Management's Role in Information Security in a Cyber Economy

Amitava Dutta
Kevin McCrohan

Security issues have always accompanied the conduct of commerce and various mechanisms have been developed over the years to address them. However, the rapid and relatively recent diffusion of Internet-based electronic commerce (EC), while bringing numerous benefits, has also demonstrated the urgent need to craft new security mechanisms in this wired economy. Carnegie Mellon's CERT (Computer Emergency Response Team) coordination center notes that the number of reported security incidents and vulnerabilities had more than doubled from 22,000 in 2000 to 53,000 in 2001. This followed a similar growth rate from 1999 to 2000. Close to 27,000 incidents have been reported in only the first quarter of 2002. However, this is just the tip of the iceberg as only a fraction of the actual security "incidents" are ever reported. With information technology now pervading all aspects of a firm's value chain, security concerns have reached the boardroom. What new vulnerabilities does EC pose and what does senior management need to understand about them? What is senior management's role in crafting security for their organizations in this wired economy? Are their organizations prepared for the 21st century's electronic customer? A core message is that good security in an organization starts at the top, not with firewalls, shielded cables or biometrics. Senior management has a much more significant role to play in achieving security than they may think.

The opinions expressed in this article are solely those of the authors. Authors acknowledge the assistance of Mr. Mark Centra, OSD Command, Control, Communication, and Intelligence (C^3I); Captain Chuck Chassot, USNR, Defense-wide Information Assurance Program; Mr. Guy Copeland, CSC and the National Security Telecommunications Advisory Committee (NSTAC); Colonel Gene Tyler USA, Defense-wide Information Assurance Program; and an anonymous *California Management Review* referee in the development of this manuscript.

Since the term EC has so many interpretations, it is helpful at the outset to clarify our interpretation of the term. For purposes of this article, EC simply means the conduct of an organization's activities with increasingly heavy reliance on contemporary computing and telecommunications technologies across its entire value chain. By taking a value chain view of organizations, it is not necessary to distinguish variants such as B2C (business to consumer), B2B (business to business), C2C (consumer to consumer), and so on for present purposes. From our standpoint, an organization has an internal value chain and has to interact with external entities at either end of this chain. These external entities may be other businesses, individual customers, or the government. These interactions must be protected from being compromised by unauthorized parties, as must activities in the internal value chain. Although we are thinking primarily of organizations operating in a competitive environment, many of these security issues also apply to public sector entities at the local, state, and federal level. In fact, as government continues to deploy Internet-based technologies to achieve better internal efficiencies and service quality, they are facing many of the same security concerns as organizations in the private sector. However, the intelligence community and Department of Defense have distinctive needs and objectives and some aspects of our framework are not directly applicable to them. It is also helpful to distinguish "security" from its close cousin "privacy." Privacy deals with the degree of control that an entity, whether a person or organization, has over information about itself. Security deals with vulnerability to unauthorized access to content. Both are important issues in business, and although they are interrelated, they are also distinct. Clearly, one cannot achieve privacy without appropriate security mechanisms. This was demonstrated when the Justice Department ordered the Department of the Interior to shut down parts of its website related to Indian affairs because the department could not secure individual information that ought to remain private.[1] In another case, Eli Lilly's settlement with the FTC has required them to develop a data security program. This followed their inadvertently exposing the names of 700 subscribers to its Prozac.com reminder service.[2] The security breach compromised customer privacy expectations. However, security is not synonymous with privacy. This article primarily addresses the issue of security. The privacy question will surface from time to time only in as much as it is affected by the implementation of security measures or lack thereof. There are a whole host of social and political issues that determine privacy rights and obligations, which are outside the scope of this article.

Amitava Dutta is a Professor of MIS and holds the LeRoy Eakin Endowed Chair in Electronic Commerce at George Mason University. <adutta@gmu.edu>

Kevin McCrohan is a Professor of Marketing at George Mason University. <kmccroha@som.gmu.edu>

Security issues will become increasingly important with wider diffusion of EC. Larger and more traditional firms will bring assets, deep pockets, investors, and customers—with all of their attendant expectations—into the wired world. These investors and customers will not be the forgiving, technologically savvy individuals of the early Internet years. If the gap between their expectations and

reality is large and if the firm has not exercised due diligence in protecting its information assets, it will encounter significant corporate, and possibly personal, liability. In fact security professionals have cited liability as the number one concern, and a recent report from the National Academy of Science's Computer Science and Telecommunications Board (CSTB) notes that U.S. companies are not using available security measures to protect themselves from cyber attacks. They further note that companies producing unsecure software should be held liable.[3] Sager and Greene also suggest that the best way to make software secure is through liability actions.[4] However, while most organizations recognize the need to secure information assets, they have viewed it mainly as a technical problem to be addressed by system managers and/or the IT function, rather than by senior management. This will no longer suffice as projections for the future indicate that blended threats will become more common. Blended threats use multiple methods of propagation, attack multiple points in a system, and require no human action to spread. For example, the Nimda worm modifies web documents and certain executable files found on the systems it infects, and creates numerous copies of itself under various file names.[5] It has the potential to affect both user workstations (clients) running Windows 95, 98, ME, NT, or 2000 and servers running Windows NT and 2000. The infected client machine attempts to transfer a copy of the Nimda code to any IIS server that it scans and finds to be vulnerable.

