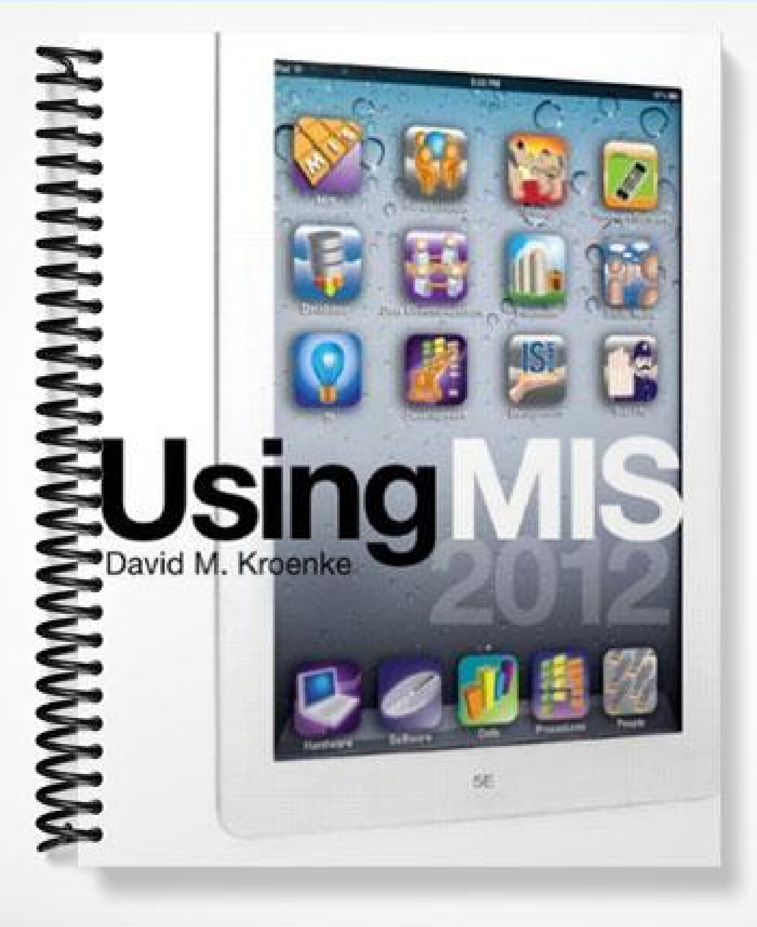
SOLUTIONS MANUAL



Using MIS 2012

David M. Kroenke

5E

TEACHING SUGGESTIONS

GearUp, Chapter 2

GOALS

Use GearUp to:

- Show a typical collaboration project in business.
- Illustrate a dysfunctional meeting.
- Demonstrate problems of irregular meeting attendance.
- Show some of the disadvantages of face-to-face meetings.
- Show some of the disadvantages of a group's use of email.

BACKGROUND

1. GearUp needs to find ways to reduce its operational expenses. Kelly has asked some of GearUp's key employees to identify ways of saving costs.
2. Felix has his own way of doing things and, if it isn't convenient to attend a meeting, he doesn't attend. That puts him behind the group's discussion, which aggravates the rest of the team.
3. This face-to-face meeting illustrates the need for collaboration IS . . . they need not meet face-to-face, nor even at the same time. An associate at Microsoft tells me that Microsoft has almost given up on face-to-face training for its employees. "It's not the expense. It's the fact that as soon as the training starts, someone's cell phone buzzes and that person leaves the room. They come back for 10 minutes and then it rings again." The scenario here illustrates that problem.
4. As discussed in the chapter, email is a poor way to share group results.
5. If they want, students can start gaining benefit from using collaboration IS with their teams in school, today! They don't have to wait until they enter business to do so.

HOW TO GET STUDENTS INVOLVED

1. Ask the students if they have attended student group meetings like this one. How have they responded? What do they do about a team member who doesn't attend the meetings?
2. Gross profit equals revenue minus costs. Felix wants to increase profit by increasing revenue; the team wants to focus on reducing costs.

