Delivering Higher-quality Security Service Using Asset Identification in Resource-constrained Environments

Vinoth Sivasubramanian, CEH, ISO 27001 LA, is an IT professional with more than six years of experience in the IT security industry. Currently employed at UAE Exchange Centre LLC, he is responsible for the IT policies of the enterprise with additional responsibilities of optimization and implementing risk management guidelines.

Not all organizations have enough resources for managing enterprise security effectively. The complexity of undertaking an enterprisewide view of security management is one of the daunting challenges facing IT security leaders/managers. These are the people who are tasked with securing the organization, but it may not be very clear as to what that means. As a result they are left with questions to answer such as:

- What needs to be secured?
- Why and with which priority?
- How best to ensure that people agree on the previous two questions?
- How can people be sure that the organization is secured?
- How best to measure the success of the security process?

This article proposes an approach for specifying and prioritizing information security requirements in organizations in which resources such as money, time and manpower are limited. In the current economic scenario with budgets limited, people are always required to do more with less. Therefore, it becomes essential that the IT security manager/leader directs resources to those requirements that are of prime importance so that the end objective of comprehensive security and service to the business can be achieved.

This is achieved by linking security with the business vision of the organization, i.e., providing business rationale for security requirements. This rationale is then used as a basis for comparing the importance of different security requirements. Furthermore, this article considers how to integrate the aforementioned solution into a service-level management process for security services. This is an important step in IT governance.

FORMULATING SECURITY REQUIREMENTS SPECIFICATIONS

A security requirement specification tells what should be secured and why. A good security requirement specification identifies the organization's needs with respect to security.

When an organization wants to secure its systems, it must first determine what requirements to meet. Given that organizations generally do not have large amounts of resources to protect their assets, it is important that they prioritize their security requirements so that maximum resources are allocated to the most important requirements. To achieve this, security requirements are mapped to the business vision of an organization. Each organization has its own business vision that defines the very principle of how it wants to achieve its goals. This vision, however, changes over time to reflect changing circumstances. Notwithstanding, business experts have identified certain patterns in the business visions of leading firms. This article uses the well-known value disciplines identified by Michael Treacy and Frederik Wiersema. Treacy and Wiersema state that there are three ways a business can excel:

- **Operational excellence**—An organization that aims to deliver operational excellence focuses on offering its products with the least amount of hassle possible or at the lowest cost to its customers.
- **Customer intimacy**—Companies that look to customer intimacy aim at delivering what their customers want by investigating the needs of the market and then customizing their offers in the market.
- **Product leadership**—Organizations develop unique, radically innovative products that steer them ahead of the competition.

Each of the three value disciplines leads to a radically different operational model for the company: the culture, processes, management systems and IT systems of the company. For instance, while operational excellence calls for highly standardized business processes, the customer intimacy discipline approach is different: it requires business processes to be as flexible as possible. Security requirements, likewise, should be aligned with the requirements imposed upon culture, process and management systems by the value discipline chosen.

CRITICAL IMPACT FACTORS

When security incidents occur, as they are bound to do, they may lead to potential damage to the reputation of the organization and impact its business goals. Critical impact factors (CIFs) indicate what kind of damage the security incidents cause for the organization. CIFs can include those that are within the control of the organization and those that are not. This article does not give guidance on CIFs, but prioritizes security through CIFs of assets, including an example of linking asset security with the business vision via CIFs (see **figure 1**).

Linking Assets With Business Vision Through CIFs

The assets are then classified according to the impacts they can have on the business vision. The assets are mapped into their business vision through their impact factors (see **figure 2**).

