

Convergent Security Risks in Physical Security Systems and IT Infrastructures



The Alliance for Enterprise
Security Risk Management™



The Alliance for Enterprise
Security Risk ManagementSM

This report was commissioned by The Alliance for Enterprise Security Risk ManagementTM (AESRMTM), a coalition formed in February 2005 by three leading international security organizations: ASIS International (ASIS), Information Systems Security Association (ISSA) and ISACA. AESRM was created to address the integration of traditional and information security functions and to encourage board- and senior executive-level attention to critical security-related issues and the need for a comprehensive approach to protect the enterprise.

AESRM's founding organizations' members—who represent more than 90,000 global security professionals with broad security backgrounds and skills—recognize that such integration, or convergence, of security roles impacts not just the security function of a given business, but the business as a whole. Similarly, the members realize that, as companies' assets become increasingly information-based and intangible, there is a greater need to integrate traditional and information security.

As individual organizations and as members of AESRM issuing reports such as this, ASIS, ISACA and ISSA lead the way in the ongoing security convergence trend.

The Alliance for Enterprise Security Risk Management™ (AESRM™, www.aesrm.org) is a partnership of three leading international security organizations, formed to address issues surrounding the convergence of traditional and logical security.

About ASIS

ASIS International (www.asisonline.org) is the preeminent organization for security professionals, with more than 34,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities and the public. By providing member and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine—*Security Management*—ASIS leads the way for advanced and improved security performance.



About ISACA

With more than 50,000 members in more than 140 countries, ISACA (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 48,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by more than 6,000 professionals since the program's inception.



About ISSA

The Information Systems Security Association (ISSA), with more than 13,000 individual members and 106 chapters around the world, is the largest international, not-for-profit association for information security professionals. It provides educational forums, information resources and peer interaction opportunities to enhance the knowledge, skill and professional growth of its members. ISSA members are consistently recognized as experts on critical issues in the area of information security, and the association is viewed as an important resource for small businesses, global enterprises and government organizations alike. Working closely with other industry organizations such as (ISC)², ASIS and ISACA, and leading worldwide initiatives like the GAISP and the recommended CISO education curriculum, ISSA is focused on providing leadership and maintaining its role as The Global Voice of Information Security.



Disclaimer

The Alliance for Enterprise Security Risk Management (AESRM) (the “Owner”) has designed and created this publication, titled *Convergent Security Risks in Physical Security Systems and IT Infrastructures* (the “Work”), primarily as an educational resource for security professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Disclosure

© 2006 The Alliance for Enterprise Security Risk Management. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written authorization from ISACA. Reproduction of selections of this publication, for internal, noncommercial or academic use only, is permitted and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

AESRM

www.aesrm.org

AESRM Member Organizations

ASIS International
1625 Prince Street
Alexandria, VA 22314 USA
Phone: +1.703.519.6200
Fax: +1.703.519.1501

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web site: www.isaca.org

ISSA Inc.
4152 Meridian Street, #105 PMB30
Bellingham, WA 98226 USA
Phone: +1.206.388.4584
Fax: +1.206.299.3366

Convergent Security Risks in Physical Security Systems and IT Infrastructures
Printed in the United States of America

Acknowledgments

From the Publisher

ISACA wishes to recognize:

Primary Researcher and Author

Eugene Schultz, Ph.D., CISM, HighTower Software, USA

Focus Group Participants

Ronald Baklarz, CISA, CISM, CISSP, IAM, IEM, GSEC,
Computer Associates, USA

Ray Bernard, Ray Bernard Consulting Services, USA

Roy Bordes, The Bordes Group, USA

Paul Kendall, Ph.D., CISM, CISSP, CHS-III, Accurdata Systems, USA

Jim Mecsecs, Covenant Homeland Security Solutions, USA

Nils Puhmann, CISM, CISSP-ISSP, Mindjet Corporation, USA

Eduard Telders, CISM, CPP, T-Mobile, USA

Rick Withers, CISM, CPP, CHS-III, CenturyTel, USA

Project Contributors

Raul Aguirre Garcia, CISSP, INSYS Mexico S.A., Mexico

Sanjay Bahl, CISM, Tata Consultancy Services, India

Anthony Barkley, MCSE, CISSP, Symantec, USA

James R. Black, CPP, PSP, CSC, TRC Security, USA

Todd W. Colvin, CISA, CISM, CISSP, Paychex, Inc., USA

Kevin Dorning, CISM, Dorning Electronic Information Services Inc., USA

Kyeong Hee Oh, CISA, CISM, CISSP, Green Soft, Korea

Peter Kolchmeyer, CISA, CISM, CISSP, Deloitte & Touche LLP, USA

Serge V. Krasavin, CISM, GSEC, GCIH, University of Illinois—

Urbana-Champaign, USA

Itamar Mor, CISM, Comsec Consulting, Israel

Kenneth Newman, CISM, PMP, ITIL, American Savings Bank, USA

Ray O'Hara, CPP, Vance, USA

Laura Taylor, CISM, Relevant Technologies Inc., USA

Francois van Staden, CISM, Abu Dhabi Gas Industries, UAE

Bruce Wilkins, CISA, CISM, CISSP, TWM Associates Inc., USA

Table of Contents

Introduction	6
Objectives	7
Background	9
Recommendations	15
Appendix 1—Summary of Roundtable Discussions	18
Appendix 2—Security Convergence Problem Stories	22
Appendix 3—Penetration Test Examples	29
Appendix 4—Applicable Standards	31

Introduction

Increasingly, as a means of reducing costs, increasing efficiencies or making better use of technology investments, organizations are integrating physical security devices for access control, monitoring and process control into the IT infrastructure. This collision of two different technology worlds, each coming from a separate management approach and protection philosophy, does not always come together easily. The differences in design, functionality, implementation, maintenance and management can present conflicts, possibly resulting in a security breach involving the IT systems, the security systems or both.

