Retail Security in a World of Digital Touchpoint Complexity

Author Greg Buzek, President of IHL Services
Sponsored by Cisco Systems Inc.

Featuring industry research by
Previously in part 1 and part 2 of our series, we discussed how critical it is for retailers to have an updated and optimized network infrastructure and how IoT opportunities in retail can enhance the customer experience and improve operational efficiencies. Here we discuss why the mindset of security as a first thought and not an afterthought is absolutely crucial to the success of retailers going forward.

As you are well aware, retailers face attacks both in the physical world and in cyberspace all day every day as one of the most targeted industries for organized crime groups and hackers. And with the breadth and depth of the threats, it is best to work with a primary vendor who understands and can provide an integrated security plan for all of your touchpoints so you can stop attacks at the edge, protect your users, control who gets on the network, simplify your administration, find and contain problems quickly when they occur and provide for continuous monitoring.

It is important to note, however, that a complete and integrated security plan is not just about cybersecurity or data security alone but is inclusive of both physical security that protects both you as a retailer, your customers and suppliers.

In fact, let’s look at physical security first. First and foremost, there is a need for systems that protect the physical security of your customers. This can include security personnel, security cameras, and proper staffing to physical barriers and access control to keep everyone safe.

Next, there is security and safety for your own employees either at stores, warehouses, and home offices. Once again, this plan includes cameras, access control systems, time and attendance systems and physical protection.

Then there is security for loss prevention that affects both employees and customers. These systems will include CCTV, behavioral analytics, cashier monitoring, checkout cameras, motion and lighting systems and electronic article surveillance along with a human team of LP professionals. Retailers lose between 1-2% of revenue annually due to shrink (either inventory losses or cash theft), and 60% of that comes with employee involvement.\(^1\)

Then there is a security of cash and receipts where smart safes, vaults, and armored personnel carriers play a role.

And finally, there is physical security to protect against false legal claim from consumers and employees, more commonly known as “slip and falls”.

All of these areas of security have both physical and systems components.

When it comes to cybersecurity there are many facets as well. Just as physical security has an IT portion, cybersecurity has both physical and cyber components. And as retailers move to improve the customer experience and operations through IT, the vast array of digital touchpoints that are added can create a dizzying number of IP connected touchpoints that must be secure or will cause a data breach and many time-consuming and financial complications for retailers. This is specifically true with the proliferation and types of wireless touchpoints, from your own internal systems, including internal WiFi, dedicated frequency
communications devices, Bluetooth, and WiFi hotspots for customers and suppliers.

The one area of cybersecurity that is most prevalent, yet unfortunately takes up way too much of the security budget due to regulations is payment security. IHL research reveals that a typical retailer spends 14% of their IT budget on things related to security. And the percent related simply to credit card or PCI security ranges from 37-55% of the total of that security budget depending on the segment. And the fact that PCI takes so much of budget and causes delays, 71% of retail executives say cybersecurity concerns impede innovation.

Payment security certainly spans the stores as well as online and mobile payment security as well. Many retailers have moved to a complete payment network that is separate from their other network.

Additionally, tokenization of transactions and Peer-to-Peer encryption are best practices in an effective plan to protect payment data.

But payments are not just an issue at the store. There is also the ecommerce side of payments and then the combined store/eCommerce part of Buy Online and Pickup In Stores (BOPIS). As hackers get more sophisticated, payment card fraud that used to be at the checkout lane has moved online. And specifically, with BOPIS, recent research has shown that fraud rates have increased 250% since EMV was implemented.\(^2\) Hackers are exploiting the fact that a chip authentication is not needed for BOPIS, since only a receipt is required for a store pickup. To protect themselves, smart retailers have deployed ID scanners that verify ID before pickup.

But cybersecurity doesn’t stop at the need to protect just credit card information.

There are also trade secrets, sensitive intellectual property, operational expertise and procedures and as well as other customer and employee data that also need to be protected. And the increase of touchpoints as well as the ability for systems to interact with people bring the need for an overarching and integrated plan for security.

In both physical and cybersecurity, a truly integrated security view has a plan for protection before, during and after a potential attack.

**Before an attack**
The before stage is where most of the planning happens. This includes the development and deployment processes and procedures that
ensure both physical and data security are considered. In physical security this can range from cameras and EAS installations to hiring practices and fraud detection and anti-theft practices, alarm and access control systems and physical loss prevention and security personnel.

On the cybersecurity front this includes such items as web reputation and filtering, monitoring of SaaS and software vulnerability, port scans and limitations, locking down peripherals and having segregated networks for key network traffic to name a few. All are critical components of an integrated security plan. As a play on an old adage, “Those who fail to plan, plan to be hacked.”

Generally good plans encompass the following aspects:
- Stop threats at the edge
- Protects users and customers wherever they work
- Control who gets into your network and what devices can connect
- Simplify the network management and segmentation process
- Policies, reporting, and logs to any exceptions to policies with continual monitoring to provide visibility on behavior anomalies within the network or physical premises to stop attacks from spreading.

And it bears noting here as well, cybersecurity planning does not need to be all about playing defense. It is also about putting into place the systems to enable the growth objectives that the company wants to achieve, understanding that nothing will do more damage to your brand than a failure to keep a customer’s data and personal identify safe.

During an attack
Despite the most well-designed plans for protection, attacks will happen and some might actually be successful. Smart retailers have a plan in place to detect, thwart, and then mitigate any attacks.

Some key components of this portion of the plan are the following:
- Artificial Intelligence and threat detection intelligence
- Antimalware systems
- File reputation systems
- Cloud data loss prevention
- Trusted partners that help monitor and test for vulnerabilities and monitor traffic abnormalities.
- Find and contain problems fast.
- Mitigation and procedures to shut down attacks from spreading.

Without question you will be probed and attacked. Your systems are being probed right now. And with the growth of IoT there are more and more places for an attack to start. And being PCI compliant has little resemblance to actual security, even in regards to payment data. Industry research has shown that over 80% of the companies that had a major data breach of credit card data were certified PCI compliant within a few months before the start of the breach.
After an attack
Once you find, stop and remove malicious content, a proper plan must be in place to fix issues going forward as well as what is shared and with whom depending on the type of attack.

Security should be an integrated strategy to produce the right business outcomes. And if we need to stress the importance further, a recent study from Deloitte showed that 73% of customers would reconsider shopping at a company if it failed to keep their data safe.

The network is the foundation of truly integrating your retail ecosystem with digital technologies and is only growing in importance with the expansion of IoT, edge computing and cloud initiatives across the entire retail journey. Leverage automation and assurance to plan and simplify your security practices. Have the right plans and systems in place for security and compliance that provide real-time threat defense and mitigation. It is time to let the network drive business innovation.

At the top level is a communication plan in place for informing necessary parties of the impact of any attacks. This can be internal only or if it involves customer or payment data, external law enforcement and credit authorities.

Internally, best practices should include sharing with management reports and log extraction data then further preparing for and mitigating any future attacks. This can be done by deploying and adding to SaaS anomaly detection, further focusing on file sandboxing and inspection processes and the deployment of cognitive threat analytics to understand the blueprint of the attack so that it can be protected against in the future.

Of customers would reconsider using a company if it failed to keep their data safe.*

Forward distribution is forbidden without written consent. If you wish to forward distribute please contact ihl@ihlservices.com or +1-615-591-2955

Sources:
1 2018 National Retail Security Survey
2 Renfrow, Jacqueline (2018, July, 2) BOPIS fraud is up 250% in 1 year. Can retailers protect their profits without losing customers? https://www.fierceretail.com/bopis-fraud-up-250