

Chapter 1

Electronic Business Systems Security

What is it?

What does it include?

How important is it?

How to get started?

INTRODUCTION

One of the major computing challenges in today's economy is the manifest lack of adequate security over the information, computers, networks, and Internet applications on which business, government, and the economy depend. Many computer security threats have been identified over the past 25 years, and each has spawned a special category of corrective actions to address it. For example, in earlier times, efforts to address the lack of automated security were variously known as computer security (COMPUSEC), communications security (COMSEC), emanations security (EMSEC), information security (INFOSEC), and information technology security (ITSEC). More recently, information assurance (IA), Internet systems security (ISS), and cyber-security have grown in popularity. Each of these areas in turn have grown subcategories of security knowledge and special safeguarding techniques that are needed to secure today's electronic business systems. There is no one security solution for an e-business system because the e-business application sits at the pinnacle of modern computing and is therefore susceptible to all the security weaknesses of the various foundation technologies.

For our purposes, e-business security acknowledges all the threats identified by each of these security categories and employs the technical security safeguards and risk mitigation techniques associated with each category as determined by the actual risks found to be threatening the business. E-business security also calls on the traditional disciplines of personnel and physical security to complete the picture of safeguards that will be needed when addressing threats to the electronic business.

Conceptually, e-business security represents an accumulation and consolidation of information processing threats that identify the need to protect the integrity and confidentiality of information and the need to secure the underlying support technologies used in the gathering, storage, processing, and delivery of that information.

But what is e-business security and why is it important? How do threats to electronic business impact the world of contemporary commerce and what must be accomplished to improve an organization's security posture—especially when it comes to “new” e-business systems?

HOW IS E-BUSINESS SECURITY DEFINED?

Some definitions:

- Assure—make safe, make certain, tell positively, give confidence.
- Information—knowledge.
- Information Technology (IT)—the technology of the production, storage, and communication of information using computers.
- Electronic Business—the application of information technology to business activities.

Using these definitions, e-business security can be said to be concerned with *making certain* that the *knowledge-value* of business information is *made safe* and is available for business processing when needed. Consequently, e-business security is concerned that the technologies used for the production, storage, and communication of information are *made safe* so that the *knowledge-value* of the information is *certain* and can be trusted when used. If information and the processing technology are *made safe*, users will have confidence that the information *positively tells* (i.e., accurately portrays) the reality of that which the information is supposed to represent. In different words, e-business security is concerned with the confidentiality of information, maintaining its *knowledge-value*, and ensuring its availability to *legitimate* users and customers when required to perform an *authorized* business activity.

By comparison, if information, and its *knowledge-value*, are not *made safe*, cannot *be trusted*, and are not readily available to legitimate users and customers, business and government activities will be adversely impacted. If by accident or deliberate action, information is stolen, becomes inaccurate or misleading, or is not available for use, business and governmental decisions and actions may become compromised, distorted, or wrong, and/or decisions cannot even be made and actions cannot be taken. When this occurs, executives, stockholders, users, customers, and citizens lose confidence in the information and may no longer trust the system, process, or organizations that make use of the information. They also lose confidence in the organization responsible for maintaining the information and the integrity of the business process. E-business security, then, is concerned with being able to assure trust in all information and the computing processes used to conduct e-business.

Is E-Business Security Really Such a Big Deal?

3

CAN E-BUSINESS SECURITY BE EXPLAINED MORE SIMPLY?

Perhaps it is helpful to view the scope of e-business security as including all those actions required to prevent, minimize, and recover from the universally appreciated threats summarized by the acronym GIGO—garbage in—garbage out. Within this context, e-business security is concerned with preventing those accidental and/or deliberate actions that may result in the introduction of inaccurate data or information to a system (GI) as well as any accidental or deliberate processing, storage, and communication activity that may produce inaccurate, false, or misleading outputs from a system (GO).

These concerns are addressed by taking action to assure the integrity and confidentiality of information and processes while at the same time assuring the ready availability of information, processes, and other system resources when required for use by legitimate users and customers. For example, “denial of service” attacks, such as those often experienced by Internet users, are currently being viewed as the number one threat to our highly automated and interconnected way of conducting business and executing the functions of government. This is because a successful denial of service attack destroys the ability of the e-business system to function at all.

