Identifying Critical Business Functions

Bonnie A. Goins

Introduction

Important to the proper implementation of a security strategy within an organization is its alignment to that organization's business objectives. Performing security activities for technology's sake does nothing to protect, or assure, those components that fall outside the purview of technical security. At a high level, people, processes, facilities, and, arguably, data typically fall outside of technical security inspection. It is clear that security, as a process itself, must consider these inputs in order to provide a comprehensive view of protection for the organization. Equally important to achieving a balanced security program is the understanding that an organization will not protect all of its assets equally; that is, aspects of the organization necessary to the continued fulfillment of the organization's business goals must take precedence over those activities or inputs that are not essential to the organization's survival. This notion is crucial to the concept of controls within the organization; resources used to protect the environment should first be allocated to those aspects of the organization that are essential for the continued operation of the business. The organization may also decide to protect aspects of its organization that are not critical to continued operation; however, it is customary for organizations to allocate fewer resources to accomplish this objective. This scenario concurs with the industry view that critical assets and functions require greater protection than noncritical assets and functions.

What Is a Critical Function?

The *Disaster Recovery Journal* formally identifies critical functions as "business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization." Before an organization can begin to identify business functions that are essential to its survival, it must understand the difference between *criticality* and *sensitivity*. Criticality relates to the importance of the asset or function in enabling the organization to operate and protect itself, and sensitivity relates to the classification of the data and systems existing within the organization.

Let's look at an example of each of these definitions. The National Security Agency's INFOSEC Assessment Methodology (NSA IAM) takes as one of its principle tenets the concept of criticality; it does so for the very reason mentioned above. Assessment of the organization's security state revolves around its definition of criticality. Senior executives are asked to identify one to ten activities that, if not performed, would cause the organization to cease to operate its core business. Many senior executives struggle with this preassessment identification because they often cannot immediately separate essential from nonessential business functions.

The concept of sensitivity is central to many regulated environments. Organizations bound by legislation, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), are guided to review their electronic data assets to determine whether those data are identified by the legislation as being central to meeting compliance objectives. In the case of HIPAA, electronic protected health information (ePHI) is identified as a sensitive data element that requires the highest level of protection. Organizations covered by this legislation (covered entities, or CEs) face stiff fines, sanctions, potential lawsuits, and even jail time for maliciously divulging this information or for failing to promote duly diligent (reasonable and appropriate) security measures within the organization.

A reader who has considered these examples carefully might be asking whether it is possible to have a business function that could be considered both critical and sensitive. If so, congratulations! Business functions that are essential to the organization's continued operations and those that process, transmit, or store sensitive data are considered to be critical *and* sensitive business functions. An example of a critical and sensitive business function is a healthcare insurer's claim processing function. Processing claims is central to a healthcare insurer's business function; as such, the claims function is critical to the organization's continued operation. Further, because a healthcare insurer is a payer, it is obliged to meet the compliance objectives contained in the HIPAA legislation; hence, the data it processes, stores, and transmits during the claims function is considered sensitive, making the function itself sensitive.

Where Do I Begin To Identify Critical Business Functions?

A good place to begin identification of critical business functions is within the organization's business units. One caveat is that each business unit is likely to view its business functions as being most critical to the organization. This is contrary to the fact that senior executives determine the criticality of business functions within their organizations. As such, it is important for senior executives to review and "rightsize" business unit expectations regarding the priority of their critical functions so they fit properly within the context of the entire organization. Working with business units can sometimes be a challenge for the security professional. Business units may be unfamiliar with the task at hand and, as such, require some coaching in order to complete the effort. Also difficult for most organizations is determination of the appropriate level of detail for describing each critical business function. Many times it is easier for the business units to identify each of their business functions, regardless of criticality, and then to prioritize the functions based on criteria that align them with their importance to the organization.

In choosing this approach, the organization has produced a complete picture of its function that can be visually depicted through data flows and other graphical methods to produce a roadmap that shows the organization its workflow. This roadmap can also help to identify functions that are missing procedures, as well as procedures that are missing functions. In each case, the organization should then determine whether these functions or procedures are extraneous to the organization's operation. If so, they can be removed; if not, then an issue with the process exists, and the organization can now evaluate that issue. This identification and activity are at the center of the business process reengineering effort for organizations.

If interviewing the business units is the approach chosen to begin the critical function identification, the security professional can ask the business units particular questions that will help them to reach the appropriate determination of criticality to the organization. Examples of these questions are listed in Table 36.1. Following is a discussion of the role of each question within the identification process.

