

Instructor Resource

Questions and answers for Security Guides, Ethics Guides, and So What Guides

Table of Contents

Security Guides.....	3
Chapter 1 - Password Etiquette.....	3
Chapter 2 - Evolving Security.....	4
Chapter 3 - Hacking Smart Things	5
Chapter 4 - Poisoned App-les	6
Chapter 5 - Big Data...Losses	7
Chapter 6 - From Anthem to Anathema.....	8
Chapter 7 - It's Not Me...It's You.....	9
Chapter 8 - Digital is Forever	10
Chapter 9 - Semantic Security	11
Chapter 10 - Exhaustive Cheating	12
Chapter 11 - Watching the Watchers	13
Chapter 12 - Psst. There's Another Way, You know.....	14
Ethics Guides	16
Chapter 1 - Ethics and Professional Responsibility	19
Chapter 2 - Big Brother Wearables.....	21
Chapter 3 - The Lure of Love Bots	22
Chapter 4 - Free Apps for Data.....	24
Chapter 5 - Querying Inequality	26
Chapter 6 - Cloudy Profit?	28
Chapter 7 - Paid Deletion.....	31
Chapter 8 - Synthetic Friends	32
Chapter 9 - MIS-Diagnosis	34
Chapter 10 - Securing Privacy	36
Chapter 11 - Training Your Replacement.....	38
Chapter 12 - Estimation Ethics	39
So What? Guides	42
Chapter 1 - A is for Alphabet.....	42
Chapter 2 - Augmented Collaboration	43

Chapter 3 - The Autonomous Race.....	44
Chapter 4 - New from CES 2016.....	45
Chapter 5 - Slick Analytics	46
Chapter 6 - Quantum Learning	48
Chapter 7 - Workflow Problems	49
Chapter 8 - Enhanced Golf Fan	51
Chapter 9 - BI for Securities Trading?.....	52
Chapter 10 - New from Black Hat 2015	54
Chapter 11 - Managing the IS Department	55
Chapter 12 - Banking on IoT	57

Security Guides

Chapter 1 - Password Etiquette

1. Here is a line from Shakespeare's Macbeth: "Tomorrow and tomorrow and tomorrow, creeps in its petty pace." Explain how to use these lines to create a password. How could you add numbers and special characters to the password in a way that you will be able to remember?

There are several correct ways to create a password from this line. One way might be to take the first letters from each word. The password would then be "tatatciipp". You could then capitalize a couple of the letters and add in a special character or numbers. The resulting password could be "T&2morrow&tciiPP". This would be a very secure password.

2. List two different phrases that you can use to create a strong password. Show the password created by each.

There will be many correct answers to this question. Using a passphrase to create a password is done by using the first letters in the phrase. Then changing some of the letters by substituting in special characters, numbers, or changes of case. For example, the phrase, "I never count my chickens before the eggs have hatched!" could create the password "iNcmCHKNSb4t3ggsHH!" This would be a great password.

3. One of the problems of life in the cyberworld is that we all are required to have multiple passwords—one for work or school, one for bank accounts, another for eBay or other auction sites, and so forth. Of course, it is better to use different passwords for each. But in that case you have to remember three or four different passwords. Think of different phrases you can use to create a memorable, strong password for each of these different accounts. Relate the phrase to the purpose of the account. Show the passwords for each.

There will be many correct answers to this question. For example, a passphrase for a university account may look something like, "I will graduate from state university before 2020 or bust!" This could yield a password that would look like "IwgfSub42020ORB!"

4. Explain proper behavior when you are using your computer and you need to enter, for some valid reason, another person's password.

In this case, say to the other person, "We need your password," and then get out of your chair, offer your keyboard to the other person, and look away while she enters the password. Among professionals working in organizations that take security seriously, this little "do-si-do" move—one person getting out of the way so another person can enter her password—is common and accepted.

5. Explain proper behavior when someone else is using her computer and that person needs to enter, for some valid reason, your password.

If someone asks for your password, do not give it out. Instead, get up, go over to that person's machine, and enter your own password yourself. Stay present while your password is in use, and ensure that your account is logged out at the end of the activity. No one should mind or be offended in any way when you do this. It is the mark of a professional.

1. This guide emphasizes how information security strategy has changed over the past two decades due to advancements in technology. What do these changes mean for you personally in managing and securing your own personal systems and data?

Private technology users encounter the same types of risks that companies encounter. If your tablet or smartphone is lost or stolen, the data on those devices can be compromised with minimal effort. If you happen to use Dropbox, this means that all of your personal photos, documents, financial statements, and even tax returns may be accessed by a third party. Furthermore, if you are tech savvy and happen to have a VPN set up to your home network, nefarious actors could access systems and other devices on your home network.

2. Take a few minutes to conduct an Internet search on insider threats. Besides some of the high-profile cases of employees stealing and selling or distributing corporate data, what other examples can you find?

Students will find a vast array of examples based on their search terms. The key point of this question is to help students recognize that insider threats are common and that the risks associated with insider threats are severe.

