

# THE CASE FOR HOLISTIC SECURITY

## The Integration of Information and Physical Security as an Element of Homeland Security

by

Caroline Ramsey Hamilton

### BACKGROUND

Since the advent of computer systems and widespread use of the internet, the function of Information Security Officer has been artificially separated from the Corporate (or Physical) Security function. Now, in an increasingly networked, post 9-11 world, these two security areas are moving closer and closer together. As both private corporations and government agencies struggle with the demands of maintaining a heightened level of security, issues of how information security should interact with physical security move into the spotlight.

There are several reasons for this convergence between information security and physical security. One of the primary reasons is because physical security elements have become increasingly computerized and networked. Physical lock and key systems have been replaced by smart cards that not only allow employees access to different areas in a facility, but also may keep audit trails of where employees spend their days.

Another example of this trend is surveillance cameras. Surveillance cameras, also known as CCTV (Closed Circuit) cameras, are used to record everything that they see on VHS tapes. The obvious problem with VHS tapes is that someone has to change the tapes frequently, that is, take out the full tape and replace it with an empty tape. Time and time again, computers and other company property would disappear at precisely the moment that the tape switch took place. Many companies have now switched to newer digital technology, which eliminates the need to change tapes and creates a continuous audit trail. Of course, this record has to be protected, because it can't be locked up in a cabinet like the old VHS tapes.

Smart buildings are another example of old technology that has been replaced with digital, networked technology. Coordinated by a single network console,

the smart buildings today can control access to different areas of the facility, control fire alarms and security system alarms, as well as control the heating and air conditioning units within the facility. A major provider of physical security solutions describes their product as "offering an all-encompassing security environment for multi-server enterprise system topology, central server systems, and mobile enterprise systems"; *supporting applications for access control, alarm monitoring, ID management, physical asset management, digital video surveillance, recording/archive management, smart card, biometrics and visitor management functions.*

These new technologies for physical security have taken the practice of physical security to a new level, yet many of the practices that are commonplace in information security have not been adopted in this new environment.

### DEGREES OF SEPARATION BETWEEN INFORMATION & PHYSICAL SECURITY

Prior to 1995, the information security management and physical security management were completely separated. The information security officer position started with simple data center security, and then grew into the information security environment in which computers were on every desktop and eventually linked to the internet. Because the computer systems operations were managed out of the MIS (Management Information Systems) department, the security function was also created at this level in the organization.

By contrast, the physical security officer was usually a former policeman, or someone with a military background, whose main responsibility was creating and/or managing a uniformed guard service, keeping track of keys and managing a visitor badging program in the front lobby.

Today, the information security officer position has become increasingly technical and may have little

knowledge, or interest, in maintaining physical controls such as barriers, badges, security alarms, or, as they say, “guns, guards and dogs”. At the same time, the physical security officer has had to become more technical to manage the new electronic controls.

Many companies have created new management structures to support the integration of information and physical security. Often, the Corporate Security Director is responsible for both types of security, with the Information Security Officer and the Physical Security Officer both reporting to the same individual. In some of the organizations that were interviewed for this article, the security offices are co-located, to facilitate information sharing between the two halves of the security program.

### **SAME WORDS - DIFFERENT MEANINGS**

Another aspect of this “dead zone” between information security and physical security is that the terminology used to describe different security functions consists of virtually the same words, but with different meanings. “Access control” in the physical security world means controlling how people get physical access to a facility. “Access control” in the information security world means a software solution for controlling which network users are able to access what information.

Intrusion detection is also a term with double meaning, depending on which side of the security fence you’re on. If you’re on the physical security side, intrusion detection could mean making sure that there are sensors around the building and on the windows, or in storm drains. If you’re on the information security side, intrusion detection would mean software controls that alert you when an unauthorized user tries to enter your network, or it could mean a managed service that provides continuous intrusion detection for the network. Other examples of same terminology, different meaning include audit trails, security policy, emergency response, disaster recovery, and maintenance.

Since September 11<sup>th</sup>, the gap between information security and physical security has been more apparent -- and more dangerous. Physical information about a facility, an airport, or an operations center of a U.S. embassy overseas including blueprints and wiring diagrams, all become very sensitive and need to be protected according to best information security practices.