How can these questions assist with identifying critical functions within the organization? By asking the business units how their functions align to the organization's business goals, it is possible to classify any outliers (*i.e.*, those functions that are performed in support of a function that is not critical to the organization's continued operations or are not critical to the continuing operation of the organization themselves) as noncritical business functions. These functions can still be prioritized but will not fall into the critical category.

Periodicity, or the frequency at which the function is performed, can also assist in determining whether a business function plays a role in continuing an organization's business operations. It is important to

TABLE 36.1 Questions To Assist in Determining the Criticality of Business Functions

What business objective does this function support for your organization?
How often is this function performed?
Is this function performed only by your business unit, or is it also performed by other business units within your organization?
Does the successful completion of this function depend on interaction with other business units, vendors, business partners, or external organizations? Does another business unit, vendor, business partner, or external organization depend on this function for successful completion of its functions?
Is there a potential for loss of life or injury to personnel, business associates, or externals if this function is not carried out?
Is there a potential for significant dollar loss to the organization if this function is not carried out?
Is there a potential for significant fines, litigation, jail terms, or other punishment for noncompliance to a required regulatory requirement?
Is noncompliance tied to a specific threshold for downtime for this function?
Is noncompliance tied to a specific threshold for data loss or disclosure of sensitive information for this function?
Is this function carried out by key personnel within the business unit?
Are other personnel within the business unit or organization available and capable of performing the function in the absence of key personnel?
What priority would your organization give this function within the entire organization?

note, however, that periodicity by itself does not determine criticality of a business function. As an example, a staff member of a large financial services firm has many job functions that he performs daily. One of these job functions is to remind business unit managers to review the organization's proposed training classes and to weigh in on the selection. Although it is important to provide training to employees, training is often curtailed as a result of reallocation of resources in the event of a disaster. Doing so does not bring operations to an end but rather frees resources to accomplish other more critical tasks. The function the staff member plays (*i.e.*, notification of the business unit managers) can be discontinued in the event of disaster with no ill effects; therefore, the function may be viewed as being low priority for continued operation of the organization.

The notion of interdependence is of extreme importance to an organization and its operational continuity. Business functions that appear to be noncritical may be identified by a business unit as critical; upon further examination, it may become apparent that critical business functions from other business units rely on input from this "noncritical" business function to perform satisfactorily! Taking a look at our previous example again, a staff member identified a business function as notification of business unit managers regarding training. We determined initially that the notification was low priority and related that assessment to the business goal of continuing operations for the organization. Let's take a deeper look, though. What if the notification involved relaying to the managers information on mandatory training for business continuity? If the business unit managers could not get that information from any other source in the organization, such notification from the staff member is now critical for ensuring that all personnel are trained in business continuity efforts. For most organizations, business continuity training is highly critical, especially in light of the lessons taught to us by September 11; therefore, any function that is key to promoting the business continuity effort may be considered to be critical.

Loss potential is another way to uncover criticality in an organization. Losses can typically be categorized as human, financial, informational, technological, or facility oriented. Any business function where the loss of life or an injury to an individual figures prominently if the function cannot be successfully completed must be considered to be critical. An example of such a function is the coordination of logistics in an army on the move. If logistics cannot be properly coordinated, troops can be placed in jeopardy.

Financial losses are frequently evaluated when determining criticality. The organization must determine for itself what the definition of "significant financial losses" really is. It is important to note that, many times, financial losses come as a result of an interaction of issues. In this case, this translates to the fact that the business functions involved must be evaluated very carefully to identify which are truly critical, if any, to the organization's operations.

Compliance to a regulated state can also pose challenges for identification of critical business functions. Most often, the challenge arises from the fact that legislation is not always prescriptive; that is, legislation is not always specific in detailing what is expected from the covered organization. HIPAA regulations are a good example of this. Implementation specifics are listed, but in an extremely broad context. The reasons cited for these broad strokes include consideration for the uniqueness of each organization and a desire to take into account the availability of resources at each organization. As such, organizations must fend for themselves, often by working together as a group or collaborative to interpret the law; the HIPAA Collaborative of Wisconsin is an example of this type of group. From their interpretation comes a recommendation for the work that is required to meet the legislation. Organizations can choose to follow the recommendations or to implement their own interpretations.

Most organizations bound by regulations come to view the regulations themselves as the critical business function and apply the policies and procedures that are derived from the regulation as satisfaction of the legislative requirement. Organizations must also take into account whether a violation of appropriate downtime, data loss, or disclosure of information will trigger a shift into noncompliance. Data gathered during the business impact assessment process can assist with providing a stated threshold within the organization that can then be compared to the stated goals of the legislation. Gaps between the organization's stated threshold and the stated goals of the legislation point to an area for remediation (*i.e.*, correction) for the organization, if it is to maintain a state of compliance.

