The Challenges of Security Management

Richard A. Caralli, William R. Wilson
Survivable Enterprise Management Team
Networked Systems Survivability Program
Software Engineering Institute

ABSTRACT

Modern organizations have a huge challenge on their hands, on a scale unlike anything they've seen since the Y2K crisis. They must "secure" the organization in the face of increasing complexity, uncertainty, and interconnection brought about by an unprecedented reliance on technology to accomplish their mission. They must also stay mindful of the heavy hand of regulation as legislators discover the importance of security. This paper explores some of the challenges that organizations must overcome to be successful in this environment and introduces ways in which a change in perspective might be the impetus for an emerging mission-driven approach to security.

Introduction

Let's start by recalling 9th grade biology class when you were introduced to the concept of a cell. You might remember that each cell in the body performs a specific function. To carry out this function, cells receive input from their environment, transform it, and create output—a continuous cycle that lasts throughout the cell's life. The success of the cell in performing this cycle is important to the larger environment in which it exists—the organs, systems, and functions of the body. Interestingly, this cycle can also be used to describe the basic functions of information systems and organizations as well. In particular, an organization can be described as an open system[1] that gives and takes from its environment to exist, to be sustained, and to succeed.

[1] System theory is concerned with describing systems and their interaction with their environment. An open system is one that is open to and dependent on its environment to succeed. The open systems

It isn't such a leap to consider today's organizations in this context. Organizations are connected to their environment in an ever increasing way, particularly because technology is a pervasive force that enables business processes and strategies. This is apparent with respect to the use of the Internet. Not long ago, many organizations actively restricted the extent and type of Internet access provided to users; today, Internet access is a part of the baseline configuration of just about every user desktop and is an essential tool for performing job functions. In some ways, the use of the Internet (and all of its underlying technologies) has become the primary means by which the organization interacts with its environment. While this brings tremendous opportunities, it also exposes the organization to new risks that must be identified, mitigated, and managed so as not to impede the organization's quest to meet its mission.

The organization as benefactor

Every cell in a living organism has a particular purpose or mission. All of the internal structures of a cell are employed in accomplishing this mission. Anything that impedes this process also interrupts the cell's ability to do its work, causing potential damage to the larger system or environment to which it belongs. Thus, ensuring that the cell can carry out its essential functions and maintain proper balance with the environment is paramount.

perspective evolved from the view that many entities—cells, communities, groups, organizations—exhibit similar system characteristics [1].

In the same way, the ultimate benefactor of the security activities that an organization undertakes should be the organization itself. Organizations deploy[2] their internal structures—core assets and processes—with the goal of accomplishing their mission and providing benefits to stakeholders. As with the cell example, anything that impedes assets and processes from doing their jobs potentially derails the organization's ability to be successful. From this perspective, ensuring that assets and processes remain productive is the real benefit and focus of the organization's investment in security.

Managing security[3] in the context of the organization's strategic drivers[4] provides both advantages and conflict. On the one hand, this approach ensures that the goals of security management are forged from and aligned with the high-level goals of the organization. On the other hand, the strategic drivers and needs of the organization are often in conflict with the actions required to ensure that assets and processes remain productive. In addition, as the organization is exposed to more complexity and uncertainty (because of the increasing use of technology and the pace at which the organization's risk environment changes), keeping security activities and strategic drivers aligned becomes more difficult. In the end, finding the right balance between protecting the organization's core assets and processes and enabling them to do their job becomes a challenge for security management—and a significant barrier to effectiveness.

[2] "Deploy" in this sense refers to the traditional accounting context of putting an asset into production for the purpose of achieving a return on investment.

[3] We describe "managing security" broadly as the process of developing, implementing, directing, and monitoring the organization's security strategy and activities.

[4] Strategic drivers refer to the organization's mission, goals, objectives, and critical success factors.