   - **Is Felix's statement that if they could increase revenue they wouldn't need to save costs accurate? Why or why not?**
   - **Is the fact that Kelly told them to focus on costs persuasive?**
   - **Kelly fired Jennifer for not creating her own ideas. So, should the team show initiative and ignore what Kelly said about their task . . . should they focus on revenue increases rather than cost decreases? Why might this situation be different?**

3. Felix was unable to open the email attachment (if, in fact, he even read the email).

   - **Have you had this experience with your groups?**
   - **What does the text say about using email for groups?**
   - **What alternatives for sharing documents exist?**

4. Not all meetings need to be face-to-face.

   - **Does this team need to meet face-to-face? Why or why not?**
   - **Under what conditions are face-to-face meetings required?**

- Do your team meetings need to be face-to-face? Why or why not?
- What IS can you use for your student teams?

BOTTOM LINE

- Face-to-face meetings have serious costs. Requiring everyone to be at the same place at the same time is expensive and aggravating.
- IS can greatly facilitate virtual meetings.
- Possibly, your default should be that all meetings are virtual . . . only special meetings need to be face-to-face.

Using the Ethics Guide: Virtual Ethics? (pages 40–41)

GOALS

- Raise students' awareness to the possibilities of virtual-meeting spoofing.
- Ask students to assess their ethics about virtual-meeting spoofing.
- Address, as a class, the issue of cheating on online tests.

BACKGROUND AND PRESENTATION STRATEGIES

Virtual meetings are convenient, and they can be efficient. With virtual meetings, however, it is impossible to know that only authorized people are attending the meetings and that people are who they say they are. In most meetings, there is no deception, but the possibility exists.

I believe that any deception is a violation of a commonly accepted business code and is therefore unethical. I once had a professor perform a review of a text manuscript by giving the manuscript to his college-age daughter to read and comment upon. He made no indication that he did this. However, my editor followed up for clarification on several points, and the professor admitted that he had not read the manuscript. All of us felt deceived and cheated. Even though his daughter had made interesting and useful comments, the editorial team felt tricked and betrayed.

One could make the argument, however, that as long as the parties are better off, then spoofing is ethical. For example, if someone sends a better-qualified coworker to a virtual meeting, then one could argue everyone is better off because the team gains the expertise of the better-qualified worker. To me, though, the deception makes the action unethical.

Students should be aware that in virtual meetings everyone may not be who they say they are. Although I think actual spoofing is rare, I think it is common for people to silently attend meetings. On any conference call or multiparty chat session, students should learn to expect that there are unannounced people in the meeting.

■ **Never criticize anyone in a conference call or chat session. For all you know, that person may be in the meeting. Never give confidential information in such a call either. You have no way of knowing who is actually in the virtual room.**

On the topic of online testing: Having "helpers" during online testing is cheating and unethical. It does not matter if "everyone else is doing it." Most likely, everyone else is *not* doing it. And, if in fact a student truly believes that, then the matter should be brought to the attention of the professor. If everyone has a helper, then having helpers should be stated as the accepted practice, or groups should be officially allowed to take tests as a group.

People sometimes argue that if you allow someone else to take your test you are "only cheating yourself." That is true as far as the gain of knowledge is concerned. However, because grades are used for competitive purposes, then those who use test helpers are gaining an unethical competitive advantage. Unless group test-taking is the accepted practice, having a helper is always cheating and is unethical.

SUGGESTED RESPONSES FOR DISCUSSION QUESTIONS

1. It is illegal to spoof policemen, firemen, and military personnel. It is probably illegal to spoof certain professionals such as doctors, nurses, architects, and licensed engineers. In general, however, it is not illegal to spoof someone. If the person who is being spoofed gives permission for the act, then he or she is culpable if the behavior is illegal.
2. Spoofing is unethical. Almost every businessperson would define deception as unacceptable. Consequently, because ethical behavior is defined as adhering to a group norm, deception in the form of spoofing is always unethical. If the person being spoofed is aware of the deception, then he or she is culpable in the unethical act.
3. None, for the reasons described in 2.
4. Communication among members of the group who were supposed to be in the meeting will be surreal. Everyone will think that others know something that they do not know. The people who were at the meeting will know what transpired. They will not be *expected* to know anything about the meeting, yet will be the only ones who do know.

