.

Joanne: Vikram will join me in discussing some of the most common computer crimes committed against commercial enterprises and government agencies.

Vikram: The first crimes that come to mind in the corporate context are extortion and theft of intellectual property.

Vikram: Extortion refers to making threats for personal gain, while theft of intellectual property involves stealing patents or trademarks.

More Information

Theft of Intellectual Property
Description: Theft of intellectual property involves stealing patents, trademarks, trade secrets, or proprietary information from an organization or individual. It is increasingly common these days for employees to steal technical knowledge from their employers and try to sell it to a competitor. Organizations expend significant time, money, and expertise in developing intellectual property. The theft of this type of asset is therefore a significant crime.

Example: A disgruntled employee steals trade secrets and tries to sell them to an overseas competitor.

Evidence: The evidence involved in this type of crime would probably be the copying of individual electronic files.

Extortion from Company Employees
Description: Extortion involves making threats in order to force an individual or an organization to do something—provide money, usually—to escape the threat.

Example: A drug gang threatens to kidnap a CEO unless a sum of money is paid to them.

Evidence: Digital evidence would probably be in the form of e-mail messages, instant messages, or phone calls. The investigation may require input from an audio expert.

Segment 2

Here is a transcript of the conversation between Joanne and Vikram.

Joanne: What are cyberterrorism and information warfare? Are they the same thing?

Vikram: Not really. Cyberterrorism uses computer technologies to instill fear in an organization or society.

Joanne: Then I suppose an attack on a nation's computer systems and information infrastructure constitutes information warfare?

Vikram: That's correct.

More Information

Cyberterrorism
Description: Cyberterrorism uses computer technologies to instill fear in an organization or society.

Example: The Tamil Tigers launch a worm against the Sri Lankan army's IT infrastructure.

Evidence: Potential evidence in this case would be the worm malware itself and information obtainable through network forensics.

Information Warfare
Description: When an individual, a group, an organization, or a nation attacks another's computer systems and information infrastructure, it is engaging in information warfare.

Example: The Russian government launches a full-scale DoS attack against the IT infrastructure of Chechnya.

Evidence: Digital evidence in such a case would reside in network log files and event information.

Segment 3

Here is a transcript of the conversation between Joanne and Vikram.

Joanne: Of course, there's also the common phenomenon of computer hacking, which entails breaking into an organization's computer systems to obtain information.

Vikram: Closely related to hacking is computer intrusion, which involves breaching an organization's information security.

Vikram: Computer fraud involves using a computer or mobile device to commit financial fraud.

More Information

Computer Intrusion
Description: Breaching an organization's security infrastructure to gain information or another type of asset.

Example: A competitor's employee tries to gain access to a company's system in an attempt to learn more about the development of a new product.

Evidence: The most likely sources of digital evidence in a computer intrusion would be found via network forensics, and might include log information from firewalls, the Intrusion Detection System (IDS), and routers.

Computer Fraud
Description: Using a computer device to commit financial fraud, such as theft of funds from a customer's stock brokerage trading account.

Example: A hacker writes a computer virus that illegally accesses others' bank accounts and makes small monthly transfers from them to the hacker's bank account.

Evidence: The type of digital evidence in this case would vary, and would involve identifying the computer virus and performing forensic analysis on the software.

Computer Hacking
Description: Computer hacking involves breaking into an organization's computer systems to obtain information. While computer intrusions are an illegal activity, hacking may also be done for reasons such as to highlight the vulnerability of an organization's network or software.

Example: A criminal organization hacks into the database of a credit card processing company.

Evidence: Potential digital evidence in this type of crime would include various hacking scripts, programs, and toolkits.

Segment 4

Here is a transcript of the conversation between Joanne and Vikram.

Joanne: You can't discuss crime against governments without bringing up drug trafficking.

Vikram: Absolutely. It's always been a major area of concern. There's also the issue of circulating obscene or offensive material.

More Information

Obscene or Offensive Material or Speech
Description: Obscene or offensive material or speech involves circulation of racial slurs, offensive e-mail messages, photos, or videos. Obscene or offensive material or speech includes content that is pornographic or contains slurs based on race, ethnicity, religion,

national origin, gender, or sexual orientation. This material can be circulated by means of e-mail, instant messages, photographs, or videos.

Example: An employee watches a pornographic video at work.

Evidence: An employee watching pornography at work is a straightforward case. Evidence would be located as a file or an encrypted file on the employee's computer. If viewed on the Internet, a forensic investigator would need to identify which Web sites the employee visited.

