CHAPTER 16

CONTROLLING COMPUTER-BASED INFORMATION SYSTEMS, PART II

This chapter continues the discussion of control in a CBIS environment. The last four areas of control are presented (numbers seven to ten). Three of these complete the discussion of general controls. See Table 16-1, on page 815, as the completion of Table 15-1. The tenth covers the more specific application controls.

The objectives of this chapter are:

- to be familiar with the principal threats to data communications and to understand the control techniques used to reduce these threats;
- to recognize the unique exposures that arise in connection with electronic data interchange and to understand how these exposures can be reduced;
- to be aware of the exposures that threaten firms that rely on microcomputers for their information needs and to understand the controls that are necessary to reduce exposure in a microcomputer environment; and
- to be able to explain the principal input, processing, and output controls that are used to ensure the integrity of computer applications.
I. Internet and Intranet Controls

Many of the data problems facing organizations today are related in part to the fact that they transfer data electronically. Although there are many benefits of communicating in this manner, there are also some real costs. The text discusses threats to communication in two ways: equipment failure and subversion.

A. Controlling Risks from Subversive Threats

Technology has changed how individuals and businesses communicate. But along with the benefits comes cost. Unauthorized access is (and will continue to be) a serious concern.

Several types of controls are discussed here. Read carefully.

1. Firewalls are electronic barriers (both software and hardware) created to keep intruders out. Two levels are discussed, network and application levels.

2. Denial-of-service attacks are used to overload TCP/IP connections to the Internet to prevent legitimate access. This problem is not easy to solve.

3. Another type of protection against unauthorized access involves coding of the data or encryption. Two methods are discussed in the text: private key encryption and public key encryption. These are designed to make intercepted data useless.

4. Several other techniques are also discussed: digital signatures, digital certificates, message sequence numbering, transaction logs, request-response techniques, and call-back devices.

B. Controlling Risks from Equipment Failure

The problems that can occur in the physical transfer of data are often frustrating. Being sure that the correct information has been transmitted is important to accountants who must have confidence in the reliability of the information in the system. Two techniques are discussed that are used to verify that the correct information has been transmitted: an echo check and a parity check. You get a small sample of
II. Electronic Data Interchange Controls

Prior to this point, we have focused on the advantages to the seller and buyer of establishing an EDI partnership agreement. These benefits do not come without a price. The differences that yield benefits also present organizations with reason to look carefully at questions of control.

The absence of human intervention shifts many of the “traditional” concerns. Your book focuses on three areas: authorization and validation, access control, and the audit trail. The discussion is brief but valuable.

III. Personal Computer Controls

PCs are everywhere. In their early days, they were often free-standing. Today, more often than not, they are tied into organizational networks. Some of the things that make PCs popular also make them vulnerable.

There are several significant concerns discussed here: weak operating systems, inadequate segregation of duties, inadequate backup procedures, and inadequate systems development and maintenance procedures. Several solutions are discussed. Note the guidelines for selecting packaged software. Compare this to the discussion in Chapter 14.

IV. Application Controls

As mentioned above. All nine areas of control discussed so far in chapters 15 and 16 can be labeled general controls. The other type of accounting controls are focused on specific applications within the accounting system. One rational way to group these controls is in terms of the activities within a system: input, processing, and output. The text follows that approach.

A. Input Controls

GIGO—“garbage in, garbage out”—is not just a cute saying. If care is taken to assure that the data input to the system is good, fewer problems will occur downstream. Input controls are designed to make sure that the transactions entered into the system are valid, accurate, and complete. They can be considered in relation to:
Each of these areas includes numerous examples. Focus on what the issues are, not just the techniques.

B. Processing Controls

Although the input process is very important, controls must be in place during the processing of the data, to be sure that operations go as planned. Your book discusses three types:

- **run-to-run controls** [which track the processing—the total pay in posting and the total when the checks are printed],
- **operator intervention controls** [to monitor human interference in processing], and
- **audit trail controls** [to assure the existence of an audit trail].

C. Output Controls

The last stage of processing is the “outputting” of something—files, documents, etc. Controls must be in place here, also. Hard copy output from batch systems can be a problem. Read this carefully. Real-time access to output on screen creates different problems.

Review Questions for Chapter 16: 1-28

Discussion Questions for Chapter 16: 1-29