# FUTURE OF CORPORATE LOSS PREVENTION

Security in 2025 *employs a modern technique to peer into the future, crowdsourcing a vision from the minds of 34 security professionals. The book's contributors, ranging from new entrants to long-time veterans of the field, offer their predictions on a wide range of security topics from many different perspectives.*

**Excerpted from *Security in 2025*:**
This chapter examines current trends that may lead to future challenges for security managers. According to Top Security Threats and Management Issues Facing Corporate America (Securitas Security Services USA, 2016), based on a survey of security professionals at Fortune 1000 companies, the top five threats were Cyber/Communications Security: Internet/Intranet Security, Workplace Violence Prevention/Response, Active Shooter Threats, Business Continuity Planning/Organizational Resilience and Cyber/Communications Security: Mobile Technology.

The top security management issues were Security Staffing Effectiveness: Training Effectiveness/Methods, Promoting Employee Awareness, Implementing Best Practices/ Standards/Key Performance Indicators and Strategic Planning. Staying Current with Technological Advances, Threat Assessments, and Regulatory/Compliance Issues (state/federal legislation) were tied for fifth place.

## Challenges

**Upgrading Physical Security Systems**
Security directors often face a challenge in attempting to gain funding for needed security upgrades. One sees that challenge reflected with the continued use of monochrome cameras where color cameras with low-light capabilities are needed, as well as the surprising number of analog systems still in use. Key systems are still widely used, even keeping track of keys issued, lost, and stolen is a difficult, outdated process.

Requests for security system upgrades may be denied partly because of a shortage of funds, but also partly because the security program did not market itself well. The security manager may not be able to change the first factor, but he or she can certainly change the second.

**Convergence**
Convergence between physical security and information technology (IT) can create conflicts within an organization. Typically the IT department controls the network, but the security department also has a substantial interest in that network. Security controls video surveillance systems, which transmit data over an organization's network; criminals can use the network to perpetrate thefts; and access control systems may also operate on the network. Neither IT nor security professionals want to be controlled by each other.

That scenario may sound frustrating, but the alternative is probably worse. In companies that lack security/IT convergence, security may have to rely on slow, dial-up systems. One proposed solution is for the organization to appoint a chief security officer (CSO), to whom both the director of security management and director of information security would report.

**Fraud**
Fraud examination is rapidly presenting itself as the next challenge. More and more companies are dealing with dishonest employees, vendors, and customers. Some terrorist groups are involved in counterfeiting.

Corporate security is usually ill-equipped to handle complex fraud investigations. Training and other resources are not readily available in the budget. Several large international companies that import goods have chosen to take part in the Customs-Trade Partnership Against Terrorism (C-TPAT). This program involves physical security audits for importers by customs agents.

**Now Until 2020**
As a security director, you should take these steps:

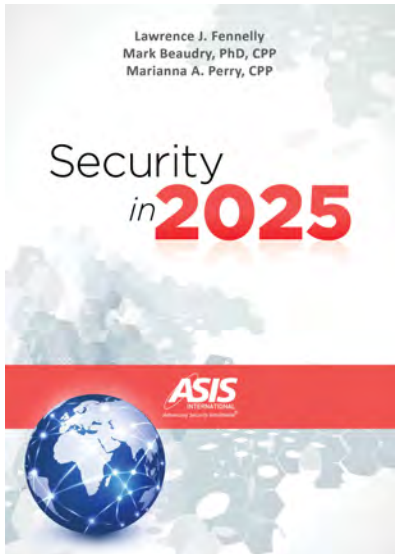
- Identify your number-one physical security upgrade need, obtain proposals for the new system, and master the budget process. You might opt for a new video surveillance system using only digital components. You might need to repair, update, or replace the fire alarm system. Perhaps you could switch to an electronic access control system instead of keys, upgrade exterior lighting with cost-effective LED bulbs, or add biometric devices to control access to sensitive, restricted areas.

- Educate yourself about the Internet of Things (loT), which consists of objects embedded with electronics, software, sensors, and network connectivity, enabling the objects to connect and exchange data. Estimates suggest there may be 50 billion connected devices by 2020. The loT will create new vulnerabilities and challenge the way we think about security, both in the physical and digital environments. Interconnectivity is the future of security.

- Boost training for all security personnel, and prepare them for certification. Earning such designations as Certified Protection Professional or Physical Security Professional shows that your security team possesses substantial relevant experience and demonstrated competence. Other certifications to consider include Certified Information Systems Security Professional and or Certified Fraud Examiner.

- Prepare for body cameras. They will soon be a part of the security officer's uniform.

From now until 2020, the security director will gain greater access to the chief executive officer, chief financial officer, and chief operating officer. such access will give him or her




*Security in 2025* is published by ASIS International



greater insight into the enterprise's focus and direction. That knowledge enables the security director to forecast more effectively regarding risks and necessary protective measures. The company's perception of security will begin to change. What was once entrusted to facility and maintenance directors will be put in the hands of security professionals. Corporate security will increasingly receive the respect it is due.