3. What kinds of collaboration tools have you used to complete class assignments and projects? Could these collaboration tools pose a risk to you? How?

Students have likely used file-sharing software like Dropbox to compile and access team resources. Dropbox users often forget to end shared access to folders and files when the project ends and thereby leave vulnerabilities open to any device linked to their Dropbox account if a former collaborator were to upload a malicious file. Students have also likely used Google Docs – other team members can easily access information shared in a Google Doc and disseminate that information to other friends or teams without the consent of the content creator.

4. How do you feel about the trend of companies using new technologies to monitor their employees? Would you want to work for a company that uses monitoring technologies? Why or why not?

The response to this question is clearly subjective and student responses will be mixed. Some students will likely encourage any measure that can be taken to secure the systems and data at their place of employment while others will consider these technologies an invasion of privacy.

5. Monitoring digital activity is not exclusive to the workplace. Internet service providers monitor your Web traffic and many Web sites monitor everything that you do while interacting with their site. What does this mean for users working from home? How might an ISP's monitoring activities be a threat to corporations?

The main tension in information security used to be between security and accessibility. Today a new tension between security and privacy has emerged. Privacy is clearly being sacrificed in most digital environments and the implications of this trend are difficult to quantify. Privacy will be a perpetual issue as technology continues to become more and more pervasive over time.

1. How many devices in your home are connected to the Internet? How much time do you spend daily, weekly, or monthly trying to ensure that these devices have the latest software and/or are secure? Think about the implications of maintaining dozens of devices with Internet access.

Managing the information systems infrastructure at a large business or government agency takes a tremendous amount of time and effort. It can be equally inconvenient for a homeowner to ensure that the operating system and software on a few home computers is up to date and patched. Managing a household of dozens of Internet-connected devices could prove to be the biggest hurdle inhibiting people from protecting themselves from any number of threats that could occur with a home filled with Internet-connected devices.

2. The article discusses the potential threat of a hacker accessing a vehicle and downloading data about the car's performance and operations. Aside from a malicious hacker acting alone, are there any businesses or government agencies that could also benefit from accessing these data?

A number of government agencies have been found to be collecting data and spying on American citizens without the proper authority. It is possible that as more and more devices have Internet access, intelligence agencies can take advantage of these devices and raise their intelligence-gathering operations to an even more pervasive level. On the business side, car insurance companies could be tempted to illegally access the data stored in vehicles to learn more about how the drivers they are covering are operating their vehicles, and potentially change insurance premiums for drivers who are operating their vehicle in a manner that introduces higher risk and thus higher likelihood of a claim.

3. How has this article changed your perception of the Internet of Things? Are you still willing to risk invasions of privacy or security vulnerabilities for convenience or to have "cool" new gadgets?

This is a subjective question – student responses will vary.

4. The Internet of Things is not solely focused on home automation or private consumer products. Businesses are using the Internet of Things to manage supply chains and streamline various business processes. What benefits or risks are associated with businesses adopting new Internet-connected devices?

As businesses have access to more and more data about supply chains and other important processes they can mitigate demand-forecasting risks like the bullwhip effect by more accurately managing the flow of resources in the supply chain. In the age of the Internet of Things, shipping containers and even individual products can be tracked around the globe in real time. However, as any device with an Internet connection can be compromised, competing firms could access shipping and other supply chain information to learn more about competitors' business processes and raw material flows to anticipate the supply of competing products. This concern is not far-fetched as companies regularly hack into the information systems of competitors to steal intellectual property.

1. Think about your use of various phone and computer apps and your interactions on social media. Have you ever experienced a breach of your privacy or personal data? What was the impact of this breach? Were you able to resolve it or were you forced to live with the consequences?

The response to this question clearly depends on the previous experiences of students in the class. While it is likely that a handful of students will have had some sort of privacy violation, be sure to call on students who are clearly comfortable sharing their experience.

2. Try to identify three different strategies that any smartphone user could follow in an attempt to minimize the risk of installing and using dangerous/risky apps.

(1) Users can avoid downloading apps with poor reviews and complaints about the functionality; these apps may be designed specifically for the purposes of accessing data and sharing it with 3rd parties. (2) Pay close attention to usage agreements when downloading new software/apps. (3) Avoid free apps as there are usually hidden costs. (4) Remove any apps on your phone that you are no longer using; there is no reason to jeopardize your data and privacy for an app that is providing no benefit to the user. (5) Carefully manage app settings on the device. (6) Monitor tech news or Twitter feeds to stay on top of announcements concerning compromised or dangerous pieces of software.

3. Reflect on the tradeoff between free apps and the potential privacy risks that these apps may introduce. Has this article changed your perception of free apps and will you continue to download these apps in the future?

The response to this question is clearly subjective in nature but can be used to generate a discussion in the class. Some students will likely express their concern and will be more hesitant when downloading apps while others will not alter their behavior. Use these varying opinions as an opportunity to demonstrate how differently people think about and approach securing their data/systems.