In the past, many government reports by the GAO (General Accounting Office) have discussed the disconnect between physical and information security, citing examples of network operations centers with all

the latest computer security devices, but without the proper level of physical security. In the GAO Report T-AIMD-98-170, May 19, 1998, Information Security: Serious Weaknesses put State Department and FAA Operations at Risk,

*“Because physical security is the agency’s first line of defense against criminal and terrorist attack, the failure to beef up physical security at air traffic control towers, terminal radar approach control facilities, and en route centers places property and the safety of the flying public at risk. Information security safeguards cannot be fully effective as long as FAA continues to operate with significant physical security vulnerabilities. Also, because FAA has not assessed physical security controls at all its facilities since 1993, it does not know how vulnerable they are.”*

### **INTEGRATION THROUGH RISK MANAGEMENT**

Risk management is a primary element of Homeland Security. Risk assessment looks at a variety of threat scenarios, factors in the value of the organizational assets, completes vulnerability assessments and then calculates both a risk factor, as well as solutions that are robust and cost effective.

The risk assessment process includes gathering information about the assets of the organizations, including all information assets such as networks, data centers, computers, hardware, software, data/information; as well as physical assets, such as the personnel who staff the organization, the network users, the physical facility and dozens of other organizational resources. In addition, the risk assessment process includes finding sources for comprehensive threat data, which may be data gathered from internal sources such as incident report data, intrusion detection software, as well as threat data such as crime statistics, industry standards and benchmarking data, and historical data about what has happened in the organization previously.

The Risk assessment programs that include both information security and physical security can assist in integrating these two security activities by assessing security across the entire enterprise, by finding out how employees perceive security in the organization and how they do their job, and by justifying the need for security improvements across the complete spectrum of security.

### **VULNERABILITY ASSESSMENTS**

Vulnerability assessment is another term that means something different whether you are analyzing a network with a penetration test, or whether you are walking around the Port of San Francisco, looking for

physical security weaknesses such as waterside access to the ships, lack of vehicle controls over truck traffic through the shipyard, or lack of personnel screening for longshoremen. As a key element of the risk assessment, both kinds of vulnerability assessment (i.e. both technical and organizational) must be conducted.

The top technical vulnerability assessment product “provides comprehensive network vulnerability assessment for measuring online security risks, performs scheduled and selective probes of communication services, operating systems, applications and routers to uncover and report system vulnerabilities that might be open to attack”. At a recent security conference, an attendee expressed interest in a new “Port Vulnerability Assessment product”, and was surprised to find out that the product was designed for seaports, not computer ports.

The total vulnerability assessment process will integrate the penetration tests done on network resources, as well as a compliance based organizational assessment to give a true three hundred sixty degree look at the organization security practices, its employees understanding of and compliance with those practices.

### HOMELAND SECURITY

One of the chief elements in current and future Homeland Security initiatives is federal grants to local (state, city and county) governments. To look at the kind of dollars that are being made available, the President’s Fiscal Year 2003 Budget proposes \$3.5 billion in funding to prepare state and local first responders for terrorist attacks. Specifically, the initiative would include grants for planning, training, exercises, and equipment. While Congress has not acted on the President’s proposal, the Federal Emergency Management Agency (FEMA) is preparing to implement the program if enacted by Congress. In addition, FEMA has requested that Congress appropriate \$326 million in FY 2002.

In a proposed organization chart for the new Department of Homeland Security, information analysis, infrastructure protection, cybersecurity, physical assets, telecommunications and cybersecurity are correctly placed in the same management structure. In addition to computer security and network security, there is an increase in the kinds of information that need to be protected. All the facility vulnerability assessments that are currently being done on federal buildings, national landmarks, bridges, and seaports, as well as all the vulnerability assessments that are done on computer systems and networks, need to be protected at the highest possible level.

One of these sensitive reports has already been disclosed. On November 24, 2002, the Orange County Register reported, “The Los Angeles and Long Beach ports remain largely exposed to terrorist attacks that could lead to mass casualties or “an ecological disaster of biblical proportions,” a report to the federal government shows. The vulnerabilities are detailed publicly for the first time in a grant request submitted this year by the nation’s largest cargo port complex. Port officials sought more than \$70 million in federal security funds. About \$6 million was received”.

“In the March 29 grant request - which was obtained under the California Public Records Act - Port of Long Beach officials paint a bleak picture of the state of security at the complex, which handles 43 percent of the nation’s container cargo traffic.

