

***REPRINTED WITH PERMISSION***  
***SECURITY TECHNOLOGY AND DESIGN – APRIL 2004:***

## **THE FUTURE OF SECURITY**

### **The Integration of Information Security, Integrated Systems Security and Physical Security**

by Caroline R. Hamilton

The single most important trend in security in the next ten years will be the integration of various security elements such as information security, physical security and integrated systems security into a single security function. The development of this trend can already be seen in the increase in the number of Chief Security Officers (CSO), elevating the security director to a “C-Level” position alongside the CEO, CIO and COO. Chief Security Officers are appearing in companies like Oracle, Hewlett-Packard, Microsoft, and General Electric.

Management consulting firm Booz Allen Hamilton recently surveyed firms with more than \$1 billion dollars in annual revenues and found that 54% of the 72 chief executive officers it surveyed have a chief security officer in place. Ninety percent have been in that position for more than two years

Security has historically been an under managed and fragmented function in many organizations. After 9/11, security has become more and more important, and more expensive, because organizations are seeking a higher level of security than ever before. Many organizations are underfunded and don't have enough money to implement every security safeguard – so how does an organization decide whether to put an authentication program in place to positively identify networks users, or whether they need to create a stand-off from the front of the corporate lobby? Proper allocation of the security budget is an important element supporting the need for holistic security programs.

The increasing sophistication of integrated system controls is another reason. Physical security systems such as access controls, building controls, and digital camera systems 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 Physical lock and key systems have been replaced by smart cards that not only allow employees access to different areas in a facility, but also may keep audit trails of where employees spend their days.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, used to record everything in view 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 in so doing 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, which 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.

### **HISTORICAL SEPARATION BETWEEN INFORMATION AND 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*”.

## **WHAT'S IN A NAME?**

As the information and physical security functions move closer together, terminology becomes an issue. Many security elements are called the same thing, but mean something completely different, depending on whether you're discussing network security or building security. '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. Other examples of same terminology but different meaning include *audit trails*, *intrusion detection*, *security policy*, *emergency response*, *disaster recovery*, and *maintenance*.

In the past, many government reports by the GAO (U.S. 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. For example, "*Information security safeguards cannot be fully effective as long as FAA continues to operate with significant physical security vulnerabilities.*" (GAO -T- AIMD-98-170).

## **COMPLIANCE & SECURITY INTEGRATED REQUIREMENTS**

Many New requirements for assessing security have been released since September 11<sup>th</sup>. These new requirements, mandating risk assessment (security reviews) on everything from Medical Records to Ships, come from the U.S. government, other federal governments around the world, and from international organizations like the ISO (International Standards Organization) and the IMO (International Maritime Organization). In many of these requirements, both information security and physical security are included together. For example, the HIPAA Final Security Rule, (Healthcare Insurance Portability and Accountability Act), which has healthcare organizations around the country scrambling to become compliant by April 2005, includes major areas such as Administrative, Physical, and Technical. A typical requirement out of the physical security section would be "Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision", CFR 164.310(a)(1).

## **INTEGRATION THROUGH RISK MANAGEMENT**

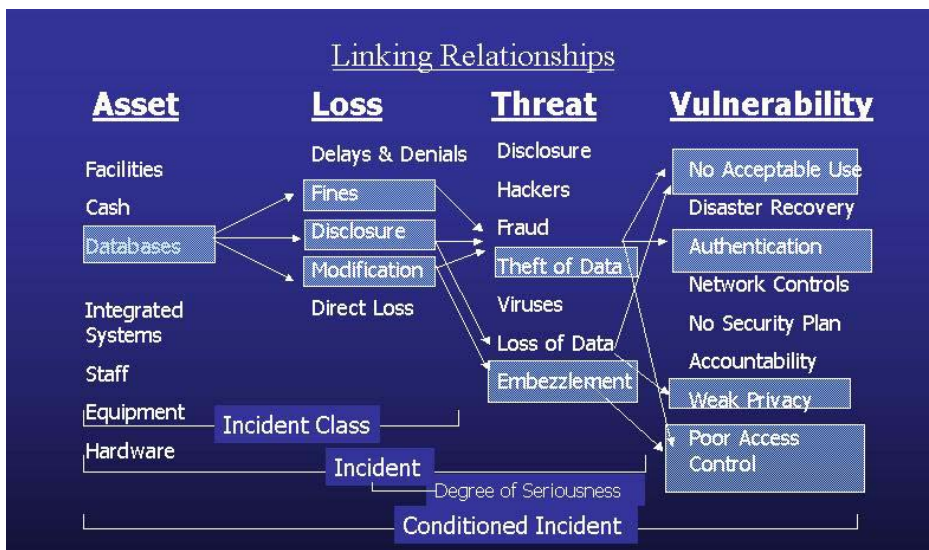
Risk management is the foundation of a holistic security program. Risk assessment looks variables such as threat potentials, loss potentials, vulnerability assessments, and existing controls and then calculates both a risk factor, as well as a cost-based prioritization of solutions that are both robust 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.