This document presents an overview examination of the issues related to the converged security risks in physical security systems and IT infrastructures. It presents the results of a research project conducted by The Alliance for Enterprise Security Risk Management (AESRM) that focused on the nature and ramifications of convergent security risks in physical security systems and IT infrastructures. The security risks and management issues associated with commingling security systems and devices, process control systems, and IT environments need to be identified and addressed by manufacturers, security architects, system administrators, information security staff members and auditors. Control solutions need to be developed within the context of an organization's overall information security strategy and design.

Objectives

The primary purpose of this project was to initiate a dialog among security professionals involved in traditional areas of protection and their colleagues responsible for information protection, as well as with members of the IT community and those responsible for designing, building, integrating and managing physical security and process control systems. These systems, since they are central to the protection of people and facilities and are increasingly being integrated into essential business processes, have taken on the characteristics of critical infrastructures. Over time, systems that had been designed, implemented and managed as stand-alone systems have been integrated into the organization's IT infrastructure. While this integration makes sense from the standpoint of effectiveness and efficiency, the features and functions of these systems have not substantially changed, as physical security and control systems have become part of a wider infrastructure built and managed within a different context. The level of protection provided by physical security systems may not meet the requirements of critical infrastructure components or the risks resulting from the convergence of systems, and IT infrastructures may limit their applicability to critical infrastructure. This project was undertaken by AESRM to:

- Identify security-related risks to an organization's IT environment due to connecting physical security and process control systems to this environment
- Identify security-related risks to physical security and process control systems resulting from the introduction of these systems within an organization's network infrastructure
- Provide recommendations that information and physical security managers can implement to effectively evaluate and manage these risks
- Provide recommendations to system and product manufacturers and developers

Project Scope

The security systems that were considered within the scope of this project are broadly classified as belonging to the following classes of security devices:

- Electronic access control, including identification technologies such as magnetic cards, smart cards, biometrics and radio frequency interference (RFI) devices
- Closed circuit television (CCTV)
- Alarm and sensor systems
- Communications and fire controls
- Environmental system controls

Analysis and evaluation were completed based on the class of security system and not on the features or functions of any particular type of device or product. The objective of this project was to provide broad guidance to security officers. An analysis that would provide more detailed and product-specific recommendations would require a substantial amount of testing, which was beyond the scope of this project.

In completing the assessment of the implications of converged security, consideration was given to traditional requirements for information protection and data security. Since physical security devices are used within the context of a security program that often has broad needs and supports diverse business requirements, additional security objectives and areas of potential risk were considered. These include the following:

- Privacy
- Integrity
- Confidentiality
- Availability
- Authentication
- Authorization
- Investigations and forensics
- Fraud prevention
- Potential for identity theft

Background

The focus group participants for this project consisted of security executives and consultants representing ASIS International, the Information Systems Security Association (ISSA) and ISACA, who came together bringing diverse experience in physical security as well as information security. The group was tasked with identifying the systems that would be considered in scope and to begin examining areas of converged security risk that could result when physical security systems and IT infrastructures come together. Areas of risk were identified in the areas of system design, deployment, use, management and maintenance. This analysis was supplemented by security practitioners on a global basis who submitted real-life examples of risks.

The following security concerns were identified in no particular order:

1. Security risks to systems and devices designed to provide physical security and process control are growing because systems are increasingly being connected to organizations' networks.
2. Special systems and devices are increasingly being deployed in a manner that exposes them to external access from the Internet. Perpetrators who gain unauthorized access to these systems and devices may be able to use them to launch attacks on other resources within the network, some of which may be business-critical.
3. Special systems and devices are becoming more sophisticated and diverse, making security increasingly difficult to control.
4. Many vendors of special systems and devices have not adequately considered security in the design, implementation and support of their products.
5. Special systems and devices are frequently deployed and managed outside of the influence of information systems and security professionals.
6. Confusion concerning applicable security standards exists.
7. Auditing security controls in special systems is often difficult.

Each is examined in further detail on the following pages.

Security risks to systems and devices designed to provide physical security and process control are growing because systems are increasingly being connected to organizations' networks.

Originally, security controls for these systems and devices were frequently sufficient to address the security risks that these systems and devices faced because they relied on direct and physical wiring installed between components. Changes in these systems and devices over time, as part of a general trend to open architectures across TCP/IP-enabled networks, have resulted in new, serious security risks that are often overlooked. Few individuals realize, for example, that closed circuit cameras are misnamed in that they are no longer "closed" from a networking standpoint. When these special systems and devices are connected to organizations' networks, they

often introduce a multitude of new, previously unanticipated security risks. Security controls that were once adequate in deployments of physical security and other systems are often still present, but they are no longer adequate. The systems and devices themselves become potential targets of attacks launched from the local network or remotely potentially originating from anywhere in the world if organizations' networks connect to the Internet. Local and remote attackers can potentially gain unauthorized access to these systems and devices, enabling them to function as authorized users. Denial-of-service (DoS) attacks against the network can render such systems and devices inoperable. Cleartext data from these devices are frequently sent over the network, making the data prime targets for anyone who has installed a sniffer along the route over which data are sent.

A real-life example involving privacy and legal responsibility issues illustrates how special system and device security can be adversely affected by their connection to an organization's network. When a system, such as a security system, captures images of individuals, logs access entry card information, or cross-references that information to existing personnel data, privacy considerations become paramount.

In one organization, the physical security department planned to upgrade its current video surveillance system. It intended to convert the existing cameras to ones with IP addresses, add additional cameras for better coverage, and add an image server/database infrastructure. The intent was for this system to be "added" to the existing general service network using the existing CAT-5 wiring, extending cabling to camera locations and placing client-side software on desktop systems so that the cameras could be viewed not only from designated guard stations, but also from certain desktop systems. Staff from this organization also intended to take a copy of key data from the existing human resources information system and populate a new system that would key this information to pictures of employees and their access card information.

The security of the image and information system soon became a major concern. The image data transferred from the camera and stored on a video capture server were flowing over the general service network. Although the data were coded in a proprietary algorithm developed by the system vendor, the system's software was freely available from the vendor's web site, enabling anyone who had access to the software unauthorized access to video images and potentially to the ability to control the system. Security controls used to protect the server and data were deficient.

