Solution and Answer Guide

Miller, Business Law Today, Comprehensive Edition: Text & Cases 13e, 9780357634783;   
Chapter 09: Criminal Law and Cyber Crime

Table of Contents

[Critical Thinking Questions in Features 1](#_Toc63157668)

[Adapting the Law to the Online Environment 1](#_Toc63157669)

[Critical Thinking Questions in Cases 2](#_Toc63157670)

[Case 9.1 2](#_Toc63157671)

[Case 9.2 3](#_Toc63157672)

[Chapter Review 3](#_Toc63157673)

[Practice and Review 3](#_Toc63157674)

[Practice and Review: Debate This 4](#_Toc63157675)

[Issue Spotters 5](#_Toc63157676)

[Business Scenarios and Case Problems 5](#_Toc63157677)

[Critical Thinking and Writing Assignments 11](#_Toc63157678)

# Critical Thinking Questions in Features

Adapting the Law to the Online Environment

1. Despite Bitcoin’s oversized presence on the dark web, only about 1 percent of all transactions using the cryptocurrency involve an illegal exchange of goods. How does this fact impact arguments in favor of banning Bitcoin?

Solution

The relatively low level of illegal activity actually associated with Bitcoin argues against its prohibition. As a society, we accept the widespread use of many items that, under certain circumstances, can be used to further a criminal goal. To use the most obvious example for this topic, even though cash is used in a great many crimes—far more than Bitcoin—nobody would suggest banning the use of cash.

Interestingly, several European countries have *limited* the amount of cash that can be legally used in any single transaction, primarily to combat money laundering and other forms of tax evasion. In these situations, one could argue that the funds themselves are part of the *actus reus* of the crime. In most cases not involving counterfeiting, however, the *actus reus* of a crime that involves the exchange of illegal goods is the exchange, not the currency used.

Managerial Strategy—Business Questions

1. Why might a corporation’s managers agree to pay a large fine rather than to be indicted and proceed to trial?

Solution

Most corporate managers choose to pay the fine because they worry that a criminal indictment will harm their corporation’s reputation, its profitability, and ultimately, its existence.

1. How do managers determine the optimal amount of legal research to undertake to prevent their companies from violating the many thousands of federal regulations?

Solution

Every manager is faced with the task of determining how best to use the limited resources at their disposal. Clearly, no manager in a small company would decide to devote 50 percent of the company’s annual costs to preventing violations of federal regulations. Hence, each manager must weigh the potential costs of violating federal rules and regulations with the legal fees that must be incurred to learn about those regulations.

Cybersecurity and the Law—Critical Thinking

1. One suggestion for alleviating the problem of “fraud sourced” money is to require proof of identity from anyone who wants to trade virtual items on online gaming platforms. Do you think this strategy would be successful? Why or why not?

Solution

The reasoning behind an identification requirement seems sound. Cybercriminals thrive on anonymity. If there is a record linking them to any suspicious activity, it will deter that activity. It also gives companies like Valve and Epic Games, which owns Fortnite, the ability to monitor the behavior of specific players and traders, and, if this activity becomes suspicious, report it to law enforcement.

At the same time, cyber criminals are skilled in hiding their identities, and would certainly put this expertise to use on online gaming markets if given an incentive to do so. Furthermore, the identification requirement is not necessarily fair to legitimate gamers, who may want to operate in anonymity for privacy reasons. Many such players would switch from online gaming platforms that did require identification to those that did not, therefore causing economic hardship to those companies trying to do the “right thing.”

# Critical Thinking Questions in Cases

Case 9.1

1. Could Crabtree have successfully avoided her conviction by arguing that her only “crime” was “naively trusting her co-workers?” Why or why not?

Solution

No, Crabtree is not likely to have avoided her conviction by arguing that her only “crime” was “naively trusting her co-workers.” This claim would have been refuted by the same evidence that supported the jury’s finding of her knowledge of, and voluntary participation in, the fraud with which she was charged.