The scope of security management

Security as it is traditionally defined in organizations is one of the most pervasive problems that an organization must address. Rarely has there been an organizational issue, problem, or challenge that requires the mobilization of everyone in the organization to solve. (In this case, the Y2K effort comes to mind with one significant distinction—security is an ongoing issue that must be managed well beyond New Year's Eve!) The sheer expanse of any problem that traverses the entire organization poses many management challenges, particularly when the focus is security. First, the most important areas of the organization must be identified and targeted. This requires the organization to take an inventory to determine what needs to be protected and why. In a large, complex organization, this can result in the identification of hundreds of assets that are important to strategic drivers. Second, to secure this collection of organizational assets requires many skills and resources that are typically scattered throughout the organization. Because security is a problem for the whole organization, it simply is no longer effective or acceptable to manage it from the information technology department. Chief Security Officers have the one of the most difficult jobs in executive-level management because their success depends on utilizing many of the organization's skills and resources. In effect, CSOs must mobilize many disparate parts of the organization to work together and to expand their core responsibilities to include security. This is not unlike a similar problem faced by U. S. automakers in the early 1980s. Faced with the need to improve quality to compete with their Asian counterparts, some U. S. automakers wisely focused on quality as a core element of their mission. As a result, quality became a part of every worker’s core responsibilities and was integrated into key business processes, and thus, the entire organization worked together to overcome these deficiencies.

Complexity is pervasive

Connecting to a complex operational environment is not a choice for today’s organizations. If the organization wants to compete and thrive, it must be willing to expose itself to operational and technical networks that enable it but also put it at risk. These networks are constantly changing and evolving, increasing the organization’s exposure (but also its potential for growth). This problem is not limited to large organizations—virtually any organization that uses a modern operating system on its desktop computers or servers has inherited a complex and dynamically changing environment that must be actively managed.[5]

This presents another challenge for managing security because the security strategy must be sufficiently dynamic to keep pace with the rate of organizational and technical change. On balance, security management must support the organization’s quest to be sensing, flexible, and adaptive to its environment and must be able to make a measurable contribution to the organization’s bottom-line and long-term resiliency.[6]

[5] In “The Future of Security—After the Storm, Reform,” Scott Berinato proclaims that “Windows will approach 100 million lines of code and the average PC, while it may cost $99, will contain nearly 200 million lines of code. And within that code, 2 million bugs” [2].

[6] Enterprise resiliency is the ability of the organization to withstand systemic discontinuities and adapt to new risk environments [3]. Supporting resiliency as a goal of security management is a primary focus of future articles in this series.

Security as an investment

Dealing with a complex operating environment is costly and can significantly impact an organization’s profitability. Protecting the financial condition and stability of an organization is one of the most important issues for management. The resulting pressures from managing to the bottom line are a rich source of challenges for many activities throughout an organization, especially for security management.

Expenditures receive much of the focus in organizations because they directly affect the organization’s bottom line. Responsible financial managers scrutinize all expenses and make implicit, if not direct, risk-versus-reward decisions. Security management is no exception—it is often an expense-driven activity that can directly affect an organization’s profitability. It is no wonder then that organizations are reluctant to view security as an investment that can generate benefits to the bottom line.

The view of security as overhead is an unfortunate outgrowth of the lack of inclusion of measurement and metrics as an essential element of security management. Organizations do not routinely require return on investment calculations on security investments, nor do they attempt to measure or gather metrics on the performance of security investments. Absent a set of established and accepted metrics for measuring security ROI, there is little an organization can do on its own in this area other than perform measurement in the context of incident avoidance or impact of a realized risk (i.e., the impact costs less than the control, and therefore provides a return). And organizations are faced with another problem: Which security investments should be measured? Technical controls, monitoring software, security staff, CSOs?[7] The measurement dilemma is pervasive across the entire security community, and lacking specific guidance, organizations have become comfortable characterizing security activities as an expense on their balance sheets.

In much the same way that information technology investments are now commonly capitalized, the challenge for security management is to drive the organization in the same direction for security. The shift to characterizing security as an organizational investment promotes the view that security can, at a minimum, preserve an organization's bottom line, if not improve it. Consider this: an organization that successfully approaches security as an investment may increase its overall value in the marketplace, and may even be able to capture this value as "goodwill"[8] on their balance sheet. In the future, a determinant of an organization's value may be the amount of goodwill on its balance sheet that is directly due to its ability to secure critical assets and processes and improve its resiliency. Certainly, an organization that can keep its core assets and processes in service in the face of an attack, accident, or failure (and actually improve their ability to adapt to future events) may be worth more than one that cannot, if only because of the competitive advantage they create. Until organizations shift their view away from

[7] Many security professionals are confronting this issue. An interesting article on the differing viewpoints of security measurement, "Measuring Security ROI a Tall Order," can be found at searchsecurity.com [4].