**2020 to 2025**

Physical security systems, convergence, and fraud examination will all progress substantially from 2020 to 2025. All security surveillance cameras will use Internet Protocol (IP), capture color, and have enhanced nightvision capabilities. Biometrics and card systems will replace keys for all points and types of entry and exit in corporate offices as well as manufacturing and distribution facilities. Convergence will take a huge step toward reality due to the use of IP cameras, which require being connected to the enterprise network. Education programs for corporate security personnel will be realized through an increased training budget.

Between 2015 and 2020, corporate security directors and managers will join the executive suite as CSOs. They will be well-versed on company objectives and know how to articulate the security program's return on investment. Security professionals will make the security decisions.

To fill those CSO positions, companies will look for people who have fully prepared themselves. Companies may look for persons who have obtained a knowledge of security management, information security, and fraud examination—all three. Certifications will prove important for demonstrating that knowledge.

Corporate security will continue its participation in the C-TPAT program. Along with security management, information security, and fraud examination, a focus on the supply chain will better protect the enterprise as a whole. Ensuring the security of the product, the conveyances on which it is transported, the people involved in the movement of the product, and the innocent bystanders past whose homes and businesses the product must travel will be the concern of both government and business. How do security professionals ensure the security of goods in transit, considering both the methods and routes of transportation? According to Gilbride and McDougall (2013), vulnerabilities can be simplified into four categories: weather-related, human-related, timing, and mechanical. Other relevant factors include these:

- Forecasting/Planning
- Purchasing/Procurement
- Logistics
- Operations
- Inventory Management
- Transport
- Warehousing
- Distribution
- Customer Service

A security program that addresses the supply chain will not only detect, deter, delay, and deny supply chain disruptions (such as gray market diversion, counterfeiting, and hijacking)—it will also reduce day-to-day security problems, such as employee theft, workplace violence, and fraud. Security management, information security, and fraud examination wrapped up with supply chain security will constitute the future of security-in-depth.

Every five years, after a company's last security systems upgrade, it will be time to identify state-of-the-art security components and bring the various systems up to that level.

**Where We Need to Go**

The following are some specific changes the security professional should strive to bring about in the future:

- Improved corporate mind-set. Managers view security as a staff function because it does not create a revenue stream. When times are tough, one of the first budgets to be cut is always security. Security management professionals must learn how to sell corporate management on the benefits of good security. It is important to build into the corporate culture an understanding that security is an investment, not an expense.
- Structured security careers. Unlike law enforcement, private security has yet to structure clear, definable career paths. These paths should be created with a focus on opportunities for advancement, job security, appropriate pay scales, and good benefits. A mechanism to offer 20+ year careers in the field would help attract more and better applicants. ASIS International can play a major role here.
- Reorganization for cybersecurity. More than 95 percent of all information in the United States is digital. Paper is disappearing quickly. Identity theft, hacking, and other computer crimes are increasing by 40 percent or more per year. IT and physical security will need to meld their efforts through an effective organizational structure.
- Law enforcement-private security cooperation. Much of the nation's critical infrastructure is protected by private security.

Law enforcement and the private sector must find new ways to cooperate and exchange information on a timely, regular basis.

Both sides are engaged against the same adversaries--criminals and terrorists. The need for coordination of resources is critical given the increasing demands of crime and terrorist threats. Both sides will be more effective once policymakers from both sectors mandate more cooperation. Chiefs, sheriffs, and security directors must get on the same page—even on occasion, in the same room. ASIS International could be that room.

In the future, the goal for corporate organizations will be to anticipate change and learn to adapt. Many of our preconceived notions about effective security will be challenged. Organizations must address cybercrime, emergency management and learn to effectively harden targets, especially soft targets.

Lawrence Fennelly, CPOI, CSSI, CHL-III; Mark Beaudry, PhD, CPP; and Marianna A. Perry, MS, CPP

# Retail Security Risks and How to Fix Them

Securing your retail building is tricky. How do you allow movement in and out of your building, but prevent shoplifting? How do you secure your stock room, but allow free exit in case of an emergency?

Enhance life safety and security measures in your building with the addition of cutting-edge technology that works in conjunction with your existing systems for a variety of applications, such as:

- Delayed Unlocking Devices/Anti-Shoplifting
- Outdoor Sales Area With Gate
- Sales Floor to Stock Room
- Tailgate Detection

**Delayed Unlocking Devices/Anti-Shoplifting**
By installing delayed unlocking devices, you can prevent unauthorized exit through secured openings and redirect foot traffic to your main doors. Delayed unlocking devices prevent shoplifting by setting off an alarm while remaining locked for several seconds beyond the initial exit attempt, giving staff a chance to respond to the unauthorized exit. Delayed unlocking devices must be tied into a fire alarm, allowing free exit in the height of an emergency.