The chart below illustrates the integration of different elements of holistic security in a HIPAA assessment:



### **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, application 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.

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 which are currently being on done federal buildings, national landmarks, bridges, and seaports, as well as all the vulnerability assessment which are done on computer systems and networks need to be protected at the highest possible level.

A good example of sensitive information on physical infrastructure vulnerabilities being disclosed is in a report printed in the Orange County Register, a major newspaper in southern California. 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”. The report was obtained under the Freedom of Information Act and printed in the Sunday paper, but the Orange County Register said it withheld the most sensitive details of the 84-page report but decided to publish the broad findings”.

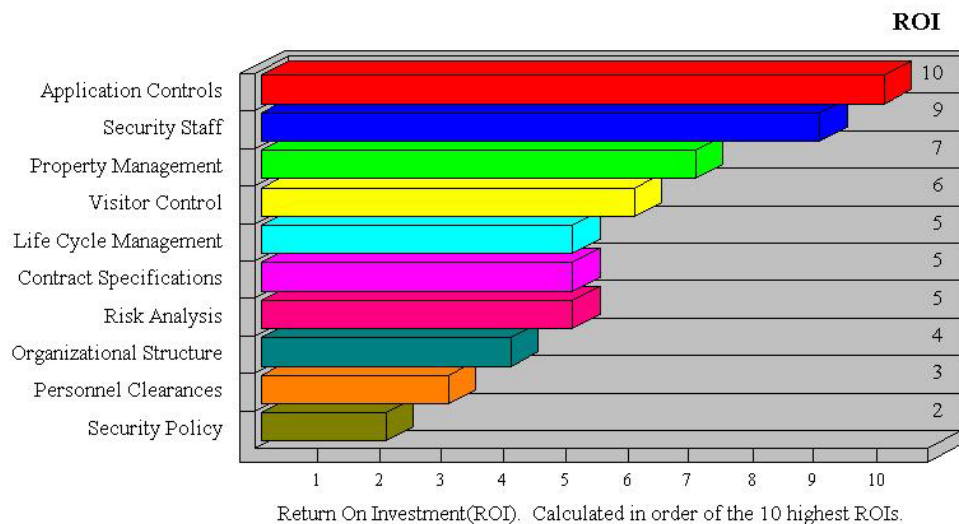
### **RETURN ON INVESTMENT**

A holistic security program looks 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 (ROI) ratio, 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 chart below illustrates possible Return On Investment recommendations.



### **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 for 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 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 requires human involvement, 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.”

“In conclusion, our review has identified a myriad of commercially available technologies that implement the three essential concepts of effective security: protection, detection, and reaction. Many of these technologies are mature and have already been deployed.....where their capabilities and effectiveness have been demonstrated. Other, newer technologies appear to offer great potential in helping agencies to ensure the security of their facilities. These technologies could be adopted in the near future. Other technologies are still in a nascent stage of development, but are maturing and appear promising. Many biometric technologies still face barriers in intrusiveness and complexity that must be addressed before they can be most effectively deployed and widely accepted by users. However, they offer greater security, and the challenges to their implementation may not be formidable. 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, integrated systems, and physical security is an important trend which is changing the role of security within organizations, and changing the role of the security officer, who is finally becoming part of the upper level management team. In the government sector, city, state and county governments are being asked to create risk management justification for their requested budgets and the controls they need are a combination of strong information controls and strong physical controls. The integration of these elements will create strong, well-managed, and adequately funded security programs that will ultimately benefit the bottom line.

**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. She served on the NSA Network Rating Model Workshop, and 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. Based near Annapolis, Maryland, she has written for the Computer Security Journal, the CSI Alert, Defense Electronics, InfoSecurity News, Access Control, the ISSA Password, and many other industry publications.