[8] For accounting purposes, goodwill is an intangible asset valued according to the advantage or reputation a business has acquired over and above its tangible assets [5]. Any factor that translates into the organization's ability to increase its earning power (or ability to accomplish its mission) can contribute to goodwill, such as its reputation, customer service, and perhaps its ability to adapt to changing risk environments.

security as a burden, the ability of security management to effectively do its job at the organizational level will be impeded.

Technological biases

The view of security as a financial impediment for the organization is often a consequence of the tendency of organizations to consider security as a technology-driven activity. The security industry itself contributes greatly to this characterization. Framing security in technical terms is a logical outgrowth of the expansive (and ever-increasing) number of technical products and services that are available to “help” organizations get a handle on security management. Worse yet, there is a propensity for organizations to frame security problems in technical terms, often ignoring the management and operational weaknesses that are root causes or contributing factors. The bias toward technological solutions or the framing of security issues in technical terms has done a great disservice to organizations in their pursuit of adequate security.

Security is a business problem

Security is a business or organizational problem that must be framed and solved in the context of the organization’s strategic drivers. However, many organizations adopt a technology-centric approach to security by default. There are several reasons why this has occurred. As stated previously, the largest contributor to the technology-centric view of security is the industry itself—there is a strong technology bias to security approaches and solutions, and even in the selection of skilled security personnel. Not only has this made organizations more likely to view security as a technical specialty, but it has also corrupted them into misplacing their most prized security resources in the IT department, further alienating them from connecting to and aligning with the organization’s strategic drivers.

The evolution of a risk-based paradigm for security has made it clear that a secure organization does not result from securing technical infrastructure alone. A security approach that is mission-centric (i.e., based on strategic drivers) strives to secure the organization’s critical assets and processes regardless of where they “live.” This can be illustrated by examining the importance of information as an organizational asset. Information is frequently stored, transported, and processed through technical means, and therefore is considered a technical asset. However, this characterization is a distortion that can lead organizations inappropriately to a technical security approach. For example, an organization may store its product designs on paper or keep its medical records in paper form—both of which may be critical for meeting the organization’s mission. Securing the organization’s technical infrastructure will not provide a proper level of protection for these assets, nor will it protect many other information assets that are in no way dependent on technology for their existence or protection. Thus, the organization would be lulled into a false sense of security if they relied on protecting their technical infrastructure alone.

In the end, the “network” that most matters is the one that defines the organization and its related boundaries. The importance of the organization’s technical network is established in its role in enabling the organization’s assets and processes, but it provides little context for which of these assets and processes matter most to strategic drivers. It is only in the organizational network where the context for the importance of each asset and process is found, as well as the rationale for what needs to be protected and why it is provided.

Regulatory biases

A final consideration for security management is the organization's regulatory environment. Just as the organization must expose itself to its environment to operate, so must it be willing to accept some of the limitations imposed on like organizations that operate in its competitive space. This brings another level of challenges that affects the organization's ability to be effective at security management.

Regulations reflect the need for organizations in a particular industry to look critically at their protection needs and to implement corresponding security strategies and controls. While this has had a positive effect in elevating the need to focus on security, for some organizations it can also be deleterious in that regulations can become an organization's security strategy by default. Regulations can draw the organization's focus away from organizational drivers and on to the compliance requirements of the moment. Complying with regulations is certainly an important activity in an organization, but it cannot substitute for a mission-focused, strategic security management process. Regulation is intended to improve the core industries on which it is focused, but compliance activities can give organizations a false sense of the overall effectiveness of their security programs. For example, compliance with HIPAA regulations may improve the security over core assets that are subject to the regulations, but other assets and processes are left unprotected. A compliance-driven approach to security can also cause costly and inefficient investments in protection mechanisms and controls to protect those assets and processes that are subject to regulation, when in fact this may not be the best use of limited resources for the organization.

Organization-centric approaches to security management consider the impact of risks and their effect on the organization to determine which security activities and practices are best for them. In effect, this allows the organization to focus on their true security needs. Security management that is subsumed by a need to comply with regulations can detour an organization from this strategy by diverting their attention away from what is best for their unique organizational context.

Security as a core competency

Organizations want to focus their energy on their core competencies—those functions and activities that define the organization's existence and its value to stakeholders. The upsurge in outsourcing of horizontal business functions by organizations supports this claim.[9] For many functions, such as payroll processing or benefits administration, this may be perfectly acceptable—if an organization cannot realize a strategic and competitive advantage from excelling at payroll processing, it may not make sense to develop a core competency in this area. However, this is why organizations may need to develop a core competency in security management based on their strategic drivers.

