

COVER STORY

Cover Story - Integrating Physical & Logical Security.

Technology is playing a much greater role in today's corporate security. Now more than ever, physical security and information security are forming a synergistic and symbiotic relationship. In this issues cover story, Michael Brookes of Honeywell details factors an organisation needs to take into account when planning a corporate security management strategy, and the role of technology in achieving an integrated security solution.



INTEGRATING Physical and Logical Security



Michael Brookes



Security managers of today are finding themselves becoming increasingly reliant on technology. The result is the physical security and information security have become more closely aligned than many in the industry

realize. The primary focus of this article is on the factors an organization needs to take into account when planning a corporate security management strategy, and the role of technology in achieving an integrated security solution.

This move towards security convergence is seeing changes not only at the technology level, but also within the corporate structure. The role of Chief Security Officer (CSO) is beginning to emerge; executives are charged with protecting the tangible and intangible assets of their organizations, and are faced with the growing challenge of balancing the correct levels of risk versus business opportunity. This is not an IT role but one of corporate governance, and the CSO's background may not necessarily be in technology.

Responsible for advising executive management and the board on issues relating to security, including critical infrastructure protection and crisis management, the CSO's role includes leadership of security risk management, including investigations, financial crime, information security, protective security and crisis management. The role extends to ensuring that security is managed for the benefit of the organization, its staff, customers and shareholders. In addition to a sound understanding of security, knowledge of business priorities is also required, to ensure that the total environment is considered when making security risk management decisions.

Drivers for convergence

Regulatory compliance, risk management and cost-saving opportunities are all elements that support the integration of physical security and information security.

Changes in legislation surrounding corporate governance are driving a worldwide trend towards greater regulation of enterprises. Executives are being held personally accountable for providing investors with reliable, open and clear financial information. Failure to comply with these regulations may result in executives facing fines or even criminal prosecution. Besides those penalties, enterprises accused of such actions often find that

their public image and brand are damaged, which can harm customer confidence and spur customer defection.

Although the focus of this legislation is on the CEO and CFO, the Chief Information Officer (CIO) also plays a vital role in the signoff of financial statements. The CIO is not only responsible for ensuring the security and reliability of the systems

“Forgotten passwords cost the typical IT department \$200 per user per year, and that 11 percent of users experience an access rights problem every month.”

that manage and report the financial data, but is also accountable for the implementation and documentation of internal IT controls.

Business continuity management is another area in which physical security and information security need to be considered as a single entity, rather than two disparate business functions. The purpose of a business continuity plan is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters, be they physical (for example, fire or flood), or digital loss or theft.

A well thought-out business continuity strategy is measured by its technical response as well as the competency and capability of its management to deliver a sound business response. Building a secure, reliable and resilient IT infrastructure is only one facet of business continuity. In addition to disaster recovery, risk management, and security elements, a well-defined business continuity strategy should also include components from facilities management, supply chain management, crisis management and communications, health and safety, quality management and knowledge management. This holistic approach will ensure that the IT infrastructure can support a CIO's timely response to a business incident.

One of the most significant reasons for merging physical and IT security systems is cost reduction. By providing users with the convenience of a single enterprise-wide credential for both physical and online access, organizations have the ability to centrally provision and administer user identities and authentication. Market analysts suggest that forgotten passwords cost the typical IT department \$200 per user per year, and that 11 percent of users experience an access rights problem every month. Research of help desk professionals indicates that 45 percent of calls to a typical help desk are for password reset

assistance. These statistics suggest that a single credential can significantly reduce support and administration costs. Such a solution can take the form of a smart card or a combination of a smart card plus biometrics. These solutions can also be extended to other business applications such as payment, loyalty, vending, cafeteria, employee benefits and parking.

Taking a standards-based approach

Building a sound security program is a continuous exercise that takes into consideration an organization's risk and exposure to internal and external threats and vulnerabilities. An organization should devise a program that is aligned to business objectives and industry best practices, and formulate an approach to obtaining the desired level of security based on an organization's needs, asset valuation and exposure to threats.

ISO17799 is a detailed security standard providing a single point of reference to assist companies in their implementation of industry best practice in information security. The standard is organized into ten major sections, each covering a different topic or area, each having specific objectives and control mechanisms.

Implementation of these standards will provide an enterprise with a structured and robust security environment that is populated throughout the organization and matched to the overall business objectives.

Security Policy

Paramount to the success of a sound security environment is the role of management in providing direction and support for information security. The issue and maintenance of an information security policy across the organization is vital to the development of a security posture that is practical and robust, and addresses all elements of an extended corporate enterprise.

Organizational security

A security management framework should be established to manage information security within the organization. The framework should encompass the internal organization, third parties, and any outsourcing arrangements, with expert security advice available either within, or external to, the organization.