4. Conduct an Internet search to identify if there have been any recent security vulnerabilities introduced through app stores. If so, conduct a brief investigation to see which apps are involved, how many people have been impacted, and whether or not the vulnerability has been resolved.

The outcomes of these searches will depend on current events. If there have not been any recent incidents, this can be used as an indication of how hard Apple and other companies are working to avoid tarnishing their brand and reputation.

1. Take a moment to think about how the trend of capturing and storing data has impacted you. What types of data have been generated about you and where are these data located? What data have you generated yourself? Can you do anything to manage access to or the security of these data?

The bulk of data generated by a college student will be in social media. This is a great opportunity to point out that comments, photos, and videos uploaded by students to social media platforms will likely remain on the Internet forever. Other data points will include articles about sports or fine arts accomplishments in high school, medical data kept by doctors and hospitals, etc. The reality is that system/social media platform users can often do very little to manage the security and access to their own data; we simply have to trust the personnel managing those systems to ensure that our data are protected.

2. Search the Web to identify new data-driven applications that Watson is being used for as IBM continues to leverage and market the power of this supercomputer.

Even a casual search will reveal that Watson is being used or considered for countless applications. Students will find examples of everything from health and business applications to fantasy football and even cooking. This question should generate some interesting discussions on the power of big data and how technology and the big data movement can impact virtually every industry.

3. The article mentions the continuing technological tension between security and convenience. How has this tension impacted your own interactions with computers? Do you err on the side of security or convenience when creating and managing your own security “policies”?

The best example of how this tension plays out in the life of students will be the security policies of their university. Students have to create a password to access registration, tuition, and course content systems. They will also have to change their password somewhat regularly. These are basic security measures and are likely not very demanding. Regarding their own security “policies”, each student has to decide whether or not to password-lock their phone, if they use security on the WiFi in their apartment (and if so what type of security), and what privacy settings they will choose to use on social media sites.

4. Have you or anyone you know purchased home automation devices? Based on a lack of emphasis on security found in many of these devices, are you willing to risk security for the convenience that these devices provide?

Students will respond to this question differently depending on their interest in technology and their aversion to risk. Some students who are excited about technology, data, and automation will risk the security vulnerabilities of these devices for the sake of the “cool” factor or the convenience it provides. Other students may simply not care about gadgets or having access to data about household devices. An important point to make here is that there is a difference in how people perceive technology and that there will always be even a small subset of people who are willing to sacrifice security for the convenience or value technology can provide.

1. How vulnerable are you right now to having your data stolen? Think about all of the cloud services that you use.

There is no easily quantifiable metric to determine one's vulnerability to data theft, however, the more cloud services and online accounts a user has, the greater the chance that a user's data will be stolen in a future breach. Users should also keep in mind that lost or stolen devices can be used to steal data, too.

2. What are some of the ways that you can mitigate the negative outcomes of your personal data being stolen?

One of the best methods for mitigating the negative outcomes of data theft is awareness. Students should try to monitor current events to stay informed on data breaches and use credit monitoring services to make sure that stolen social security numbers are not used for criminal purposes. Students should also be judicious in choosing what data they store online, in deciding the types of online accounts that they will create and maintain, and whether or not they will encrypt files stored locally on their devices or encrypt files stored in the cloud.

3. The article explains how Anthem failed to encrypt account information thereby exacerbating the risk associated with customer records being stolen. What does it mean to "encrypt" data and do you know how easy or difficult it is for you to do?

Encrypting a file means taking plaintext and encoding it to create ciphertext. The ciphertext will be an unintelligible body of characters that can only be reversed back to meaningful plaintext using the encryption key. Encrypting files can be very easy to do. On a Windows machine, users can choose to encrypt all of the files placed inside of an encrypted folder. Users can also install AxCrypt, a free tool for easily encrypting files on a Windows machine.

4. How have prior data breaches impacted your consumer behaviors? Have you stopped shopping at Home Depot or Target because of their respective security breaches?

Student responses to this question will vary, but most students will likely report that they have not altered their online shopping or file management practices at all in response to high-profile security breaches (e.g., Target, Home Depot, and Anthem). A discussion based on this question would be an ideal time to encourage students to more closely monitor their online activities and behaviors in order to avoid becoming a victim of a future data breach.

5. How can having a higher awareness of security best practices, and a habit of monitoring security breaches, help you when you get a job?

Data is now one of the most valuable assets possessed by corporations. If you can demonstrate to employers that you are a security-conscious individual, you will likely be perceived as a valuable asset to your organization. People are often perceived as being one of the most vulnerable areas of a company's security policy – if you can demonstrate that you are one less thing for security professionals at your company to worry about, you will have a competitive advantage over your peers!

1. Have you ever witnessed someone stealing something at work? If so, it was probably very apparent to both you and the perpetrator that they were doing something wrong. Why do you think employees are so willing to steal data when they would be unlikely to steal tangible items like laptops or other expensive organizational assets?