The legal department and a law enforcement agency were asked to review the deployment plan. They both concluded that data access was too broad and uncontrolled. The legal department was concerned that a potential for invasion of privacy litigation existed if the many people who had access to the

active cameras used them in unauthorized ways such as “monitoring” certain activities of the opposite sex. There was also concern that the images captured from the system could easily be captured and e-mailed offsite because they were resident on systems connected to a general information network.

Penetration tests also serve as pointed case studies of how special system and device security can be breached because the systems and devices connect to organizations’ networks as well as to the Internet. In one case, a penetration testing team was able to use network access to gain control of process control systems. It made general packet radio service (GPRS) devices inoperable. In another case, a penetration team gained unrestricted access to core IP-enabled devices such as camera and card-access systems that were connected to networks. Because there was also no encryption of traffic, such as video streams from these devices and systems, it could also capture and read the content of such traffic.

Special systems and devices are increasingly being deployed in a manner that exposes them to external access from the Internet. Perpetrators who gain unauthorized access to these systems and devices may be able to use them to launch attacks on other resources within the network, some of which may be business-critical.

Those who deploy special systems and devices often overlook the security risk that these systems and devices create for the rest of the network. Again, they frequently assume that security controls for these systems and devices are adequate—something that may have been true in the past. These systems are frequently deployed without considering where they are placed within the network, the types of unauthorized access that are possible between them and other systems (especially business-critical and operationally critical systems), and the implications for network security. An attacker who gains unauthorized access to one or more of these special systems and devices may be able to launch vulnerability scans from them, and use the results to initiate DoS attacks against one or more parts of the network, to gain unauthorized access to other systems, and so forth.

Examples of the security risks that special systems and devices can create for the rest of the network come from penetration testing. In one case, supervisory control and data acquisition (SCADA) systems were on the same network as market trading systems. The SCADA systems were intermediate systems that bridged information so traders could sell power on the open market. Breaking into the former led to full trusted access to the latter. In another case, access to power-controlling systems led to unauthorized access to clearinghouse systems. A penetration tester could send a ticket to tell another operator to generate a considerable amount of power without a legitimate request, resulting in denial of service. Situations such as these would not occur very often, however, as the level of trust between systems was at least well defined.

Special systems and devices are becoming more sophisticated and diverse, making security increasingly difficult to control.

The types and sophistication of systems are proliferating, making the achievement of security control more difficult. Not that long ago the functionality of systems was limited to the extent that they could not be remotely accessed by anyone, let alone attackers. Even if they could be remotely accessed, they often did not possess sufficient functionality to allow malware to infect them or a perpetrator to use them to launch attacks on other systems. Even if they did, they were limited in the control functions they supported to the point that security breaches in them could result in compromise of a single or very limited set of physical security or plant process control function(s). Now the opposite has become true: today's special systems and devices have become multifaceted and multifunctional, resulting in increased difficulty in controlling security risks.

Many vendors of special systems and devices have not adequately considered security in the design, implementation and support of their products.

Vendors have too often designed and implemented physical security and control systems and devices under the assumption that they would not be connected to any network, or, if they were, that they would connect to a separate, dedicated network. Consequently, these systems and devices often come with easy-to-guess passwords (or sometimes with no passwords whatsoever), few if any auditing capabilities, and other weaknesses. Worse yet, when systems are implemented, the presupplied passwords frequently are not changed or may be hard-coded into the system.

Over time, vendor products have grown considerably in functionality, especially in network functionality, without including concomitant security functionality. Vendors tend not to use standard IT terminology to talk about their systems, which makes providing meaningful information to IT personnel difficult. Security system and other vendors need to be able to communicate meaningfully with IT staff, yet confusion concerning the meaning of terms, e.g., client and server, abounds among vendors. Furthermore, vendors frequently do not supply customers with trustworthy and complete documentation that describes security features and capabilities, recommended configurations, vulnerabilities that require workarounds, encryption capabilities (if available), how to close ports to prevent certain kinds of attacks (if this capability exists), and other important information. Finally, vendor training seldom includes security-related training.

An example of the security risks that vendors can introduce in special systems and devices comes from one of the members of the project focus group: a penetration tester. This person stated that in his years of penetration testing of such systems and devices, he has easily gained access to them many times because they had no passwords or retained the well-known vendor-supplied passwords that technical staff had not changed.

Special systems and devices are frequently deployed and managed outside of the influence of information systems and security professionals.

For a variety of reasons, individuals who have the best levels of knowledge and skill needed to achieve suitable integration of security systems into the IT infrastructure or the protection of these systems have frequently not been involved in decisions related to the purchase, implementation or management of such systems and devices. IT systems personnel responsible for systems management, networking and change processes are often not consulted when physical security systems are added to the IT infrastructure or are not provided with the information that is useful in planning and completing the integration of these systems into the IT infrastructure. System vendors and integrators may not have detailed, complete or comprehensive information that is expressed in terms that are typically used to describe network bandwidth utilization or system performance. Information security personnel may not be involved in physical security system specification, implementation or integration. To the extent that physical security systems and devices are considered part of an organization's critical infrastructure, communicate sensitive or essential information, or support a critical business process, these systems need to be included in an organization's overall security and business continuity plan.

Confusion concerning applicable security standards exists.

A plethora of standards that apply to physical security, plant process control and other special systems exists. At the same time, however, this "standards plethora" has resulted in confusion concerning the ones that genuinely need to be implemented, especially when security-related controls are concerned. No widely accepted security standards that apply to such systems exist, and current standards seldom recommend priorities in selecting and implementing needed security-related controls in such systems. Standards, which are typically used in relation to system design, functionality, development, deployment and use, are often not used as references for physical security systems, even though physical security systems may need to comply with these standards when they become part of the larger IT infrastructure.

Auditing security controls in special systems is often difficult.

