

# LOGICAL PROTECTION OF PHYSICAL AND ELECTRONIC SECURITY SYSTEMS VITAL TO SECURING ASSETS



*With 15 years of experience in the security industry, Jeremy Brecher is vice president of technology services for Diebold, Incorporated. Brecher leads all technology field services, including the Diebold enterprise security customer support department. His key areas of expertise include security and IT technologies, support and managed services for the commercial and government industries.*

**Jeremy Brecher**  
**VICE PRESIDENT OF TECHNOLOGY SERVICES**  
**Diebold Security**

Today's digital technologies present new challenges for securing an organization's logical assets and systems. Organizations face threats from hackers, malicious software and insiders looking to compromise data assets and computer networks. Fortunately, many organizations are taking necessary steps to mitigate these threats by implementing sound logical security programs.

But even with their focus on securing network and information resources, many organizations overlook a critical component of their programs – the logical protection of their physical and electronic security systems.

Applications like access control and video systems, which were once completely stand-alone systems, are now part of complex Internet Protocol-based networks. These systems include cameras, access readers, intercoms and a variety of other Windows-based devices. Internet Protocol (IP) allows organizations to extend these systems beyond the physical boundaries of facilities, which provides efficiencies and new capabilities for security personnel.

At the same time, IP-enabled devices that organizations leave unprotected have the potential to open doors for the penetration and infiltration of networks. For example, a perpetrator could remove an unprotected IP intercom or reader from a building and then compromise the access control system. In doing so, that individual may be able to gain unauthorized access to an organization's security network and even its facilities by obtaining false credentials.

Considering this scenario, it's clear that organizations need to apply logical security practices to their physical and electronic security systems. Diebold believes logical security should be a standard component – and a best practice – in the development and deployment of physical and electronic security systems, including video systems, access control, perimeter protection, identity management and more. Unfortunately, organizations too often address these systems after a serious issue has occurred. To ensure the

logical protection of physical and electronic security systems, Diebold recommends that organizations shift their focus from responding to crises to identifying and mitigating threats. In addition, Diebold advocates creating a culture of security, defining roles and responsibilities for security-related activities, and enlisting the support of a security provider.

## Identifying Threats

A security assessment can identify potential logical threats to physical and electronic security systems. Whether conducting an assessment independently or with the help of a security provider, this tool can proactively identify an organization's vulnerabilities, as well as uncover gaps in its security defenses. This is a vital first step in implementing a comprehensive data security program to mitigate risks and safeguard security-related systems.

Following an assessment, an organization may discover it faces multiple user-based threats related to electronic and physical security systems. For example, it may find that a large group of individuals shares usernames and passwords for critical systems like security workstations or networked video. Suppose a user accesses the video system and deletes video showing incriminating activity. With multiple parties using the same login information, the organization will have difficulty investigating the incident because it can't definitively know who accessed the system at the time of the breach.

Aside from user-based threats, organizations also face threats via the very technology they are implementing to better secure their environment. For example, today's access panels offer functions like Web-based management, FTP uploading and direct video integration. These expanded features make panels more susceptible to Denial of Service attacks and manipulation. Organizations need to ensure these devices support encrypted communication and have undergone vulnerability testing. In addition, they should place these panels behind network access



SECURITY

lists that limit communication to specified devices by ports, network segments, IP addresses or some other identifier to enhance security.

### Mitigating Threats

Organizations can close many of the logical gaps that exist in today's security systems by implementing robust security policies, which may include:

- Using Robust Usernames and Passwords: Default and weak user logins open the door for unauthorized access to systems and assets.
- Enforcing System Log On and Log Off Procedures: Requiring employees to log on and off of workstations each time they arrive at or leave their stations creates an audit trail that can assist with compliance reporting and investigations.
- Restricting USB Port Access: Limiting USB port access minimizes the potential of the introduction of a worm or virus to an organization's network via a portable USB drive.
- Implementing Dual Controls: Setting dual controls for data manipulation minimizes the potential for an individual to capture, alter or erase sensitive data.
- Enabling Data Encryption: Failure to encrypt backend user and transactional databases can compromise data security and may be in violation of compliance laws.
- Updating and Scanning Systems Proactively: Ensuring systems are up to date with the latest security patches and scanned frequently using antivirus software is vital to the security of networked systems.
- Implementing a Proactive, Positive Security Model: Whereas antivirus programs monitor for malicious software, a proactive, positive model does not rely on detection of an intrusion before flagging a process. Instead, it only allows preapproved activities for system users, applications and data access.

### Creating a Culture of Security

Organizations are more effective in their security endeavors when they embrace a culture that transcends departments to make security everyone's responsibility. A culture of security is one in which all employees are aware of security needs, have a working knowledge of security practices, are committed to protecting the organization's assets, understand and comply with security policies and procedures, and fulfill their security responsibilities.

### Defining Roles and Responsibilities

Organizations also need to define which parties are responsible for specific security-related activities. Many of the logical gaps that exist in today's security systems can be closed through collaboration between an organization's security and IT departments and a qualified security provider. For example, these parties can address responsibilities for managing Windows patching and antivirus updates for physical and electronic security systems. Defining clear roles and responsibilities minimizes the chance that an organization will overlook this important activity.

### Enlisting Support

Protecting logical assets and physical and electronic security systems is absolutely vital to the success of an organization. Keeping a network secure and an organization compliant is an enormous, never-ending task. And it can be daunting, especially when organizations address logical security on their own. A security provider can be a valuable contributor to help an organization address the intersection of logical, physical and electronic systems to identify vulnerabilities and implement strategies that mitigate risk.

#### Total Solutions

Hardware  
Software  
Installation  
Service

Diebold, Incorporated  
P.O. Box 3077  
Dept. 9-B-16  
North Canton, Ohio  
44720-8077

800.999.3600 USA  
888.545.9444 Canada  
330.490.4000 International  
productinfo@diebold.com  
www.diebold.com

Diebold is a registered trademark of Diebold, Incorporated.  
Copyright Diebold, Incorporated, 2010. All rights reserved.  
Litho in USA. File No. 70-1480