Asset classification and control

Applying and maintaining appropriate protection of organizational assets will ensure that all major information assets are accounted for and have a nominated owner. By implementing solutions that enable the capture and analysis of asset data from multiple sources (IT assets, fixed assets, and so on.) an organization can obtain a consolidated



inventory of assets, helping ensure that effective asset protection takes place. Real time asset tracking and the matching of assets to personnel can assist in providing levels of protection commensurate with the value and importance of the assets.

Personnel security

Reduction of the risks of human error, theft, fraud or misuse of facilities can be achieved through the deployment of advanced technology such as digital CCTV that uses complex video algorithms for motion and non-motion detection. Such technologies can assist in the detection of abnormal behaviour and suspicious packages/vehicles in areas such as car parks and building perimeters, providing protection from unauthorised access, damage and interference.

Physical and environmental security

Integrated solutions that offer secure access for both physical and logical environments, allow organizations to use smart cards and/or biometrics to manage access to critical infrastructure or systems. Government and defence organizations may wish to extend the integration to include Type 1 security systems for high security environments.

This approach enables the prevention of unauthorised access, damage and interference to business premises and information as well as preventing loss, damage or compromise of assets and interruption to business activities.

Communications and operations management

To ensure the correct and secure operation of information processing facilities, responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating instructions and incident response procedures. The risk of systems failures should be minimised through advanced planning and preparation to ensure the availability of adequate capacity and resources.

The integrity of software and information should be protected through the detection and prevention of malicious software such as computer viruses and network worms, and safeguards put in place to ensure the protection of information in networks and the supporting infrastructure. Routine procedures should be established for the back-up of data, and the rehearsal of its restoration.

Access control

Access to information, and business processes

should be controlled on the basis of business and security requirements. Protection should also be extended to remote access, a key component of any network architecture. Business needs demand that users are capable of accessing files and applications quickly and securely from any location, however, protecting the confidentiality, integrity and availability of key internal systems should be a key consideration. Multifactor authentication can be implemented to control and authorise access to corporate resources, intellectual property and mission-critical business applications. Access patterns can be monitored and notifications raised upon deviations to common access paths.

Systems development and maintenance

An organization should ensure that security is built into information systems, including infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of information systems, and appropriate controls and audit trails designed into application systems.

Business continuity management

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural

disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls. The consequences of disasters, security failures and loss of service should be analysed and contingency plans developed and implemented to ensure that business processes can be restored within the required time-scales.

Compliance

To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements is a high priority within any organization. Advice on specific legal requirements should be sought from the appropriate legal channels. Regular audits of information systems should be performed against the appropriate security policies. Protection is also required to safeguard the integrity and prevent the misuse of audit tools.

A consolidated security infrastructure

Taking the example of a large multi-site corporation, a consolidated security infrastructure can offer benefits both in the level of security achieved and the cost savings that can be realised. Some areas that may be addressed in a consolidated security infrastructure may include:

Access control

A single system, utilising distributed architecture can be deployed, integrating multiple building systems into one "data management layer".



This allows for a common time and attendance and access control system to be used across all buildings, identifying who is at each building, and their location, making sure that people are restricted to the areas to which they are authorised.

Digital CCTV can be integrated with building events, allowing for attempts at unauthorised access to be captured for forensic analysis. Advanced video processing systems can also be used for non-motion and object size detection to identify objects left in clearways, fire exits, etc. (bomb risk).

“Creating a culture in which physical security and IT personnel work well together can be difficult; these staff often have different perspectives.”

By using a common management application that allows the systems to communicate or share information, efficiency is dramatically improved, both in the way the data is managed, and how it is accessed. If these systems are built on a common backbone infrastructure, then there is a greater increase in asset utilisation. This creates consistency in the way the buildings are operated, and greater access to information, in turn reducing the overall operational costs.

Single credential

Providing a single smart card platform allows for efficient physical and logical access control across multiple sites. This allows for the protection of company data, enabling secure logon, data access and data transmission within sites, between sites and via remote access. Smart cards can be combined with a biometric platform for high security areas such as computer rooms and laboratories/research areas.

Identity management

Use of an identity management platform ensures that only appropriate users have access to corporate resources, and by integrating into systems such as HR as an authoritative source, minimise the risk of stale user accounts as a result of staff changes. As identity management systems are role based, that is, functional roles within the organization have pre-defined levels of access, changes to staff positions result in changes to permissions. These systems have the ability to audit and track users accounts, and automatically revoke access. They provide a centralised point of control for security and

audit processes, and are an effective means of evaluating regulatory compliance.

The financial benefits of an identity management solution are typically derived from the lower costs of administration and support. New employees entering the organization are provided with physical and logical access based on their role. Information is entered once into a source of trust such as the HR system, which through integration into the identity management solution, automates the activation of user privileges.

These solutions typically utilise a form of single-sign-on technology that removes the need

for users to remember multiple passwords. This reduces the number of calls to the help-desk for forgotten passwords, hence reducing the associated support costs.