Based on the discussion in the article of the white-collar crime triangle, many people cannot rationalize stealing tangible property from a company (e.g., a laptop) as it is clearly a crime. However, the value of data can be very difficult to quantify and in many cases certain types of data may appear to have no inherent value at all (or a person can rationalize that the data have no value). Furthermore, the information age continues to be plagued from a legal standpoint in that there is a lack of legal precedent for so many different types of “digital” activities. For example, it is very difficult to prosecute someone for threatening someone on social media as laws have not been created yet for many types of behaviors that would be considered crimes not committed in a digital context.

2. Take a moment to search the Internet for cases of white-collar crime. Find a specific example and see if you can identify the three elements of the white-collar triangle as being factors that contributed to that crime being committed.

Students will likely identify a variety of white-collar incidents which have occurred and been reported in the popular press. It should be fairly easy to identify the pressure (the person needed the money) or rationalization (they developed the IP for a product or everyone else in the department got a bonus but the perpetrator did not and felt that they deserved one...).

3. How do you feel about the fact that many companies are investing in tools to monitor employee behavior? Would you want to work for a company that audits email logs and analyzes your activity on the company's network?

Students will have different opinions on this question based on their personal feelings about privacy and employee monitoring. This is yet another example of the tension that occurs between those who want more security for the greater good and are willing to sacrifice individual privacy versus those who feel that personal privacy should not be infringed upon for any reason.

4. The article mentions that encryption can be a tactic used to thwart employees from taking data with them. Explain how encryption can be used effectively in this context.

Encryption can be used to render data inaccessible if it is taken off of a given machine and accessed elsewhere (e.g., refer to the encryption tools offered in the Windows operating systems). In this context, data can be encrypted on company servers so that it is accessible to employees but not accessible if it is removed off of those systems. Setting up this type of encryption could reduce the motivation and likelihood that an employee would try to steal data and use it to secure a job elsewhere.

1. The article emphasizes that criminals and corporations both seek out the private information of Internet users for their own gains, but they are not the only ones trying to access your information. Do you think universities or future employers will attempt to access information about you when making admissions or hiring decisions?

Absolutely – there are reports in the popular press almost weekly about how employers and universities are trolling social media sites attempting to learn more about their applicants and the information gleaned from these efforts is often used to aid in making acceptance/rejection decisions. The purpose of this question is to help students recognize that privacy concerns are not centric to theft or commercial purposes, but are much more pervasive than many students may initially recognize.

2. You likely heard news reports about the iCloud and Sony breaches, both of which resulted in private photos and emails being shared with the masses on the Internet. However, can you recall hearing reports about the perpetrators being brought to justice? If not, why do you think this is the case?

To date there has been no indication that the perpetrators of either breach have been arrested or subsequently brought to justice. Aside from the fact that cyber criminals can be extremely difficult to track down, the legal system is still in many ways ineffective against the types of crimes that are perpetrated in cyberspace. For both of these reasons, many cyber crimes go unpunished, thereby yielding a forum rich in opportunities and thus very attractive to cyber criminals.

3. The Internet is not the only medium by which your privacy can be breached. Stolen or compromised devices can also be used to access your information, even if that information has been deleted. Search the web for information about recovering files and find out (1) whether or not deleting a file actually eliminates it from the memory of your device, and (2) if it can be recovered.

Tangible devices also present a medium by which privacy can be violated. When users delete a file on a computer many think that the file is permanently gone, but in actuality, the computer simply deletes the file pointing to that data on the hard drive but the data actually remain. File recovery programs, many of which are free and easy to operate, can be used to scan hard drives and recover files that have been “deleted” but not permanently removed from the hard drive. File shredding utilities can be used to scramble free space on hard drives thereby rendering data formerly stored on the drive extremely difficult to recover.

4. Take a few minutes to reflect on your online habits. Do you have a tendency to send emails or post messages or images that could be perceived as offensive, inflammatory, or controversial in nature to others? If so, what could the end result of this behavior be?

The end result of such behavior could be more far-reaching than students initially think. Building on the answer to Question 1, poor behavior on the Internet can negatively impact any number of future opportunities or relationships, and all users should recognize that simply deleting content on a social media site does not actually delete that information forever. It is possible that this information could be recovered, accessed, and distributed online at some point in the future.

1. In your own words, explain the difference between access security and semantic security.

Access security concerns the authorized and authenticated control of access to data, systems, and networks. Semantic security concerns the unintended release of protected information through the release of a combination of reports or documents that are independently not protected.

2. Why do reporting systems increase the risk of semantic security problems?

Reporting systems increase the risk of semantic security problems because information from two different reporting systems can be combined with publicly available information to produce, or calculate, confidential information. This is a semantic security problem.

3. What can an organization do to protect itself against accidental losses due to semantic security problems?

To protect themselves from accidental data losses, organizations should only release information to employees if it is necessary for them to complete their jobs. They also need to be more consistent about labeling confidential information, and labeling personally identifiable information that could be used to “triangulate” other data from outside information sources.

4. What legal responsibility does an organization have to protect against semantic security problems?

Organizations have a legal requirement to protect personally identifiable information (PII) they collect. Additional requirements apply to financial, medical, and tax (just to name a few). Organizations must keep information secure when it is being stored, processed, or transmitted.