Drug Trafficking
Description: Drug trafficking involves the sale and distribution of illegal drugs.

Example: Opium farmers sell their crops to dealers, who distribute the processed heroin throughout Europe.

Evidence: In this type of case, in addition to traditional physical evidence, a digital investigator would look for evidence on computers as well as embedded systems, such as cell phones.

Topic 4: Relevance of Computer Evidence

How Relevant Is Computer Evidence?

The relevance of digital evidence can vary significantly according to the specific legal case. Digital evidence can play a minor role or a substantial role in a given case.

Example: Major Role
A digital investigator was looking into an online harassment complaint against a man named Scott Jamieson. When searching for evidence related to the harassment complaint, the investigator noticed some pornographic pictures of children on Jamieson's computer. The investigator obtained a warrant allowing him to search for child pornography on Jamieson's computer. Eventually, Jamieson was charged with 19 counts of possession of child pornography and convicted on 18 counts. For the harassment complaint, Jamieson was tried in a separate proceeding for unlawful use of a computer and disorderly conduct.

Reference: Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet* (3rd ed.) (pp.59). Waltham, MA: Academic Press.

Example: Minor Role
There are some cases in which digital evidence plays only a minor role. Consider the case of a man being sued for at-fault divorce by his wife on the grounds that he committed adultery. In this case, his cell phone might have the telephone numbers of other women with whom he is associated. However, the mere fact that the man has the names and numbers of other women stored in his phone's contact list by no means proves that he is guilty of adultery. Other types of evidence will need to be obtained and verified for a judge to evaluate during the divorce proceedings.

Topic 4: Relevance of Computer Evidence

Evaluation Criteria

Introduction

One major test of whether evidence is valid is the hearsay rule, governed by the Federal Rules of Evidence. Under this rule, if one person makes a statement—possibly about a technology—another individual can express doubts about the accuracy of this statement, provided it is an opinion rather than a factual statement. Generally speaking, hearsay evidence is not admissible in most court cases.

No matter how relevant digital evidence might seem, it must meet the following criteria established by law in order to be considered legally valid.

- **Admissibility:** Evidence must be acceptable in a court of law. To determine admissibility, a judge can carry out legal tests to assess a piece of evidence.
- **Authenticity:** Authenticity of evidence refers to establishing the credibility of evidence in a court of law. A court must be convinced that evidence was acquired from a specific location, and that it is accurate and unchanged from the time it was acquired.
- **Reliability:** The reliability of evidence can be established by determining whether the computer from which the evidence was acquired was functioning normally, and by examining the evidence to detect tampering or other damage.
- **Completeness:** Evidence must be complete, and not partial. The facts revealed by the evidence must be conclusive, and not open to interpretation.

Reference: Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet* (3rd ed.) (pp.58–61). Waltham, MA: Academic Press.

Legal Case Analysis

Question 1: The digital forensic investigator on a case was able to image and analyze only part of a 200 GB hard drive. This evidence includes only one-third of the data on the hard drive. Which of the following criteria would this evidence not meet?

a. Admissibility
b. Reliability
c. Completeness
d. Authenticity

Correct Answer: Option c

Feedback:
As the investigator analyzed only part of the hard drive, the digital evidence in question would not satisfy the evaluation criterion of completeness. In this case, the investigator was not able to obtain and analyze all the relevant evidence on the hard drive.

Question 2: A judge is trying to decide whether a piece of digital evidence should be permitted to be shown to the jury. Which criterion for evaluating evidence would the judge apply?

a. Authenticity
b. Reliability
c. Completeness
d. Admissibility

Correct Answer: Option d

Feedback:
The admissibility criterion establishes which types of evidence are acceptable or presentable in court.

Question 3: Since a court-approved piece of software was not available to a forensic investigator, the investigator decided to use a new open-source software tool to analyze evidence. This tool was recently released on the Internet by an independent developer in Germany. What aspects of the forensic analysis is the judge likely to raise as issues?

a. Admissibility
b. Reliability
c. Completeness
d. Authenticity

Correct Answers: Options b and d

Feedback:
Given that the software used to analyze the evidence is a new open-source tool, the judge is likely to raise concerns about the authenticity and reliability of the evidence.

Topic 5: Controlling Digital Evidence after Acquisition

Challenges and Risks

Working with digital evidence presents a unique set of challenges and risks.