- Authoritative Source – exploitation of existing software investments such as HR, CRM or ERP
- Identity Repository – central user vault of identity information with a ‘single view of the customer’
- User Provisioning – common security administration mechanism to create and delete accounts and manage passwords
- Access Management – common security authentication and authorisation mechanism
- Role Based Access Control – role based design

to ease administration and reduce costs

- Protection – single control point for protection and risk avoidance of the security infrastructure

Asset control

Using a consolidated security infrastructure allows organizations to match people and assets (for example, laptops) for security and asset management. Implementing a real time asset location system allows for assets to be classified and for access and/or removal of assets to be restricted to the nominated asset owners. Integration of these systems with digital CCTV allows for attempts at unlawful access or removal of assets to be captured.

Real time asset location can reduce the costs associated with lost or stolen assets, as well as assist in identifying the true utilisation of selected assets. Decisions can then be made based on factual data as to the level of inventory to be held and maintenance requirements, as well as being able to recall assets in line with any leasing arrangements.

Forensic analysis

Real-time behavioural analysis and forensics is achievable through the consolidation of physical and IT security audit data. By collecting and correlating security related data from across the enterprise and analysing it on a 24 x 7 basis, detailed forensic analysis can be performed in the event of a security breach. This enables organizations to quickly and automatically detect suspicious behaviours and establish accountability



in case of a security incident. Deviations to common access paths can generate alerts and logical access can be matched to physical access for user authentication.

Implementation challenges

The convergence of physical security and information security is not without its challenges. Creating a culture in which physical security and IT personnel work well together can be difficult; these staff often have different perspectives, priorities and reporting relationships. This factor alone suggests that a culture of corporate security management needs to be driven from the highest levels within the organization, ideally with visibility and representation at board level.

There needs to be a demonstrable return on investment (ROI) and an alignment with the overall business objectives; all initiatives should be part of a longer term strategy to decrease the level of security risk and exposure. This strategy needs to cascade down through the organization to match business unit goals, and needs to have similar levels of priority as the business initiatives.

The process for successfully implementing a converged security infrastructure requires focus in a number of areas.

Organizational alignment

By obtaining a thorough understanding of the organizational tolerance to risk, the depth of security requirements can be ascertained. This needs to take into account the security requirements at a business unit level.

Roles and responsibilities for security need to be defined throughout the organization with involvement from physical security personnel, IT, business units and vendors.

Process alignment

The security requirements of business processes and operations should be defined, with enterprise-wide security solutions being integrated into processes and applications. Process owners and users need to be made aware of the importance of security.

Strategies and architectures

Security strategies and architectures need to be clear and actionable, with a level of flexibility to address potential changes to the organization or technology.

Technology integration

It is important to be involved in selecting the technology solutions to ensure that organizational

requirements are met. It is wise to pilot selected technology to validate the solution. Once validated, the solution should be implemented in phases, allowing for the highest priority areas to be dealt with first, with ongoing testing of performance and functionality.

Roll-out

A roll-out strategy should be developed that allows for the solution to be deployed in phases. It is vital to ensure that all of the stakeholders are adequately trained in order to gain their continued buy-in. Once rolled out, ownership should be transferred to the appropriate business units or functions.

Maintenance

Ongoing maintenance of corporate security management requires adherence to the initial business policies and procedures. Regular audits should be performed to confirm that policies and rules are being abided by, and the solutions modified in line with changes to the business.

Summary

There are clear benefits to be derived from an active, strategic approach to corporate security management and the implementation of a converged security infrastructure. Organizations can take a holistic view towards risk management and compliance whilst reaping the rewards of systems that have lower costs of administration and support.

Organizations seeking to embark on such

a strategy need to be clear on the outcomes expected, and ensure that buy-in is gained at all levels; these strategies need to be closely aligned with business objectives, and should not be viewed as simply an IT security project. A phased approach should be taken and appropriate time allocated to the process. Key objectives should be set to measure the benefits of each stage as it is rolled out.

It is important to work with organizations capable of delivering comprehensive and best-of-breed security solutions. This provides the benefits of accountability, risk mitigation and knowledge transfer not typically available from a multi-vendor approach.

Finally, it is vital to implement auditing, monitoring and reporting processes to ensure on an ongoing basis that requirements are being met, and to adjust the systems according to changes in the business or risk profile. ■

References

Yahya Mehdizadeh. "Convergence of Logical and Physical Security" SANS Institute (October 2003)
 Kevin Shaw. "Identity Management" Deloitte (March 2005)
 Frost and Sullivan. "Strategic Analysis: North American markets for integration of building security systems with BAS" #A840-19 (2004)
 BSI. "British Standard: Information technology – Code of practice for information security management" BS ISO/IEC 17799:2000, BS 7799-1:2000
 Steve Hunt. "Trends 2005: Security Convergence Gets Real - A Market Niche Matures" Forrester Research (January, 2005)