This evidence included the testimony of HCSN employees that Crabtree complied with their requests to modify patient notes to satisfy Medicare qualifications. Further, Crabtree acknowledged in conversation that some of the patients suffered from conditions that were unsuitable for treatment at HCSN. In addition, there was the evidence that Crabtree fulfilled requests to change and falsify notes for billing and Medicare purposes. This supported the finding that she voluntarily joined the conspiracy.

1. It seems reasonable to assume that one of the purposes of any business is to “maximize billing potential.” When does conduct to accomplish that purpose become unethical?

Solution

Conduct to “maximize billing potential,” or to realize any other financial objective, becomes unethical when decisions and actions fail to reflect “good corporate citizenship.”

In the *Crabtree* case, for example, the defendant (and, of course, others who participated in the fraud with which she was charged) failed to evaluate—at a minimum—the legal implications of their conduct before engaging in it. Most importantly, Crabtree should have taken into account the health needs of the patients whose therapy she vouched for. She might also have given thought to the possible consequences of her ill-conceived actions on her family and her reputation, as well as within the healthcare community generally.

Case 9.2

1. Why was Sisuphan convicted of embezzlement instead of larceny? What is the difference between these two crimes?

Solution

One of the key differences between embezzlement and larceny has to do with the element of possession. Larceny involves the wrongful taking of property in the possession of another, as does robbery (the latter crime involves the violent taking of the property). Embezzlement, in contrast, involves the wrongful appropriation of property that has been entrusted to the person appropriating it, typically an employee. In other words, the property is already in the perpetrator’s possession. Thus, Sisuphan was convicted of embezzlement instead of larceny because, as a dealership employee, he was in legitimate possession of the money until he took the added step of keeping it.

# Chapter Review

Practice and Review

Edward Hanousek worked for Pacific & Arctic Railway and Navigation Company (P&A) as a roadmaster of the White Pass & Yukon Railroad in Alaska. As an officer of the corporation, Hanousek was responsible “for every detail of the safe and efficient maintenance and construction of track, structures, and marine facilities of the entire railroad,” including special projects. One project was a rock quarry, known as “6-mile,” above the Skagway River. Next to the quarry, and just beneath the surface, ran a high-pressure oil pipeline owned by Pacific & Arctic Pipeline, Inc., P&A’s sister company. When the quarry’s backhoe operator punctured the pipeline, an estimated one thousand to five thousand gallons of oil were discharged into the river. Hanousek was charged with negligently discharging a harmful quantity of oil into a navigable water of the United States in violation of the criminal provisions of the Clean Water Act (CWA). Using the information presented in the chapter, answer the following questions.

1. Did Hanousek have the required mental state (*mens rea*) to be convicted of a crime? Why or why not?

Solution

Yes, because he was the corporate officer responsible for the project and had the power to prevent the criminal violation. Corporate directors and officers are personally liable for the crimes they commit, and can also be held liable for the crimes of employees under their supervision. Because Hanousek was the corporate officer responsible for every detail of the “6-mile” quarry, he had the power to prevent the criminal violation. Therefore, Hanousek can be held criminally negligent for the backhoe operator puncturing the pipeline.

1. Which theory discussed in the chapter would enable a court to hold Hanousek criminally liable for violating the statute regardless of whether he participated in, directed, or even knew about the specific violation?

Solution

Under the responsible corporate officer doctrine, a corporate officer can be held liable for a crime because he was in a responsible relationship to the corpora­tion and could have prevented the violation. The corporate officer does not have to intend the crime or even know about it, to incur liability under this doctrine.

1. Could the backhoe operator who punctured the pipeline also be charged with a crime in this situation? Explain.

Solution

No, because he did not have the required mental state (mens rea) and was not a cor­porate officer in a responsible position to prevent the criminal violation. Criminal liability requires a guilty act at the same time as the defendant had a wrongful mental state. In this situation, the backhoe operator did pierce the pipeline (the guilty act), but he did not have a wrongful mental state because he was unaware that the pipeline was there. As an employee, a court would not use the same standard as if he were a responsible corporate officer who “knew or should have known” of the existence of the pipeline. Because both elements of criminal liability (guilty act and wrongful mental state) did not occur, the backhoe operator could not be charged with a crime.

1. Suppose that, at trial, Hanousek argued that he could not be convicted because he was not aware of the requirements of the CWA. Would this defense be successful? Why or why not?

