DATA SECURITY MANAGEMENT

THE BUSINESS CASE FOR INFORMATION SECURITY: SELLING MANAGEMENT ON THE PROTECTION OF VITAL SECRETS AND PRODUCTS

Sanford Sherizen

INSIDE

INTRODUCTION
If the world was rational and individuals as well as organizations always operated on that basis, this article would not have to be written. After all, who can argue with the need for protecting vital secrets and products? Why would senior managers not understand the need for spending adequate funds and other resources to protect their own bottom line? Why not secure information as it flows throughout the corporation and sometimes around the world?

Unfortunately, rationality is not something that one can safely assume when it comes to the field of information security. Therefore, what is needed are strategies by which senior managers as well as information security professionals can maximize their specific interests.

This article is based on over 20 years of experience in the field of information security, with a special concentration on consulting with se-

PAYOFF IDEA
Rationality is not something that one can safely assume when it comes to the field of information security. Therefore, what is needed are strategies by which senior managers as well as information security professionals can maximize their specific interests. This article looks at the dialogue between information security and senior executives, offers reasons why such exchanges often do not work well, and suggests ways to make this a successful discussion.
nior- and middle-level managers. The suggestions are based on successful projects and, if followed, can help other information security professionals achieve successful results with their management.

THE STATE OF INFORMATION SECURITY
Improving information security for an organization is a bit like an individual deciding to lose weight, to exercise, or to stop smoking. Great expectations. Public declarations of good intentions. A projected starting date in the near future. And then the realization that this is a constant activity, never to end and never to be resolved without effort.

Why is it that there are so many computer crime and abuse problems at the same time that an increasing number of senior executives are declaring that information security is an absolute requirement in their organizations? This question is especially perplexing when one considers the great strides that have been made in the field of information security in allowing greater protection of assets. While the skill levels of the perpetrators have increased and the complexity of technology today leaves many exposures, one of the central issues for today’s information security professional is nontechnical in nature. More and more, a challenge that many in the field face is how to inform, convince, influence, or in some other way “sell” their senior management on the need for improving information security practices.

This article looks at the information security–senior executive dialogue, offering the reasons why such exchanges often do not work well and suggesting ways to make this a successful discussion.

SENIOR MANAGEMENT VIEWS OF INFORMATION SECURITY
Information security practitioners need to understand two basic issues regarding their senior management. The first is that computer crime is only one of the many more immediate risks that executives face today. The second is that thinking and speaking in managerial terms is a key to even gaining their attention in order to present a business case for improvements.

To the average senior executive, information security may seem relatively easy — simply do not allow anyone who should not see certain information to see that information. Use the computer as a lock against those who would misuse their computer use. Use all of that money that has been given for information technology to come up with the entirely safe computer. Stop talking about risks and vulnerabilities and solve the problem. In other words, information security may be so complex that only simple answers can be applied from the nonpractitioner’s level.

Among all the risks that a manager must respond to, computer crime seems to fall into the sky-is-falling category. The lack of major problems with the Y2K issue has raised questions in some managerial and other cir-
icles as to whether the entire crisis was manufactured by the media and technical companies. Even given the extensive media coverage of major incidents, such as the Yahoo, etc., distributed denial-of-service attack, the attention of managers is quickly diverted as they move on to other, "more important issues." To managers, who are faced with making the expected profits for each quarter, information security is a maybe type of event. Even when computer crime happens in a particular organization, managers are given few risk figures that can indicate how much improvement in information security (X) will lead to how much prevention of crime (Y).

With certain notable exceptions, there are fundamental differences and perceptions between information security practitioners and senior executives. For example, how can information security professionals provide the type of cost-justification or return-on-investment (ROI) figures given the current limited types of tools? A risk analysis or similar approach to estimating risks, vulnerabilities, exposures, countermeasures, etc. is just not sufficient to convince a senior manager to accept large allocations of resources.

The most fundamental difference, however, is that senior executives now are the Chief Information Security Manager (or Chief Corporate Cop) of their organizations. What that quite literally means is that the executives — rather than the information security manager or the IS manager — now have legal and fiduciary responsibilities to provide adequate resources and support for information protection.

Liabilities are now a given fact of life for senior executives. Of particular importance, among the extensive variety of liability situations found in an advanced economy, is the adequacy of information protection. The adequacy of managerial response to information security challenges can be legally measured in terms of due care, due diligence, and similar measures that indicate what would be considered as a sufficient effort to protect their organization’s informational assets. Unfortunately, as discussed, senior executives often do not know that they have this responsibility, or are unwilling to take the necessary steps to meet this responsibility. The responsibility for information security is owned by senior management, whether they want it or not and whether they understand its importance or not.