The independent audit function helps assure that deployed controls are sufficient in managing risk and that risks that are accepted will not adversely impact the organization. Due to a variety of factors—among which is lack of suitable audit standards—physical security, plant process control and other systems are not, however, often adequately audited. Auditors often do not genuinely understand the nature, purpose, technology and vulnerabilities of such systems. Additionally, special systems and devices often lack the sophistication of auditing functionality to allow evaluation of individual accountability. Finally, as discussed previously, there is a lack of uniform, widely accepted standards for security controls in such systems.

Recommendations

To adequately address the security-related risks described in this report, organizations should consider the recommendations outlined in the following subsections.

Establish a governance framework for managing security-related risks in systems such as physical security systems and process control systems.

This is the most important step in dealing with security risks in these systems. Organizations must create a policy that specifies the elements of a risk management program for special systems and devices and a management infrastructure for providing resources, establishing accountability and ensuring compliance. Issues such as roles and responsibilities, separation of duties, data classification and data retention need to be addressed. Detailed procedures and standards pertinent to security in special systems and devices need to be written and constantly updated.

Define security requirements for physical security, plant process control and other similar systems early in the planning cycle.

Failing to define applicable requirements upfront almost invariably results in cost escalation, including costs associated with retrofitting features to meet newly created requirements. Security is no exception. The process of defining the requirements for such systems thus needs to include the convergence of these systems with the IT infrastructure. Planning should involve a wide range of functions within an organization, including physical security, IT, information security, risk management, auditing and general counsel.

Understand the technology better.

A widespread lack of understanding of the technology exists, and the implications of integrating this technology into the wider IT infrastructure need to be recognized. Insufficient understanding, in particular when systems are network-connected, increases vulnerability to attacks and increases points from which attacks can be launched against other computers on the same network. Similarly, many individuals assume that because systems such as SCADA systems are complex and require specialized knowledge to understand, successfully attacking them is nearly impossible. This assumption is false, however, as the numerous documented break-ins to these systems show. Auditors should better understand special systems and risks to identify security-related impacts to the enterprise.

Analyze and understand security-related cost-benefit trade-offs.

Connecting special systems and devices to organizations' networks introduces new and usually serious levels of risk. The trade-offs between connecting these systems to organizations' networks and the security risks that doing so introduces thus need to be better analyzed and understood.

Develop a unified set of meaningful standards.

As discussed, there is no absence of relevant standards relating to physical security systems. The problem is instead related to the plethora of standards that exist. It is difficult to determine which particular standards among the many are most important, and also how to comply with them. Governments need to write more condensed and specific guidelines concerning how to secure security and process control systems. Standards need to be applicable not only to entities that deploy these systems, but also to vendors.

Deploy special network security controls.

If special systems and devices must be network-connected, they should be located in an isolated and specially controlled part of the network—an isolated “security zone.” Network security controls such as firewalls, intrusion detection systems and intrusion prevention systems need to be implemented to better protect systems such as physical security systems and process control systems.

Implement effective authorization, accountability and auditability controls.

In closed systems, or when systems are not part of the critical infrastructure, actions by users, operators or supervisors may not need to be restricted, recorded or audited. When systems take on a more significant role, or are included in an infrastructure where accountability, authorization and the ability to audit are requirements, these functions need to be provided. Physical security systems should be able to be integrated into the organization’s formal access structure. For example, when role-based access is implemented organizationwide, physical security systems should be able to incorporate the same control structures.

Critical systems need to be treated as critical and included in the organization’s continuity plans.

To the extent that physical security systems are considered critical or support critical business functions, they need to be included in the organization’s disaster recovery and business continuity plans. Data and applications need to be classified according to criticality and sensitivity. Data recovery needs to be considered when offsite records retention and recovery plans are developed. Similarly, security systems and security system services and functions need to be considered when developing recovery and continuity plans are created. These systems also need to be included in recovery plan tests to ensure that plans are effective.

Physical security systems serve as important sources of information in corporate investigations.

Systems need to be adequately protected to ensure their integrity and their usefulness in supporting forensic activities. Physical security systems may

provide important forensic information required to support an investigation. These systems may also be significant to support an investigation of a network compromise if they are involved in this compromise. Physical security systems that are part of the network need to be deployed so their system clocks and that of other network devices are consistent. This way, actions that are part of an intrusion can be more easily traced. System integrity needs to be provided for, so any change or use of the system can be identified and explained as part of system operation. Procedures need to ensure the proper protection of system records in the event of an investigation. Security for the system needs to be defined in such a manner that physical security systems and their components are protected from intrusion, misuse or tampering.

Require that the amount of auditing and logging in special systems be increased.

Given the risks that security and process control systems introduce, the availability of audit data that readily identify attempted and actual security breaches, and the source of such attempts, is a critical consideration. At a minimum, system auditing (where available) should be configured to yield information necessary to answer such questions. Better yet, special auditing and logging that are available only through third-party tools should be implemented to enable analysts to determine whether the use of security and process control systems has been legitimate.

Develop and require tailored security training and awareness.

Lack of knowledge concerning security-related risks and suitable control measures concerning convergence risks is currently prevalent among users, system administrators and managers/owners of security and process control systems. Tailored security training and awareness among these groups would go far in combating these risks.

Put increased pressure on vendors to play a more active role with respect to security.

Vendors need to do more than create and offer products that incorporate necessary security controls and eliminate common vulnerabilities. They should create baseline security standards for these products. Additionally, they need to standardize key terms and definitions and produce detailed documentation for their products. They need to also create and offer training and awareness that focus on security-related issues.

Expand the audit function to cover special systems and devices.

Audit functions within organizations need to be expanded to focus specially on systems such as physical security systems and process control systems and the convergence problems that these systems and devices introduce.

Appendix 1—Summary of Roundtable Discussions

The following comments recorded by the project team highlight some of the specific security issues that need to be considered when physical security systems are integrated into the IT infrastructure.

Closed Circuit Television (CCTV)

Security issues to consider for CCTV include:

- Many operational uses of CCTV exist outside of security, e.g., for process control.
- Sophisticated video storage and archiving systems that create pressure on IT for storage are being introduced.
- Vendors of control room equipment have no idea what ports on their systems are open or the implications for the potential of being attacked and compromised. Most vendors look for support from developers such as Microsoft for answers. Systems may not even provide an opportunity to close open ports that are not needed.
- Video DVR records what data have been accessed but not viewed—one can see all information on the hard drive; there is no limitation on access.
- Access controls and audit information for physical access may not be established for video systems.