Solution

No, because Hanousek was the corporate officer responsible for the project and should have known the requirements of the law. Because Hanousek was in a responsible position at the corporation and specifically in charge of the 6-mile quarry, a court would find that he “should have known” of the requirements of the law. Therefore, lack of knowledge of the requirements of the Clean Water Act would not operate as a defense in his case.

Practice and Review: Debate This

1. Because of overcriminalization, particularly by the federal government, Americans may be breaking the law regularly without knowing it. Should Congress rescind many of the more than four thousand federal crimes now on the books?

Solution

Drastic times require drastic measures. This nation now has more than three hundred million residents who move frequently. Moreover, the pervasiveness of the Internet means that business fraud is increasing at a rapid rate. Consequently, the federal government must step in to make sure that criminal actions do not go unpunished. That’s why so many new federal crimes have been added to the body of criminal statutes.

The Constitution reserves for the states police powers for activities within state boarders. Crimes have always been defined by state and local governments. Just because we have a larger population that has access to the Internet does not mean that Congress should be in the business of creating so many federal crimes. Moreover, many new federal criminal statutes do not require intent—a cornerstone of the prosecution of most crimes for ages.

Issue Spotters

1. Dana takes her roommate’s credit card, intending to charge expenses that she incurs on a vacation. Her first stop is a gas station, where she uses the card to pay for gas. With respect to the gas station, has she com­mitted a crime? If so, what is it?

Solution

Yes. With respect to the gas sta­tion, she has obtained goods by false pretenses. She might also be charged with larceny and forgery, and most states have spe­cial statutes covering illegal use of credit cards.

1. Without permission, Ben downloads consumer credit files from a computer belonging to Consumer Credit Agency. He then sells the data to Dawn. Has Ben committed a crime? If so, what is it?

Solution

Yes. The Counterfeit Access Device and Computer Fraud and Abuse Act provides that a person who accesses a computer online, without permission, to obtain classified data—such as consumer credit files in a credit agency’s database—is subject to criminal prosecution. The crime has two elements: (1) accessing the computer without permission and (2) taking data. It is a felony if done for private financial gain. Penalties include fines and imprisonment for up to twenty years. The victim of the theft can also bring a civil suit against the criminal to obtain damages and other relief.

Business Scenarios and Case Problems

1. **Types of Cyber Crimes.** The following situations are similar, but each represents a variation of a particular crime. Identify the crime and point out the differences in the variations. (See *Cyber Crime*.)
2. Chen, posing fraudulently as Diamond Credit Card Co., sends an e-mail to Emily, stating that the company has observed suspicious activity in her account and has frozen the account. The e-mail asks her to reregister her credit card number and password to reopen the account.

Solution

This is a form of identity theft. The traditional crimes of theft (rob­bery, burglary, larceny, and other) consist of wrongfully taking and carrying away an­other’s per­sonal property with the intent of depriving the owner permanently of it. Unique to crimes of identity theft is that they involve taking another’s identity, and unique to cyber variations of the offense is that the criminal acts are committed with computers, often online. A stolen identity is typically used to commit more crimes.

1. Claiming falsely to be Big Buy Retail Finance Co., Conner sends an e-mail to Dino, asking him to confirm or update his personal security information to prevent his Big Buy account from being discontinued.

Solution

As in the previous problem, this is a form of identity theft. This problem de­scribes a factual situation referred to as *phishing*. In such a set of circumstances, once an unsuspecting individual responds by entering the requested information, the phisher can use it to pose as that person or to steal the funds in the victim’s bank or other account.

1. **Cyber Scam.** Kayla, a student at Learnwell University, owes $20,000 in unpaid tuition. If Kayla does not pay the tuition, Learnwell will not allow her to graduate. To obtain the funds to pay the debt, she sends e-mails to people that she does not know asking them for financial help to send her child, who has a disability, to a special school. In reality, Kayla has no children. Is this a crime? If so, which one? (See *Cyber Crime*.)