INFORMATION SECURITY VIEWS OF SENIOR MANAGEMENT

Just as there are misperceptions of information security, so information security practitioners often suffer from their misperceptions of management. At times, it is as if there are two quite different and quite unconnected views of the world.

In a study done several years ago, CEOs were asked how important information security was to their organization and whether they provided what they felt was adequate assistance to that activity. The results
showed an overwhelming vote for the importance of information security as well as the majority of these executives providing sufficient resources. However, when the IS, audit, and information security managers were asked about their executives’ views of security, they indicated that there was a large gap between rhetoric and reality. Information security was often mentioned, but the resources provided and the support given to information security programs often fell below necessary levels.

One of the often-stated laments of information security practitioners is how difficult it is to be truly heard by their executives. Information security can only work when senior management supports it, and that support can only occur when they can be convinced of the importance of information protection. Such support is required because, by the nature of its work, information security is a political activity that crosses departmental lines, chains of command, and even national boundaries.

Information security professionals must become more managerial in outlook, speech, and perspectives. What that means is that it is no longer sufficient to stress the technical aspects of information protection. Rather, the stress needs to be placed on how the information security function protects senior executives from major legal and public relations liabilities. Further, information security is an essential aspect of managing organizations today. Just as information is a strategic asset, so information protection is a strategic requirement. In essence, information security provides many contributions to an organization. The case to be made to management is the business case for information security.

THE MANY POSITIVE ROLES OF INFORMATION SECURITY

While people may realize that they play many roles in their work, it is worthwhile listing which of those roles apply to “selling information security.” This discussion allows the information security practitioner to determine which of the work-related activities that he or she is involved in has implications for convincing senior management of the importance of that work and the need for senior management to provide sufficient resources in order to maximize the protection span of control.

One of the most important roles to learn is how to become an information security “marketeer.” Marketing, selling, and translating technical, business, and legal concepts into “managerialeze” is a necessary skill for the field of information security today. What are you marketing or selling? You are clarifying for management that not only do you provide information protection but, at the same time, also provide such other valuable services as:

1. Compliance enforcer and advisor. As IT has grown in importance, so have the legalities that have to be met in order to be in compliance with laws and regulations. Legal considerations are ever-present to-
day. This could include the discovery of a department using unauthorized copies of programs; internal employee theft that becomes public knowledge and creates opportunity for shareholder suits; a penetration from the outside that is used as a launching pad to attack other organizations and thus creating the possibility of a downstream liability issue; or any of the myriad ways that organizations get into legal problems.

– Benefit to management. A major role of the information security professional is to assist management in making sure that the organization is in compliance with the law.

2. Business enabler and company differentiator. E-commerce has changed the entire nature of how organizations offer goods and services. The business enabler role of information security is to provide an organization with information security as a value-added way of providing ease of purchase as well as security and privacy of customer activities. Security has rapidly become the way by which organizations can provide customers with safe purchasing while offering the many advantages of e-commerce.

– Benefit to management. Security becomes a way of differentiating organizations in a commercial setting by providing “free safety” in addition to the particular goods and services offered by other corporations. “Free safety” offers additional means of customer satisfaction, encouraging the perception of secure Web-based activities.

3. Total quality management contributor. Quality of products and services is related to information security in a quite direct fashion. The confidentiality, integrity, and availability of information that one seeks to provide allow an organization to provide customer service that is protected, personal, and convenient.

– Benefit to management. By combining proper controls over processes, machines, and personnel, an organization is able to meet the often contradictory requirements of production as well as protection. Information security makes E-commerce possible, particularly in terms of the perceptions of customers that such purchasing is safe and reliable.

4. Peopleware controller. Peopleware is not the hardware or software of IT. It involves the human elements of the human-machine interface. Information security as well as the audit function serve as key functions in controlling the unauthorized behavior of people. Employees, customers, and clients need to be controlled in their use of technology and information. The need-to-know and separation-of-duties concepts become of particular importance in the complex world of E-commerce. Peopleware are the elements of the control structure that allow certain access and usage as well as disallow what have been defined as unauthorized activities.
– **Benefit to management.** Managerial policies are translated into information security policies, programs, and practices. Authorized usage is structured, unauthorized usage is detected, and a variety of access control and similar measures offer protections over sensitive informational assets.