One of the obstacles in engaging senior executives to address information security is the difficulty of connecting security expenditures to profitability. In fact, increases in security will have the opposite impact by increasing costs and in some cases reducing efficiency. Intangible benefits, such as customer confidence and goodwill are difficult to measure. Nevertheless, customer concerns with privacy and the resulting need for organizations to secure customer information have made the need for this justification process more urgent. Vijayan notes that customers injured by the loss of sensitive data may seek compensation;[6] and the National Academy of Sciences (NAS) has called for legislation that would increase the exposure of software and systems vendors and system operators for system breaches.[7] One insurer has increased premiums for clients that use Microsoft's Internet Information Server software.[8] While the focus appears to be on vendors at this time, it is very likely that in our litigious society, firms that unwittingly participated in a denial of service attack may also share liability. Therefore, firms will need to show due diligence in securing their systems. This will require a strong managerial focus on information security that goes beyond implementing technologies such as firewalls, intrusion-detection tools, content filters, traffic analyzers, and virtual private networks and will require having best practices for continuous risk assessment and vulnerability testing. It will also mean having corporate policies and procedures to initiate and manage these actions. This can only occur with a strong managerial emphasis on security. A recent KPMG study emphasizes this point, noting that multinational corporations are still far away from securing their networks and seem to be focusing on the wrong threats.[9] The study found that 85 percent of the respondents felt they gave enough attention to protecting their information, approximately 40 percent

thought their company could suffer a serious breach of security, and the majority of respondents believe that the best approach is to buy the right technology.

There are three main messages. First, security is not a technical issue; it is a management issue. It rests on three cornerstones—critical infrastructures, organization, and technology. One of these, critical infrastructures, is beyond the direct control of the organization and is subject to physical and cyber attack from an increasing number of players with a variety of motives. However, it is the responsibility of management to balance the three supports. Second, total security is a myth. Not all information is of equal value, nor is it technically possible to protect all information assets, and the firm must plan for continuity of operations in the event of security being compromised. Therefore the organization must determine what information assets must be protected and the degree of protection required for them. Third, as Internet-based commerce diffuses through society, there will be decreasing tolerance on the part of customers for cyber-related vulnerabilities. These three messages lead us to suggest a framework that can help organizations craft a more realistic and effective security solution compared to the current technology-dominated view.

Security is not a technical issue; it is a management issue.

A major implication of the proposed framework is that only senior management can initiate the plans and policies that address the different aspects of security in a balanced and integrated manner. Leaving security primarily to the IT function will strengthen just one of the cornerstones—namely, technology—and will not yield intended results. Security lapses are management failures more than technical failures. Senior managers can use the proposed framework as a roadmap to initiate security plans and policies and audit their implementation.

The Threat

In a recent annual Computer Security Institute (CSI)/FBI computer security study,[10] ninety percent of respondents, primarily large corporations and government agencies, detected security breaches. As was the case last year, forty percent of respondents, up from twenty-five percent in 2000, detected a system penetration from the outside. As in previous studies, the most serious financial losses occurred through theft of proprietary information. Forty-four percent of respondents were willing or able to acknowledge financial losses due to computer breaches. Respondents detected a wide range of attacks and abuses. They include denial of service attacks (forty percent) and computer viruses (eighty-five percent).

A host of adversaries are aligned against the firm's information, systems, and the critical infrastructures that support them. They include disgruntled current or former employees, hackers, virus writers, criminal groups, those engaged in corporate espionage, terrorists, foreign intelligence services, and information warfare by foreign militaries and various other actors. Hacking tools are readily

available on the Internet, with scores of hacker publications, hundreds of bulletin boards, and hundreds of thousands of web sites dealing with "hacking tips." At the present time, governments in approximately one hundred countries are engaged in developing the processes, doctrine, and tools to conduct information attacks.[11] Just as we have become more aware of cyber-threats to information assets, we are now aware of the concept of asymmetric warfare. The attacks on September 11st underscore the need to consider strategic planning issues related to critical infrastructure protection due to the dependence of EC on critical infrastructures outside an individual firm's direct control. The concept of "defense" has expanded from that of protecting the nation's people and physical assets to also include its information assets, as our economic and social well being becomes ever more dependent on them. An implication of this expanded concept of defense is that senior management needs to view information security planning through a lens that, while focusing primarily on the needs of their specific organization, also perceives the wider interdependence between individual organizational security actions and the nation's collective security.

Barriers to Security

The very nature of EC has the ability to amplify the number of accidental or deliberate "errors" and their adverse impacts on an organization. One aspect is just the worldwide diffusion of the Internet. While this opens up new business opportunities, it also increases an organization's vulnerability since so many more individuals of unknown origin and intent now have access to its systems. Managers need to recognize that many of the technical components of Internet-based EC that contribute to its reach, power, and flexibility are the very same ones that increase security risks. For instance, active web content, such as Java applets, enhances interaction with customers and suppliers. However, this technical capability requires programs created by external entities to run on an organization's machines. It is not possible to determine the full impact of each and every applet prior to running it. For instance, this threat can be present when users send each other animated jokes or greeting cards. In addition, many organizations seem to equate security with protecting content while in transit. They employ elaborate encryption techniques to protect passwords and credit card numbers during transmission and yet keep them completely unencrypted on their servers. Anyone who is able to break into the server will have access to private information. Organizations may have an extensive partnering network, making it more difficult to define the boundaries of their information systems. There is an inherent conflict between security and "open systems" architectures that facilitate EC interactions.