Among the problems: A lack of patrol boats and law-enforcement officers leaves many critical port facilities largely unprotected from a waterborne attack. Hazardous chemicals stored in above-ground containers near shore could be targeted by terrorists, creating toxic clouds that would injure or kill hundreds of thousands of people living downwind. The port has no efficient system for screening cargo containers that enter the port from the land side, leaving the complex vulnerable to weapons of mass destruction loaded inside the United States. A shortage of ground police patrols and surveillance cameras allows trespassers to wander around sensitive port facilities with little scrutiny. No system exists for providing evacuation information in the event of a terrorist attack, and officials fear lives could be lost as scores of visitors and employees scramble to escape the sprawling complex. The Orange County Register withheld the most sensitive details of the 84-page report but decided to publish the broad findings”.

*-- The Orange County Register*

### RETURN ON INVESTMENT

The new Homeland Security funding initiatives look at the total security profile of an organization and, using a risk assessment process, prioritize the potential security expenditures by their Return On Investment, that is, which new safeguards provide the “most bang for the buck”. How else does an organization decide whether to implement personnel screening procedures, or hire additional guards, or invest in a managed service to protect their networks?

The cost benefit analysis combines information from the vulnerability assessment along with relevant threat data and asset information such as present day replacement

values, criticality, integrity and availability of the information contained in the system under review, as well as how completely safeguards are currently being implemented. The result of the cost benefit analysis will be to create a return on investment ratio (ROI), balancing the value of the information against the cost of controls to protect it. By establishing Return On Investment data, managers and directors can strengthen their grant requests and make more informed decisions regarding which controls to implement, based not strictly on initial cost, but also on the current threat exposure of the organization.

### **THE THREE INTEGRAL CONCEPTS OF HOLISTIC SECURITY**

According to GAO Report GAO-02-687T April 25, 2002, "The terrorist attacks of September 11 have heightened concerns about the physical security of federal buildings and the need to protect those who work in and visit these facilities. These concerns have been underscored by reports of long-standing vulnerabilities, including weak controls over building access. There are several commercially available security technologies that can be deployed, ranging from turnstiles, to smart cards, to biometric systems. Although many of these technologies can provide highly effective technical controls, the overall security of a federal building will depend on **robust risk management processes** and implementing **the three integral concepts of a holistic security process: protection, detection, and reaction**".

The report continued, "The approach to good security is fundamentally similar regardless of the assets being protected. As GAO has previously reported, managers are being asked to create risk management justification for their requested funds and the controls they need are a combination of strong information controls and strong physical controls.

Additionally, in an environment in which many information technology budgets have been reduced, the application of homeland security and information systems security, applying risk management principles, can provide a sound foundation for effective security, whether the assets are information, operations, people, or federal facilities".

**"Protection** provides countermeasures such as risk assessment, policies, procedures, and technical controls to defend against attacks on the assets being protected. **Detection** monitors for potential breakdowns in protective mechanisms that could result in security breaches. **Reaction**, which, responds to detected breaches to thwart attacks before damage can be done. Because absolute protection is impossible to achieve, a

security program that does not also incorporate detection and reaction is incomplete. Protection, Detection, and Reaction are Integral Security Concepts".

"However, of foremost importance is to continue to bear in mind that effective security can never be achieved by relying on technology alone. People will always play a fundamental role in all phases: from planning to implementation and to enforcement. Accordingly, technology and people must work together as part of an overall security process, beginning with a risk management approach and incorporating, implementing, and reinforcing those three essential concepts".

### **THE CASE FOR HOLISTIC SECURITY**

The integration of information security and physical security is an important trend that is becoming more widespread across both private corporations and government agencies. City, state and county governments of information security practices and new physical security technologies allows both better security overall, as well as continues to advance the state of information security.

### **ABOUT THE AUTHOR:**

*Caroline R. Hamilton is President of RiskWatch, Inc., a company specializing in security risk management software for both information and physical security. She was a Charter member of the National Institute of Standards and Technology's Risk Management Model Builders Workshop from 1988 to 1995. From 1996-1998, she served on the working group to create a Defensive Information Warfare Risk Management Model, (DIWRM2) under the auspices of the Office of the Secretary of Defense. She is a member of the ASIS International Council for Information Security and Technology, and the Maritime Security Council.*