5. Suppose semantic security problems are inevitable. Do you see an opportunity for new products from insurance companies? If so, describe such an insurance product. If not, explain why.

An organization like an insurance company may be interested in accessing multiple data sources to help estimate an individual’s likelihood of making a claim. For example, they might want to correlate voting records with “anonymized” medical study data. This could yield information about potential clients that might be susceptible to certain expensive medical conditions. Conversely, an insurance company may offer an “information” product that protects clients from information triangulation. They could offer protection against a variety of information or identity theft incidents.

1. What other technologies now included in cars could pose a potential risk to users? Based on the Volkswagen incident, are the technological advancements we have seen in the automotive industry worth these risks?

A new technology that is now prominently featured in car advertisements is Internet access. However, numerous studies have demonstrated that cars with such capabilities can be accessed and compromised remotely. For example, hackers have been able to demonstrate the ability to apply breaks, turn the stereo system on or off, and control other functions within the car without any direct access to the vehicle. This type of vulnerability would not be possible without the proliferation of computers in almost every aspect of a car's operations. The value of increasing computer use in cars' operations, versus the risks, is a subjective point that each student will likely perceive differently.

2. The article introduces the term "black box". Take a few minutes to brainstorm other examples of systems or technologies that could be considered a black box. Try to identify some of the risks that may exist due to our inability to understand how these systems operate.

The technology used to manage the stock market is a perfect example of a black box. Very few people understand the technical components involved in managing all of the digital trading that takes place every day. A book was published several years ago (*Flash Boys*) which argued that the stock market is rigged because heavy-hitting trading firms were paying for maximized transaction speeds and taking advantage of their rapid access. This lack of understanding of exactly how the trading system functions is a great example of a black box.

3. Aside from tarnishing Volkswagen's brand, the company experienced a substantial decline in its stock price. Why do you think the stock price dropped so significantly even though it is a global brand with popular vehicles?

One of the biggest drivers of Volkswagen's plunging stock price is the uncertainty regarding the potential cost of recalling ~11 million vehicles. Simply overwriting software for these vehicles to eliminate the "cheating" code would be time consuming and costly in its own right. However, if mechanical parts of the car need to be modified or replaced, such a recall could pose a tremendous financial imposition on the company and jeopardize its financial viability.

4. Do you side with Elon Musk and Stephen Hawking and thus consider super-advanced AI systems to be a potential threat? Alternatively, are you skeptical that computers will ever have the capability to pose any form of risk to end users? Be ready to explain your position.

Students' opinions on the potential threat of AI will vary. This question is intended to promote a lighthearted yet curiosity-inducing discussion on the potential AI capabilities of future systems. This is also a discussion in which IBM's Watson can be discussed as it is currently one of the best examples of AI being used for a variety of positive applications.

1. The article discusses the use of security audits to ensure that employees are not doing anything that they should not be doing on their employer's systems. In what other contexts are audits conducted?

Audits can be used in virtually every industry. Students will likely identify accounting as the most common application of audits as accounting auditors work to make sure that a company's financial records are accurate. These audits can be further categorized into specialized audits, including financial, compliance, operations, investigative, and information systems. However, any type of organization can conduct an audit to ensure that the subject matter is free of misstatement. Even research can be audited to ensure that data reported in a journal paper are not fabricated or tampered with.

2. Define what a rootkit is and conduct a search online for examples of how rootkits have been used.

Rootkits are malicious pieces of software that are used to gain unauthorized access to another system or piece of software. Rootkits are often the basis for security breaches – a quick search of the Internet will likely identify numerous breaches in which rootkits were used to gain access to a corporate server or other type of system.

3. One strategy for preventing IT employees from violating their extensive system access is 'separation of duties'. Can you think of any other examples of how a function or task is split into multiple pieces or assigned to multiple individuals to prevent abuse of that function?

We can look to the military for numerous examples of separation of duties. Weapon systems are often broken into numerous components with various operators controlling the disparate modules of the system. For example, on a nuclear submarine, launch codes to deploy weapons requires authorization from numerous individuals. This serves as a safety mechanism to prevent one individual from initializing a weapon without proper authorization.

4. Take a moment to think about all of the different types of devices that you use on a daily basis. How could these devices be compromised to invade your privacy? Is this risk of privacy invasion enough to make you stop using these devices?

Looking around a random house or apartment would probably reveal numerous technologies that could be used to invade privacy. Web cameras or baby monitors designed to keep an eye on members of the family can be hacked or more easily accessed if the user does not change the default security settings. New gaming consoles have built in microphones that are in standby mode continuously waiting for the voice prompt of a user to activate the system; if accessed by a nefarious actor these microphones could be used for other purposes. Cellphones can also be compromised and people carry these devices with them everywhere; as cameras and microphones are ubiquitous on these devices they present a potential attack vector for invading privacy. The question students will have to consider: are they willing to forego the benefits these devices provide to ensure the protection of their privacy? Responses will vary.