Quite apart from the technical aspects of EC that increase vulnerability, the aspects of leadership, management policy, organizational culture, and structure also have significant impact on security. For example, sophisticated security technologies can be rendered ineffective by a failure to differentiate among critical information assets, poorly designed operating procedures, or lax attitudes

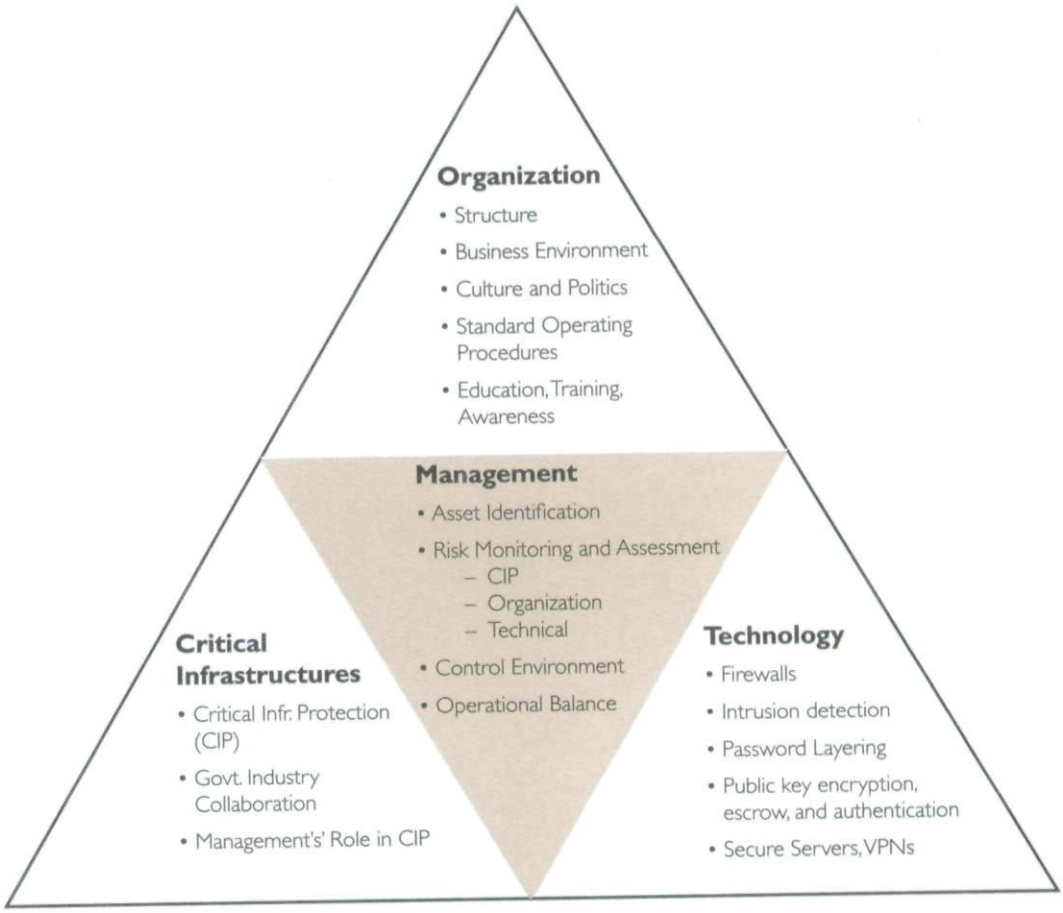
towards security within the organization. Our own experience with commercial and defense organizations bears this out. What good is a firewall if the e-mail account of a dismissed employee is not deleted for two years after his departure, or if intrusion detection logs are seldom checked? How effective can virus protection software be when employees do not care to update their virus signature files on a regular basis at work, or when they work on files using home computers without updated virus signature files? Organizations commonly look for technical certification when hiring IT staff, but how often is any effort made to educate these new security workers on the organization's strategic focus or to communicate to them the criticality levels of their information assets? Our experience and research indicates that this is seldom done in the private sector, leading to concern over just what is actually being safeguarded. This is not a concern with the integrity of IT staff, but with the fact that in the typical organization they are left without guidance concerning the importance of specific information assets.

While the firm has some control over the role of management and the technology and organization used to achieve security, it still faces threats to its operations from those who would attack the critical infrastructures that underpin EC and who are outside the direct control of the organization. The release by the FBI's National Infrastructure Protection Office (NIPC) of advisories dealing with Central European hackers (NIPC Advisory 01-003, March 2001) and the May Day attacks on U.S. web sites (NIPC Advisory 01-009, May 2001) are examples of these external threats. The only truly effective strategy for mitigating these threats lies in awareness and cooperation between private sector organizations and the public sector agencies charged with addressing them. This was demonstrated during the Code Red Virus in 2001 (CERT advisory CA-2001-19) as the public and private sector worked together to identify the threat, seek solutions, and then to ensure the broadest notification to users. The Code Red Virus is a self-propagating piece of code that exploited certain vulnerabilities in Microsoft's IIS server. From an infected machine, the virus would attempt to connect randomly, from day 1 to 19, to other hosts in order to propagate the worm. From days 20-27, it would launch a denial of service attack on a specific host. The worm would remain dormant on day 28 to the end of the month. Web pages on compromised machines were sometimes defaced by the following message "HELLO! Welcome to http://www.worm.com! Hacked By Chinese!"

In the case of the Central European hackers, the FBI took the unusual step of releasing information on an ongoing investigation. The hackers had taken advantage of a two-year old Microsoft Advisory that numerous firms had ignored. This occurred in spite of a subsequent Microsoft Advisory and an earlier NIPC Advisory. The failure of many firms to heed the earlier advisories exemplifies the problem. There was obviously a lack of managerial oversight, a failure of policies and procedures, a failure of technological solutions, and a failure to be aware of and cooperate with public sector efforts to

Security requires an end-to-end view of business processes.

FIGURE 1. Three Components of a Balanced Approach to Organizational Security



ensure information security. Senior managers need to remember that security depends on the strength of the three cornerstones—critical infrastructures, organization, and technology. They must also recognize that security requires an end-to-end view of business processes.

What specifically, then, can senior management do to carry out this responsibility? An organizational security approach can serve as a roadmap to help senior management identify risk areas and establish appropriate plans and policies. This approach specifically recognizes the three cornerstones identified above, enabling senior management to address security as the sociotechnical problem that it really is. Figure 1 illustrates the main elements of the roadmap. Senior management is located at the center to emphasize its pivotal role in identifying information assets, assessing risk, and initiating planning and policymaking. The corners illustrate major issues that must be addressed in each of the three areas in order to achieve a coherent security posture. In fact, using this

roadmap, one can clearly see the need for a balanced approach to organization's security, one that does not focus solely on technological solutions.