What is the possibility for an organization to continue operations if its key (read critical) personnel are no longer available to perform their job functions? If no surrogate, or back-up, resources are available who can perform these critical functions in the absence of primary or key personnel, then it is likely that continued operations will be extremely difficult and haphazard, at best. It is extremely important for an organization to identify individuals key to its function. When a business unit manager is asked for his or her key personnel, typically the answer that is given corresponds to the set of activities (or business functions) he or she performs. This assists the security professional in identifying two critical elements in one round of questioning; the business unit's critical functions and the personnel responsible for carrying them out.

Although it is often the case that the business units within an organization view their functions as being of the highest priority to the organization, it is still worth the time to ask the business units where they think their business functions fall with regard to priority within the organization as a whole. In some cases, the request for the business units to look at the bigger picture may yield unexpected results. In the case where an organization's personnel has longevity and the organization is supportive of promotions, lateral moves to different business units, and job sharing, personnel may indeed have a deeper perspective of how the organization functions as a whole. Because experience brings so much to the table in this endeavor, it is advisable to at least make the effort to inquire.

Functions *Versus* Procedures

As we stated above, ultimately senior executives are responsible for identifying their organization's critical business functions. Often, these functions are further elaborated in an organization's business plan and reports to the organization's board of directors, stockholders, and employees. Some organizations do not document their critical functions as such, but rather identify core competencies. This can be workable if senior executives can identify how those core competencies are broken into functions and are represented by workflow in the organization. If the senior executives are not successful at doing this, then the core competency identification is at too high a level to be productive for this identification of critical business functions within the organization.

Many organizations also confuse business functions with functional procedures. It is often useful to view the business functions as the "what," or a set of procedures which themselves are the "how" with respect to implementing the business function. The combination of these interact to complete a business objective, when combined with appropriate policies. Sometimes, we see that the relationship of a critical function to a procedure is one to one; that is, one procedure can elaborate an entire business function.

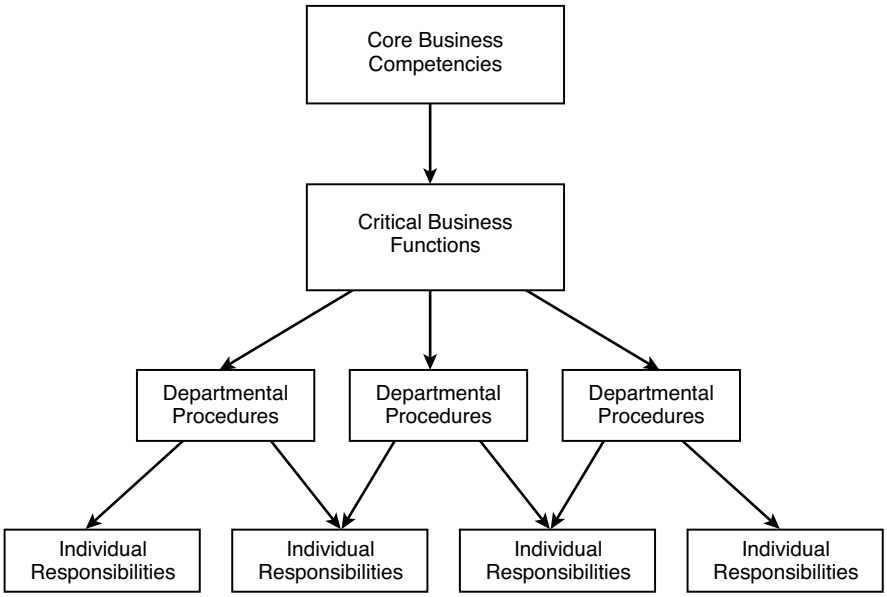

FIGURE 36.1 Functional hierarchy.

Many times, however, we see that the correspondence between a business function and its corresponding procedures is one to many; that is, more than one procedure elaborates a business function. Consider the example of an information technology department. One of its stated critical business functions is to build appropriate architecture to support the business processes that drive the organization. An organization's technology architecture consists of several layers: network devices, such as routers, switches, and firewalls; network servers (perhaps with different operating system needs); application systems; and end-user systems. This is a very simplistic view of architectural needs, but it demonstrates the notion of multiple procedures for one business function. Clearly, the procedure for building a firewall, with its complex set of rules, is not the same procedure an organization would use for building an application server of any kind. Figure 36.1 depicts the hierarchy of business functions, procedures, and individual responsibilities, or accountability, for completion of the procedures.

