SECURITY today

Security Strategy

Are you thinking omni-channel or "omni-chance"? Here are 3 areas for your security team to review

By John Carter

While many security teams at retailers are concerned about the potential for a big data breach, everyday security threats, like social engineering and shoplifting, are heightened in a world of omni-channel retail. While unfortunately these physical security threats are more predictable than a data breach, the good news is that predictability is exactly what makes them more manageable with the right tools and intelligence.

The common thread between these threats is understanding and controlling who has access to what assets and data. There are three areas worth revisiting in light of the latest threats and available technology solutions to ensure that your company is best protecting people, assets, and the bottom line. These three areas are connected: keyless access control, sensors across the omni-channel landscape and optimizing case management.

Rethink the Brass Keys with Intelligent Access Control

With the advancement of tools and sensors, one of the most underused areas for retail is access control. Steve Lindsey, a veteran of retail security who managed physical security at Wal-Mart for more than 30 years, understands better than anyone the need for these tools.

Lindsey recently visited a big box store and had a common experience: purchasing a gift card that understandably was under lock and key. It took a trusted employee several minutes, manager approval, and a patient customer, to complete the transaction. Naturally, Lindsey had some questions about how they manage access to important assets. "Do you trust this employee?" he asked the manager with the brass keys. "Of course," the manager said, then Lindsey asked him why the employee couldn't have access to unlock the gift card he was trying to buy, and the reality is that physical possession of brass keys

supersedes employee experience and trust.

The challenge with brass keys is compounded by everyday life: the inconvenience when someone accidentally brings them home, or the holder of the keys is busy and customers are left waiting. Surely technology can help us overcome this, and it has with access control, but why aren't retailers embracing better solutions?

Lindsey has seen some examples of retailers that offer the ideal experience: you're in a store, need access to an item behind lock and key, and an employee opens the display case with the tap of a badge or the swipe of a finger. This experience is less common than it should be, and he is still surprised by the reluctance of retailers to move to modern access control methods, with everyday card keys or biometric readers that allow trusted employees to do their jobs faster and more efficiently.

"It is time for retailers to rethink the brass keys," Lindsey said. "Better access control improves the customer experience with faster turnaround, and increases employee productivity. The cost of copying keys can reach tens of thousands of dollars annually for a large retailer—that alone should motivate these locations to make a change to keyless access control."

The use case for keyless access extends beyond the traditional brick and mortar locations to employee areas, warehouses, lockers, and anywhere that people and merchandise are coming and going. In our omni-channel world, it's about having flexible access to align with flexible logistics. The advancement of access control when implemented at scale increases transparency and accountability for people and inventory.

Put Sensors to Work Across Channels

"Omni-channel brings interesting opportunities and risks to physical security teams", said Clayton Brown, product manager at ReconaSense, a proactive situational awareness platform.

A recent report from McKinsey and Company notes that "In several sectors, 'click and collect' is proving a popular and increasingly efficient means of serving the customer. More than 50 percent of Walmart's online sales and around 40 percent of Best Buy's already are picked up in stores—a multichannel mind-set must be embedded in the store design and in employees' new ways of working."

Like the challenge of protecting assets with better access control, the flexibility of omni-channel means that for retailers to be successful, inventory is dispersed. So tracking it, and reducing shrink, is more complex and more important than ever.

At the same time, every retailer's goal is to take the customer experience across channels to make shopping seamless and relevant. IoT devices that are in use today, including beacons for real-time offers and sensors to optimize store layout, are just some of the technologies that could also be leveraged for physical security.

"What retailers are not doing yet is looking at every single connected sensor as an input to your physical security posture. We look at each one of these devices as giving us contextual clues to detect potential theft and other threats before an incident takes place," Brown said.

Today customers can receive their order myriad ways: order online and pick up in store, retrieve from a locker, or have their order delivered at home through a network of contract drivers. The convenience of these options means a better customer experience with increased risk to you: your chance of experiencing theft, less employee accountability, and variance across your supply chain increase greatly.

To mitigate the risks that these options bring, Brown suggests rethinking the intent of each IoT sensor.

"It's time to look beyond how these connected sensors were meant to be used to see how they can be optimally used," Brown said. "Every place from your social media account, to your parking lot, distribution center, and delivery drivers offer clues about security of your entire operation. Putting these patterns together puts your security team in control."

Getting to that point will accelerate the value that you will derive from sensors. McKinsey said, "Interoperability between IoT systems is critically important to capturing maximum value; on average, interoperability is required for 40 percent of potential value across IoT applications and by nearly 60 percent in some settings."2

For retail security teams to get the most out of technology investments, it's going to take partnership across departments, and the right platform to make these devices talk to each other, and work together, for you.

Check Your Case Management System

Case management is one of the most important tools for security teams to communicate about cross-site threats. But many retailers lack the insight and shared resources to make the most of this information. There is potential with shared information and better case management. Today, cases are disparate and each holds clues to security threats like crime rings, but there is no way to correlate this information across multiple sites. It's time for this valuable information to be more accessible and actionable.

The combination of centralized access control and omni-channel sensor information means that when cases are open they are automatically more informative. With a platform that pulls in big data from across IoT sensors, and allows for centralized case management, patterns and predictors of crime are more easily identified, so retailers can get ahead of threats.

The technology to enable more sophisticated case management exists today, which is the great news. Now it's time for the cutting-edge retailers to start testing the limits of the latest solutions available that integrate big data from across sensors and produce intelligent case management outputs. The power of the technology comes when you use it in combination with access control and a platform approach to sensor management to truly stop physical security threats in their tracks.

Moving Away from Chance

Retail today is complicated, as is physical security, and your business needs to look at the next strategic steps to shift from where you are today to more sophisticated analysis and tools. McKinsey notes that "capturing the full potential of IoT applications will require innovation in technologies and business models, as well as investment in new capabilities and talent."2

Industry experts agree. Lindsey emphasizes that for retailers to move forward.

"It's time to think broadly rather than siloed in physical security lanes," Lindsey said. "The Internet of Things is a huge opportunity for security teams, and it's exciting to see the new tools available to help physical security teams move to the next generation."

Improvements in the three areas of keyless access control, omni-channel sensors, and optimized case management are possible today with the latest tools and a willingness to try a new platform.

John Carter *is the president and CTO of ReconaSense.*

1. http://www.mckinsey.com/industries/retail/our-insights/making-stores-matter-in-a-multichannel-world

2. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world