Critical Infrastructures

Involvement in critical infrastructure protection initiatives is the first cornerstone that supports efforts to establish a robust information security foundation. Critical infrastructures are defined as those that are so vital that their damage or destruction would have a debilitating impact on the physical or economic security of the country. These include telecommunications, energy, and banking, all of which have been attacked at some point by malicious hackers. Critical infrastructures are, in large part, owned by the private sector, used by both the private and public sectors, and protected in large part by the public sector.

Critical Infrastructure Protection

As one step in protecting the digital economy, President Clinton signed Presidential Decision Directive 63 concerning Critical Infrastructure Protection, on May 22, 1998. This order created a Presidential Commission charged with formulating policy recommendations to the President on measures to protect the critical infrastructures of the United States from cyber-based attack. At the same time, the Critical Infrastructure Assurance Office was established. These initiatives are continuing under the Bush Administration with Executive Order 13010 in October 2001. The genesis for these initiatives was the realization on the part of the scientific and national security community that the digital environment brought a counter-balancing array of threats along with its obvious advantages. Some early assessments of the nature of warfare in the digital arena suggested overwhelming advantage for the technologically sophisticated nations. These views were radically changed by a series of initially highly classified exercises named Eligible Receiver (1997) and the Evident Surprise Series (1996, 1997, and 1998) conducted by the U.S. Atlantic Command. Findings from these exercises were rapidly declassified as the true extent of the threat to the national information infrastructure emerged. At the present time, the public sector, and the federal level in particular, is well aware of the extent of the threats to national security and the economy. Prior to September 11, 2001, the private sector did not appear to share the same types or level of concern. In general, businesses were more concerned with economic loss stemming from actions of individuals or competing firms than with nation-state and non-nation-state actors and nation-state corporate espionage. They also were less willing to discuss these issues because of the loss of customer confidence and possible legal liabilities. However, following September 11st there has been a sense of urgency in both the private and public sectors that cooperation is necessary to understand the complete nature of the threat and develop effective solutions.

Government-Industry Collaboration

While government-industry cooperation in critical infrastructure protection has had some difficult moments, there are several examples of successful collaboration that have enhanced security. For example the Armed Forces Communication and Electronics Association (AFCEA) is an industrial association that represents 27,000 individual members and 12,000 corporate associates from government, military, and industry. AFCEA provides a forum in which leaders and decision makers from both government and industry can meet to exchange ideas and concepts, discuss current problems and solutions, and identify future technical requirements.

One of the best examples of government-industry cooperation is the National Security Telecommunications Advisory Committee, which was established in 1982 by President Reagan. It brings together the Executive Branch and twenty-three agencies with up to thirty CEOs from the Telecommunications/Information Industry. Over the years, they have conducted a number of programs and assessments, such as the National Coordinating Center for Telecommunications, the Commercial Network Survivability Assessment, and the Electromagnetic Pulse Assessment. While these organizations contribute to critical infrastructure protection, each fills a specific role and no single one can accomplish the mission of information security.[12] The NIPC is engaged in significant outreach efforts with industry sectors through their partnerships with industry Information Sharing and Analysis Centers (ISACs). This collaboration between government and industry allows both parties to capitalize on their strengths and provides a central point for information sharing. The NIPC is linked electronically to the rest of the federal government, including other warning and operation centers as well as private-sector ISACs. These ISACs allow the both government and industry to benefit from the sharing of information concerning threats, vulnerabilities, incidents, and reconstitution efforts. When threats or vulnerabilities are identified, these groups work together to develop appropriate guidance on additional protection measures to be taken. The value of ISACs has been demonstrated in a number of cases, most dramatically following the September 11st attacks, but also with the Code Red (NIPC Alert 01-016, July 2001) and Nimda (NIPC Advisory 01-022, September 2001) viruses and the Simple Network Management Program Internet vulnerability (NIPC Advisory 02-001, February 2002). In all of these cases, the sharing of information within and across ISACs led to more rapid reconstitution and remediation efforts.

Management's Role in Critical Infrastructure Protection

Although there are benefits accruing from public-private sector information security partnerships, cooperation has not been easy or automatic. First, trust relationships can be difficult to achieve and maintain. Second, any cooperative effort must be supported with personnel and funding, and resources are scarce within both sectors. It also requires leadership that can merge the interests and cultures of both sides. This may prove particularly difficult for the

private sector since they still appear to be struggling with the cost of information security at the enterprise level. Third, due to Freedom of Information Act (FOIA), Federal Agencies may not be able to guarantee the protection of propriety information. While this may limit private-sector information sharing, there are legal opinions that indicate that FOIAs are not as much of a barrier as they are perceived to be. Additionally, legislative efforts are underway to defuse the FOIA issue.

There are several benefits to public-private partnerships. They offer management the opportunity of reducing costs through sharing of common solutions to security problems, as well as the opportunity to present their point of view on the economic impact of the international aspects of information security. Additionally, it allows them to play a role in the evolution of "best practices" and help shape legal and government policies in the areas of Freedom of Information Act (FOIA), anti-trust, and other issues of mutual concern. Finally, such cooperation increases the firm's name recognition with government customers while at the same time developing managerial insights into governmental relations.[13]

It is incumbent on senior management in both the public and private sectors to provide the leadership to break down the cultural and organizational barriers to collaboration.

In short, management's role is to first recognize that critical infrastructure protection is an essential component of corporate governance as well as organizational security, and one that is beyond their direct control. This statement applies to senior management in both the private and public sectors; hence, they each have a vested interest in collaboration. It is incumbent on senior management in both the public and private sectors to provide the leadership to break down the cultural and organizational barriers to collaboration.