1. If, in your absence, your roommate opens your desk and eats the top layer of your 2-pound box of chocolates, you'll know it; at least you'll know they're gone. But, if in your absence, your roommate uses your computer to copy your MIS term project onto his flash drive, do you know? If so, how? If not, why not?

It's very unlikely that a student would notice if a file was copied from their computer. It's possible that they could have turned on security logging for computer access. Some operating systems (like Windows) do have this feature. Others may not. Then the student would have to check the logs regularly for unauthorized access. It's possible that the student may remember the exact time he was out of the apartment and notice the intrusion. That, of course, assumes that the student locks his or her computer each time they walk away from it. Many people don't lock their computers when they walk away from them because they assume they are in a safe place.

2. Of course your roommate wouldn't steal your term project. So, instead, suppose the person across the hall obtains the name of your computer and your logon name (the name you enter when your computer starts). She could surreptitiously watch you enter your password and learn it, too. But let's say instead that she notices the 75 pictures of your family basset hound, Fido, taped to your desk and correctly guesses that your password is Fido. With that data and a little knowledge, she uses your dorm's network to access shared folders on your computer from her computer. (Search the Internet for How to share a folder in Windows (or Mac) if you don't know what shared folders are.) When she finds your MIS term paper in one of your shared folders and copies it to her computer, do you know? Why or why not?

For the same reasons listed in the question above, without turning on security logging and checking logs regularly it's nearly impossible to detect this type of intrusion. In this case the student might have an intrusion detection system, or a data loss prevention (DLP) system running to catch these types of unauthorized actions, but this is very unlikely.

3. How does the situation in question 2 differ from packet sniffing? What's required for her to steal your paper from a shared folder? What's required to steal that paper using packet sniffing? Which is easier?

The situation in question 2 differs from packet sniffing in that situation 2 is the unauthorized access of a file stored on a file share, whereas packet sniffing is a type of man-in-the-middle attack where data are intercepted as they are being sent over a network. To steal the file from the shared folder the attacker would need authorized credentials, or use automated software that can take advantage of a vulnerability in the computer hosting the file. To steal the paper using packet sniffing the attacker would have to have access to the network where the packet was being sent from, and the data connection would have to be unencrypted. Currently, it's probably easier to steal from a shared network location because most data connections are now encrypted. This makes it difficult, but not impossible, to steal data being sent over networks.

4. As a student, you're unlikely to share many folders, but once you start work, you're likely to do so. Is the scenario in question 2 possible at work? Does it matter if your employer has strong network security? What is the one thing you can do to protect yourself from the person in the cubicle down the hallway accessing your shared folders?

Yes, the situation in question 2 is likely in a work environment. Yes, if your employer has strong network security it would be much more difficult, but not impossible, to steal the file. Strong network security would be able to see who was accessing which network shares, and monitor the movement of data files. To protect yourself from these types of attacks you should encrypt your files, share your file shares with as few people as possible, and make sure your file shares are secured with strong credentials.

5. Now consider the suppliers in this guide who had their designs stolen. Will they know their designs were stolen? How will they find out? How will they know which designs were taken? How can they assess their damages?

It's unlikely they will immediately know their files were stolen. They may find out their files were stolen after the fact when a competitor produces a similar part without any research and development expenditures. It's unlikely they'll know exactly which files were taken. They'll be forced to assume that all related files were taken. It will also be extremely difficult to access the damages of this data loss. If the files were key to their competitive advantage the loss of these files could be catastrophic.

6. It's possible for companies to configure their network so that email can only be sent to their own Internet service provider. Such a configuration would thwart the ACAD/Medre.A worm, and indeed it did, for all the companies that had such security. Companies with large, knowledgeable IS departments (see Chapter 11) most likely will, but in this case hundreds did not. If you're the owner of a small business, what can you do?

For small businesses with limited in-house technical expertise, the best option might be outsourcing their email function to a managed service provider. Many managed service providers offer very reasonable rates for managing corporate email. They also have the technical expertise to stop these types of attacks.

7. Search the Internet for the term industrial espionage. Find one example of espionage that has been conducted using malware. Summarize the problem and the damages. What could the companies involved have done to avoid losses?

Student responses to this question will vary. There are many examples of corporate espionage using malware. One famous attack occurred in 2013 when hackers stole nearly 70 million of customer accounts from Target Corp. using custom malware. The malware was used to copy customer account information from point of sale (POS) systems and then send it to external servers. This information was later sold and netted hackers between \$20M and \$50M.

Ethics Guides

Overview: Goals and Two Ethical Theories

The ethics guides in early editions of this text relied on the students' applying a personal ethical standard. Over time, it became clear that this reliance was ineffective because too many students find just about anything plausibly ethical. However, if we try to insert our own ethical standards into the discussion we become 'Preachers' and the discussion devolves into telling students what they should believe. That's hardly teaching.

This text is for use in an MIS course and it is inappropriate to address the same issues, at the same depth, that the business ethics course teaches. We need a brief form of solid ethical theory for use as a standard.

