Reading Assignment

Chapter 12:
Information Security Management

Suggested Reading

See information below.

Learning Activities (Non-Graded)

See information below.

Course Learning Outcomes for Unit VIII

Upon completion of this unit, students should be able to:

3. Examine the importance of mobile systems and securing information and knowledge.

Unit Lesson

In the last unit, we discussed outsourcing, the functions and organization of the IS department, and user rights and responsibilities. In this final unit, we will focus on security threats to information systems.

PRIDE and System Security

PRIDE processes privacy settings on the server and returns a code that indicates which of the four privacy levels defined for PRIDE govern a particular individual with a particular report/data requestor. By processing settings on the server, those settings are not exposed to the Internet. The return code is, however, and the operational system should probably use https for both the code and to return the report. This was not done in the prototype, though.

The relationship between patients and PRIDE participants is N:M. One patient has potentially many organizations, and an organization has potentially many patients. What this means is that a patient has a relationship, potentially, to many participants of a given type: many doctors, many health clubs, many insurance companies, and even many employers. In addition, a patient has a relationship to, potentially, many types of participants.

Given the N:M relationships, a natural place to put privacy settings is in the intersection table. That table serves, intuitively, as an opacity filter between a given patient and a given doctor (or other person/organization).

The tension in the dialog between Maggie and Ajit at the beginning of Chapter 12 regarding what terminology to use with Dr. Flores is intended to set up a discussion from both perspectives. It is a common problem for techies when talking with business professionals: How much technical language should I use? It is important to use enough to demonstrate competency, but not so much as to drown the businessperson in terminology.

Using the Ethics Guide: Securing Privacy

In this chapter, we discuss three categories of criteria for evaluating business actions and employee behaviors:

- legal
- ethical (categorical imperative or utilitarianism)
- good business practice

We can clearly see the differences in these criteria with regard to data security. A doctor's office that does not create systems to comply with HIPAA is violating the law. An e-commerce business that collects customer data and sells it to spammers is behaving unethically (by either ethical perspective). An e-commerce business that is lackadaisical about securing its customers data is engaging in poor business practices.

Even still, business professionals today need to be worried, much more so than they are, about sending email over wireless networks. Unless the email is encrypted, and it almost never is, its contents are readily available.

We cannot overemphasize the importance of creating and using long, effective passwords. Professor Boyle's observation that he receives more than 1,000 intrusion attempts per night on a computer that is open to the Internet is sobering! Also, see the argument in Question 8 on page 477 that as major sites become more difficult to infiltrate, criminals will turn to smaller, less difficult sites. Stealing $50 from a million people nets $50 million. Longer term, something like FIDO in Case Study 12 on page 486 will have to be created.

Two guidelines that apply to the principle "The best way to solve a problem is not to have it" are:

- Resist providing sensitive data.
- Do not collect data you do not need.

Be aggressive about not divulging personal data. You may find that about 95% of the time, when you challenge someone about why they need some piece of personal data, they may respond, "Oh, don't bother—we don't have to have it."

When someone says, "All answers are strictly confidential," consider the source. If that statement comes from the university computer security staff, we can conclude that they understand what they are claiming to provide and will take every professional effort to comply with that statement. If it is made by a team of undergraduates with majors that predispose you to believe that they know little of computer security, then they may not know what they are claiming to provide. Furthermore, in the event of a security system failure, the university has deep enough pockets to provide compensation for damages. It would be difficult to obtain compensation from a group of undergraduates. Do not provide data to sources with questionable data security!

Using the Security Guide: Metasecurity

Considering accounting controls, most such controls have a strong procedural component. The payables system, for example, is set up so that one person authorizes a payment, a second person generates the check (or uses an information system that causes the check to be created), and a third person accounts for the payment. That separation of duties and authorities is crucial to effective control.

Future managers need to understand the reason and validity of such procedural controls, and they need to manage accordingly. The security of such systems lies in the hands of the managers on the front line.

This knowledge is especially true for managers who work at help desks that have privileges to reset or override passwords or that provide other computer account services. Typically, security administration systems create logs that show summary data, such as how any passwords were reset, which accounts were reset, whether an appropriate notification was sent to the customer, and so forth. If the control requires the help-desk manager to review or reconcile these totals against other data, the manager should take such reconciliation very seriously.

Here, we consider the management of a white-hat hacker employee. The two crucial questions about managing such an employee are: how do you know you learned all of the problems, and what do you do with that person next?

Unlike a consultant, an employee has a continuing need for an account and password in your organization's network. But, that person is situated to take advantage of any problems that he or she did not reveal. As the guide points out, given that person's expertise, do you want him or her to have access to your network? This guide overdraws on this issue in such a way as to promote further discussion.