Organization

The second cornerstone that supports management's security efforts is an understanding of the organizational environment of the firm. All organizations are made up of individuals and they share certain common characteristics. Some of the key ones are structure, business environment, culture, politics, and standard operating procedures. Each of these characteristics affects organizational security and must be managed appropriately to achieve an overall security profile.

Structure

The structure of an organization determines the locus and ownership of the individual activities that support its business objectives. For instance, if there is no structural unit that is specifically responsible for security, implementation of security initiatives will be fragmented and may therefore be ineffective.

Extensive use of outsourcing would also be a structural characteristic that has an impact on security. If there is a security unit, its position in the organizational structure will have a major impact. For instance, if it is part of the IT operations unit, rather than in the CIO office, the security function may have limited authority to implement organizational changes necessary to improve security. Organizations with matrix structures have more complex information flows compared to purely hierarchical ones, making the former more vulnerable to compromise. Management's role therefore, is to ensure that an organization's structure facilitates the execution of business processes while keeping security needs in mind. This may mean isolating especially sensitive operations into distinct structural units and building additional security mechanisms around them. It may also require alteration of lines of communication, authority, or responsibility to achieve the desired security goals.

Business Environment

The Computer Security Institute identifies four factors of the firm's business environment that affect its potential for cyber-attack.[14] They note that an analysis of the value of the firm's intellectual property, the degree of change the firm is facing, its accessibility, and its industry position will provide some perspective on the level of threat in it's environment. To that we would add the extent of competition in the firm's core markets. For example, a rapidly growing firm with significant investments in R&D and proprietary information—one with a large network of customers and suppliers that is in fairly intense competition across markets and cultures—would face a very high probability of some form of cyber-attack. Additionally, firms that are in the news due to mergers, acquisitions, and major product introductions tend to be popular hacker targets. Given the dynamic nature of the business environment, only the involvement of senior management can ensure that the required degree of attention is paid to these threats at the appropriate time.

Culture

All organizations have a set of unwritten norms and values to which their members subscribe. This cultural dimension is a powerful force in enhancing or compromising security. For instance, universities are notorious for having a culture that is, at best, ambivalent towards security. In the recent past, there have been cases where foreign entities first compromised the information system of some U.S. university and then used that identity to launch cyber attacks against sensitive commercial and government web sites within the United States. Occasionally, a positive cultural trait can also compromise security. For instance, an organizational culture of high customer service may lead an employee to bypass standard operating procedure and give out sensitive information over the phone without adequate verification. Senior management's role here is to provide the leadership that establishes security as an important issue in the organization's psyche.

Standard Operating Procedures

Standard operating procedures are an important characteristic of any organization. They specify rules guiding the execution of common repetitive activities that underlie all business processes of an organization. Security considerations need to be built into such procedures. For instance, procedures for issuing or reissuing passwords, reporting security incidents, responding to security incidents of different severities, configuration control, and maintaining access logs are all standard operating procedures that can enhance security. Inherent in this is a set of procedures that establishes a culture of accountability for security and sensitive information.

Education, Training, and Awareness

To establish the concept that network security is important, users must be actively engaged in education and training that enhances security. Education should focus on how the security policy protects the assets of the organization and what happens if the policy is not followed. These consequences can be immediate, in terms of the negative consequences of not following the procedures. However, of much greater importance to the organization and the employees is the damage that can be done to the assets and survivability of the firm.

In addition to education, an organization should conduct training that will inform its employees of specific actions that need to be taken to protect against security violations. Training should also cover basics of technical tools that are available to mitigate the negative consequences of cyber attacks. Achieving a security posture involves a major organizational effort and senior management has a significant role to play in engineering these desirable organizational characteristics through proper planning and resource allocation.

Technology

Technology that is tailored to the market and to the security needs of the firm is the third cornerstone of support for the firm's security initiatives. While technological solutions are the responsibility of the IT staff, senior managers must be familiar with some of the critical components of security technology. They must also recognize the need for applying the concept of "Defense in Depth,"[15] including firewalls, intrusion detection software, password protection, key encryption and escrow accounts, authentication, secure servers, and virtual private networks.

Firewalls and Intrusion Detection

A firewall is simply a perimeter defense device that splits a network into trusted or protected, and un-trusted or unprotected side elements. The best firewall balances functionality, risk reduction, and cost in a well-managed fashion. Part of any defense will also require a network-based intrusion detection system (IDS) and procedures for monitoring and reporting incidents.

Password Layering

In addition to rigorous policies addressing the use of passwords, information should also be protected by password layering to protect differing levels of sensitive data and/or to allow different classes of workers access to the data. With such layering, a user who has access to only a limited amount of networked information will cause less harm if their system login password is compromised. Password layering involves technical as well as administrative issues since the technology must, first of all, permit the securing of information assets at different levels of granularity. However, administrative policies also govern who should have access to different granules of content. Enforcement of strong password policies may be the least costly and highest impact action that can be taken.

Public Key Infrastructure

Public key infrastructure consists of different technical and industry components that provide security and authentication based on the public key encryption method. Security protects content in transit and digital certificates provide the electronic means of identifying the sender. These certificates are issued by so-called certificate authorities that are supposed to verify the identity of the requester by independent means. One should realize that digital certificates, in and of themselves, do not offer any kind of guarantee that the sender is who they say they are. The rigor of the identification process used by a certificate authority is key.

Secure Servers

While advances in computing power have brought innumerable efficiencies, they have also brought intrinsic flaws arising from the extensive suite of functionalities in most servers. Any one firm does not require all of these functionalities. Hence, functionality can be restricted to provide only what is required. Limiting the purpose of a server has the additional benefit of reducing exposure to new security problems. This process requires a high level of interaction among users, managers, and systems administrators.

