



# Information Security Management in the 21st Century

by Lawrence D. Dietz

Director, Market Intelligence  
Symantec Corporation

**INSIDE** INSIDE

- > The nature of the threat
- > Security management from the top down
- > Goals of Information Security Management

# Contents

The situation today . . . . .	3
The nature of the threat . . . . .	3
Blurred attack vectors . . . . .	5
Enterprise targets are softer . . . . .	5
Security management from the top down . . . . .	6
Information security management—the systems perspective . . . . .	7
Goals of Information Security Management . . . . .	7
Conclusion—the big picture . . . . .	11
About the Author . . . . .	12

## > The situation today

There is no doubt that the worldwide dependence on information technology continues to accelerate. Businesses, governments, and other organizations are no longer able to function without computers and the networks that connect them. No one can go back to the simple days of pencils, papers, and calculators. This dependence has brought with it the increasing possibility that acts of nature and of the organization's adversaries may have an unanticipated negative effect on the ability of the organization to function.

### THE NATURE OF THE THREAT

Most experts agree that there are four major classes of demonstrated threats:

#### 1. Hackers and crackers

*Hackers* and *crackers* are outsiders who are performing acts designed to explore and likely degrade the IT infrastructures of their targets. The jargon is a bit misleading because in some circles *hackers* are considered 'good' and *crackers* are considered 'evil'. Nevertheless, both of these parties are credited with being technologically knowledgeable and able to use a variety of sophisticated as well as unsophisticated tools to penetrate a target.

#### 2. Authorized Insiders

Individuals who are properly authorized and given access to the IT infrastructure can—and often—perform operations that are improper. Many applications have been designed with on/off security so that access to the application enables a full range of privileges, many of which may not be relevant to the individual's role in the organization. For example, an administrative assistant may be given access to payroll records or expense reports even though the nature of their work has nothing to do with either.

Experts differ on whether outsiders or insiders represent the biggest danger, but there is no doubt that both represent potential harm to the organization and that steps need to be taken to minimize the potential damage.

#### 3. Hactivists

Generally outsiders, these individuals want to champion a cause to the detriment of their target. The most common action is web defacing where the attacker alters the appearance of the target's Web site to convey the attacker's message rather than that of the site's owners.

#### 4. Script Kiddies

These are more or less the stereotypical teenager or youthful hacker. They are outsiders who are motivated by the thrill of the hunt and/or the challenge of defeating a technological opponent. They have the time and the computer access but generally lack technical skills and therefore rely on the burgeoning inventory of 'hacker tools' that are freely available across the Internet. The nickname implies young adults without technical knowledge who rely on tools (scripts) to function.

There are three other classes of attacks but experts differ on their prevalence and likelihood.

1. **Information Warfare (IW)**

Information Warfare is defined as attacks against a nation's infrastructure by another nation, probably through the military. Today's lexicon divides Information Warfare into Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND). The nature of attack and defense should be obvious. One is designed to inflict damage and the other is designed to prevent it. CNE includes measures by which the adversary uses the advantages, features, benefits, etc. of the network to their own advantage. For example, hiding messages or using applications for reasons adverse to the target. CNE can also include passive measures such as capturing information and passwords for later use and nesting malicious code within the IT infrastructure for operations at a later time.

2. **Cyberterrorism**

Cyberterrorism is similar to IW because it employs the same types of acts but differs because the perpetrator is not a nation state but some other type of organization such as Al Queda, Hamas, etc.

3. **Organized Crime**

Another potential threat is organized crime. The famed bank robber, Willie Sutton, has been quoted as saying that he robbed banks because "that's where the money was." In today's world, much of the 'money' is in electronic form. Intellectual property, including trade secrets—not to mention account balances and key personal/customer information—and more are all stored electronically. Furthermore, electronic keys unlock functions that can transfer electronic and real assets at the click of the mouse. Given crime's historical flexibility by constantly moving to lucrative targets, it is not unreasonable to assume that this transference of power from the physical to the electronic has not gone unnoticed by criminals. So far, however, the 'big hit' has yet to be uncovered and organized crime's threat to information technology has not been regarded as severe, although that could change with tomorrow's headlines.

