

From *Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

---

# INTRODUCTION TO ACHIEVABLE ENTERPRISE SECURITY

When organizations begin to implement security plans, their frequently stated goal is complete security for their data and computing resources. If the organization launches a security project in response to a recent break-in or malicious compromise of the computing infrastructure, the goal becomes an imperative. Unfortunately, complete security is an impossible dream, no more achievable than complete security of one's home or person. However, by using the Enterprise Security Plan (ESP) presented in this book, companies can maximize security within the constraints of technology and the resources allocated to this problem.

## WHY CAN'T DISTRIBUTED SYSTEMS BE SECURED COMPLETELY?

By design, most computer systems are not secure. Computers are designed to process and communicate information, not to protect it. The networks that connect computers are also designed with communication, not security, in mind. So, when thousands of computers connect over even more network segments, numerous opportunities to breach security exist. In this context, layering security technologies over this computing infrastructure cannot create bulletproof system integrity.

Computer security systems attempt to minimize certain classes of identifiable risks. Similarly, a homeowner may choose to protect the house from burglary and fire, but not to protect it from tornadoes and earthquakes. A homeowner cannot possibly protect a house from every calamity, so maximum protection is obtained only for threats that he has specifically identified.

From *Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

---

Even if security managers limit security concerns to identifiable risks, they cannot attain complete security. Protecting the home against burglary, the homeowner cannot protect it against every conceivable means of malicious entry, so he has to be content with making the house impractical to break into by most of the common means of entry. Likewise, security managers can only contain even identifiable risks within defined limits.

Thus, the correct way to view the security question is to ask, "What level of security is achievable?"

## **WHAT IS ACHIEVABLE SECURITY?**

Going well beyond technology, the answer to this question requires companies to assess organizational structures, individual relationships, policies, and even the shadowy area of corporate politics. The likely result of this assessment is an extensive and possibly overwhelming list of security problems for security managers to address. Companies cannot address these problems all at once; nor can they address any of them overnight. However, by applying (ESP), companies can achieve a very secure computing infrastructure within the constraints of normal business operations, the resources a company is willing to invest, and today's technology.

## **WHAT IS ESP?**

ESP is a methodology that delivers the highest level of achievable security to the enterprise. It is a practical process and methodology for designing and implementing security, as well as a practical philosophy for solving basic business security problems. ESP is neither idealistic nor architecturally elegant. Rather, ESP is an approach derived from numerous successful security implementations rather than from academic theory.

From *Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

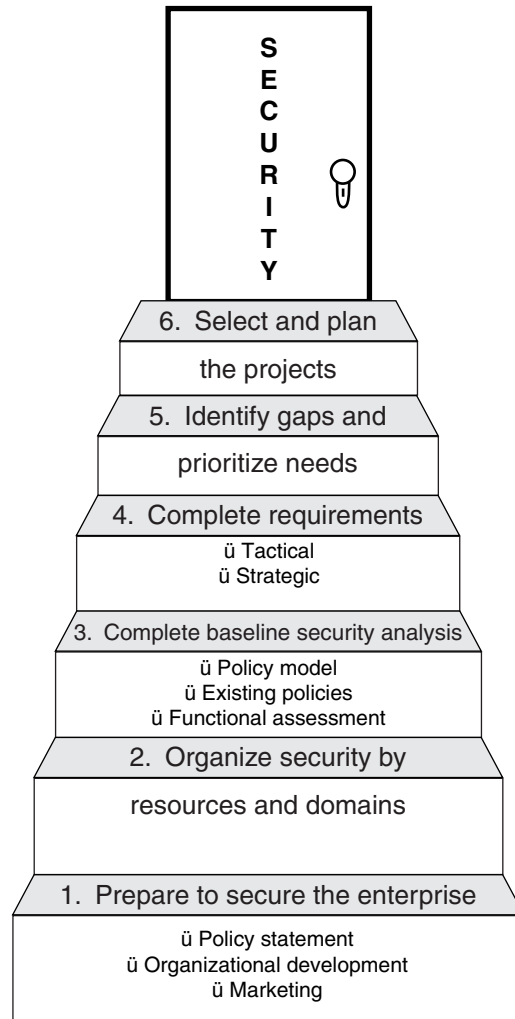
## **The ESP Approach to Achievable Security**

Applying ESP is not a completely sequential process. While this book divides ESP into six steps to better explain the tasks involved in the process, some tasks repeat themselves or overlap other tasks. The framework of the six steps should serve as a guide that an enterprise can tailor to its specific needs. Figure 0-1 shows the ESP steps. An overview of ESP that briefly describes each step in the process follows the diagram.