Solution

Kayla has committed fraud in an e-mail sent via the Internet. The elements of the tort of fraud are as follows:

1. The misrepresentation of material facts or conditions was made with knowledge that they were false or with reckless disregard for the truth.
2. There was an intent to induce another to rely on the misrepresentation.
3. There was justifiable reliance on the misrepresentation by the deceived party.
4. Damages were suffered as a result of the reliance.
5. There was a causal connection between the misrepresentation and the injury.

If any of Kayla’s recipients reply to her false plea with cash, it is likely that all of these requirements for fraud will have been met.

1. **Business Case Problem with Sample Answer—White-Collar Crime.** Matthew Simpson and others created and operated a series of corporate entities to defraud telecommunications companies, creditors, credit reporting agencies, and others. Through these entities, Simpson and his confederates used routing codes and spoofing services to make long-distance calls appear to be local. They stole other firms’ network capacity and diverted payments to themselves. They leased goods and services without paying for them. To hide their association with their corporate entities and with each other, they used false identities, addresses, and credit histories, and issued false bills, invoices, financial statements, and credit references. Did these acts constitute mail and wire fraud? Discuss. [*United States v. Simpson*, 741 F.3d 539 (5th Cir. 2014)] (See *Types of Crimes*.)

Solution

Yes, the acts committed by Matthew Simpson and the others, and described in this problem, constitute wire and mail fraud. Federal law makes it a crime to devise any scheme that uses the U.S. mail, commercial carriers (FedEx, UPS), or wire (telegraph, telephone, television, the Internet, e-mail) with the intent to defraud the public.

Here, as stated in the facts, Simpson and his cohorts created and operated a series of corporate entities to defraud telecommunications companies, creditors, credit reporting agencies, and others. Through these entities, Simpson and the others used routing codes and spoofing services to make long distance calls appear to be local. They stole other firms’ network capacity and diverted payments to themselves. They leased goods and services without paying for them. And they assumed false identities, addresses, and credit histories, and issued false bills, invoices, financial statements, and credit references, in order to hide their association with their entities and with each other. The “scheme” was to defraud telecommunications companies and other members of the public to the perpetrators’ gain of a variety of goods and services. Wire services—the Internet, and presumably phones and other qualifying services—were used to further the scheme.

In the actual case on which this problem is based, a federal district court convicted Simpson of participating in a wire and mail fraud conspiracy (and other crimes). On appeal, the U.S. Court of Appeals for the Fifth Circuit affirmed the conviction.

1. **Defenses to Criminal Liability.** George Castro told Ambrosio Medrano that a bribe to a certain corrupt Los Angeles County official would buy a contract with the county hospitals. To share in the deal, Medrano recruited Gustavo Buenrostro. In turn, Buenrostro contacted his friend James Barta, the owner of Sav–Rx, which provides prescription benefit management services. Barta was asked to pay a “finder’s fee” to Castro. He did not pay, even after frequent e-mails and calls with deadlines and ultimatums delivered over a period of months. Eventually, Barta wrote Castro a Sav–Rx check for $6,500, saying that it was to help his friend Buenrostro. Castro was an FBI agent, and the county official and contract were fictional. Barta was charged with conspiracy to commit bribery. At trial, the government conceded that Barta was not predisposed to commit the crime. Could he be absolved of the charge on a defense of entrapment? Explain. [*United States v. Barta*, 776 F.3d 931 (7th Cir. 2015)] (See *Defenses to Criminal Liability*.)

Solution

Yes, Barta could be absolved of the charge of conspiracy to commit bribery on a defense of entrapment.This defense is designed to prevent police officers and other government agents from enticing persons to commit crimes so that they can later be prosecuted for criminal acts. For entrapment to succeed as a defense, both the suggestion and the inducement to commit the crime must take place. The critical question is whether the person who is charged with the commission of a crime was predisposed to commit it or did so only because the officer induced it.

In this problem, the government, through its agent George Castro, entrapped Barta into participating in a conspiracy to bribe a fictional county official. The government conceded at Barta’s trial that he was not predisposed to conspire to commit bribery. Castro frequently e-mailed and called Barta over a period of months, with no response from him, even when the messages included deadlines and ultimatums. And Barta’s statement, when he eventually did write a check on his company’s account to Castro, that it was to help his friend gave the government reason to believe that Barta was making a deal only to benefit his friend.