In conclusion, e-business security is concerned with all aspects of how business information is collected and handled, how hardware and software process and communicate that information, how information is stored and protected from eavesdroppers, and how system resources are configured and *made safe* to ensure their ready availability to legitimate users and customers.

IS E-BUSINESS SECURITY REALLY SUCH A BIG DEAL?

To the extent that business information and the technology used to produce, store, or communicate that information are considered important to an organization’s e-business operations, the definitions and discussions outlined in this chapter are consistent with the intent of Presidential Decision Directive-63 (PDD-63) on Critical Infrastructure Protection and other initiatives calling for the protection of the nation’s critical information infrastructure. In a practical sense, if information and/or its processing were considered mission-critical or mission-sensitive for Y2K purposes, it should probably now be considered critical for the intent of e-business security.

Presidential Decision Directive-63 directs that information integrity, confidentiality, and availability be assured, not only for government systems but also for all information processing systems on which the nation depends. E-business systems certainly fall within this definition. The intent of the directive can be accomplished only if all aspects of information collection, production, storage, and communication are *made safe* (i.e., secured). By inference, this includes how

e-business systems are designed, managed, configured, accessed, and operated. It also includes how software and databases are designed, programmed, and tested; how system changes are made and validated; how systems are monitored for incidents; and how critical information and backup systems are protected. By establishing information, computer, and communications security controls sufficient to prevent and mitigate anticipated risks, and by establishing a continuous security monitoring and security improvement process, the intent of PDD-63 can be satisfied.

All aspects of computing and communicating impact the objectives of assuring integrity, confidentiality, and availability and should therefore be within the scope of an e-business security initiative.

IS E-BUSINESS SECURITY MORE IMPORTANT THAN OTHER INFORMATION TECHNOLOGY INITIATIVES?

E-business security is an overarching business issue that, based on analyzed risks, establishes the threat acceptance and reduction parameters for the *safe* use of technology. As an overarching issue, e-business security can be thought of as being absolutely fundamental to the effective and efficient use of information technology (IT) in support of e-business. E-business security enables the operational concepts of e-business or e-government to become a viable way of conducting the affairs of the corporation and the government. Having built an electronic business or government world, our dependency on information and its confidential, accurate, and timely processing has grown to the point where compromises of information, loss of integrity, and/or failures of the underlying support technology may be catastrophic.

How much or how little security is required in any given instance is a “due diligence” issue for management. Determining what constitutes a “pound of security” and the associated costs are decisions that can be made only after considerable analysis—analysis that requires the direct involvement of senior executives of the corporation. If information and its supporting processing and communicating technologies are not important to your organization, little attention need be given to these issues. However, if information processing and its supporting technologies are central to the conduct of your business, a great deal of security work may be necessary. It all depends on your situation, how well you know your risks, and what has previously been done to address those risks.

The question that needs answering is “what risks threaten your e-business and how are your customers, employees, partners, investors, and shareholders impacted should any of those threats materialize?” The answer to “how much or how little security is required” must consider a great many variables that change over time and therefore require a continuous improvement mind-set and the establishment of security management processes that allow threats to be monitored so that continuous security posture improvements can be made.

How Does an Organization Get Started?

5

HOW DOES AN ORGANIZATION GET STARTED?

First, an organization must know the actual security posture of their existing e-business processes so that management is aware of system vulnerabilities and how they may adversely impact business operations. Management can then intelligently choose, in the light of analysis, what degree of risk to accept. When was the last computer and network security assessment conducted? If your company is like most companies, it has been several years and does not reflect the new distributed e-business and Internet applications the company has been building or integrating from off-the-shelf products. Additionally, your organization was distracted for several years with the Y2K problem and all the work and expense that was needed to correct it. Consequently, most organizations must begin anew to determine an appropriate course of e-business security action for their company.

Beginning anew means to start with a formal assessment of the vulnerabilities, threats, risks, and potential adverse impacts associated with how information technology is now being used to support the electronic business processes of the organization. Such an assessment will identify ways in which information and processing integrity can be compromised, confidentiality breached, and availability of computing services denied (Chapter 3).