Challenges
After digital evidence has been acquired from its source, it is the responsibility of the forensic investigator to ensure that this evidence is properly controlled and is not exposed to the risk of inadmissibility in court.

Digital Evidence Can Be Voluminous
Digital evidence is likely to be large in size. Although the volume of data collected varies depending on the nature of the legal case, it is common practice to gather every potential source of evidence during the acquisition process. For instance, 50 client computers on a local area network (LAN) will take a long time to image, analyze, and prepare for court proceedings.

In a major federal case involving the collapse of a large, publicly traded company, there could be more than 1,000 computing devices—computers and servers—that have to be imaged and analyzed by federal law enforcement agencies.

Digital Evidence Must Adhere to Standards
Digital evidence must adhere to the Federal Rules of Evidence. This codification of legal standards details the requirements for admissibility of evidence in a legal case. Therefore, it directly affects how forensic investigators handle digital evidence to ensure its integrity. For example, Rule 105,"Limited Admissibility," allows a judge to determine what evidence is admissible and if it can be submitted by one party or the other. The judge can also determine whether the evidence should be considered by the jury in reaching their verdict.

Reference: Cornell University Law School, Legal Information Institute (n.d.). Rule 105.Limited admissibility. *Federal Rules of Evidence.* Retrieved from http://www.law.cornell.edu/rules/fre/rules.htm#Rule105

Digital Evidence Can Be Tampered With
In April 2006, the U.S. Supreme Court gave its approval to proposed amendments to the Federal Rules of Civil Procedure regarding electronically stored information. These changes recognized the challenges inherent in handling digital evidence[1]. For instance, Rule 26, "Duty to Disclose; General Provisions Governing Discovery," discusses the numerous requirements related to the treatment of evidence, including expert witnesses, copies of evidence, and specific limitations on electronically stored information[2].

Reference:
[1] Roberts, C. G. (2006, August).The 2006 discovery amendments to the Federal Rules of Civil Procedure. *Law Practice Today*. Retrieved from http://apps.americanbar.org/lpm/lpt/articles/tch08061.shtml

[2] Cornell University Law School, Legal Information Institute (n.d.). Rule 26.Duty to disclose; general provisions governing discovery. *Federal Rules of Civil Procedure.* Retrieved from http://www.law.cornell.edu/rules/frcp/Rule26.htm

Risks
Each scenario listed here presents a different risk regarding digital evidence. Match each scenario with the appropriate risk.

Scenario	Risk
1. Digital evidence is not placed in special tamper-proof bags and evidence rooms with environmental controls.	A. Evidence tampering
2. Digital forensic evidence is lost due to a fire.	B. Degradation or deterioration of evidence
3. A non-forensic specialist working for a police department wants to view a disk drive image because the case involves an old friend of his.	C. Loss or destruction of evidence
4. Digital evidence is not acquired using industry standard practices and procedures.	D. Inadmissibility of evidence

Correct Answer: 1-B, 2-C, 3-A, 4-D

Feedback:
Not placing digital evidence in tamper-proof bags and evidence rooms with environmental controls can lead to degradation or deterioration of the evidence. Unauthorized or undocumented access to evidence qualifies as evidence tampering.

If evidence is destroyed intentionally or unintentionally, as in the case of a fire, then it is simply not available for use in a legal case. This amounts to loss or destruction of evidence. Inadmissibility of evidence is a key concern for a digital forensic investigator. If the evidence is not obtained using industry standard practices, a judge may deem it inadmissible. This could destroy the prosecution's entire case.

Topic 5: Controlling Digital Evidence after Acquisition

Controlling Digital Evidence

Like any other type of evidence, digital evidence needs to be controlled and handled professionally. These control measures mitigate the risks of mishandling, destruction, and inadmissibility of evidence.

Step 1: Use Property Tags and Identification Labels
Digital forensic investigators need to attach property tags to computer hardware or software media. The tags are attached so as to avoid damaging the media while providing reference to the case number, property custodians, investigators, and related information.

Identification labels are similar to property tags. However, they are used for computer-generated copies of media, paper files, and other case-related evidence.

Step 2: Use Evidence Bags
Tamper-proof evidence bags are required to maintain the physical integrity of the evidence and protect it against damage from environmental factors.

Step 3: Place Evidence in a Secured Facility
Digital forensic investigators need to place evidence in a room or facility that is monitored and secured. This is frequently referred to as an evidence room by law enforcement agencies. This location must be under constant surveillance and security monitoring to deter unauthorized access to or tampering with evidence.