From *Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series



OM12727

**Figure 0-1. The steps in the ESP process.**

## **Step 1. Prepare to Secure the Enterprise**

This step is the most important in ESP, because without adequate preparation, any security program is doomed to failure. This preparation involves three tasks:

From *Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

- Building a foundation using the enterprise's need for security management
- Ensuring that the security systems are supported by an appropriately structured security organization
- Ensuring that the entire enterprise is motivated to support the new security initiatives

Motivating enterprise staff to support security is a key task in any ESP implementation. The effort starts with selling them on the general security program and continues through the last step, in which the security manager markets the recently implemented ESP projects throughout the organization.

The security program will create new roles and responsibilities. Users might have to adopt new procedures. For the entire enterprise to accept and implement these changes, management must be very supportive of the project. If the site has recently suffered a major breach, this support will come easily and even enthusiastically. But in the absence of this external incentive, the enterprise must maintain the support of management through the development period, especially, through the implementation and rollout of the security measures. Again, this first step is the single most important factor in the success of ESP.

## **Step 2. Organize Security by Resources and Domains**

Most organizations use a variety of computing platforms, operating systems, applications, and database management systems (resources) for a variety of discrete business functions (domains). Any attempt at correcting security problems must consider that the problems to be corrected outnumber the staff and money available for correcting them—at least in the short term. One step in planning security improvements is to assess and prioritize risk. However, long before reaching that step, the company must determine which areas of risk to assess.

Today's distributed computing environment offers too many risks to address them all. The process of selecting potential solutions starts by determining the problems. To do so, your security analysis must divide all the enterprise's resources—the business objects that require protection from unauthorized access—into security domains. These domains will allow managers to prioritize the risks they need to address later. This categorized information enables them to design a realistic and effective plan for implementing security where it is most needed.

### **Step 3. Complete the Baseline Security Analysis**

In this step, the security manager creates an inventory of the current state of security policies in a useful form and to a usable depth. He documents this baseline as a set of policies focused on the status of domains under study. Later, this set of policy statements either serves as the base document for expressing the changes to be made in the security policies, or it can be reused in the final policy documents.

### **Step 4. Complete Requirements**

Although by this point the security manager is likely to have some general sense of how secure the resources are and what security mechanisms reside in the company systems, he must now define the security requirements. Then, he needs to determine how management is enforcing security policies throughout the enterprise. Completing this definition leads to Step 5, which is the first occasion to compare the present reality with the stated goals.

### **Step 5. Identify Gaps and Prioritize Needs**

From the documents generated in Steps 3 and 4, the security manager can draw a fairly complete picture of the existing security system. In Step 5, he inventories the

From *Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

business issues of resource owners and the enterprise. When he compares this inventory to current procedures to reveal the gaps, he has the basis for formulating a list of tactical objectives—ones that security management can reach in a year or slightly more with current security technology.

Then the security manager easily can use the same information, the goals and objectives for resource owners and for the enterprise, to develop a list of strategic objectives—ones that will take longer than a year either because of the immensity of the task or because the technology is too immature or otherwise insufficient.

Once the security manager articulates these two sets of goals, he can establish a security-technology strategy. From this work, a security architecture emerges, one built on the security policies and technologies needed to satisfy the tactical and strategic objectives the security manager identified.

The security manager attacks the gaps described previously through individual security projects. Because he cannot bridge all the gaps at once—the company may not have the resources, technology, or time to do so—he must prioritize the tasks, giving higher priority to the ones that are most urgent and achievable. This activity involves analyzing risks to security.

By first dividing the scope of security analysis into “domains,” the security manager can divide problems into smaller units of work. In all areas of information technology (IT), smaller projects are more likely to succeed, generally because they require fewer resources and less time than large-scale projects. Frequently, the largest problem looks like the most important one. For example, at two separate client sites, the director of security walked around installing virus-detection software on individual PCs because this task was the biggest one on his to-do list. Certainly, the need for protection from computer viruses is an important issue. However, the task of installing virus-detection software is probably not the most important problem a

From *Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

---

director of security should attack. In fact, the task of installing software should belong to the technical personnel in the IT group. Security managers should be focused on more important security management tasks, such as planning and implementing ESP.

