

# CLOSING THE LOGICAL SECURITY GAP



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

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

The following Diebold column was originally published in the *Today's Systems Integrator* e-newsletter on September 7, 2010.

A sound logical security strategy has become essential to the modern security practice. During the past few years, integrators have spent countless hours working with end users to create and execute security strategies that will enable the protection of digital assets. But even with the focus that's been placed on securing network and information resources, many end users overlook a critical component of their logical security programs: the protection of their physical and electronic security systems. Logical security must become a standard component – a best practice – in the development and deployment of physical and electronic security systems. As integrators, we can educate our customers to help them mitigate threats by closing security gaps.

### Identifying and Mitigating Threats

Unfortunately, integrators are far too often engaged in the logical protection of an organization's security systems after a breach has occurred. We must work with our customers to shift the focus from responding to crises to identifying and mitigating threats.

Applications such as access control and video, which were once stand-alone, are now part of complex, IP-based networks that connect devices such as cameras, access readers and intercoms. IP allows us to extend these systems beyond the physical boundaries of the facility. However, end users often don't consider the steps they need to take to secure the new endpoint. Left unprotected, an IP intercom or reader could be easily removed from an unsecured external area, exposing full unauthorized access to an organization's entire security network.

New vulnerabilities also exist at the front line. Let's say an end-user has a security workstation installed "as is," right out of the box. The operating system isn't secured and access permissions aren't defined. The guards that commonly use these workstations can log in and out using default passwords or passwords that are shared by multiple users across an entire shift. As a result, guards may have unfettered access to security systems and limited accountability relative to how they're using the workstation. In this scenario, what's to stop a guard from accessing video, downloading clips and sharing them with the world via YouTube? And what's to keep that same guard from downloading those clips to an unauthorized external device at the same time, infecting the workstation with a virus? If left unprotected, this scenario could become a dangerous reality.

These are but two examples of the vulnerabilities that exist in physical and electronic security systems. There are countless other potential gaps, and many important questions to ask. For example, what is an organization doing to protect all points of its security system – even those that extend beyond the physical facility? Do employees have access to all areas of the security applications, or only those necessary for their specific job function? Are network passwords changed regularly? Do former employees, including security personnel and service technicians, still have valid passwords for secure systems?

### Closing Gaps

Many of the logical gaps that exist in today's security systems can be closed through collaboration between the integrator and the end user's security and IT departments.

For example, Windows patching and antivirus measures are critical to any network. But oftentimes, the importance of these measures for security systems is overlooked because the systems are placed on "closed" or dedicated networks. Working together with an organization's IT department, such gaps can be identified and addressed as part of enterprise-wide logical security activities.

Another way to close the logical security gap is to effectively monitor and control security system access points. Security workstations are often excluded from typical security measures. By extending such measures – securing the operating system, limiting the system to operate only core tasks, requiring individualized login to the PC, defining access permissions for users – end users can protect their security systems and help mitigate day-to-day threats.

### Educating End-Users

Clearly, there is a logical security gap that threatens the very systems integrators design to protect our customers' organizations. As security integrators, we must take responsibility for closing those gaps. We must take a leadership role in educating our customers about the risks of failing to safeguard their physical and electronic security systems. Our expertise in and understanding of integrated security systems makes us valuable partners in leveraging logical security strategies to ensure the protection of all elements in an organization's security program.