#### BLURRED ATTACK VECTORS

Until recently, computer attacks were regarded as more or less unidirectional. In the past few years however, there has been a blurring of the axis' or main directions of attack. Threats come by way of hackers, crackers, unauthorized acts by legitimate users, malicious code (viruses, worms, etc.), and through the exploitation of product vulnerabilities. Threats from any of these directions could be serious and in today's IT environments we are seeing combined or blended threats combining one or more attack vectors.

Overall, the nature of the threat is becoming more complex and more difficult to protect. Consequently some organizations are turning to an effects-based approach where the goal is to reduce negative effects on the ability of the organization to function. Increased target vulnerabilities are discussed below.

#### ENTERPRISE TARGETS ARE SOFTER

The nature of enterprises and their IT infrastructures are more open to attack for a variety of reasons. Business environments are becoming more complex because more components and software are being added to the mix. Applications are multiplying and the drive to optimize integration of legacy systems with the latest Internet technology continues unabated. Fueling the IT mix are an increasing number of new devices (mostly mobile) and wireless Local Area Networks (LANs), each of which exacerbates the security dilemma.

Additionally, business paradigms are changing from closed IT infrastructures to open access for employees, contractors, customers, partners, and others while security products have historically been designed to thwart particular threats—not combined or blended ones.

This helter skelter growth results in enterprises not being able to see the state of their security insecurity. Their security infrastructure is composed of products and services from different vendors that generate log and alarm data in different formats and languages. This mass of heterogeneous data generates a blurred/incomplete view of the overall security picture. This blurring of the traditional corporate perimeter has stimulated the need to distribute security controls throughout the organization.

## > Security management from the top down

Organizations need to assess their overall security using a top-down approach to get into what is needed for information security. At the top level there are three major components: physical security, personnel security, and information security. It would be impossible to address all aspects of these three areas in this paper. For the sake of illustration we will review comments on *Physical and Personnel Security* from International Standards Organization (ISO) Standard 17799.

Domain 7 of ISO 17799 divides Physical Security into several sub-sections:

- AREA SECURITY includes the physical security of the perimeter including physical entry controls. Securing offices, rooms, and facilities, working in secure areas, and isolated delivery and loading areas are the five major secure-area attributes.
- EQUIPMENT SECURITY includes addressing equipment siting and protection, power supply, capability security, equipment maintenance, security of organizational equipment that is off-premises, and the secure disposal or re-use of equipment by others.

The general controls of a clear desk and clear screen policy and guidelines covering removal of property round out the physical security arena.

ISO 17799 addresses personnel security in Domain 6 where it is divided into three areas: 1) Security in Job Definition and Resourcing, 2) User Training, and 3) Responding to Security Incidents and Malfunctions.

Key concepts are that everyone has a responsibility as a part of their job. Appropriate personnel screening needs to be in place along with confidentiality agreements and integrated security responsibilities amongst the terms and conditions of employment. End users must receive adequate security education and training.

Incident response consists of reporting security incidents, weaknesses, and software malfunctions, as well as methodology to learn from incidents and apply a disciplinary process if necessary.

References for physical security include:

- <http://www.asisonline.org/>
- <http://security.uchicago.edu/docs/physicalsec.shtml>
- <http://www.cerias.purdue.edu/coast/hotlist/physical/>
- <http://nces.ed.gov/pubs98/safetech/chapter5.html>
- <http://www.oa.doe.gov/sase/physical-sec.html>

Information security, in turn, consists of the combination of policies, procedures, and technologies. Policies and procedures are the heart of how security operates and include such areas as response to incidents as noted above. They will differ markedly from organization to organization. Policies and procedures need to be documented so that they are easily referenced and understood.

The technology implementing information security is a combination of hardware, software, and services. Services can be further divided into professional services, educational services, and managed security services. Professional services include help with policy design and development, technology procurement and implementation, etc. Educational services are mainly provided for awareness training for employees, contractors, and perhaps even partners. Managed Security Services deliver a variety of security functions for a monthly fee.