Virtual Private Networks

Virtual Private Networks (VPNs) are a relatively new concept in that the intent is to provide the security of a private network while operating over the public Internet. The attraction of this concept is that as the Internet diffuses nationally and internationally, VPNs offer the promise of leveraging this added reach in a secure manner for commerce and other activities. VPNs are especially significant for conducting distributed activities in a secure manner from ad hoc locations. In today's global economy, an organization's workforce may need to communicate sensitive content from a variety of locations on demand. VPNs offer a technical means to leverage the reach of the global Internet to perform this communication in a secure manner.

Clearly, there are many technical components that need to be put together in a coherent architecture to improve an organization's security posture. While crafting the technical architecture clearly falls within the domain of the IT function, senior management's role is to be aware of the capabilities of these different technologies and make the appropriate cost/benefit tradeoffs. This role is critical since there is no such thing as perfect security. An organization has to accept this reality and rationally decide what level of risk it is willing to assume. Only senior management is in a position to make that assessment, and this is another reason why organizational security cannot be handed over to the IT function.

There is no such thing as perfect security. An organization has to accept this reality and rationally decide what level of risk it is willing to assume.

Managerial Implications

Senior management's role in leading the information security posture of the organization is complex. It requires that senior managers understand the relationships among critical infrastructures, the organizational environment, and the technological base as they coordinate the process of asset identification, risk assessment, overseeing the establishment of a proper control environment, and achieving a balance between the costs and benefits of control.

Asset Identification

The process of asset identification allows senior managers, key users, and systems administrators to develop an understanding of the information that is critical to the firm and the systems that contain that information. It requires the management team to identify their information assets and the importance of attributes such as confidentiality, integrity, and availability. This process flows from the understanding that not all information should be protected at the same level and that some information and systems are so critical that their loss would have a negative impact on the continuity of the firm.

For example, a firm might classify the confidentiality, integrity, and availability requirements for customer information to all be high, whereas the confidentiality, integrity, and availability requirements for supplier information might be rated low, medium, and low respectively. As a result, information systems personnel can provide a level of security commensurate with the value of the information. Information asset identification is a nontrivial activity for all but the smallest organizations. Very few of them even know how many different systems they have, let alone the nature of their configuration. This shortcoming was very much in evidence during the Y2K crisis.

Risk Assessment

Since the nature and degree of threats faced by organizations vary, there needs to be a risk assessment of the likelihood that security will be compromised. Compromised security can mean theft or corruption of information assets or the inability to provide customer service for sustained periods. The risk to all three components of security needs to be assessed in a balanced way. For example, reducing technical risk without also reducing organizational risk does not result in reduced overall risk. Resources must be judiciously allocated among the three security components to address vulnerabilities and threats.

Vulnerabilities arise from weaknesses in each of the three components of overall risk. These weaknesses present opportunities for compromise and also affect the extent of damage when a failure occurs. For example, a lack of security training and inadequate background checks are weaknesses that can be exploited to damage organizational activities, while a lack of intrusion detection or backup and recovery mechanisms is a clear vulnerability on the technical dimension. Each risk component—critical infrastructure, organization, and technical—has its distinct sources of vulnerability. These vulnerabilities need to be identified and assessed as part of any security planning exercise.

Threats stem from combination of the actors and events that exploit vulnerabilities. Since September 11, 2001, there is a heightened awareness that there are many actors with the will and means to exploit critical infrastructure vulnerabilities. However, one need not be thrust into a situation of national crisis for threats to exist. For example, the "actor" can be nature. Fire, floods, and other acts of nature have been more frequent threats to critical infrastructure than determined terrorists. Organizational threats can arise from disgruntled employees with access to sensitive information or from competitors who are willing to probe the vulnerabilities of rivals. Technical threats arise from weaknesses in hardware, software, or networking elements that have the potential to compromise security. Identification of risk levels for all three types needs to be carried out in a structured and systematic manner involving the collective judgment of managers, end users, technical people, and appropriate public sector personnel.

The Control Environment

The ideal control environment starts with a simple statement of corporate security policy, endorsed by the CEO, that is widely disseminated and incorporated in standards of conduct for employees as well as in its business processes. This security policy is then translated into the appropriate control environment through actions taken by management.

A control environment can be broken down into two broad categories—general controls and application controls. General controls apply to any IT related activity within the organization, while application controls are specific to individual systems that support targeted applications.

General Controls

General controls are often broken down into the following subcategories: physical, data, implementation, operations, and administrative.

Physical controls are meant to protect and track elements such as hardware, software, and networks, as well as selected physical facilities. It is surprising to find that organizations often have difficulty keeping track of their physical information systems assets. Asset management software is available, but management needs to commit the resources to implement an asset tracking system. With the proliferation of powerful but cheap desktop and handheld computing devices, assets are increasingly being diffused across the organization, making them more difficult to trace and control. The loss of a laptop containing extremely sensitive plans from the State Department is just one high profile example of the lack of physical controls. The lack of a fire suppression system in a data center or locating the data center in the basement of a building that is in a flood area are other examples of a lack of physical controls.

Content is, generally speaking, much more valuable than the physical devices that store and disseminate it. Identifying content in a way that is relevant for security purposes is even more formidable than for physical asset identification. Content needs to be identified at the appropriate level of aggregation, as does the relationship among different information fragments. Data controls determine who has access to what content and for what purpose. That determination is a function of organizational policy, relevant laws, and business processes.

Implementation controls set up the proper checks to control design, development, and implementation of information systems. For instance, programmers in overseas countries performed many of the Y2K fixes. The Y2K problem may have been fixed, but what assurance is there that these non-U.S. personnel did not introduce yet-undetected vulnerabilities into the system? Separating the testing and development team and allocating adequate resources for testing are two examples of implementation controls.

