SIMON ASHENDEN

Associate Managing Director,
Asia Pacific Head
Security Risk Management
Singapore
simon.ashenden@kroll.com

NICK DOYLE

Managing Director, EMEA Head
Security Risk Management
London, UK
ndoyle@kroll.com

TIMOTHY V. HORNER

Senior Managing Director, Global Head
Security Risk Management
New York, NY, US
thorner@kroll.com

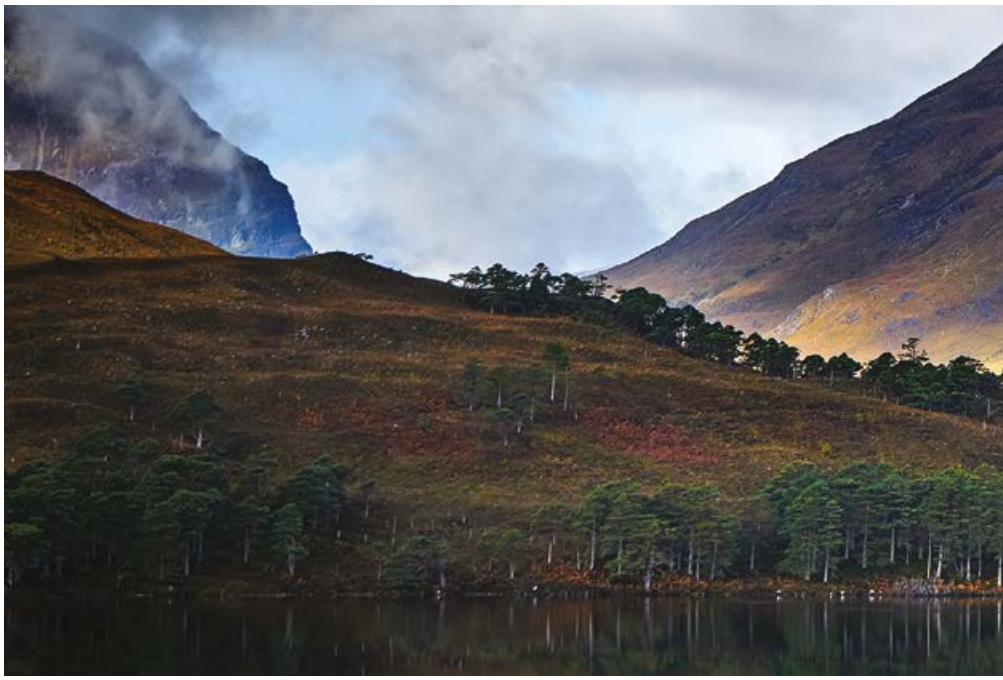
RAFAEL LOPEZ

Associate Managing Director
Security Risk Management
Mexico City, Mexico
rafael.lopez@kroll.com

Avoiding a False Sense of Security

An organization's physical security program may not be commensurate with the actual risks and threats the enterprise faces. Development of a master security plan can lead to rightsized solutions.

This year's *Global Fraud and Risk Report* highlights how the risk landscape has broadened to include social media, geopolitics and other threat vectors. Even with the addition of these concerns, however, physical security—controlling access to facilities and assets and protecting personnel—remains a central component of risk management. Evidence of this can be seen in two results of our survey. Two of the three most frequent types of incidents—leaks of internal information and data theft—often involve unauthorized access to, or use of, company assets. Second, employees are the most common perpetrators of both incident categories. In combination, these two findings underscore the importance of access control in mitigating theft and misappropriation. Many organizations that experience these and other types of intrusions have installed physical security systems such as access control card readers, video surveillance cameras, security guards and vehicle bollards. Yet there is often no underlying strategy for which systems are implemented or how they are to be employed. The result is a hodgepodge of frequently misused tactics that fails to provide the basis for comprehensive protection, detection and response.



HOW PHYSICAL SECURITY FAILS

Consider video surveillance cameras, for example. Used properly, these systems can be highly effective in helping organizations detect and respond to unauthorized access incidents. But effective use requires cameras that are appropriately positioned and fully operational, as well as active monitoring of the video feeds by a sufficient number of personnel trained in threat response. However, this scenario rarely occurs. Instead, cameras are often placed in low-risk locations, camera functionality goes untested, monitoring stations are understaffed and workers are poorly trained. A video surveillance system, like any technology, isn't self-sustaining. To be effective, it must be supported by the right procedures, policies and personnel.

Necessary risk-management initiatives can sometimes be sidelined because security measures are viewed by company leaders as undermining the organization's culture. This perspective has become increasingly common as more enterprises adopt informal, egalitarian workplaces. For instance, a company may balk at the recommendation that access to the offices of its C-suite leaders be restricted with keypads or card readers, believing this barrier would hinder a spirit of open collaboration. The reality, however, is that a chief executive officer or chief financial officer is more likely to have sensitive material in his or her office and to be the target of disgruntled employees. Companies with egalitarian cultures should understand that equality among people doesn't necessarily mean equality in their threat profiles.

Unfortunately, the weaknesses caused by an ineffective risk management program are usually not immediately apparent. The enterprise may appear to be well secured until an incident occurs, an antagonist strikes or a threat is imminent. Kroll's Security Risk Management team is frequently contacted by companies that have received threats from a recently fired employee or that realize a former employee may still be in possession of trade secrets or other sensitive information. In such cases, the first step is to review the security procedures currently in place. This often uncovers shortcomings that require immediate action, such as significantly increasing on-site security staff or locking down portions of the premises—remediations that can be far more costly, disruptive and unnerving to employees than building in adequate physical security procedures from the beginning.

MOVING FROM GUESSWORK TO CLARITY

Organizations can avoid these problems by conducting a thorough threat and risk assessment. This assessment incorporates multiple factors, including how facilities are laid out, which employees need access to which assets and how valuable the relevant assets are. The assessment also includes gathering intelligence to determine whether the firm or its principals could be targets of malicious actions and evaluating collateral risks arising from facility locations and nearby enterprises. For example, are the parking lots in the area susceptible to automobile break-ins? Is the facility located next to an enterprise involved in high-risk or controversial activity that could invite protests or violence? In addition, the assessment systematically analyzes the history of incidents experienced by the company to uncover patterns of vulnerability that might otherwise go unnoticed.

Following a threat and risk assessment, an organization can develop a master security plan that includes the following components:

- The types of electronic security measures needed (such as access-control card readers and intrusion detection systems) and their minimum specifications and implementation requirements
- The types of architectural security measures needed (such as vehicle bollards and window blast protection) and their minimum specifications and implementation requirements
- The policies and procedures necessary to support those measures
- Training for security staff as well as the larger workforce
- A plan for integrating security measures with one another and into operations
- A system for regularly auditing, testing and maintaining security system performance
- Contingency plans for scaling, if needed

The security master plan would also specify access-control measures, including where card readers need to be placed, the types of credentials to be used, methods for determining access privileges, who will grant and update access privileges and how anomalies or exception events are monitored and investigated. It would outline the coordination of access permission with human resources procedures for hiring and termination. The plan would also discuss ways of integrating card readers with the video surveillance system to capture attempts at forced or unauthorized entry. Repeating this level of analysis for all systems results in a comprehensive framework for effective physical security.

No matter how digital the economy becomes, the physical protection of facilities and people will always present a fundamental security challenge. Basing physical security on a detailed threat and risk analysis can help ensure that such measures provide real protection when threats materialize.

> Risk management weaknesses are usually not apparent at first. The enterprise may appear to be well secured until an incident occurs, an antagonist strikes or a threat is imminent.