**Outdoor Sales Area With Gate**
Weatherized panic devices are designed to withstand the elements while delayed unlocking prevents shoppers from slipping out with merchandise. Access control devices allow entry from outside with the use of a keypad or card reader. Weatherized door prop alarms further add to your outdoor security with an audible warning when doors are held or propped open.

**Stock Room**
This system deters customers from entering stock rooms, but during an emergency provides a life safety path through the stock room. This system should include access control keypads and/or card readers so your employees can access the stock room. A door prop alarm can be added to alert staff to a propped open door.

**Tailgate Detection**
Whether you have a members only fitness facility, a card-required warehouse store or a corporate office, tailgate detection will enhance your access control. The tailgate detection system assures that only one individual enters a secured doorway for each authorized card read. The tailgate detection system is compatible with most access control technologies, is easy to retrofit, and has an integrated door prop alarm for extra security.


The right components are critical to securing your retail building from inside and outside threats.

**Putting all the right pieces in one place for complete peace of mind**
Ensuring all the pieces of technology will work together is key. Manufacturers and some dealers will create a kit to fit your application that includes best-in-class products along with wiring and riser illustrations. Failing to install the items correctly can create years of headaches and wasted money. Ensure the supplier understands your needs and offers time-tested products. Additionally, make sure they can support the installation with wiring diagrams, riser illustrations and technical support.

# Protecting People From Things | Protecting Things From People

Store Name: Hard Ta Knock Shoppe. Location: Cincinnati, OH 45225. Heavy duty steel storefront gates have proven they will withstand the "crash and grab" trend. Thieves attempted to drive into this Cincinnati boutique, slamming a car through the front door three times. But even a vehicle couldn't get past the heavy duty steel Illinois Engineered Products security gate.

A Loss Prevention Case Study Secure Product From steel mesh cabinets to pallet gates; from portable gates to area cages and wire partitions, our specialty is designing physical security solutions so you can "secure it where you store it." Protect your inventory from theft, shrinkage and damage, with convenient visibility: whether it's on the sales floor, in a warehouse, a backroom, or receiving areas.

Heavy duty steel storefront gates have proven they will withstand the "crash and grab" trend. Thieves attempted to drive into this Cincinnati boutique, slamming a car through the front door three times. But even a vehicle couldn't get past the heavy duty steel Illinois Engineered Products security gate. Store surveillance recorded the incident, including a perpetrator attempting to walk in through the damaged, yet still secure gate. The business owners were still able to open the next day because their after-hours loss prevention solution held up against a brutal assault.

Solutions for:

- Shrinkage Prevention + Loss Abatement
- Employee Safety • Inventory Protection
- Visible Security + Inspection
- Anti-Theft Solutions
- Storefront Access Control
- Secure Storage

Your Custom Applications:

- Data Centers
- Schools
- Warehouse + Industrial Facilities
- Boiler Rooms
- Liquor Section + Aisle Access
- Breweries + Distilleries
- Pharmacies

**Secure Product**
From steel mesh cabinets to pallet gates; from portable gates to area cages and wire partitions, our specialty is designing physical security solutions so you can "secure it where you store it." Protect your inventory from theft, shrinkage and damage, with convenient visibility: whether it's on the sales floor, in a warehouse, a backroom, or receiving areas.

**Secure Areas**
Section off entry to any space with our custom solutions, including heavy duty folding gates, wire mesh caging, and portable gates of any size. Keep the right people and things in the right places, whether for safety or asset protection. Manage incidents before they happen with proactive protection of areas while also projecting an image of authority, safety, and security.

**Secure Access**
Meet/exceed safety and security standards in your industry with our access control solutions, designed with your business' needs in mind. Solutions include temporary and permanent fixtures, from heavy duty to polite discouragement. Avoid internal/external theft, unauthorized entry, and OSHA compliance issues. The 2015 National Retail Security Survey identified that 72.5% of Inventory Shrinkage is due to Employee Theft and Shoplifting.

More than 160 years of loss prevention experience in an ever-changing world has earned us the reputation as the leading security solution provider, as we have continued to adapt to serve evolving technology and threats. Armed with our arsenal of effective physical security solutions including an impressive portfolio of 100% American-made products, we continue to be the leading loss prevention specialists in the industry. Whether a bulk-order for traditional steel folding gates or a limited production run of a one-off emergency fix for 200 locations, we bring those solutions to you with our extensive design and factory services.

Learn more about Loss Prevention Solution:
losspreventionsolution.com • 1.844.850.6700

LOSS PREVENTION SOLUTION.com

For product info #22 securitymgmt.hotims.com