Access Control

Security issues to consider for access control include:

- There is a lack of understanding in the physical security world of role-based access controls.
- Access can be gained through the panel switch. From there, data can be downloaded or modified, granting unauthorized access to protected areas.
- Each panel needs to be identified as a specific device to the system and authorized for certain activities.
- Operators can open doors, leaving no record of who entered, because they may not have to swipe a card and may not have to sign in.
- Wireless access devices can store 4,000 entries that may not be encrypted.
- The problem of “enrollment on first read” persists.

Environmental Controls

Control systems in which individuals can control the temperature for their area potentially pose many risks. For example, can someone who is not authorized gain control and change environmental settings? These issues can have implications for areas in which environmental requirements are important.

Command and Operations Centers

Security issues to consider for command and operations centers include:

- The more systems converge, the greater is the need for more granular access control, such as logging, and procedural controls, such as background checks, two-person rules and the identification of single points of failure.
- When multiple officers work a common command center, they often share the same ID and stay logged in for a shift. There are often poor password controls that result in outcomes such as writing passwords in operator logs or taping them to the side of terminals. The ability to establish accountability is lost. The problem of people engaging in unauthorized actions and/or misusing authority and/or using systems to gain unauthorized access or privilege in corporate network and systems is serious.

General

General security issues to consider include:

- Network availability often depends on the particular time of day; some organizations may bring down the network at night or may be less concerned from an IT operations standpoint about service outages when security systems are most required.
- Voice-over Internet protocol (VoIP) is a technology that has generally well-documented bandwidth requirements. Physical security devices have not been documented to the same extent, however, so it is difficult to effectively plan and anticipate the requirements with these devices.
- With physical security systems, there is little real operational testing, so it is difficult to anticipate performance.
- Vendors do not have trustworthy documentation with regard to bandwidth and other IT-related requirements.
- Auditing physical security systems is difficult, since there are generally few, if any, applicable standards that can be used as the basis of the audit.
- There is an issue of system architecture and deployment requirements. Physical systems are often deployed without understanding the network architecture (switches and routers), network configuration and routing implications.
- Physical security device manufacturers and integrators have done a poor job of documenting how systems really work and in training people in operations.
- The evolution has been from firmware development to software in DoS and then Windows operating systems. Companies have done only enough to get products out the door without the rigor that is normally part of systems development. Quality control is missing.
- Vendors have not used standard IT terminology to talk about their systems, which makes providing material to IT personnel difficult. There is also confusion about what terms mean, e.g., server and client. These are used in different ways, adding to the confusion.

- System specifications need to spell out architecture and components within the architecture.
- There is a difficulty planning bandwidth in particular, as events cannot be planned and the demand for bandwidth requirements and utilization cannot be predicted.
- Physical security products typically have long life cycles.
- Large companies are reluctant to invest in technologies where there are no standards.
- Security system vendors need to be able to talk to IT staff and provide meaningful information.
- Security systems are conceived and designed within the context that they are local, but the deployment is increasingly enterprisewide.
- Compliance is forcing organizations towards standardization.
- The company needs to address the question of who administers systems—IT or physical security department personnel—and who is accountable.
- In most organizations, IT controls the network and has the budget power.
- Physical and IT security have a great deal in common.
- Auditors need to look at separation of duties, the need for which may cause changes in system design and operational characteristics.
- For federal agencies, physical systems are considered to be part of the IT infrastructure and are, therefore, subject to the same regulations.
- For the customer, integrator or manufacturer, liability for system flaws does not exist.
- Standards and testing, e.g., Underwriters Laboratories Inc. (UL), for fire and life systems exist. Physical systems do not have to meet these standards, although they can be defined as being part of the critical infrastructure.
- Fire systems liability can be spread among design, implementation, testing agencies (e.g., UL) and fire marshals, who approve systems once they are implemented.
- Security managers may not be able to answer detailed questions about systems they have deployed or plan on implementing, since they tend to purchase the system as a whole and do not look at or have easy access to detailed system information such as the encryption algorithms being used. The vendor or integrator may not have this information, either.
- Security system data may be covered by privacy regulations and there may be a need for reporting when personal information is disclosed.
- Security system data should be classified and protected. Owners of security system data should be defined, as is common for other corporate data. Retention, storage and destruction requirements should be specified.
- Security departments should require a warrant when records are requested.
- There needs to be consistency in data retention. For example, in some airports, seven days of video footage is available before destruction. At other airports, video footage is available for longer periods. Some may keep data for variable time periods.

- Physical security system data need to be handled according to their classification (sensitivity, criticality).
- Access levels for viewing and monitoring need to be defined in security procedures.
- There needs to be an audit trail of operator actions. Operators need to be accountable for their actions. Currently there may be no way to verify what has changed or who changed it; fully tracing events may not be possible.
- There are often no physical security controls over physical security devices and control rooms.
- All physical security systems should share a common time stamp with all other networked devices.
- Physical protection for equipment needs to be provided. Access controls need to be placed in areas where sensitive devices such as control panels are located. Tamper switches may be bypassed or may not be in place, however.
- Physical security systems should be treated as part of the critical infrastructure because of life safety issues, legal liability implications, protection of proprietary data, protection of critical assets, continuity of business and data integrity-related issues. They should be placed in protected data centers.
- Patching physical systems is not always feasible because of system development issues.
- Logical system security failure may adversely impact physical systems. Real-world examples include:
 - A university hack, where access to lighting control systems from the Internet allowed unauthorized control of facility lighting systems
 - A hack gained control of environmental systems
 - An Internet worm caused a denial of service to Cisco VoIP systems
 - The MS Blaster worm, which exploited a vulnerability and enabled a hacker to gain control over power plant systems in the Northeast US

Appendix 2—Security Convergence Problem Stories

These stories were provided to further illustrate the nature of problems associated with the convergence of physical security devices and IT infrastructures. In some cases, the resolution of the problem was not complete or would not be acceptable to some organizations. These are included to demonstrate the problems that can be encountered when physical security systems are integrated with the IT infrastructure without fully comprehending the problems that can result.