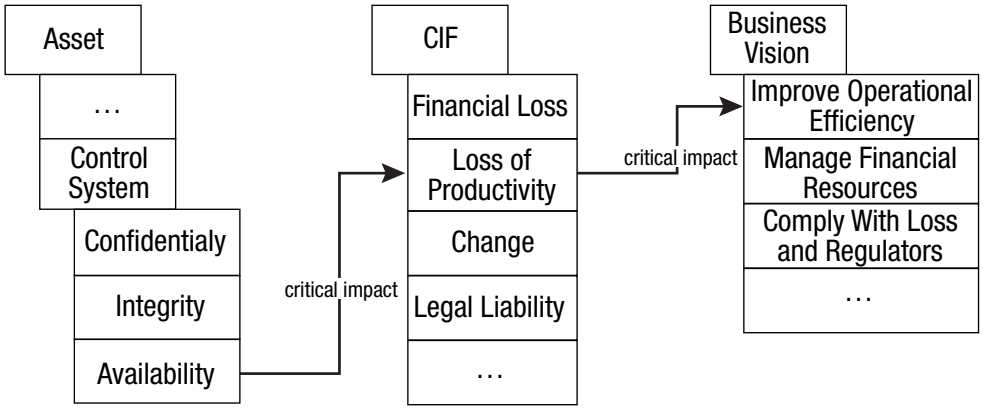
Using the impact diagram in **figure 2**, it is possible to categorize and prioritize the different security requirements by analyzing the critical impacts the assets make on business vision. An asset that causes critical impact on a business vision needs to be addressed with the highest priority. It is also possible that an asset can cause multiple critical impacts. For example, if a control's system availability has marginal impact on legal compliance and critical impact on productivity, which, in turn, affects operational excellence, that asset should be marked as an asset with critical impact.

Advantages of Linking CIFs With Business Vision

When a business vision is outlined, the stakeholders need not have a security focus in mind and can concentrate on the business vision. The CIFs, on the other hand, reflect the business implications when security is compromised. This makes it easy for the IT security leaders to prioritize resources and obtain resources in cases of need.

Figure 1—Aligning Business Vision With Security Requirements

Figure 2—Asset Mapping With Business Vision Using CIFs



Once the requirements are categorized and prioritized, other techniques such as attacks and threats can be envisioned easily on categorized and prioritized assets. Having CIFs linked to the business vision helps the IT security leaders plan accordingly.

INTEGRATION OF SLAs INTO THE SECURITY SERVICE

In the growing era of regulations such as the US Sarbanes-Oxley Act, IT governance plays an increasingly important role in organizations. IT governance aims to improve the quality of IT services by introducing or improving controls and practices and stressing the need for definition of roles and responsibilities among IT personnel and management. Service level agreements (SLAs) are the fundamental way to define expected quality for a certain supplied service and are widely used not only with third parties but also between units within the same company. In the latter case, this enforces responsibility since units together define what the expected service is and help avoid unpleasant situations.

Steps for integrating the prioritized security requirements into the security management life cycle include:

1. A business unit starts to define its business vision by identifying its value discipline. If the business vision already exists, this step can be omitted or the business vision can be reassessed, if needed.
2. The assets that are of value to the organization in coherence with the business vision of the organization are noted.
3. CIFs are identified based on a combination of industry-specific CIFs, review of peer CIFs and the internal security personnel's input.
4. The assets are then tagged with their impact factors; this step is performed by the IT and business units together.
5. After the assets are tagged with their potential impact factors in alignment with their business vision, the IT unit envisages the desired properties of the assets.
6. SLAs are then prepared and proposed to the business units. In certain cases, the business unit can accept a critical impact in return for a lower level of service, which may occur due to budgetary and manpower constraints.
7. Once the SLA has been agreed upon, the IT unit must review the agreement again to ensure that accepted high levels of risk in one unit do not pose an unacceptable level of risk in other units, as this might happen due to an interdependence on processes.

CONCLUSION

The framework that has been discussed is useful only if it is embedded into a concrete process of security management. Giving business units the ability to make decisions regarding CIFs makes it easy for the IT security leaders/managers to define suitable roles for their people and themselves and achieve the end objective of serving the organization's mission and vision through security.

REFERENCES

CERT, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Software Engineering Institute, *www.cert.org/octave*

IT Governance Institute, CobiT, 1996-2007, *www.isaca.org*

Office of Government Commerce, IT Infrastructure Library (ITIL), UK, 2007, *www.itil.co.uk*

Swanson, M.; "Security Self-assessment Guide for Information Technology Systems," technical report, National Institute of Standards and Technology (NIST), Special Publication 800-26, *www.nist.org*

Treacy, M.D.; F.D Wiersema; "Customer Intimacy and Other Value Disciplines," *Harvard Business Review*, 71(1):84-93, January 1993