   This example is so overdrawn that it is almost silly. It points, however, to the communication problems that develop in organizations where deception is practiced.
5. The only difference between text chat and speaker phones or conference calls is that it is easier to spoof

with text chat. Yes, we have always had these problems, and yes, they have always been unethical. Text chat makes it easier and therefore possibly more prevalent. For any virtual meeting, whether via voice or text chat, always assume that unknown, unannounced people may be on the call or in the meeting.

6. I think this gets into a gray area. If you are setting up the meeting and if you know that Bill has an interest in the outcome, you probably do have an ethical responsibility to invite him. However, if you have no particular responsibility to invite Bill, if Bill would not feel betrayed by you for not inviting him, then your action may not be unethical. You do not, after all, have an ethical responsibility to bring trouble into your business life.

7. No, not ethical. This sort of behavior has a way of coming back at the perpetrator. “What goes around, comes around.” Being criticized for her thinking that you advanced as your own is the universe getting even. You can't disclaim those ideas; and if you try, you'll look even worse.

8. It is always cheating and unethical to have a helper on an online test. You are not justified in having a helper even if you believe “everyone else is doing it.” If you believe that is the case, raise the issue with your professor. Whether such tests should be used at all depends on the importance of the grade of the test. If the test largely determines a course grade, I believe that their use should be avoided.

WRAP UP

- **In any conference call, speaker-phone call, or multiparty chat session, assume that unannounced guests may be on the line. Govern your comments as if you do not know who is in the room, because, indeed, you do not know.**
- **Spoofing someone is always unethical and it may be illegal, depending on whom you are spoofing. If you know that someone is spoofing you, you share responsibility for the unethical behavior.**
- **Having helpers on online tests is cheating and is always unethical.**

YOU BE THE GUIDE

Using the Guide: Securing Collaboration (pages 64–65)

GOALS

- Raise students' awareness of security risks and potential problems when using collaboration software.
- Understand the risks to organizational data when data is shared with nonemployee personnel.
- Learn differences in security capabilities of Google Docs, Windows Live SkyDrive, and Office 365.

BACKGROUND AND PRESENTATION STRATEGIES

Collaboration tools enhance collaboration but introduce serious security risks. The more people who have access to data, the greater the likelihood of data loss. For example, if the probability that any single person uses data in only authorized ways is 0.99, if the group has three people, the probability that everyone in the group uses data only in authorized ways falls to 0.97 (assuming equal probability and independent events). However, if the group has 50 people, the probability that everyone in the group uses data in authorized ways falls to 0.61. This change occurs simply because with more people there is more chance that someone will use the data inappropriately.

Now, there is always risk in sharing data. If I attach a document with confidential data to an email and send it to a large group of people, I am exposing that confidential data to considerable risk. However, it is just one document. Suppose, instead, that I place numerous documents, schedules, tasks, and sketches on a Windows Live SkyDrive site and open that site to a large number of people. I am exposing that semantically linked group of documents to considerable risk. In some ways, the risk of sharing a SkyDrive site is greater than sharing a file server. Most file servers have so many documents that it can be difficult to find everything about some topic. All of the documents on a team site, however, contain data of interest to the purpose of the team. Critical documents have been centralized in one spot.

The problem of sharing confidential data with outsiders is not new. However, the problem of sharing an entire team's document set with outsiders is new. Again, the consequences may be higher because there are many documents, all with a similar purpose.

Of the three collaboration tools presented in this chapter, SharePoint has the potential for the most security. It has only the *potential* for the most security because the features and functions for excellent security are in the product, but it is incumbent on those who set up the SharePoint server and sites to create and implement security.

However, the adage "A chain is only as strong as its weakest link" pertains to document security. Documents can be highly protected on a SharePoint site, but if legitimate SharePoint users download that data to a Windows Live SkyDrive site, or to a Google Docs site, then the security enforced by SharePoint may have been overcome.

Digital rights management is a means of restricting the use of Microsoft Office documents. With it, the content of documents can be restricted to viewing by particular people or for particular periods of time and in other ways. This technology, however, is seldom used and has numerous holes.

The bottom line: Sharing confidential documents in team sites exposes those documents to increased security risks. This risk increases dramatically with employee's use of personal mobile devices. The IS Department has little to no control over their use and it is presently unclear how organizations can deal with security breaches via personal devices.