Accordingly, we consulted a colleague, Charles Yoos, emeritus professor of the U.S. Air Force Academy and one of the key thinkers regarding the use and evolution of the honor codes at the U.S. military academies. Dr. Yoos has taught business ethics for several decades and we asked him "If you had only 30 minutes to describe two useful ethical theories, ones that could be used in business practice, what would those theories be?" Dr. Yoos' response was a) Kant's categorical imperative and b) Bentham and Mills' Utilitarianism.

Armed with that guidance, we re-wrote all the guides from prior editions to use these theories. Our goal is to layout the principles of the theories and then ask the students to use those theories as criteria for making ethical assessment. In this way, students will be forced to view ethical issues more broadly and from a more mature perspective. Chapter 1 introduces Kant's Categorical Imperative (CI) and Chapter 2 introduces utilitarianism.

As a bonus, we can use Kant's theory of imperfect duties as a way of also teaching social responsibility. This is done in later chapters, once students have had a chance to use CI's perfect duties and utilitarianism.

Kant's Categorical Imperative

Immanuel Kant defined *categorical imperative* as the principle that *one should behave only in a way that one would want the behavior to be a universal law*. Stealing is not such behavior because if everyone steals, nothing can be owned. Stealing cannot be a universal law. Similarly, lying cannot be consistent with the categorical imperative because if everyone lies, words are useless.

When asking whether a behavior is consistent with this principle, a good litmus test is "Are you willing to publish your behavior to the world? Are you willing to put it on your Facebook page? Are you willing to say what you've done to all the players involved?" If not, the behavior is not ethical, at least not in the sense of Kant's categorical imperative.

Kant defined *duty* as the necessity to act in accordance with the categorical imperative. *Perfect duty* is behavior that must always be met. Not lying is a perfect duty. *Imperfect duty* is action that is

praiseworthy, but not required according to the categorical imperative. Giving to charity is an example of an imperfect duty.

Kant used the example of cultivating one's own talent as an imperfect duty, and we can use that example as a way of defining professional responsibility. Business professionals have an imperfect duty to obtain the skills necessary to accomplish their jobs. We also have an imperfect duty to continue to develop our business skills and abilities throughout our careers.

Students sometimes mistakenly equate the categorical imperative with the Golden Rule ("Do unto others as you would have them do unto you."). The two differ because the Golden Rule injects subjectivism into ethics. If I happen to not be bothered by some behavior (even though most would consider it highly unethical), then the Golden Rule is too loose. On the other hand, if I'm a guilt-induced fanatic, finding people who, say, jaywalk as unethical, then it may be too restrictive to be a general rule.

Utilitarianism

In brief, the principal guideline for utilitarianism is "Does the act result in the greatest good to the greatest number?" This is not, by the way, the same as saying, "Does the act avoid the most pain for the most people?" (A difference worth discussing with the students.)

One of the problems of utilitarianism is that human rationalization is so flexible that it seems possible to use it to justify about anything, if one is willing to work hard enough at the justification. This characteristic can be used with students, however, to flesh out lots of different perspectives about an act in class discussions.

We posed the problem of using utilitarianism to justify anything to Dr. Yoos and he replied that it's a calculation, not unlike cost-benefit analysis. His full response was:

Here is Bentham's poetic version of the dimensions of a utilitarian "calculation":

"Intense, long, certain, speedy, fruitful, pure—

Such marks in pleasures and in pains endure.

Such pleasures seek, if private be thy end:

If it be public, wide let them extend.

Such pains avoid, whichever be thy view:

If pains must come, let them extend to few."

Thus, criteria to consider are:

1. Intensity

2. Duration

3. Certainty or uncertainty

4. Propinquity or remoteness

5. Fecundity

6. Purity

From time horizon to span of effects, I agree that it may be problematic and opportune. Nevertheless, don't businesses still do cost-benefit analyses, albeit with more narrow scope? Perhaps what I'm thinking, "because we can't do it perfectly means we can't or shouldn't do it?" Of course, it must be addressed genuinely, sincerely, forthrightly, with no attempt to "rationalize" an outcome already preferred on perhaps personal, selfish grounds.

Additionally, we have found it worthwhile to juxtapose utilitarianism with Kant's categorical imperative. Often Kant's perspective is more conservative, but not always, as students will see in different Ethics Guides in the chapters that follow. A corollary for the categorical imperative is sunshine: Are you willing to tell everyone involved exactly what you're doing? (The converse isn't true, however. There can be times when you don't tell others what you're up to because of legitimate proprietary interests.)

Unlike the categorical imperative, utilitarianism will often bring the various players in the matter to light, and then sunshine can be used to ask, "Are you willing to tell them?" If not, and if not to protect proprietary data, your action is possibly not for the greatest good to the greatest number.

By the way, many flavors of utilitarianism exist that differ on whether it is the intended consequences or the actual consequences that matter in judging ethics.