In the actual case on which this problem is based, Barta was arrested, charged, and tried for conspiracy to commit bribery. He pleaded entrapment but was convicted. The U.S. Court of Appeals for the Seventh Circuit reversed his conviction, on the reasoning stated above.

1. **Fourth Amendment Protections.** Federal officers obtained a warrant to arrest Kateena Norman on charges of credit card fraud and identity theft. Evidence of the crime included videos, photos, and a fingerprint on a fraudulent check. A previous search of Norman’s house had uncovered credit cards, new merchandise, and identifying information for other persons. An Internet account registered to the address had been used to apply for fraudulent credit cards, and a fraudulently obtained rental car was parked on the property. As the officers arrested Norman outside her house, they saw another woman and a caged pit bull inside. They further believed that Norman’s boyfriend, who had a criminal record and was also suspected of identify theft, could be there. In less than a minute, the officers searched only those areas within the house in which a person could hide. Would it be reasonable to admit evidence revealed in this “protective sweep” during Norman’s trial on the arrest charges? Discuss. [United States v. Norman, 637 Fed. Appx. 934 (11th Cir. 2016)] (See *Constitutional Safeguards*.)

Solution

Yes, it would be reasonable to admit evidence revealed in the “protective sweep” of the defendant’s house in this problem during Norman’s trial on the arrest charges.

The Fourth Amendment to the U.S. Constitution protects the “right of the people to be secure in their persons, houses, papers, and effects.” Under this amendment, before searching private property, law enforcement officers must obtain a search warrant. Evidence obtained in violation of this requirement is not admissible at trial. But a warrantless search can be reasonable when probable cause and exigent circumstances exist. Thus, when an officer possesses a reasonable belief based on specific facts that an individual posing a danger is hidden inside a certain location, a search for the individual—a “protective sweep”— confined to those places on site in which a person might be hiding would be reasonable.

In this problem, from outside a house belonging to Kateena Norman, during the execution of a warrant for the arrest of Norman on charges of credit-card fraud and identity theft, federal officers saw another woman and a caged pit bull inside. The officers further believed that Norman’s boyfriend, who had a criminal record and was also suspected of identify theft, could be inside. In less than a minute, the officers searched only those areas within the house in which a person could hide. Under these circumstances, the warrantless search was reasonable and therefore any evidence discovered in the search would be admissible during her trial on the arrest charges.

In the actual case on which this problem is based, Norman filed a motion to suppress this evidence, which the court denied. The U.S. Court of Appeals for the Eleventh Circuit affirmed. “The protective sweep was reasonable.”

1. **Types of Crimes.** In Texas, Chigger Ridge Ranch, L.P., operated a 700-acre commercial hunting area called Coyote Crossing Ranch (CCR). Chigger Ridge leased CCR and its assets for twelve months to George Briscoe’s company, VPW Management, LLC. The lease identified all of the vehicles and equipment that belonged to Chigger Ridge, which VPW could use in the course of business, but the lease did not convey any ownership interest. During the lease term, however, Briscoe told his employees to sell some of the vehicles and equipment. Briscoe did nothing to correct the buyers’ false impression that he owned the property and was authorized to sell it. The buyers paid with checks, which were deposited into an account to which only Briscoe and his spouse had access. Which crime, if any, did Briscoe commit? Explain. [*Briscoe v. State of Texas*, 2018 WL 792255 (Tex.App.—Texarkana 2018)] (See *Types of Crimes*.)

Solution

Briscoe committed the crime of obtaining property by false pretense. This is a crime in which the goal is economic gain through the acquisition of another’s money, services, or property. This type of theft is accomplished by trickery or fraud.

In the *Briscoe* case, Briscoe leased Chigger Ridge Ranch for twelve months. The lease delineated the vehicles and equipment that belonged to the ranch, and which VPW could use for the term, but the lease did not convey any ownership interest. Despite the lack of ownership rights, Briscoe had his employees sell some of the vehicles and equipment. The buyers had the impression that Briscoe either owned the property or was authorized to sell it, and he did nothing to correct their false impression of this pretense. The buyers paid with checks, which Briscoe deposited in his own account. The goal of this scheme was to acquire the buyers’ money. The theft was accomplished by fraud.