Step 4: Use Environmental Controls
Forensic investigators must ensure the use of proper environmental controls, including air conditioning and humidity controls, in the evidence room or other evidence storage facilities.

Step 5: Lock Boxes that Contain Evidence
It is essential to lock all boxes that contain digital evidence, even though the boxes are placed in a secure evidence room. Locking these boxes helps deter tampering.

Step 6: Prevent Unauthorized Access and Use Log Sheets
The evidence room must have controls in place to prevent unauthorized access. Physical controls such as security guards, closed-circuit television surveillance, and proximity card readers are three common effective measures.

In addition, it is crucial to use a log sheet or a similar form to document every time a piece of evidence is moved. This form should record who moved the evidence, when and where it was taken, and when it was returned. Every action needs to be thoroughly documented to eliminate all doubt regarding the Chain of Custody later in the investigation.

Topic 6: Sharing Evidence

To Share or Not to Share

Back at Southern TelcoSol, Timothy, the CIO; Nelson, the CISO; and Brad, the CEO, are discussing the question of how much information to share with the DEA in its investigation of Alana.

Here is a transcript of the conversation among Brad, Timothy, and Nelson.

Brad: We need to tackle a very fundamental question: whether or not we should actively share evidence with the DEA.

Timothy: Most organizations request the involvement of law enforcement only if their case involves a serious criminal matter, has an international dimension to it, or is related to cyberterrorism.

Timothy: If that is not the case, we should conduct an internal investigation.

Nelson: Given that Alana's case is likely to be a criminal matter rather than a civil one, we should seek advice from legal counsel regarding access to evidence.

Timothy: Yes, and if gathering and analyzing evidence warrants the involvement of law enforcement, we can always contact the DEA for consultation.

Analysis

Sharing Evidence with Law Enforcement
The conversation among Southern TelcoSol's CIO, CISO, and CEO led them to compile a generic list of advantages and disadvantages of sharing evidence with law enforcement.

Advantages	Disadvantages
1. Developing a good relationship with law enforcement. 2. Securing additional digital forensic expertise to aid an investigation. 3. Increasing the digital forensic knowledge base within the organization.	1. Providing access to non-case-related information that might be damaging to the company. 2. Developing a bad reputation if the company is seen as incapable of dealing with its own digital forensic investigations. 3. Promoting a perception that law enforcement is a free resource that any organization can call upon for assistance.

Topic 7: Activity

Activity—The Investigation

Introduction
With detailed cybersecurity policies in place at Southern TelcoSol, Nelson, the CISO, and Timothy, the CIO, are confident that they should undertake the investigation of Alana's case internally. Together with the CEO, they have decided to use advanced enterprise forensic software to examine Alana's computer. The software allows them to access Alana's computer surreptitiously over the company's network.

After all the digital evidence has been acquired, Southern TelcoSol needs to label the evidence properly and store it securely. Given the lack of secure storage areas for evidence and the fact that Nelson is not a full-time forensic examiner, this investigation is a bit of a challenge for the company. Nelson does, however, have industry certification in the field of digital forensics. He senses that he can gather a lot of useful evidence to support the investigation.

Internal Investigation
Question 1: What types of files is Nelson likely to find on Alana's computer hard drive?
a. A significant amount of e-mail messages
b. Electronic spreadsheets
c. An anti-forensic software application
d. Video files

Correct Answers: Options a, b, and d

Feedback:
Since it is already known that Alana has a corporate e-mail account and possibly another personal one, Nelson is likely to find e-mail messages on her hard drive. Because she is the vice president of marketing, Alana's hard drive would likely also contain different types of electronic spreadsheets related to budgets, consumer research, marketing campaigns, and possibly even her drug deals.

Video files may also be found relating to Alana's work in the marketing department. As for anti-forensic software, unless Alana is a very sophisticated criminal, it is unlikely she would have this installed on her hard drive.

Question 2: Which of the following types of evidence would be inadmissible in court in this case?
a. E-mail messages
b. Family photographs
c. Electronic spreadsheets
d. Database files

Correct Answer: Option b

Feedback:
Family photographs are personal information and are therefore not likely to be considered admissible by a judge in this case. However, e-mails, spreadsheets, and

database files could qualify as admissible evidence.

Question 3: From where could the CISO obtain or develop a comprehensive Chain of Custody form?

a. A professional colleague from the field of computer forensics
b. A Department of Justice publication
c. A computer forensics textbook
d. His local office-supply store

Correct Answers: Options a, b, and c

Feedback:
Office-supply stores do not carry forms or other documents used in the field of computer forensics.