ESP requires security managers to identify security problems as variances from a desired state—the difference between the security measures currently in place and the security measures the enterprise needs. Understanding this key point allows security managers to perform analysis and prioritize tasks strictly in the context of the security goals for the organization.

## **Step 6. Select and Plan the Projects**

Developing sound plans for security projects is a primary goal of any ESP implementation. If a security manager can do the correct things in the best possible manner with the resources available, he serves the goal of achievable security: building an appropriately secure enterprise.

## **Modifying ESP for the Enterprise**

This book is intended for use in midsize enterprises—those with 3,000 to 50,000 employees. If the enterprise lies in a smaller range, security managers can probably bypass some steps. However, for organizations larger than 50,000 employees, security managers will most likely have to subdivide some of the steps, repeating the same processes at several levels of detail to complete the project. Ways to scale ESP for larger enterprises are discussed in detail in Chapter 7.

## **Seeing How ESP Works in Practice**

Some ESP processes explained in this book are better understood when presented using an example. To this end, Chapter 10 presents scenarios from two fictional corporations that show, step by step, how the directors of

*From Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

security in these enterprises use ESP to improve security. Documenting every task in a real situation would take too much space, so the sample scenarios highlight the most important tasks. Chapter 11 then shows how security managers implemented the security projects that were identified in the two scenarios.

## **USING TODAY'S TECHNOLOGY AND PLANNING FOR TOMORROW**

Security managers cannot provide security to an organization effectively if they do not understand what technology is currently available and what will be available in the foreseeable future. Security technologies are advancing at an almost unbelievable rate, due in large part to the constantly changing nature of the techniques used for gaining illegal systems access. The rapidity of change also reflects considerable advances in security technology, especially hardware.

Planning, even for the short term, is difficult when security managers must formulate strategies on the basis of today's technology—without knowledge of what the future holds. When the complexity of distributed computing systems is added to the mix, planning a workable security architecture requires significant knowledge of available tools.

Chapter 8 explains how to formulate a technology strategy to implement projects selected by the ESP steps. Chapter 9 explains the technologies themselves, their level of maturity, and the role they can fill in a security-conscious enterprise.

In addition to pure technology, knowledge of several best practices used at advanced IT sites today is important.

Two practices closely tied to enabling technology are important in meeting long-term security goals. The first of these is single-point administration (SPA), implemented through role-based authorization (RBA). SPA enables security managers to administer security for an individual

From *Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

---

from one point in a distributed system. Implementing SPA is no easy task and requires a good deal of planning, as illustrated later.

The second technique is single sign-on (SSO). From the users' perspective, having system security established so that they need to sign on only once to access all the resources their jobs require is highly desirable.

For example, an average employee had more than 20 separate sign-ons to perform. This situation reduces productivity, increases support costs, and earns the security officer the enmity of everyone from clerks to the CEO. So, reducing the number of sign-ons is a frequent driver for security projects. The supposed solution is software that delivers an SSO architecture. However, such software is not sufficiently mature to meet large organizations' enterprisewide needs without incurring very high costs. Still, using ESP, a company can begin implementing SPA and SSO and move quickly toward these best practices. This book covers SPA in Chapter 12 and SSO in Chapter 13. These detailed explanations are presented independent of the technology so security managers can choose the most effective means of implementing them for their specific site without tying the company to a single security package.

*From Securing Business Information: Strategies to Protect the Enterprise and Its Network*

by Dale Kutnick and F. Christian Byrnes

Intel Press IT Best Practices Series

## **ENSURING THE SUCCESS OF ESP PROJECTS**

Security projects fail primarily because the ESP management does not effectively market the projects to the enterprise staff, and the organizations created to support them are poorly structured. Therefore, security managers must do the following:

- Attend to organization, process, and political issues
- Strongly communicate and market security
- Recognize the inherent shortcomings of the available tools

If security managers attend to these needs, working through the ESP steps discussed in the rest of the book will be an enormous and important step toward ensuring the security and integrity of enterprise data and resources.