## > **Information security management—the systems perspective**

### GOALS OF INFORMATION SECURITY MANAGEMENT

The goal of information security management is to present a comprehensive, accurate, and timely picture of the state of the organization. This picture enables the organization to minimize the possibility of harm or interruption to the organization and, in the event of an adversarial event (incident), to mitigate the effect of the incident on the organization to allow full operations as soon as possible.

While the goals of information security management may be relatively simple to state, the practice is another matter. The reasons for this difficulty are discussed above but bear repeating here:

- Growing complexity of IT infrastructure
- Increased number and complexity of applications
- Greater access to more information by more people and organizations
- Growing threat complexity and increased capabilities of adversaries
- Information security architectures are heterogeneous resulting in data from security sensors being reported in varying formats and languages
- New areas of vulnerability created by wireless devices and LANs

Prior to discussing the nature of information security management it is necessary to establish some common terminology.

**EVENT** Any observable security-related occurrence in a system or network

**INCIDENT** Any adverse security event or condition, or the threat of the occurrence of such an event that requires action and closure; examples include unauthorized use of another user's account or system privileges, or execution of a blended threat attack such as Nimda.

**INCIDENT MANAGEMENT** Analysis through correlation of event and/or condition activity across a parent organization or constituency to help determine scope, priority, and impact to the business. Incidents may be thought of as events that require management attention. Events must be collected and managed from all security sensors throughout the enterprise. Another source of incidents is the existence of a known product vulnerability. To make certain that the organization is able to deal with vulnerabilities, they need a topical and reliable source of this information. Typically, this information is included as part of a response organization. Response includes the process by which an analyst identifies, contains, eradicates, and recovers from an incident. Reporting and measuring response times and compliance with service level agreements is another responsibility of the organization managing the incidents. From a legal perspective, incident management includes data forensics, which is the ability to create, validate, and preserve data in such a way as to be legally admissible in a court of law.

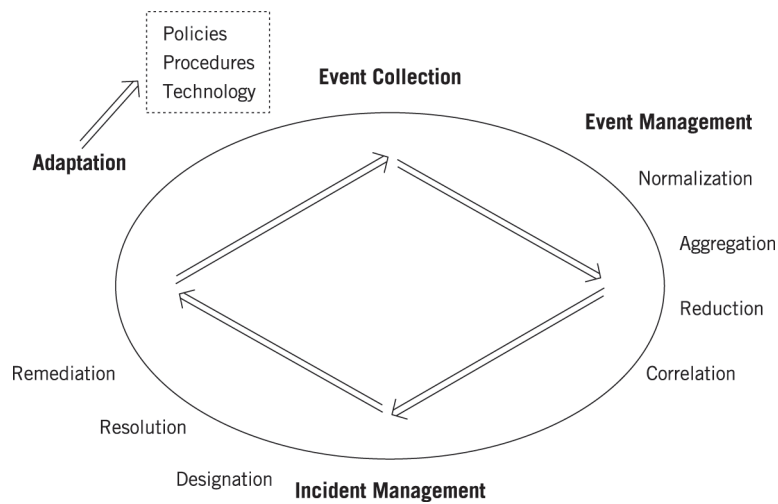


Figure 1. Security management flow.

Security Management is grounded in the organization’s management via policies and procedures. These policies and procedures form the roadmap of what is to be permitted or prohibited. The starting point for security management is the collection of the various events generated by antivirus, firewall, intrusion detection data sensors and by vulnerability assessment input. As noted above, a combination of information security functions needs to be performed in order to minimize the danger from blended threats. Each sensor generated log data that can be captured as events. The incompatibility of log data thrown off by so many different devices from several vendors makes the mass of data unworkable. Consequently additional processing is needed. Large, complex networks generate a tremendous amount of traffic. Part of the essential challenge of information security management is to determine which pieces of the traffic are relevant to the information security picture.

The relative order of magnitude of traffic, events and incidents is shown in the following diagram.