Operations controls ensure that procedures are correctly applied to hardware, software, content, and networks on a continuous basis to reduce the likelihood of the system being compromised by accident or design. Monitoring of threat logs, performing regular backups, automatic fault detection and recovery processes, and automatic updates to virus profiles are all examples of operations controls.

Administrative controls place limits on business processes, personnel, and organizational structure in a way that enhances an organization's security posture. For instance, compartmentalization of structure and the associated stovepipes of information, long practiced by the intelligence community, can protect or enhance security. However, this may be impractical in a commercial setting where integrated business processes demand sharing of information across structural components of the organization. However, data controls can help mitigate this problem. Performing security checks when hiring systems

personnel and blocking access rights immediately upon termination of employee status are two more examples of administrative controls.

Application Controls

Application controls are specific to individual system components, and they depend on the functionality of the system concerned. An Intranet, for example, should only be available to persons within the organization. Hardware and software techniques to ensure that restriction would be examples of application controls. Firewalls and proxy servers are examples of specific applications and their filtering rules would also be examples of this type of control. Limiting the size of attachments on e-mail messages or the locations from where salaries can be changed in a human resource database are also examples of application control. Care should be taken to ensure that only authorized personnel can effect changes in administrative controls.

Balancing Costs and Benefits

While controls produce benefits, they also entail costs. In a commercial setting, it is necessary to make the business case for significant investments in security. While it is difficult to specify an algorithm for achieving this balance, it is possible to devise a systematic way of arriving at an appropriate level of security.

- Step 1: Identify information assets at an appropriate level of aggregation—e.g., specific databases, files, or transactions.
- Step 2: Identify the financial consequences of these information assets being compromised, damaged, or lost. For instance, revenue loss from a system being rendered unusable for a certain period of time can be estimated from historical data on transaction volumes and past revenues. Identifying the financial consequences of loss requires analyses of business processes that use these information assets.
- Step 3: Identify the costs of implementing the control mechanisms that are being proposed to enhance organizational security. These include the direct costs of the technologies and training as well as the so-called hidden costs of altering business procedures and organizational policies.
- Step 4: Estimate overall risk based on the likelihood of compromise.
- Step 5: Estimate the benefits expected by implementing the proposed security mechanisms. The benefits can be viewed in terms of cost avoidance. Expected benefits are obtained by comparing the loss figures obtained in Step 2 with the probability of compromise obtained in Step 4.
- Step 6: Compare the expected benefits obtained in Step 5 with the cost estimates obtained in Step 3. The costs associated with implementing security measures are not probabilistic since they are incurred whether or not security breaches occur, whereas the losses stemming from security lapses are probabilistic.

Management Actions

Corporate boards should ensure that senior managers buy into the process of risk assessment. While risk assessment in information security is currently more art than science, senior managers must actively participate in the process. Failure to exercise due diligence in information assurance, computer network defense, and security in general exposes the organization to liability and litigation risk in the event of a loss of data, services, or privacy. Senior managers should also understand that participation in national-level critical infrastructure protection efforts is also a matter of good corporate governance.

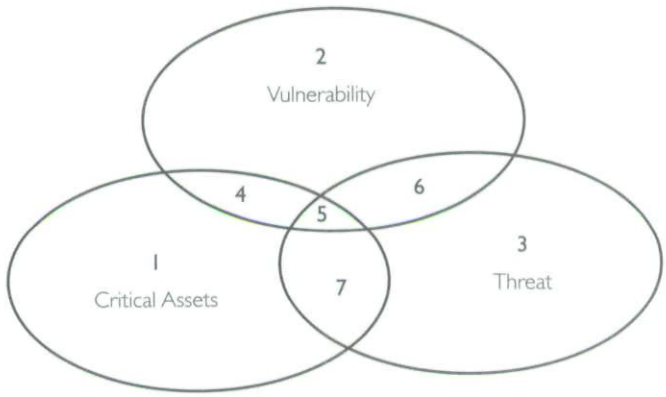
Senior managers also need to ensure that their technical and operational staff understand each other's requirements and are cooperatively engaged in the process. Organizations should adopt a security-oriented, minimalist approach to the acquisition of new technologies—and they should demand the same from their vendors. All potential technology acquisitions should be evaluated not only on their increased efficiencies, but also on their impact on security. All personnel should realize that new technological attributes might contain significant vulnerabilities. One effective way to implement this approach is to make security parameters an explicit and mandatory part of all requests for technology acquisitions. Security requirements should also be an explicit and mandatory part of all configuration control and testing procedures during the implementation of acquired technology. Finally, senior managers have the ability to influence external network factors. For example, they should require their external service providers to identify their continuity of operations plans for services to the organization. If the service provider's plans are not robust enough to meet management's requirements, they can request the necessary upgrades or find a new supplier.

All potential technology acquisitions should be evaluated not only on their increased efficiencies, but also on their impact on security.

While planning for information security is critical, an ongoing process of monitoring risk is just as important. Risk levels are not static. Technological vulnerabilities are uncovered over time, new actors with malicious intent appear on the scene, and political as well as economic relations among nations evolve over time. The corporate rhythm changes in response to these stimuli and there must be an organizational process for continual risk assessment. The process may be as simple as a monthly review by committee, or it may involve more complex real-time monitoring with alarms being triggered by preset conditions. Moreover, the government-industry partnership will, for many industries, play an important role in continual threat monitoring. Such continual threat monitoring will enable an organization's security posture to keep pace with evolving circumstances.