By referring to a Justice Department publication or a computer forensics textbook, Nelson might be able to develop his own template for a Chain of Custody form for this and future projects. A professional colleague in the field of computer forensics might also be able to provide Nelson with a Chain of Custody form.

Question 4: What medium is the best choice for Nelson to use in making daily images of Alana's computer?

a. Floppy disks
b. Optical disks
c. External hard drives
d. A folder on a file server in the marketing department

Correct Answer: Option c

Feedback:
External hard drives are current technology. They are easy to use and have ample storage space. Nelson could use one drive for each day.

Floppy disks are much too small for the amount of data that Alana would have on her computer. As for optical disks, they are not very popular in the field because they require a special type of reader. A folder on the marketing department's file server would be in view of other users, including Alana, and might arouse suspicion.

Question 5: What should the CISO use to label each piece of media properly?

a. Sticky notes
b. Envelopes
c. File folders
d. Evidence tags

Correct Answer: Option d

Feedback:
Evidence tags represent a professional method of controlling and storing digital evidence. Sticky notes, envelopes, and file folders should not be used as they are susceptible to physical damage, deterioration, or loss.

Question 6: Southern TelcoSol does not have an evidence room like one at a police department. Through his training, Nelson knows that the evidence must be properly secured. What should he do to resolve this issue?

a. Purchase a small, fireproof safe and place it in a locked desk drawer
b. Ask the cashier's office to store the evidence
c. Take the evidence home every night
d. Leave the evidence in plain view on his desk

Correct Answer: Option a

Feedback:
Purchasing a fireproof safe and placing it in a locked desk drawer is the most secure and reasonable approach to take. Storing the evidence in the cashier's office, taking it home every night, or leaving it in plain sight presents many risks related to loss, damage, or tampering.

Question 7: At the time of the investigation, was Southern TelcoSol adequately prepared for gathering authentic digital evidence?

a. No, they should have hired an external consultant.
b. Yes, it appears so.

Correct Answer: Option b

Feedback:
Given that Southern TelcoSol had a trained, industry-certified CISO who could properly acquire digital evidence, the company was prepared for this type of forensic investigation. Even though some workarounds were required, Nelson adequately demonstrated his capability.

Question 8: A meeting is finally scheduled between Jennifer, the DEA agent, and Southern TelcoSol's CEO, CIO, and CISO. Whom should the Southern TelcoSol team consult regarding this situation before the meeting takes place?

a. Southern TelcoSol's Chief Financial Officer (CFO)
b. Alana
c. The manager of Southern TelcoSol's data center
d. Legal counsel

Correct Answer: Option d

Feedback:
Seeking legal advice is very important before meeting with law enforcement agents. A lawyer will be able to advise Southern TelcoSol's CEO, CIO, and CISO regarding what to say and what not to say, and also educate them regarding the laws relevant to the case.

Southern TelcoSol's CFO and data center manager do not have any role to play in the investigation. Besides, it is prudent not to discuss this matter with any individuals who do not need to be involved. Since Alana is the suspect, it would not be appropriate to speak with her.

DEA Investigation
Timothy, the CIO of Southern TelcoSol, along with Nelson, the CISO, and Brad, the CEO, meets with Jennifer, the DEA agent.

Here is a transcript of the conversation among them.

Jennifer: The DEA is in the process of conducting a nationwide investigation into a Colombian drug cartel controlled by the Perez family in Cali.

Jennifer: At this time, we believe that one of your company's employees is helping this cartel smuggle and distribute cocaine in the United States.

Jennifer: The evidence that we have gathered so far points to Alana Blank. She is our prime suspect.

Timothy: Please allow me to introduce you to our CISO, Nelson Gomez, who is a Certified Computer Examiner and a member of the local InfraGard chapter. He will explain his internal investigation.

Nelson: Over the past week, I have observed some suspicious activities related to her interactions on a professional networking site called Plugg-In.

Nelson: I noticed that she was communicating with Taylor Anthony—a suspected drug trafficker—and I became concerned.

Nelson: I began to use our computer systems to closely monitor Alana's online activities.

Jennifer: May I ask what the current scope and preliminary findings of your investigation are?

Nelson: I have been accessing Alana's computer via the network using advanced enterprise forensic software.

Nelson: Based on screen captures and communication logs of the Plugg-In chat application, I also think she might be involved in a local drug-dealing racket.