SUGGESTED RESPONSES FOR DISCUSSION QUESTIONS

1. When using a public wireless network, you should assume that any email you send or any IM message you write can be published on the front page of your campus newspaper tomorrow. Write only what you are willing to have published.
2. The financial exposure is much higher for businesses than for individuals. Again, any email or IM sent over a public wireless network is open and can be read by anyone. If you are using, say, Google Docs, to share accounting data with one of your clients over a public wireless network, you are exposing that data to snooping. Do not transmit sensitive data over a public wireless network.
3. Employees who process work emails on Gmail are exposing the content of those emails over the public Internet. Even if the employee is working inside the corporate network, and even if that

network is secure, as soon as the email goes on to the public Internet, it is vulnerable to snooping. If no public wireless network is used, then the snooper would have to physically tap into a wired network, which is much harder than wireless snooping, but it is still a possibility.

More important, Gmail is free software, and Google severely limits its liability for the quality of the product or service. Of course, Google would suffer an enormous public relations loss were its email servers to be compromised or lost, but, even still, any employee who stores company email on a Gmail server (and you cannot use Gmail without doing so) is exposing the company's data to the security policy established by Google. The company may or may not determine that to be an acceptable risk, but when employees do this on their own, their companies do not even know. It is a messy issue with no clear solution (nor barrier).

4. Organizations have no control over the ways that SharePoint Online (part of Office 365) sites are shared. An employee could store sensitive data on a SharePoint Online site and inadvertently share that site publicly, or share it inappropriately. An employee might give update permission to someone who has no authority to make updates. Partners could copy sensitive data from a SharePoint Online site and send it to competitors. Furthermore, the organization has no control over how Microsoft treats the data on its site. Microsoft could be hacked and lose data and, absent gross carelessness, the organization that lost the data would have no recourse. Ironically, ease of use is the culprit here. Both Google Docs and SharePoint Online are readily accessible and quite easy to use. This means that employees with less knowledge of the risks of sharing can readily use these services. Consider, too, that employees can be accessing Google Docs or SharePoint Online using their own iPhones or iPads, using network access that is paid for by the employee. The organization has no control over such use. **It is not much ado about nothing.** Organizations today have serious challenges to security in these services.

5. The risks of using SharePoint Online or Google Docs are no greater than the risks of using any file server. Few organizations today would disallow file servers, and thus few would be likely to disallow SharePoint Online or Google Docs on this same basis. In general, it is very difficult to enforce the prohibition of using particular programs. Even if the employees cannot install software on their work computers, they can install it on their own computers and copy data from the work computer to their home computer.

   Chapter 12 discusses these issues in more detail. In general, it is cheaper and easier to perform security background checks on employees in sensitive positions, and to train those employees on security policy, than it is to prohibit employees from using certain software. With the numerous computing alternatives available today, employees can usually find a way around some prohibition if they are sufficiently motivated.

WRAP UP

- **Collaboration software opens the door to security risks. Always think about security when you set up a team site. Realize that team members can always remove data to other locations and process it or transmit it elsewhere without your knowledge.**
- **Sharing data with nonemployees is risky. Sharing Google Docs, or SharePoint Online sites with outsiders is even more risky because many related files and documents are consolidated at a single location.**
- **Organizations have a serious security vulnerability from employees' use of personal, mobile devices such as iPhones, iPads, Android phones, and the like. Education and training of employees is crucial!**

YOU BE THE GUIDE

Using the Guide: Egocentric Versus Empathetic Thinking

(pages 66–67)

GOALS

- Raise the level of professionalism in the class.
- Explore empathetic thinking and discuss why it's smart.
- Discuss two applications of empathetic thinking.
- Emphasize that a problem is a perception and that perceptions differ among people.
- Discuss that different problem perceptions require different information systems.

BACKGROUND AND PRESENTATION STRATEGIES

How many times have we all been asked, "I couldn't come to class. Did we do anything important?" I'm always tempted to say, "No, when I saw you weren't here, I took all the important material out." Another rejoinder, more mature on my part is, "Well, first tell me what you think important material is." If they say, "Is it going to be on the test . . . ?" then we have some talking to do.

You might want to underline the corollary about not asking your boss, when you've missed a meeting, "Did we do anything important?"