Figure 2 is a simple visual that can help senior managers organize their thinking. Region 1 represents critical assets—physical systems, content, people, and facilities—for which there is no known vulnerability and no known threat exposure. Region 2 covers vulnerabilities in systems, people, content, and

FIGURE 2. A Simple Risk Model



Based on Department of Defense, "DoD Insider Threat Mitigation: Final Report," April 24, 2000, p. 7.

facilities that are not associated with critical assets and for which there is no known threat exposure. Region 3 is the threat environment from which there is no known threat to critical assets or access to vulnerabilities. Region 4 identifies critical assets for which there are known vulnerabilities but no known threat exposure. Region 6 identifies threats that have acquired specific knowledge and/or capabilities to exploit a known vulnerability, although not a critical asset vulnerability. Region 7 consists of critical assets for which there are no known vulnerabilities, but which are exposed to a specific threat. Obviously, the region that demands immediate and constant attention is region 5, which consists of critical assets for which there are known vulnerabilities and which are exposed to threat. Notice the repeated use of the word "known"—which implies that the boundaries of the different pieces of the Venn diagram will change as knowledge of threats and vulnerabilities evolves.

Conclusion

Our increasing dependence on information technology in all spheres of activity, the increasing sophistication and attendant complexity of information technology, and exposure to diverse sources of cyber attacks has raised security concerns to new heights. Since security has technology, organizational, and critical infrastructure elements, senior management awareness and commitment is required to develop a control environment that balances the costs and benefits of security controls, keeping in mind the level of risk faced by the organization. The guidelines provided above can become the basis for planning and implementing a balanced approach to organizational security.

In the long run, a running public-private sector dialog would be most beneficial to reducing cyber-vulnerabilities in both sectors, as each side has

something to learn from the other. Elements within the public sector are uniquely designed to identify many of the threats that private sector firms face. The private sector owns, operates, and services the national information infrastructure. They are in a unique position to identify vulnerabilities in technological systems. However, it will take leadership and understanding on both sides to overcome some natural barriers to this collaboration, which include differences in organizational goals and views of threats, as well as cultural differences. Historically, industry has been skeptical of government leadership, but security is one area where the public sector, particularly the Defense establishment, has much to offer by way of experience and lessons learned. For its part, government has at times been reluctant to share its findings with the private sector. However, its dependence on the private sector for critical infrastructures makes that kind of isolationism counterproductive.

Notes

1. Jennifer Disabatino, "Department of Interior Shut Off From Internet Access," *Computer World*, December 7, 2001, <http://www.computerworld/storyba/0,4125,NAV47_STO66426,00.html>.
2. Reuters, "FTC To Settle Eli Lilly Privacy Probe," January 11, 2002, <http://news.c0m.com/2100-1023-808735.html>.
3. Linda Rosencrance, "CSTB Report Says Companies are Neglecting Security," *Security Focus*, January 8, 2002, <http://www.secyrityfocus.com/news/304>.
4. Ira Sager and Jay Greene, "Commentary: The Best Way to Make Software Secure: Liability," *Business Week*, March 13, 2002, <http://www.business.com/magazine/content/02-11/b3774071.htm>.
5. Symantec, "The New Danger: Blended Threats," article number 967, December 13, 2001, <http://enterprisesecurity.symantec.com/a...le.cfm?articleID=967&PID=9834967&EID=151>.
6. Jaikumar Vijayan, "IT Security Destined for the Courtroom," *Computer World*, May 21, 2001, <http://computerworld.com>.
7. Will Rodger, "Punish Security Lapses, NAS Urges," *SecurityFocus*, February 10, 2002, <http://www.securityfocus.com/news/304>.
8. Robert Bryce, "Hack Insurer Adds Microsoft Surcharge," *Interactive Week*, August 19, 2001, <http://www.zdnet.com.com/2100-1104-503993.html>.
9. Robert Lemos, "Report: Business Fails On Global Security," November 14, 2001, <http://www.zdnet.com/zdnn/stories/news/0,4586,5099609,00.html>.
10. Computer Security Institute, "Computer Security Issues and Trends: 2002 CSI/FBI Computer Crime and Security Survey," 2002, <http://www.gosci.com>.
11. Arnaud De Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, and Michele M. Ledgerwood, *Cyber Threats and Information Security Meeting the 21st Century Challenge* (Washington, D.C.: The Center for Strategic and International Studies, 2001).
12. Specifically, Presidential Decision Directive 63 (PDD-63) tasked federal agencies to assure the security of federal systems. It designated federal government "lead agencies" to work with private sector counterparts to address infrastructure assurance issues. It also encouraged the creation of mechanisms to facilitate establishment of a private sector entity to share information among industry owners and operators as well as creating a National Coordinator for Security, Infrastructure Protection and Counter-Terrorism to coordinate implementation of PDD-63. It also established a Critical Infrastructure Working Group (CICG) as an interagency coordinating mechanism for PDD implementation and established the National Infrastructure Protection Center (NIPC) in the Federal Bureau of Investigation (FBI) as the government focal point for responding to attacks. Finally, it directed increased government research and development to support protection efforts. The Critical Infrastructures and lead agencies are:

    Information and communications—Department of Commerce
    Banking and finance—Department of Treasury

Water supply—Environmental Protection Agency
Transportation—Department of Transportation
Emergency services
Law enforcement—Justice
Fire—Federal Emergency Management Agency
Medicine—Health and Human Services
Electric power, oil and gas—Department of Energy
Government services
Law enforcement and internal security—Department of Justice
Intelligence—Central Intelligence Agency
Foreign affairs—Department of State
National defense—Department of Defense

13. National Industrial Defense Association (NDIA), "Computer Network Defense: An Industry Perspective," an NDIA Study in support of U.S. Space Command, unclassified, (December 2000).
14. Ibid.
15. Richard Power, *Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare* (San Francisco, CA: Computer Security Institute, 2000).
16. Gerhard Cronje, "Choosing the Best Firewall," April 10, 2001, <http://www.sans.org/infosecFAQ/firewall/best.htm>.