Jennifer: That information is very useful to our investigation. Would you be willing to share the data with me?

Analysis

Analyzing the Situation

Question: Do you think Southern TelcoSol should share the information that Nelson has gathered with the DEA?

a. Yes
b. No

Feedback:
There is no correct or incorrect answer to this question. Given the specific circumstances of the Alana Blank case, Southern TelcoSol would have to make its own decision about whether to share evidence with the DEA.

The potential advantages of sharing evidence are as follows:

- It could result in Southern TelcoSol building a good rapport with the DEA, which may be helpful for future forensic investigations involving criminal or terrorism-related activities.
- Management would be seen as "doing the right thing" in terms of corporate ethics.
- After the investigation is made public, Southern TelcoSol employees would likely take pride in their company management for not tolerating employees involved in criminal activities.

The potential disadvantages of sharing evidence are as follows:

- The company might face a lawsuit from Alana.
- The DEA might grow suspicious regarding other corporate matters that they might want to investigate. This suspicion and consequent investigations could result in a bad relationship between Southern TelcoSol and the DEA.

Topic 8: Summary

We have come to the end of Module 3. The key concepts covered in this module are listed below.

- Computer crimes can be committed against individuals, as well as against private- and public-sector organizations.

- Computer crimes commonly committed against individuals include cyberstalking, harassment, cyberbullying, identity theft, spam, and phishing.

- Crimes committed against commercial enterprises and government agencies include theft of intellectual property, extortion, cyberterrorism, information warfare, computer hacking and intrusion, computer fraud, drug trafficking, and circulating obscene or offensive material.

- To qualify for consideration in a legal case, digital evidence must meet the criteria of admissibility, authenticity, reliability, and completeness.

- There are various advantages and disadvantages to an organization's sharing evidence with law enforcement, depending on whether the case involves a serious criminal matter, has an international dimension to it, or is related to cyberterrorism. It is advisable for an organization to conduct an internal investigation on its own, as far as possible.

Glossary

Term	Definition
Admissibility of Evidence	Admissibility of evidence refers to the acceptability of evidence in a court of law. Evidence must be acceptable to the court. To determine admissibility, a judge can carry out legal tests to assess a piece of evidence.
Authenticity of Evidence	Authenticity of evidence refers to establishing the credibility of evidence in a court of law. To establish authenticity, a court must be convinced that evidence was acquired from a specific location. Evidence must be proved to be accurate and unaltered from the time it was acquired.
Cyberbullying	Cyberbullying involves using computer and Internet technologies to intimidate or threaten another person.
Cyberstalking	Cyberstalking refers to the use of technology, such as a cell phone or e-mail, to monitor another person's movements or actions.
Cyberterrorism	Cyberterrorism is a type of politically motivated terrorism that uses the Internet and computers to spread panic, commit violent acts, and cause loss of life.
Denial of Service	Denial of Service (DoS) attacks flood a target site with large volumes of traffic using "zombie" servers. This flood of traffic consumes all of the target site's network or system resources and denies access to legitimate users.
Extortion	Extortion is the act of threatening or coercing an individual or an organization in order to achieve financial or other gain.
Federal Rules of Evidence	The Federal Rules of Evidence are a protocol governing the admission of facts in civil and criminal cases.
Harassment	Harassment includes sending threatening or annoying communications to a person targeted because of gender, sexual orientation, race, or religion.
Identity Theft	Identity theft involves stealing someone's identity and using it for malicious purposes—for instance, stealing someone's mail to get his or her credit card number and bank account information.
Information Warfare	Information warfare is an attack by an individual, a group, an organization, or a nation on another's computer systems and information infrastructure.
InfraGard	InfraGard is a national-level, nonprofit organization that brings together the DEA, state and local law enforcement agencies, academia, and businesses for the purpose of intelligence sharing.
Intellectual Property Theft	Intellectual property theft is the theft of proprietary information owned by a company, such as ideas, technical knowledge, or trade secrets.

Term	Definition
Optical Disk	An optical disk is a plastic-coated disk that has pits etched along its surface. Optical disks store digital data that can be read by a laser.
Phishing	Phishing is the act of sending a message that plausibly claims to be from a legitimate source, and which requests personal information like credit card numbers or bank account details.
Spam	Spam, also known as unsolicited commercial e-mail, often seeks to have computer users buy products. Some spam may also infect recipients' systems with malware.
Theft of Personal Information	Theft of personal information includes the illegal appropriation of data such as a person's Social Security number, or medical or tax records.