Story 1

An organization routinely performs wireless access point (WAP) site surveys at each company facility to determine if rogue devices are in use. During two recent site surveys, access points were discovered. After much walking around the facility and crawling inside of ceiling panels, the access points were discovered inside closets containing the physical security monitoring system. As it turns out, the access points were installed by two unique vendors but with the same default configuration. The default configuration was right out of the box with SSID broadcasts, the Admin password and IP address space all open to the world. The monitoring elements and computer were open to access as a result of this configuration.

Consequences of the Problem

Fortunately, none of the elements were dual-homed, so the equipment was entirely off of the network. This type of configuration may lead to disabling a physical security system in advance of a break-in. It is clear that additional training is necessary so the organization's physical security counterparts are up to speed on current best practices for wireless security.

Remediation

The organization notified each physical security provider of the discovery and instructed them on how to change the default configuration of a WAP.

Story 2

Data leakage from the use of cell phone cameras was occurring.

Consequences of the Problem

Confidentiality breaches existed for confidential information, including drawings, documents and site plans.

Mitigation

Employees, contractors and visitors must surrender their cell phones, leave them off or tape the camera's lens when entering a secure area of the facility where sensitive and confidential information is available.

Story 3

Monitoring staff harassed a temporary employee using CCTV in the front of the women's rest room.

Consequences of the Problem

The harassed employee quit her job.

Mitigation

No corrective measures were taken because the harassed temporary employee did not file a complaint and was not available to provide other testimony to investigators.

Story 4

This involves issues of privacy and legal responsibility. When any system is implemented, it is necessary, and sometimes legally required, that issues of privacy be considered. This is especially true when a system captures images of individuals, log access entry card information, and cross-references that information to existing personnel data. In this instance, the physical security department made plans to upgrade its video surveillance system. It intended to convert the existing cameras to IP-based cameras, add cameras for better coverage and add an image server/database infrastructure. The intent was for this system to be “added” to the existing general service network, using the existing CAT-5 wiring. The department extended cabling to camera locations and placed client-side software on desktop systems so the cameras could be viewed from designated guard stations and certain desktop systems. It also intended to take a copy of key data from the existing human resources information system and populate a new system that would key this information to the images of employees and their access card information.

Consequences of the Problem

The concerns that arose were related to the security of the image and information system. The image data transferred from the camera and stored on a video capture server were flowing over the general service network. Although the data were proprietary to the vendor, the system vendor's software was freely available from the web site of the software vendor that created it. The security methodology used to protect the server and data was weak.

The legal department was asked to review the plan, as was a law enforcement agency. They both concluded that access to the data was too broad and uncontrolled. The legal department was concerned that there was the potential for invasion of privacy litigation if the large number of people who would have access to the active cameras were discovered to be using them to “monitor” the opposite sex. There was also concern that the images captured from the system, because they were resident on a general information network, could easily be captured and e-mailed to other locations.

There was also concern that the employees had not been adequately notified of the pending project, and there might be litigation and union issues.

According to the US federal government, any information about people (stored in a system) that can be retrieved using keys is considered to be sensitive information. When sensitive information is gathered, it is required that employees be notified in writing, and that they sign a privacy act statement acknowledging that they are aware of the collection of this information. The privacy act statement must inform the person signing the reason the information is being collected and how it will be used. By law, it cannot be used for any other purpose.

The physical security department did not intend to issue a privacy act statement for its new system. It was also determined by the legal department that the use of existing personnel information to populate a new system would violate the privacy act statement previously signed by the employees and would also violate the legal status of the system as a registered “system of records.” This means that to legally create this new system of records, the department must issue a new privacy act statement to be signed by all employees and must apply through Washington DC, USA, for official status of this new system of records.

Adding hardware and software to a network requires consideration by the IT departments that manage the various aspects of the network. None of the upfront work had been done to ensure that the network had adequate bandwidth to handle the traffic. There had also been no contact with server operations personnel to determine if they could manage the servers required, nor with database management personnel to determine if they could maintain the database required. Finally, no contact had been made with the client support staff to determine whether they were prepared to support new desktop applications that would be installed.

Overall, this was a case of poor planning. The threats and privacy issues were considered severe enough by the legal department to force a stop to the project.

Mitigation

The project was stopped and restarted. A project manager was assigned and the project was redirected through a full IT project management life cycle process, which included full cybersecurity, privacy and legal reviews, as well as participation by each IT discipline involved.

Story 5

The IT division of a police department experienced a theft of random access memory (RAM) from servers in a computer room. The surveillance cameras in the computer room had failed.

Consequences of the Problem

Memory was removed from two servers after normal working hours. Initially the IT network team thought the servers crashed. However, upon investigation it was found that memory was missing from both of the affected servers. The affected servers were gateways that provided access to the mainframes, which caused downtime to all police stations with access to mainframe applications. The videotapes were checked and found to have no recordings. The surveillance cameras in the computer room were not functioning at the time of the event.

Mitigation

The failed cameras had been reported to the concerned government department approximately a month earlier, but the government department responsible for maintaining the access control for the building claimed that it had not budgeted for maintenance of the closed circuit camera system. The problem was eventually fixed after pressure was applied to the concerned department.

Story 6

A global organization with more than 50,000 associates did not have standardized access control across its various offices. Each office had a system from a local vendor. In some offices, no access control mechanism was installed.

Consequences of the Problem

Requirements dictated that access control systems that granted or revoked access of associates in an organization be implemented. They were, to some extent, implemented, but access control systems were not integrated into building management systems.

Mitigation

The organization rolled out smart cards that had to be used for physical access. Tailgating was forbidden; a training and awareness campaign was included with the initiative. The accuracy of data for incorporation and distribution of smart cards and the maintenance of access records were ensured.

