Call Us: 402.289.4126 | **Email :** sales@primecominc.com

Prime communications

19
SEP2018

4

The New Normal: Designing Security to Fight Organized Retail Crime

Bold, well-orchestrated – sometimes violent – organized retail crime (ORC) has reached a new level of intensity. That means loss prevention and asset protection also must rise to new heights. Fortunately, new technologies make it possible to more effectively reduce shrinkage and improve asset protection.

The FBI now estimates ORC losses at more than $30 billion per year. The National Retail Federation polled members in 2017, and 95% said they had been victimized by organized theft and fraud operations, with costs rising to more than $700,000 for every $1 billion in sales.

The key to understanding the ORC new normal is to think like the members of these criminal teams. This article explores who they are, actions they may take and why, as well as fraud detection and security strategies likely to become lasting solutions: better inventory management, security systems integration all the way to the shelf level, working backwards towards solutions, and establishing open-architecture digital security systems to save time and money.

Who Is Involved in Organized Retail Crime, and What Are They Thinking?

“There is no industrywide magic fix for ORC yet. It’s just too large of a problem at this point,” said Brian Freeman, VP of National Sales for Prime Communications, Inc. (PCI) which recently was named a top-50 security dealer and systems integrator. “However, those of us who have been in the industry for a long time know you can’t begin at the end, with the theft event itself — you have to begin at the beginning. Ask yourself who these criminals are, what they are targeting, and what technology is available to deter and detect them.”

The ORC new normal includes well-trained teams of thieves who use clever strategies. They operate in sophisticated organizations with a hierarchy of players: leaders, middle managers, fences, clandestine distribution center personnel, and front-line thieves. “Our job is to understand their motivation and operation and outthink them, designing formidable security strategies just as bold and well-organized as they are,” Freeman explained.

To begin, he suggested thinking of the enterprise (distribution centers or stores) as a network of locations this hierarchy may be targeting, then apply safety and security measures by location to improve loss prevention capabilities. PCI creates strategic maps of facilities to help assemble layered fraud detection and security plans that integrate equipment, strategies, training and protocols.

ORC Security for Distribution Centers

Effective solutions for minimizing theft risk include:

People entering and leaving the facility. Crime bosses stay up at night thinking about how to get in and out undetected. Installing videosurveillance and automated gate controls, such as badges and smart turnstiles, helps ensure only vetted personnel

enters. For an added layer of security, metal detectors and handheld wands help staff check for weapons, including guns and knives providing an added layer of security.

Trucks entering and leaving the facility. Criminals look for opportunities to gain control over trucks packed with high-value goods. Deploy security protocols to accurately identify drivers as well as trucks at the greatest risk for theft. Park trucks containing at-risk goods in areas with extra layers of security. Use license plate identifying software to automatically confirm arrivals and departures.

Goods at rest. Think like criminals to determine where goods at rest are most likely to be compromised. Use customized exterior and interior cameras strategically to monitor all shipping and receiving areas. Customized mounts allow cameras to see inside trailers during the loading and unloading process. Install lighting that exposes cargo all the way to the back.

Exit routes. Criminal team organizers must identify quick escape routes. By nature, distribution centers are located near easy transportation routes. Ensure a perimeter clear of obstacles and a clear line of sight from the guard shack to all exit points.

Shift changes. The controlled chaos of shift changes provides cover for thieves to hide or take away goods. Deploy alarms and monitors that help security staff watch people during shift changes.

Parking lots. Teams of thieves may assemble in a parking lot before entering or regroup there after stealing goods. Make sure lots are well-lit and well-maintained. Appropriate deterrents include cameras on light poles, with signs notifying criminals they are being watched. Some cameras include speakers through which guards can notify criminals they have been seen.

Property lines/perimeters. Well-layered security includes looking beyond the property line. What will criminals be doing before they reach your property? Make sure camera views and protocols extend well beyond fences.

ORC Security in Stores

Strategies to reduce theft include:

Parking lots and property lines/perimeters. Risks and solutions are similar to those outlined above for distribution centers.

Shelves and aisles. In-store video and sensor technology — even facial recognition software upon entry to the store — have advanced to the point that it's possible to monitor and detect unusual activity at the shelf level. Use the same software to analyze buying habits and inform marketing. "Ask about PCI's retail analytics package," Freeman suggested. "One of our clients is using a mobile app to integrate mobile

technology with their customer loyalty program to assist in reducing loss with scan and go deployments."

Show people their own image. Many thieves are desperate and on-edge. Seeing themselves on a public view video monitor might be enough to stop them from stealing.

Point-of-sale locations. Video cameras can be integrated with point-of-sale software to identify when goods are sold at a lower-than-normal cost or given away. This strategy can foil UPC scams and sweetheart transactions.

Match Multiple Layers of Organized Crime with Multiple Layers of Security

Detection and analysis strategies need to be just as layered and well-integrated as ORC teams. To make the best use of available equipment and software, consult an experienced integrator with deep understanding of inventory management best practices, fraud, and security protocols, as well as software at the core of video and sensor management. Effective integrators not only possess sophisticated knowledge and project management experience but are easy to work with, including communicating promptly and providing effective training.

Many camera and equipment options are available, but you must make sure you're using the right one for the specific field of view and potential criminal activity. "There is a lot of math to selecting the right camera and getting it in the right place," Freeman said. "We complete detailed engineering drawings and 3-D renderings to avoid wasting time and money."

It's critical to build a security system on open digital architecture with software to link systems. Freeman said, "This means you can simply upgrade current software to take advantage of new technology and customize it without spending the half a million dollars it could cost to replace it."

Finally, Freeman suggests the most important piece of advice of all: Reset expectations properly and create a comprehensive plan that truly fits your organization *before* implementing any new fraud detection or security strategies to reduce shrinkage. "That's how to respond to the new normal," he said. "Let them come. You'll be ready."

Engineered Delivery of Security & Infrastructure Solutions

Our Headquarters
22145 W Maple Road, BOX 131, Elkhorn, NE 68022
Phone: 402.289.4126
Email: sales@primecominc.com