Part of the reason for this guide is to raise the level of professionalism in the class. I find students' maturity rises to meet expectations. By asking them to engage in empathetic thinking with regard to not coming to class, I'm also asking them to step up in their maturity:

- **If you choose not to come to class, that's your choice. But, realize there's a cost to me and our teaching assistants, and do what you can to minimize that cost.**

Empathetic thinking does result in better relationships, but this guide says that businesspeople should engage in it because it's smart. Negotiators, for example, need to know what the other side wants, what's important to it, what issues they can give on, and what ones are nonnegotiable.

Here's a simple example:

- **Suppose you have an employee who wants more recognition in the group. You know the employee is doing a good job, and you want to reward her. Not engaging in empathetic thinking, you give her a pay raise. What have you done?**
- **How could empathetic thinking have helped you in this situation?**

So, using this example, just what is empathetic thinking?

- **Understanding the other person's perspective (See the Guide "Understanding Perspectives and Points of View" in Chapter 1)**
- **Realizing that people who hold a perspective different from yours are not necessarily WRONG (but you don't have to be wrong, either)**
- **Not attempting to convince the other person that his or her perspective should be changed to match yours**
- **Adapting your behavior in accordance with the other person's perspective**

- **Does thinking empathically mean that you change your way of thinking to match the other person's?**

  (No.)

- **Does it mean always giving the other person what he or she wants?**

  (No.)

- **What are different ways you could adapt your behavior in accordance with another person's perspective?**

All of us have been in meetings that are going nowhere. Whenever we find ourselves in such a meeting, is the problem due to different perspectives? If so, one can sometimes find the root cause by engaging in empathetic thinking.

The scenario at the end of the guide is right on point. If three factions hold three different problem definitions, and if they don't realize they hold those different definitions, then the meeting will go nowhere. And it doesn't matter what the "facts" are. The facts aren't the problem; the different problem definitions are.

SUGGESTED RESPONSES FOR DISCUSSION QUESTIONS

1. Considering the other person's perspective:

- **What are some examples of egocentric thinking?**
- **What are some examples of empathetic thinking?**

2. Read the minutes, if any. Ask others who were at the meeting. Prior to the meeting, ask someone else to take notes or make a recording. If possible, let your boss know ahead of time that you'll be absent, and why. Otherwise, apologize for your absence, explain why, and say that you have the information. Minimize the burden on your boss!

3. A problem is a perception. Different people perceive in different ways. So, different people can have different problems, *even though they may give the same name to the problem*.

4. First, based on her words, the *real problem* is that you know she is not engaged in empathetic thinking. Notice that you are in a much stronger position than she is. You know that there are two (yours and hers), and possibly more, different problem definitions. Unlike her, your thinking is broad and flexible enough to understand that multiple perceptions, and hence multiple problem definitions, can exist at the same time.

You have at least four different strategies: (1) Change your definition to match hers. (2) Try to teach her about empathetic thinking. (3) Without saying anything about her thinking skills, and without needlessly repeating your understanding of the problem, use your understanding of her and her definition to arrive at a solution that is mutually acceptable. (4) Say something polite and close the conversation because you're just wasting your time.

- **Under what circumstances would you use each of these strategies?**

5. Restate his position to him. "You perceive the problem as . . . ," and do the best possible job of restating his position. This does not mean you agree with his position, but it will let him know that you understand his words. He'll know, if you continue to disagree with him, that it's not because you don't understand him.

Having convinced him that you understand his position, you should attempt to express your view of the problem. His knowing that you understand his position may allow him to be able to understand yours. However, he may not be able to, in which case there may be no possibility of good communication with him on this issue.

6. It comes down to power. You are in a much more powerful position if you understand other people's perceptions and your own, but they understand only their own. You can imagine solutions and possibilities that they cannot. Also, as countless books on negotiating skills imply, understanding someone else's point of view enables you to manipulate them, if you are so inclined.

Finally, empathetic thinking results in better relationships, and in the final analysis, business is nothing but relationships. Businesses themselves do nothing. Business is people working together in relationships. Better relationships equate to better business.

WRAP UP

Sometimes I end with a little practice:

- **Anybody learn anything today? What?**

- **All right, let's practice. Using empathetic thinking, tell me why you think I included this exercise in today's presentation.**