The organization standardized the access control system across the organization and ensured that it could be integrated to CCTV, alarms, fire and environmental systems, and building management systems, and could be used as a single card for the logical/cyber aspects, such as authentication and digital signatures.

One of the critical aspects identified for the smooth rollout was having the correct data for each associate, along with the location to be captured from the enterprise database. The organization realized that there were data-related issues. To address them, it embarked upon an enterprisewide awareness and corporate communication exercise. This exercise helped create awareness of the smart card, its benefits and the proposed rollout timelines among all associates. The communication was done through the enterprise portal and through posters in the offices. With this communication, the organization was also able to request that associates validate and correct their data within a given deadline. The initial mass distribution of the cards across the organization was smooth. The much-publicized launch of the event was helpful in capturing the correct data and creating awareness among associates.

To ensure that the cards are used and that the organization maximizes their effectiveness, each card is used in taking attendance. Smart cards can also help track assets, such as laptops, for associates who have been provided one by the organization. This helped in complying with the legal requirements of tracking the entry and exit of laptops in the organization, as desired by the government. All these measures helped ensure that the usage of smart cards for the purpose of physical access was followed diligently; it also helped reduce tailgating.

The organization had to address the requirement of storing access data for the purpose of investigations or analysis and as per regulatory norms. At issue was who would be responsible for backup and verification of their usability at a later date. Per the organization's processes, it ensured that the IT infrastructure services department would be responsible for the backups on a regular basis and this would be checked periodically by the administration department. This helped ensure segregation of duties and also that flaws in the process were corrected.

It is crucial to understand that, for a project of this nature to be successful, a clear architecture must be in place. Technology standards and their interfacing and integration requirements need to be clearly understood, and the physical requirements also need to be understood upfront so their processes (such as monitoring requirements) can be defined. It is also necessary to define all the operational processes at a detailed level, with a clear definition of responsibilities and tasks and understanding of the behavioral and nontechnical aspects. A risk assessment must be completed, the project must have a strong project management team and governance process in place, and the commitment of top management must be obtained.

Story 7

This example concerns an organization's accountability implementation of centralized users' resources, authentication, authorization and administration. The objective was to maintain the same independent services for each mechanism, yet integrate the events to be able to correlate them and optimize them through a centralized operation. The main problem was obtaining a complete solution.

Consequences of the Problem

Much time was wasted, due mainly to problems in integrating roles and responsibilities.

Remediation

Although it was not the goal of remediation efforts to reassign responsibilities, this became necessary because of the functionality of a tool that was implemented. Not all of the goals and functions (including privacy, data integrity, continuity of service, authentication, authorization, investigation and forensic use of data, fraud, confidentiality, custodianship of data, and data retention and destruction) were possible.

The solution was to implement an integrated access control system that centrally integrated the authentication, authorization and administration functions to optimize functions and responsibilities, identify incidents, and correlate events. The main objectives were to:

- Control physical access—Who should and should not physically enter places?
- Change to a culture that stresses objectives and optimization of the use of job time
- Control surveillance in the different shifts
- Where and when necessary, optimize access to the different places users must go

Story 8

This story concerns network throughput impacts caused by changes in the use of physical security devices over the backbone extranet network connections to a remote office. The system was initially specified as an exception-based connection to digital CCTV monitoring systems in a financial institution. The concept is that connection across the company network would be infrequent and based on short periods of use. The office undergoes a maintenance cycle, which takes the local alarm systems offline. Management asked the central monitoring station to actively use the CCTV to remotely protect the site until the local alarms could be reconnected. As such, the throughput generated by constant surveillance of the office generated network impacts. The network staff, responding to what appears to

be a negative impact to other customers of the network, shut down the connection to mitigate impacts to other users, thereby shutting down the surveillance.

Consequences of the Problem

The site was unprotected for the duration of troubleshooting to determine the cause of the shutdown and what to do about it. The throughput of continuous connections was beyond the capacity of the available network bandwidth.

Remediation

Although the needs of life safety quickly determined that other services needed to be shut down instead of the security services to the site, it nonetheless had an immediate business impact. As a result of the need to “throttle down” the throughput on the network:

- The resources on the network needed to be reanalyzed for current and foreseeable throughput requirements
- Changes to priority network traffic needed to be agreed upon in advance
- Bandwidth limitation precipitated a reconstruction of the network segments affected
- Communication protocols needed to be established to include the network operation center during physical security escalation situations

Appendix 3—Penetration Test Examples

Penetration Test Example 1

The interviewee is a senior consultant with a security company that focuses on the transportation industry, utilities and airports. He designs security for physical security systems and is responsible for convergence between consulting and design engineering.

Security systems have traditionally been closed, but they are not any longer. Problems range from security systems not working because a huge magnetic resonance imaging (MRI) file is being transferred over the network, to downtime in Windows systems. Security systems can thus negatively impact operations.

He participated in a mock penetration test conducted by the US Federal Bureau of Investigation (FBI) at a local meeting. Organizers set up a mock SCADA network (i.e., data network used to remotely run facilities). Security is being integrated into SCADA networks, but they get intermingled with business systems. Servers and workstations were set up in the mock network. There also was a mini pump station. Traffic going over the network was sniffed, enabling those who conducted the investigation to figure out the function of each computer. Operators could not see changes in reservoir levels because these machines were taken over using normal hacking programs. Extra code was written to produce special displays for the observers.

It is possible to avoid problems by taking the network off the corporate network or Internet, even though this approach is not currently in fashion. If a user is on or near a business network, he/she is vulnerable. In one case, the mayor of a city was not able to get into his office because of a security breach on such a network. Manufacturers' products are often chosen because of compatibility with existing IT environments and not because of security considerations. Manufacturers are trying to address vulnerabilities, and patches are being created, but some are better than others.

Penetration Test Example 2

Control systems are usually considered the most sensitive environment. From the corporate side, hackers were able to gain control of a control system, but they were unable to control process control systems (which typically have poor passwords, often just the serial number or something similar). GPRS devices did not work.

SCADA systems are tied into market trading systems. If a user breaks into a process information (PI) system, he/she gets full trusted access to market trading systems. PI systems are intermediate systems that bridge information so traders can sell power on the open market.