One last observation: Using both perspectives together may raise inconsistencies and lead away from any definitive answer, which will drive some students crazy. I think their response is just a signal of their current level of cognitive development, and their frustration leads to richer learning, or at least it can. Sometimes it is worthwhile to have the more mature thinkers in the class explain, in their own words, that often there isn't one single answer to a question, and quite often that's beneficial, if confusing.

1. Restate Kant's categorical imperative using your own words. Explain why cheating on exams is not consistent with the categorical imperative.

Immanuel Kant defined *categorical imperative* as the principle that *one should behave only in a way that one would want the behavior to be a universal law*. Cheating is not such behavior because if everyone cheated, exams and school would be worthless. Learning could not be measured, and the value of school would approach zero. Cheating cannot be a universal law. Similarly, lying cannot be consistent with the categorical imperative because if everyone lies, words are useless.

2. While there is some difference of opinion, most scholars believe that the Golden Rule ("Do unto others as you would have them do unto you.") is not equivalent to Kant's categorical imperative. Justify this belief.

Students sometimes mistakenly equate the categorical imperative with the Golden Rule ("Do unto others as you would have them do unto you."). The two differ because the Golden Rule injects subjectivism into ethics. If I happen to not be bothered by some behavior (even though most would consider it highly unethical), then the Golden Rule is too loose. On the other hand, if I'm a guilt-induced fanatic, finding people who, say, jaywalk as unethical, then it may be too restrictive to be a general rule.

3. Using the Bateson definition (discussed in Q5) that information is a difference that makes a difference:
 - a. Explain how the features of the graph in Figure 1 influence the viewer to create information.

The features in the graph in Figure 1 make it look like there was a huge increase in units sold without any labels on the vertical axis. The difference in the graph makes the reader think there was a substantial increase in sales. However, the difference did not make a difference. The manipulation of the scale could cause the reader to create misleading information.

- b. Explain how the features of the graph in Figure 3 influence the viewer to create information.

The features in the graph in Figure 3 are drawn to scale. Properly scaling of the vertical axis influence the viewer to think that the number of units sold did not increase. The graph of the units sold looks flat.

- c. Which of these graphs is consistent with Kant's categorical imperative?

Kant's categorical imperative states that one should behave only in a way that one would want the behavior to be a universal law. In other words, are you willing to tell everyone involved exactly what you're doing? In this case, the manipulation of the scaling would likely be perceived as deceptive by the executive committee. If you had to tell the executive committee that you intentionally rescaled the axis to show an increase in units sold, they would perceive this as unethical behavior. Figure 3 would be consistent with Kant's categorical imperative.

4. Suppose you created Figure 1 using Microsoft Excel. To do so, you keyed the data into Excel and clicked the Make Graph button (there is one, though it's not called that). Voilà, Excel created Figure 1 without any labels and drawn out of scale as shown. Without further consideration, you put the result into your presentation.

a. Is your behavior consistent with Kant's categorical imperative? Why or why not?

Yes, this might be consistent with Kant's behavior because you didn't manipulate the scale, or notice that it was improper. It might be sloppy and careless, but not unethical.

b. If Excel automatically produces graphs like Figure 1, is Microsoft's behavior consistent with Kant's categorical imperative? Why or why not?

Yes, it probably is because Microsoft is open about its automatic scaling within charts and graphs. If they are willing to tell everyone involved exactly what they are doing, then it's ethical. It's the maker of the graph that is responsible to check for proper scaling.

5. Change roles. Assume now you are a member of the executive committee. A junior marketing professional presents Figure 1 to the committee, and you object to the lack of labels and the scale. In response, the junior marketing professional says, "Sorry, I didn't know. I just put the data into Excel and copied the resulting graph." What conclusions do you, as an executive, make about the junior marketing professional in response to this statement?

Student responses here may differ. The junior marketing professional could have just been sloppy in preparing the graphs. This would be an issue of competence. However, he or she may have also intentionally left out the vertical axis labels. Considering that labeling is default in Excel charts, it's more likely that he or she was malicious. But the executive might want to consider what's worse, being incompetent or malicious?

6. Is the junior marketing person's response in question 5 a violation of a perfect duty? Of an imperfect duty? Of any duty? Explain your response.

If the junior marketing person was just sloppy in the preparation of the graph, then it was a violation of an imperfect duty by not being more careful. If he or she was malicious and intentionally altered the labels, then it was a violation of a perfect duty.

7. If you were the junior marketing professional, which graph would you present to the committee?

Ethically, the Figure 3 would be the most accurate graph to show.

8. According to Kant, lying is not consistent with the categorical imperative. Suppose you are invited to a seasonal barbeque at the department chair's house. You are served a steak that is tough, overcooked, and so barely edible that you secretly feed it to the department chair's dog (who appears to enjoy it). The chairperson asks you, "How is your steak?" and you respond, "Excellent, thank you."

a. Is your behavior consistent with Kant's categorical imperative?

No, Kant's categorical imperative states that one should behave only in a way that one would want the behavior to be a universal law. In other words, should everyone say all bad food is good? No, if they did there would be a difference between good and bad food.