[9] Horizontal business functions are those that are commonly found across many different types of organizations and are fundamental to managing a business, such as payroll processing and accounts payable.

Security is so inextricably tied to the success of the organization in accomplishing its mission and improving its resiliency that it is in the organization’s best interest to be competent at securing itself.

Unfortunately, the high cost and limited availability of security resources (particularly technical resources) has made it cost-prohibitive for some organizations to develop this competency. The issues of cost and retention of key security personnel also has not made executive-level managers willing to embrace security as a legitimate long-term investment in the organization’s strategic plan.

Conclusions

It is no wonder that security is so difficult to manage in modern organizations. The practice of security management continues to evolve inside organizations, and therefore has yet to garner its fair share of attention and resources. This is partially the consequence of the organization’s inability to see the value of security outside of technical constraints and regulatory compliance. In addition, the industry’s affinity for technology-based solutions alienates the “business people” in the organization. There is hope however that organizations and the security industry are evolving in this respect.

Many organizations are adopting a risk-based approach to security. The move to a risk-based paradigm is a catalyst for moving security from a technical specialty to an organizational competency. Applying a risk perspective to security is a logical progression—risk management is a basic business function, and whether it is done implicitly or explicitly, it must be performed at an organizational level to be purposeful.

But even this paradigm for security has significant challenges to overcome, notwithstanding the many definitions of “risk” and the somewhat negligent way in which risk is bandied about as the new security buzzword. For example, the security industry offers many options and services for performing security “risk” assessments; however, at the nucleus of these offerings is usually a traditional vulnerability assessment with very little connection to risk drivers. Organizations must also be cognizant that a risk perspective alone is not a panacea for solving all of the issues that they face in elevating security to the level of other pervasive business problems.

In pursuit of addressing the challenges noted herein, the first obstacle that an organization must confront is to determine what they are trying to accomplish with their security activities. In essence, the organization must ask what benefits they get from “doing security.” The organizational perspective is essential to determining these benefits and for setting appropriate targets for security.

One of the most important characteristics of cells and larger organisms is their ability to adapt to new or changing environments. Organizations, like cells, also must continually adapt to their environment and emerging risks—risks that are perhaps unknown until the organization is impacted by them. In order to do this successfully, organizations need to view security in the context of the larger picture—one of organizational or enterprise resilience. A resilient approach transforms the basic premise of security—that of “locking down” an asset so that it is free from harm—to one that positions security as a contributor to strengthening the organization’s ability to adapt to new risk environments and accomplish its mission. Aiming to make the organization more sensing, agile, and prepared provides a clearer purpose, direction, and context for security management. Looking beyond security (to resiliency) may provide the change in perspective that organizations need to balance security and risk management with the organization’s strategic drivers.

Series in Enterprise Security Management/Enterprise Resiliency

This article is the first in a series exploring a new view of security in today’s complex organizations. In future articles, we’ll discuss in more detail the evolutionary shifts that are needed in organizations to allow them to be more effective at managing security across an ever-changing enterprise. We’ll also present our current research on a process-centric view of security as a vehicle for improvement. Finally, the concepts of enterprise resiliency will be introduced, and we’ll explore the role that enterprise security management plays in the pursuit of resilience.

References

1 Hong, Namsoo; Al-Khatib, Wallid; Magagna, Bill; McLoughlin, Andrea; & Coehttp, Brenda. *Systems Theory*. http://www.ed.psu.edu/insys/ESD/systems/theory/SYSTHEO2.htm

2 Berinato, Scott. “After the Storm, Reform.” *CIO Magazine*, Dec. 15, 2003. http://www.cio.com/archive/121503/securityfuture.html

3 Starr, Randy; Newfrock, Jim; & Delurey, Michael. “Enterprise Resilience: Managing Risk in the Networked Economy.” *Strategy & Business*, Spring 2003. http://www.strategy-business.com

4 Mimoso, Michael S. “Measuring Security ROI a Tall Order.” SearchSecurity.com, April 15, 2002. http://www.searchsecurity.com

5 WordNet. Cognitive Science Laboratory, Princeton University. http://www.cogsci.princeton.edu