Access to power-controlling systems led to clearinghouse systems. A ticket could be sent to tell another operator to generate a lot of power without a legitimate request. This would result in denial of service. This kind of thing may not occur often, however, as the level of trust between systems tends to be well defined.

Recommendations include:

- Have a layered security model.
- Implement basic security measures, such as patching systems and enforcing the choice of strong passwords.
- Adhere to pertinent standards—they are often overlooked or people give up trying to comply with them.

Penetration Test Example 3

More IP-enabled devices, such as camera and card access systems, are being connected to networks without considering bandwidth and security control to protect these devices. For example, firewall rules are often not changed to help secure these devices. Penetration tests show that there is unrestricted access to devices. There is also no encryption of traffic, so anyone who sniffs the network can see data, such as video streams.

Physical security and logical security should be better integrated. Few tests show that one can get unauthorized access to other resources once one gets access to devices, however. Until recently, vendors built in little security, so one can usually compromise an older device more easily.

Penetration Test Example 4

In nine out of 10 times, consultants who are testing physical security controls can get into a so-called secure facility without breaking through any barrier. A simple excuse such as “We need to bring a package to Mr. Brown” usually works. In one case, a company was having a conference across the street from its office building. A consultant who appeared to be from the conference went to the office building and said that he wanted to go upstairs and see someone. He was allowed to do so without having to show any identification. Tailgating—following someone who has a badge—also works. Once, at an insurance company, someone watched executives drive into the office building’s garage. They drove in unchallenged. There was no secondary barrier in the garage, such as being required to provide evidence of access gained by being photographed.

One cannot forget the physical aspects of security. An organization may have put up significant barriers on the network, but once people have physical access to security and process control systems, they can take over very quickly.

Appendix 4—Applicable Standards

The following list includes many meaningful and relevant standards related to security in physical security systems and process control systems.

American Gas Association, “AGA Report No. 12, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan,” USA, 14 April 2005

American Petroleum Institute, API Standard 1164, “Pipeline SCADA Security,” USA, September 2004

Chemical Industry Data Exchange, *CIDX Guidance for Addressing Cybersecurity in the Chemical Sector*, USA, May 2005

International Electrotechnical Commission, IEC 62351-1, “Data and Communications Security, Introduction,” Switzerland, April 2005

International Electrotechnical Commission, IEC 62443, “Security for Industrial Process Measurement and Control,” Switzerland, 13 May 2005

International Electrotechnical Commission, IEC TR 62210, “Power System Control and Associated Communications—Data and Communication Security,” Switzerland, May 2003

Institute of Electrical and Electronics Engineers, IEEE Std 1402-2000, “IEEE Guide for Electric Power Substation Physical and Electronic Security,” USA, 30 January 2000

International Organization for Standardization, ISO/IEC 17799, “Information Technology—Code of Practice for Information Security Management,” Switzerland, 15 June 2005

International Organization for Standardization, ISO/IEC 27001, “Information Technology—Security Techniques—Information Security Management Systems—Requirements,” Switzerland, 15 October 2005

ISA, ISA-99.00.01, “Security for Industrial Automation and Control Systems, Part 1: Concepts, Terminology and Models,” USA, March 2006

ISA, ISA-99.00.02, “Security for Industrial Automation and Control Systems, Part 2: Establishing an Industrial Automation and Control System Security Program,” USA, April 2006

ISA, ISA-TR99.00.01-2004, “Security Technologies for Manufacturing and Control Systems,” USA, 11 March 2004

ISA, ISA-TR99.00.02-2004, “Integrating Electronic Security into the Manufacturing and Control Systems Environment,” USA, 12 April 2004

National Institute of Standards and Technology, NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems,” USA, February 2005

National Institute of Standards and Technology, NIST Special Publication 800-82, “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security,” DRAFT, USA

National Institute of Standards and Technology, “NIST System Protection Profile—Industrial Control Systems,” USA, 26 May 2004

North American Electric Reliability Council, NERC Standard CIP-002 through 009, “Cyber Security,” USA, May 2005

North American Electric Reliability Council, NERC Security Guidelines, “Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment,” USA, 4 June 2002

The Alliance for Enterprise Security Risk Management (AESRM, www.aesrm.org) is a partnership of three leading international security organizations, formed to address issues surrounding the convergence of traditional and logical security.

About ASIS

ASIS International (www.asisonline.org) is the preeminent organization for security professionals, with more than 34,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities and the public. By providing member and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine—*Security Management*—ASIS leads the way for advanced and improved security performance.



About ISACA

With more than 50,000 members in more than 140 countries, ISACA (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*[®], develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA[®]) designation, earned by more than 48,000 professionals since inception, and the Certified Information Security Manager[®] (CISM[®]) designation, a groundbreaking credential earned by more than 6,000 professionals since the program's inception.



About ISSA

The Information Systems Security Association (ISSA), with more than 13,000 individual members and 106 chapters around the world, is the largest international, not-for-profit association for information security professionals. It provides educational forums, information resources and peer interaction opportunities to enhance the knowledge, skill and professional growth of its members. ISSA members are consistently recognized as experts on critical issues in the area of information security, and the association is viewed as an important resource for small businesses, global enterprises and government organizations alike. Working closely with other industry organizations such as (ISC)², ASIS and ISACA, and leading worldwide initiatives like the GAISP and the recommended CISO education curriculum, ISSA is focused on providing leadership and maintaining its role as The Global Voice of Information Security.





The Alliance for Enterprise
Security Risk ManagementSM

The Alliance for Enterprise Security Risk Management (AESRM) was formed in February 2005 by ASIS International, the Information Systems Security Association (ISSA) and ISACA to encourage board and senior executive attention to critical security-related issues and the need for a comprehensive approach to protect the enterprise. The alliance brings together more than 90,000 global security professionals with broad security backgrounds and skills to address the significant increase and complexity of security-related risks to international commerce from terrorism, cyber attacks, internet viruses, theft, fraud, extortion, and other threats.