In the actual case on which this problem is based, Briscoe was convicted in a Texas state court of giving a false statement to obtain property. A state intermediate appellate court affirmed. “Briscoe obtained the checks by deception—that is, by failing to correct [the buyers’] impression that he . . . owned the equipment or was authorized to sell it.”

1. **A Question of Ethics—The IDDR Approach and Identity Theft.** Heesham Broussard obtained counterfeit money instruments. To distribute them, he used account information and numbers on compromised FedEx accounts procured from hackers. Text messages from Broussard indicated that he had participated previously in a similar scam and that he knew the packages would be delivered only if the FedEx accounts were “good.” For his use of the accounts, Broussard was charged with identity theft. In defense, he argued that the government could not prove he knew the misappropriated accounts belonged to real persons or businesses. [*United States v. Broussard*, 675 Fed.Appx. 454 (5th Cir. 2017)] (See *Cyber Crime*.)
2. Does the evidence support Broussard’s assertion? From an ethical perspective, does it matter whether he knew that the accounts belonged to real customers? Why or why not?

Solution

No, the evidence does not support Broussard’s assertion. In fact, it suggests the opposite—that Broussard knew what was going on.

In this problem, Heesham Broussard obtained counterfeit money instruments. To distribute the items, he used FedEx account information and numbers misappropriated by hackers. Broussard’s text messages indicated that he had participated in an earlier, similar scam. Further, the messages showed that he knew the packages would be delivered only if the FedEx accounts were “good.” Charged with identity theft, he argued that the government could not prove he knew the FedEx accounts belonged to real persons or businesses. His text messages, however, indicated the contrary. A judge or juror could infer from these statements that he knew the packages would not be delivered successfully unless the account information and numbers belonged to real customers.

From an ethical perspective, it does not matter whether Broussard knew that the accounts belonged to real customers. And it does not matter whether he knew the owners of the accounts, whether they knew him, or whether the accounts belonged to persons or businesses. Broussard committed a crime. An accompanying violation of any standard of ethics is certain. Here, he acted dishonestly, with fraudulent intent, misrepresenting himself as the authorized sender of FedEx packages filled with counterfeit money instruments.

In the actual case on which this problem is based, the court convicted Broussard of the charge of identity theft. The U.S. Court of Appeals for the Fifth Circuit affirmed the conviction, responding to his argument on appeal according to the reasoning stated above.

1. Assuming that FedEx knew its customers’ account information had been compromised, use the IDDR approach to consider whether the company had an ethical obligation to take steps to protect those customers from theft.

Solution

The conclusion seems foregone—if FedEx knew that its customers’ account information had been compromised, the company had an ethical obligation to take steps to protect those customers from theft.

The first step of the IDDR approach is an Inquiry—identify the issue, the stakeholders, and ethical standards. In the facts of this question, hackers stole the account information of FedEx customers. Was FedEx obligated to act to protect those customers from theft? Besides those customers and FedEx, the stakeholders could include the owners and employees of the company, as well as the society as a whole. Relevant ethical standards could derive from the company’s policies, or from religious, philosophical, or other standards. These would include such general principles as acting for the benefit of the most people.

The second step of the approach is a Discussion to analyze actions that might address the issue. Factors include the strengths and weaknesses of those actions, considering their consequences and the effects on stakeholders. To protect against theft through the use of stolen account information, FedEx might have to do as little as assign its customers new account names, numbers, or passwords. If the information could be used for illicit purposes other than fraudulent delivery charges, FedEx could notify its customers, publicize the theft, and alert law enforcement. The company might offer to pay to monitor victimized customers’ credit information. None of these actions would seem to be weak or costly, and their results and effects could be almost entirely beneficial—customers might feel protected, society’s interest in the reliability of FedEx accounts could be reassured, and the owners and employees of the company might believe more strongly in its continued success.