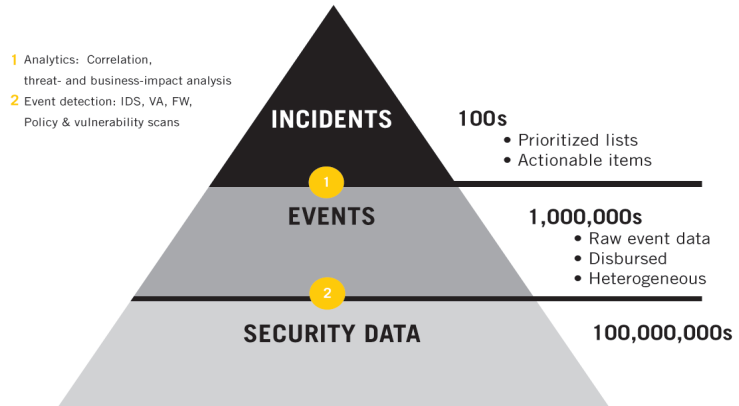


Figure 2. Order of magnitude for traffic, events, and incidents.

IT organizations are laboring under budget and manning constraints. Consequently they cannot afford the time or resources to wade through superfluous data. This means that once events are collected additional processing is needed as shown in Figure 3.

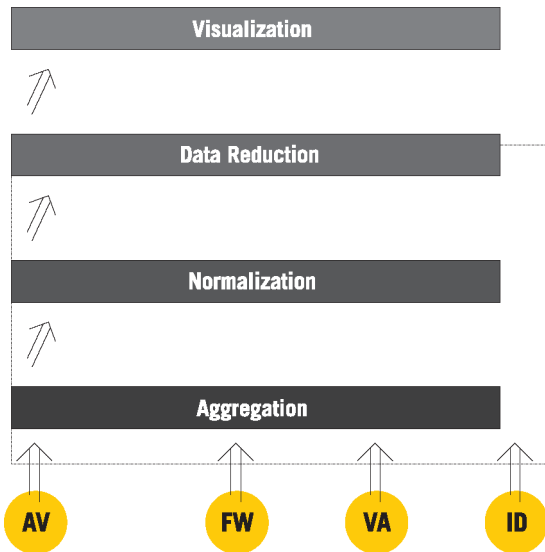


Figure 3. Event processing.

Events are collected and managed within each function. Event managers process events collected by all security sensors addressing the specific security function, e.g. antivirus, firewall, vulnerability, or intrusion detection. Managers forward all events for aggregation typically in a data store of some type. Once aggregated, the events are normalized, meaning that they are re-formatted for easy comparison and manipulation. Once normalized it is possible to eliminate events that are not relevant, i.e. data reduction. With respect to product vulnerabilities it is important to emphasize that today's threats have multiple attack vectors including exploiting known product vulnerabilities. It is therefore critical to categorize a vulnerability as an incident requiring management attention. This is a two-step process. First, there must be an awareness that the vulnerability exists. Given the large number of vulnerabilities reported daily this is a daunting requirement in and of itself. The next step is to determine if the vulnerability has been corrected. An incident is created when the vulnerability is discovered in an uncorrected state.

Subsequent actions on the reduced, normalized and aggregated data include visualization and reporting. The ability to analyze a variety of events from multiple sources to come up with predictors of future activity is called correlation. Correlation techniques are often employed within individual security functions and at the enterprise level.

Symantec's approach to information security management is embodied in our Symantec Security Management System products that have been built in conformance with the Symantec Enterprise Security Architecture (SESA). SESA provides common ground rules for Symantec product development and an open framework for other products as well. Symantec products are built with event collection and management capabilities and event collectors are or will be available for other major security products as well.

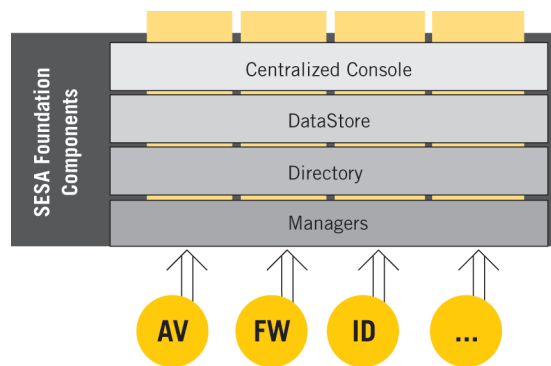


Figure 4. SESA Foundation.