The many roles of information security are of clear benefit to commercial and governmental institutions. Yet, these critical contributions to managing complex technical environments tend not to be considered when managers view the need for information security. As a result, one of the most important roles of information security practitioners is to translate these contributions into a business case for the protection of vital information.

**MAKING THE BUSINESS CASE FOR INFORMATION SECURITY**

While there are many different ways to make the business case and many ways to “sell” information security, the emphasis of this section is on the common body of knowledge (CBK) and similar sources of explication or desired results. These are a highly important source of professional knowledge that can assist in informing senior executives regarding the importance of information security.

CBK, as well as other standards and requirements (such as the Common Criteria and the British Standards 7799), are milestones in the growth of the professional field of information security. These compendia of the best ways to evaluate security professionals as well as the adequacy of their organizations serve many purposes in working with senior management.

They offer information security professionals the ability to objectively recommend recognized outside templates for security improvements to their own organizations. These external bodies contain expert opinion and user feedback regarding information protection. Because they are international in scope, they offer a multinational company the ability to provide a multinational overview of security.

Further, these enunciations of information security serve as a means of measuring the adequacy of an organization’s information security program and efforts. In reality, they serve as an indication of “good practices” and “state of knowledge” needed in today’s IT environments. They also provide legal authorities with ways to measure or evaluate what are considered as appropriate, necessary, or useful for organizations in protecting information. A “good-faith effort” to secure information, a term used in the U.S. Federal Sentencing Guidelines, becomes an essential legal indicator of an organization’s level of effort, concern, and adequacy of security programs. Being measured against these standards and being found lax may cost an organization millions of dollars in penalties as well.
as other serious personal and organizational punishments. (For further information on the U.S. Sentencing Guidelines as they relate to information security, see the author’s publication on the topic at http://www.computercrimestop.com/.)

MEETING THE INFORMATION SECURITY CHALLENGE

The many challenges of information security are technical, organizational, political, legal, and physical. For the information security professional, these challenges require new skills and new orientations. To be successful in “selling” information security to senior executives, information security practitioners should consider testing themselves on how well they are approaching these decision-makers.

One way to do such a self-evaluation is based on a set of questions used in forensic reviews of computer and other crimes. Investigators are interested in determining whether a particular person has motive, opportunity, and means (MOM). In an interesting twist, this same list of factors can be helpful in determining whether information security practitioners are seeking out the many ways to get the attention of their senior executives.

1. **Motivation.** Determine what motivates executives in their decisions. Understand the key concepts and terms they use. Establish a benefits approach to information security, stressing the advantages of securing information rather than emphasizing the risks and vulnerabilities. Find out what “marketeering” means in your organization, including what are the best messages, best media, and best communicators needed for this effort.

2. **Opportunity.** Ask what opportunities are available, or can be made, to meet with, be heard by, or gain access to senior executives. Create openings as a means to stress the safe computing message. Opportunities may mean presenting summaries of the current computer crime incidents in memos to management. An opportunity can be created when managers are asked for a statement to be used in user awareness training. Establish an Information Security Task Force, composed of representatives from many units, including management. This could be a useful vehicle for sending information security messages upward. Find out the auditor’s perspectives on controls to see how these may reinforce the messages.

3. **Means.** The last factor is means. Create ways to get the message heard by management. Meeting may be direct or indirect. Gather clippings of current computer crime cases, particularly those found in organizations or industries similar to one’s own. Do a literature review of leading business, administrative, and industry publications, pulling out articles on computer crime problems and solutions. Work
with an organization’s attorneys in gathering information on the changing legal requirements around IT and security.

**CONCLUSION**

In the “good old days” of information security, security was relatively easy. Only skilled data processing people had the capability to operate in their environment. That, plus physical barriers, limited the type and number of people who could commit computer crimes.

Today’s information security picture is far more complicated. The environment requires information security professionals to supplement their technical skills with a variety of “soft skills” such as managing, communicating, and stressing the business reasons for security objectives. The successful information security practitioner will learn these additional skills in order to be heard in the on-rush of challenges facing senior executives.

The technical challenges will certainly not go away. However, it is clear that the roles of information security will increase and the requirements to gain the acceptance of senior management will become more important.

**Additional Reading**


Sanford Sherizen, Ph.D., CISSP, is president of Data Security Systems, Inc., in Natick, Massachusetts.