The third step of the IDDR approach is to make a Decision and state the reasons. The decision is clear—FedEx should act to protect its customers and the other stakeholders. The actions the company should take include those discussed above. The reasons for this conclusion are also stated above—to benefit those customers, the owners and employees of the company, and the public generally. This would further assure these stakeholders of the commitment of the firm to the continuing viability of its business.

The final step of this approach is a Review to weigh the success or failure of the action to resolve the issue, and satisfy the stakeholders. According to the facts, FedEx policy is to deliver packages only if an account is “good.” Thus, if FedEx were to take the steps indicated above, its actions would likely prove successful. The stolen data would not be able to initiate FedEx deliveries, and would become potentially useless for almost any other purpose. These results could satisfy all of the stakeholders.

Critical Thinking and Writing Assignments

1. **Critical Legal Thinking.** Ray steals a purse from an unattended car at a gas station. Because the purse contains money and a handgun, Ray is convicted of grand theft of property (cash) and grand theft of a firearm. On appeal, Ray claims that he is not guilty of grand theft of a firearm because he did not know that the purse contained a gun. Can Ray be convicted of grand theft of a firearm even though he did not know that the gun was in the purse? Explain. (See *Types of Crimes*.)

Solution

No. A separate crime occurs only when there are separate distinct acts of seizing the property of another. In the circumstances described in the question, Ray committed the crime of grand theft because of the value of property in the purse, including the value of the gun. Only one crime of theft occurred, however. Ray saw the purse and took it without know­ing what it contained: there was one intent and one act.

1. **Time-Limited Group Assignment—Cyber Crime.** Cyber crime costs consumers millions of dollars every year. It costs businesses, including banks and other credit card issuers, even more. Nonetheless, when cyber criminals are caught and convicted, they are rarely ordered to pay restitution or sentenced to long prison terms. (See *Cyber Crime*.)
2. One group should formulate an argument that stiffer sentences would reduce the amount of cyber crime.

Solution

It goes without saying that the higher the anticipated cost of engaging in cyber crime activity, the lower will be the amount demanded. In other words, heavy fines and long jail sentences would have some deterrent effect. The real question is by how much. Many hackers who bring down corporate and government computer systems are teenagers. They cost businesses billions of dollars yet gain no monetary reward for their hacking—they do it to prove that they are as good or better than other hackers. If caught, they could not engage in much meaningful restitution to their corporate victims. In contrast, adult cyber criminals who engage in identity theft, credit-card fraud, and online auction fraud often make large sums of money from this criminal activity. They could be forced to engage in meaningful restitution to their victims. They could be sentenced to long jail terms, just as we routinely do for traditional thieves. Restitution and long jail terms might serve as a deterrent to such cyber criminal activities. U.S. authorities, though, cannot easily arrest, try, convict, and sentence cyber criminals living and operating in, say, Russia.

1. A second group should determine how businesspersons can best protect themselves from cyber crime and avoid the associated costs.

Solution

Protection against cyber crime starts with the awareness at management and staff levels of the potential harm that could result. Even the temporary loss of a system’s functions while its software is replaced due to a virus’s infection or other destructive event could prove costly. Thus, management should make appropriate funds available to pay for security, impose procedures to identify the system’s vulnerability, require the use of security hardware and software, and conduct security audits on an ongoing basis. The use of passwords among those with access to the system is also an important step when used correctly. Backed-up data can be key, and storing the backed-up data off-site can be even more effective.

1. A third group should decide how and when a court should order cyber criminals to pay restitution to their victims. Should victims whose computers have been infected with worms or viruses be entitled to restitution, or only victims of theft who have experienced financial loss? What should the measure of restitution be? Should large companies that are victims of cyber crime be entitled to the same restitution as individuals?

Solution

Cyber criminals could and should arguably be ordered to pay restitution to their victims whenever those persons or businesses suffer a financial loss. The victims whose computers are infected with worms or viruses most likely must pay for cleansing software or a security sweep, or more, to clear their data of the infections. Victims of theft of course experience financial loss.

The measure of the restitution might include the value of what was taken, the cost to recover it, the expense of repair, and the price of the investigation that it may have taken to discover the illegal breach.

There is no reason why large companies—such as Facebook, Apple, Netflix, or Alphabet—should not be entitled to the same restitution as other victims.