Questions concerning the cost of bringing e-business systems up to an acceptable level of security can be answered only after the security assessment has been conducted and senior management has contemplated the “quantifiable” losses and a series of potential adverse impacts that are generally “unquantifiable” (Chapter 7).

In addition to identifying technical security weaknesses, this assessment should attempt to discover the extent to which IT support organizations and/or contractors adhere in their daily operations to system management “best practices” and security “best practices” being advocated by security experts. Adherence to these practices is crucial if the e-business operations of the organization are to be executed in a well-managed, stable, dependable, and *safe* manner (Chapters 4, 6, and Appendix B).

Following an assessment of technical weaknesses and management practices, a plan of corrective actions or “road map” should clearly outline appropriate safeguard actions, their costs, and the anticipated costs needed to design and execute a security program of corrective actions and day-to-day management of that program (Chapters 4, 6, and Appendix B).

Security assessments for e-business systems come in many flavors depending on the complexity of the business and computing environment to be analyzed, the amount of time that has elapsed since the last assessment, and the dollars available to conduct the analysis.

E-business security assessments may evaluate the security posture of the entire enterprise, focusing on vertical “legacy” business systems or new e-business applications, or may determine the effectiveness of security practices at a system-specific operational level. A new aspect of a traditional security assessment

growing out of the Y2K experience is an analysis that crosses all system interfaces of a “supply chain” made up of various interdependent businesses. This will be especially appropriate where just-in-time processing is occurring or where business to business (B2B), business to customer (B2C), or business to government (B2G) is a growing part of the business model. For corporations that are already heavily networked, an essential element of the e-business security assessment is to immediately begin monitoring current system traffic to discover what is actually going on at the systems and network level (Chapter 5).

Finally, a major question that most organizations should ask regarding e-business assessments is whether their employees have the technical, security, and “best practices” knowledge and experience needed to conduct the type of analysis that factors in all the technical innovations and associated threats that have been introduced into the e-business processing mix in recent years. Beyond the act of assessing (and even more important, what does an organization do with the findings from an assessment after it is completed?), the real measure of worth for an e-business security assessment lies in whether the findings and recommendations are feasible and capable of being implemented and administered. Are the recommendations truly practical or are they merely a collection of actions resulting from the use of checklists? Is there an attempt to integrate the recommendations into a set of system controls that is consistent with the way business is actually being conducted by the organization? Does management know how business is being conducted at the operational level? Is there a process for reconciling apparent conflicts between processing efficiency and the possible imposition of security and internal controls? Of equal concern, how does an organization plan to maintain the secured processing environment after recommendations are implemented and how will the continuing IA posture be monitored during daily operations?

If there are any doubts about the abilities of an organization’s internal staff to conduct the security assessment, there also must be doubts about their ability to determine a course of corrective action, devise an implementation strategy, and maintain a secured environment in the face of rapid technological change. It is therefore essential to look beyond the assessment to the entire *security life cycle* to plan and budget sufficiently for the implementation of corrective actions and the maintenance of a secured operational environment.

There are many sources for conducting security assessments, but few that can provide follow-up on *security support services* based on standardized and repeatable methods recommended by the standard-setting bodies of the world such as the National Institutes of Standards and Technology (NIST) and the International Standards Organization (ISO) guidelines (Chapter 4).

What Should an Organization Be Doing?

7

INSTEAD OF PLAYING “CATCH-UP,” WHAT SHOULD AN ORGANIZATION BE DOING TO DESIGN E-BUSINESS SYSTEMS THAT ARE SECURE IN THE FIRST PLACE?

The answer to this question begins with the system management practices of the IT support organization and/or contractor. The “Holy Grail” of security professionals has always been to influence systems while they are in development and to design security in rather than add it on after the fact. This has proven to be elusive for a number of reasons having to do generally with how IT is managed by the majority of businesses and governments and particularly how system development projects are often mismanaged. The bottom line is that security cannot be designed into an e-business system if these systems are not being defined, designed, programmed, tested, and deployed in a disciplined manner. Furthermore, security cannot even be effective as an add-on if systems are not maintained and operated in a disciplined manner. Put simply, *you cannot secure what you are not managing—and you cannot manage without enforcing the discipline of a “structured” software and systems engineering methodology* (Chapter 6 and Appendixes A and B).