All major software vendors, including Microsoft, Oracle, SAP, Siebel, and others are obvious targets for security attacks. Every one of those companies has a staff of in-house hackers and other security experts who have the knowledge and access to create havoc in their networks. What do you think these companies do to prevent this?

What extra precautions can you take when you hire and manage employees such as white-hat hackers?

Some possible solutions include: perform substantial background checks, require such employees to sign specially written employee contracts, regularly investigate the employees' lifestyle and spending habits, require periodic lie-detector tests, and perform unannounced security audits of the employees' computers and accounts.

The above measures are fine for sophisticated software companies. But what about a company like AllRoad Parts? It does not have the expertise, employees, or resources to perform, for example, an unannounced computer and account audit. Such precautions are beyond the financial resources and expertise of AllRoad Parts. The company can best protect its data by hosting its Web sites with professional hosting services, by limiting access to sensitive data, by implementing employee termination procedures, and by buying insurance. The insurance vendor may help AllRoad Parts decide what additional measures it needs to take.

Openness can improve security. One good example concerns the separation of duties and authorities. If everyone is trained that mangers review logs of their activity, if everyone knows that random checks are made by calling persons whose accounts have been modified, if everyone is trained on such procedures and understands the need for them, security will improve. By the way, when such procedures are presented as standard business practice for a well-managed company, then no one needs to feel that they are under suspicion or that they are not trusted.

In a related vein, if employees understand all of the capabilities that their passwords give them they will be more likely to safeguard them. If, for example, the employee's account and password provide unlimited access to the employee's salary, benefit, and other personal data and if every employee is aware of that fact, password management will improve.

As a manager, you may have control responsibilities for the security system. If so, take those responsibilities seriously. Securing security is a challenging, interesting, difficult, and important problem.

Using the Guide: The Final, Final Word

Although Harry Dent's prediction that a 30,000 Dow Jones average in 2010 seems ludicrous today, his analysis about the second wave, the application of technology use, seems sensible. Getty Images (GYI) is an excellent example of success through innovate application of IS and IT. The company has harnessed database technology to create a system that produces images at near-zero marginal cost. YouTube was purchased by Google for $1.62 billion after just over a year of operations.

Getty Images and YouTube are not the last companies to find innovative applications of technology as many, many more similar opportunities exist. Applications of IS, no matter how clever or how innovative, must reinforce the organization's competitive strategy. The importance of the opportunities for nearly free data storage and data communications cannot be overemphasized. Here are some developments to consider:

- Numerous cities are sponsoring projects to provide fiber-optic cable to the home.
- Wireless networks are everywhere—city parks, public buildings, coffee shops, and so on.
- The entertainment, computer, and data communications industries are reinforcing one another.
- Blogs have revolutionized mainstream media and, in the process, are changing the dynamics of politics.
- Twitter provides a podium for everyone and enables readers to consume the products on their own time and in their own, very flexible space.
- Cheap storage and data communications, along with standards like SOA, will have a major, possibly revolutionary, effect on inter-organizational activities such as supply chain management.
- Business use of social networking and UGC will continue to grow, if not explode.
- Social CRM fundamentally changes the customer-vendor relationship.
- Enterprise 2.0 will dramatically alter the social dynamics and management in many organizations.

Suggested Reading

To learn the fundamentals of phishing, visit
www.microsoft.com/protect/fraud/phishing/symptoms.aspx

To see recent examples of phishing attacks, visit
www.fraudwatchinternational.com/phishing/

Chapter 12 Presentation

Greene. T. (2011, March 1). PayPal CISO: DDos one big security threat among many. *Network World*. Retrieved from http://www.networkworld.com/article/2200501/software/paypal-ciso--ddos-one-big-security-threat-among-many.html

The Economist. (2014, May24). Computer security: Divided we stand. Retrieved from http://www.economist.com/news/science-and-technology/21602664-organisms-stop-infections-spreading-being-diverse-so-can-computer-apps-divided

Learning Activities (Non-Graded)

Course Flashcards:
http://media.pearsoncmg.com/ph/bp/bp_kroenke_umis_7/flashcards/index.html

From the Textbook:
Using MIS InClass 12, Phishing for Credit Cards, Identifying Numbers, Bank Accounts, p. 462
Ethics Guide, Securing Privacy, pp. 464-465
Security Guide, Metasecurity, pp. 480-481
Guide, The Final, Final Word, pp. 482-483
Using Your Knowledge, p. 485
Case Study 12, Will You Trust FIDO? pp. 486-487
The International Dimension: International MIS, pp. 489-505

Non-graded Learning Activities are provided to aid students in their course of study. You do not have to submit them. If you have questions, contact your instructor for further guidance and information.