The figure above shows how the security sensors feed into event managers which are a part of SESA. The DataStore provides a repository for security data and the centralized console provides a window into that data. Since the DataStore is maintained in a standard database such as DB2, Oracle, or SQL Server, traditional database management and data-mining techniques and tools can be further employed to analyze the data.

Once events have been properly formatted and stored the next challenge is to determine which of those events require further attention by management. Incidents have been defined as any adverse security event or condition or the threat of which requires action and closure.

Incident management is an ongoing process that consists of six phases: prepare, identify, contain, eradicate, recover, and document. *Prepare* means to lay the groundwork and inventory the components of the IT infrastructure. It also presumes to set up priorities, standard operating procedures, etc. *Identify* is confirming the nature of the incident; *contain* is to limit the damage; *eradicate* is to eliminate the threat; *recover* means to restore operations and data to their previous condition; and *document* means to record everything that you have done in the process.

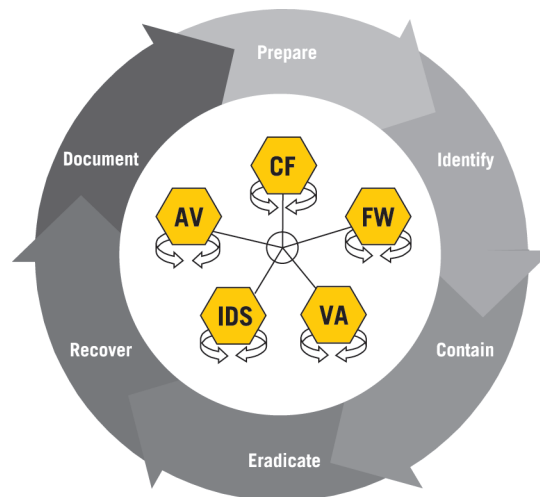


Figure 5. The Incident Lifecycle.

Antivirus and intrusion detection in particular have historically employed past behavior (virus definitions and intrusion detection signatures) as the way to determine likely problems. It has become clear that tomorrow's attacks are likely to be markedly different from today's and that reliance on previously discovered patterns may not be a completely reliable methodology in the future. Addressing this issue is correlation. The *Merriam Webster* definition of correlation is the process of connecting in a systematic way or establishing the mutual relationships. Correlation, in the context of information security, means the ability to draw conclusions from a mass of data where patterns may not have previously existed. The exact nature of correlation is beyond the scope of this paper but suffice it to say that information security managers will become more conscious of correlation capabilities over time.

## > Conclusion—the big picture

Information security management will become a more critical function of organizations as they continue to place increased reliance on the Internet and field more complex IT infrastructures. The heterogeneous nature of IT environments and the information security infrastructure that supports them will require significant attention as the business and regulatory climates add to the pressure.

Effective and flexible information security management is the key to business continuity. Large end-user organizations in particular must know the state of their security at any point in time and at any point in the enterprise. The notion of a closed perimeter is as much a part of history as the Maginot line and there is a pressing need to apply prudent security measures to safeguard ever-changing business models.

> **About the Author**

Lawrence Dietz has over 30 years of military and commercial experience. Previous roles have included senior research, marketing, and customer support roles. He is a licensed attorney in California and retired from the Army Reserve as a Colonel after 27 years of intelligence and information operations assignments. He holds BS in BA from Northeastern University; MBA, Babson College; JD, Suffolk University; LLM in European Law; and MS in Strategic Studies from the U.S. Army War College.

**SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.**

**FOR MORE INFORMATION, PLEASE VISIT [WWW.SYMANTEC.COM](http://WWW.SYMANTEC.COM)**

**WORLD HEADQUARTERS**

20330 Stevens Creek Blvd.  
Cupertino, CA 95014 U.S.A.  
408.517.8000  
800.721.3934

[www.symantec.com](http://www.symantec.com)

**For Product information  
In the U.S. call toll-free  
800.745.6054**

**Symantec has worldwide  
operations in 38 countries.  
For specific country  
offices and contact numbers  
please visit our Web site.**