It is important to note that the detail to which unique organizations define and elaborate business functions may vary; that is, some organizations are much more specific in defining their business functions. A good example of this difference can often be seen at organizations that are being held to compliance, or regulatory, requirements. For example, senior executives at publicly held companies are now obligated to attest to the accuracy of their financial reporting. Along with this requirement comes the requirement to fully document the financial reporting environment. For this reason, many organizations choose to upgrade their businesses' functional definitions to more easily comply with the legislation. For more information on elaboration of business functions with regard to such legislation, see discussions regarding the Sarbanes–Oxley Act elsewhere in this book.

Conclusion

Although identification of critical business functions may be, at times, difficult, certain practices can assist the security professional with completion of this important activity. Constructing an appropriate data gathering instrument, such as a business impact assessment questionnaire, is a first step (see Figure 36.2). When this data has been gathered, analysis of the important elements — maximum downtime; maximum allowable data loss; cost to the organization; resumption and recovery time objectives; key infrastructure, applications, and personnel; and others — will provide the information necessary to identify activities that can keep an organization operational, even into times of need.

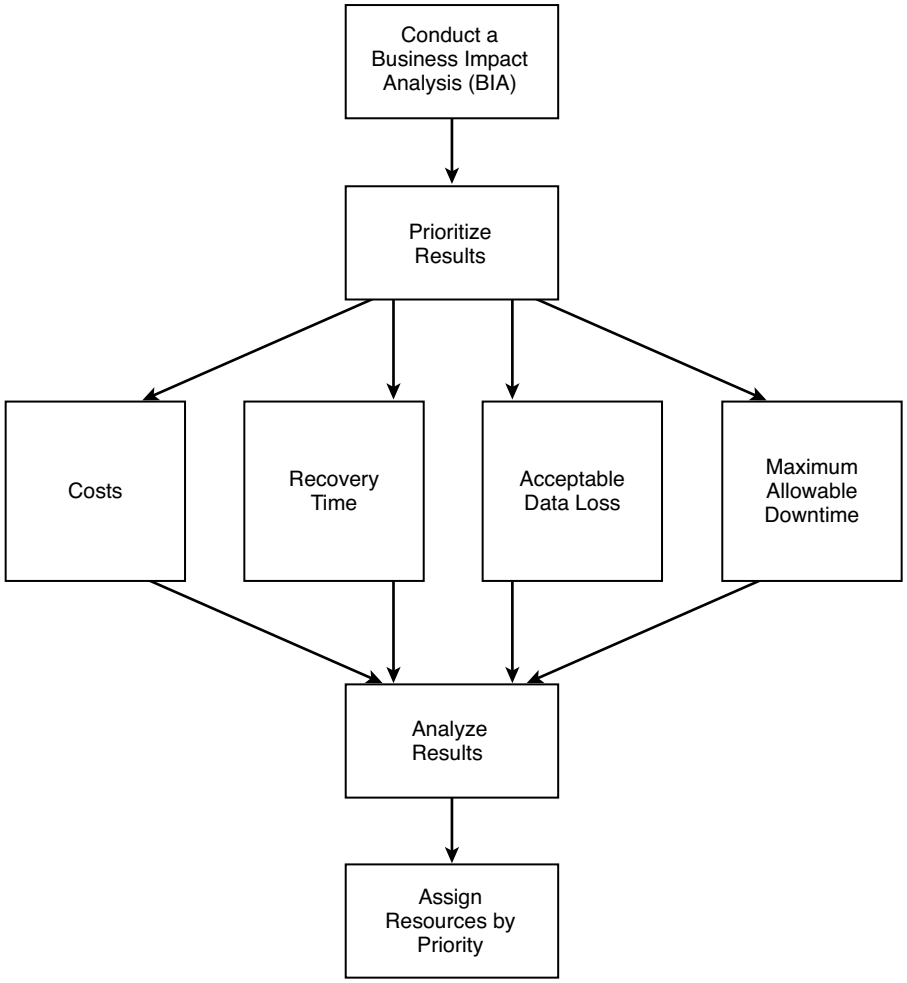

FIGURE 36.2 Business function prioritization flow.

References

Carnegie Mellon University, Software Engineering Institute, SSE-CMM, www.sei.cmu.edu/publications.
Disaster Recovery Journal, www.drj.com.
FFIEC. 2003. *Business Continuity Planning*, Washington, D.C.: Federal Financial Institutions Examination Council.
Health Insurance Portability and Accountability Act of 1996 (HIPAA), www.hhs.gov.
Information Systems Audit and Control Association (ISACA), www.isaca.org.
International Standards Organization (ISO) 17799/British Standard (BS) 7799.
National Institute of Standards and Technology (NIST), www.nist.gov.
National Security Agency Information Assurance Methodology (NSA IAM), www.nsa.gov.
Sarbanes–Oxley Act, www.aicpa.org.