Why Hackers Love Retail

And What You Can Do About It with Cisco SAFE

Today’s retail industry is more at risk than almost any other industry. The current combination of mobile devices, distributed services, increased customer expectations, virtual systems, and changing business goals has created new levels of vulnerability for your retail brand. In the age of digital transformation, weak security can profoundly damage brand loyalty and critically affect your customers’ trust. The great majority of shoppers (86 percent) have said that they will reconsider using a company if it fails to keep their data safe.[1]

For this reason, innovative retailers understand that risk management is a vital customer experience and revenue opportunity. You need to find new ways to turn your cybersecurity preparedness into a competitive advantage. To accomplish this in the face of today’s many security challenges, your digital capabilities need to:

- Protect cardholder, company, and partner data
- Protect your brand and reputation
- Mitigate theft and fraud
- Secure physical and digital assets
- Simplify regulatory and process compliance

The common perception is that security is an enormously complex problem to solve. However, this does not necessarily have to be the case. Cisco simplifies your security deployment by providing a manageable, modular methodology for the Secure Store that we call SAFE. This approach addresses each threat to the retail branch with corresponding security capabilities, architectures, and designs–guiding you in a holistic manner to a complete security solution.

> “We need security minds to start thinking away from the old model of defense-centered thinking (and) into the new model of security enablement.”
>
> – Mike Dahn, Head of Data Security Solutions, Square

The Challenges of Security in Retail

Cybersecurity is a board-level priority for retailers, including concerns about protecting cardholder data (Payment Card Industry Data Security Standard compliance), physical security, and proprietary company data. According to the Ponemon Institute, retail organizations are victimized by at least eight cyberattacks per year (nearly one per month).[2] The annualized average cost of a successful cybercrime to a retail company in 2016 was US$7.2 million.[3] However, the damage over time is more long-lasting. Nearly a quarter of the organizations that suffered an attack lost substantial business opportunities. One in five lost customers due to an attack, and nearly 30 percent lost revenue.[4]

While the focus is generally on protecting and preserving the organization, 35 percent of retailers say the main purpose of cybersecurity is to enable growth.[5] However, in a recent Cisco study, no less than 71 percent of executives overall said concerns over security are hindering their ability to innovate, and 39 percent said they have stopped a mission-critical initiative because of security problems.[6]

Inadequate Cybersecurity Stifles Innovation

SURVEY

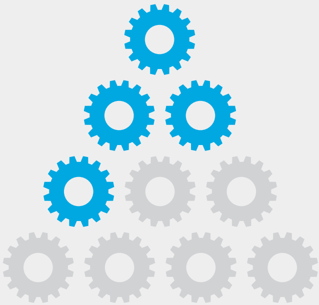
"Cybersecurity risks and threats hinder innovation in my organization"

71%

Agree

SURVEY

"My organization halted a mission-critical initiative due to cybersecurity concerns"



39%

Agree

SURVEY

"The main purpose of cybersecurity is to enable growth"

35%

Agree

Top Security Problems in Retail

The Cisco 2017 Annual Cybersecurity Report is an annual survey that includes 130 organizations across all industries. This study identifies a number of problem areas that are frequently seen in retail.

Perhaps the most startling of these findings is that due to various constraints, organizations investigate only 56 percent of the security alerts they receive on a given day. Half of the investigated alerts (28 percent) are deemed legitimate; less than half of those (46 percent) are remediated. Reasons for this include:

- Security solutions create a hodge-podge of vendors, tools, and solutions–28 percent of survey respondents cited this as a major block to advanced security implementations. The less integrated an organization's security capability is, the more vulnerable it is. Most companies use more than five security vendors and more than five security products in their environment. Fifty-five percent of security professionals use at least six vendors, 45 percent use anywhere from one to five vendors, and 65 percent use six or more products.
- Other blocks to a secure environment include lack of funding and IT talent. The top constraints to adopting advanced security are budget (cited by 35 percent of the respondents), certification (25 percent), and talent (25 percent).[7]

Organizations that have not yet suffered a security breach tend to believe their networks are safe. This confidence is probably misplaced, considering that almost half (49 percent) of security professionals said their organizations have had to manage public scrutiny following a security breach. On average it takes 197 days to detect an advanced threat, and time to containment takes another 39 days![8] Worse yet, according to a three-year study by Verizon Enterprise Solutions, retailers discovered breaches through their own monitoring only five percent of the time on average.[9]

Evolving Security Problems

A 2014 report by Interactions Consumer Experience Marketing found that, until the last couple of years, 97 percent of attacks involved payment system tampering. However, new threats are increasingly emerging. They include:

- **Seventy-five percent of surveyed companies are affected by adware infections.** Adversaries can potentially use these infections to facilitate other malware attacks. Increasingly, the operators behind malvertising campaigns are using brokers (also referred to as "gates"). Brokers enable them to move with greater speed, maintain their operational space, and evade detection. These intermediary links allow adversaries to switch quickly from one malicious server to another without changing the initial redirection.[10]
- **Spam accounts for nearly two-thirds (65 percent) of total email volume,** and research suggests that global spam volume is growing due to large and thriving spam-sending botnets. About eight to 10 percent of global spam in 2016 could be classified as malicious. In addition, the percentage of spam with malicious email attachments is increasing, and adversaries appear to be experimenting with a wide range of file types to help their campaigns succeed.[11]
- **Most dangerous of all is ransomware, currently on pace to become a US$1 billion industry in 2017.** Traditional attackers primarily steal information and maintain long-term access to the systems and resources of their victims. Ransomware hackers, on the other hand, lock up your data and systems, and force you to pay to recover access to your files. The emergence of anonymous currencies such as Bitcoin and Ripple give attackers an easy way to profit with relatively low risk. It is projected that future versions will propagate like worms, spreading throughout the organization in a coordinated manner and aggregating the ransom demand.[12]

> Organizations that have not yet suffered a security breach tend to believe their networks are safe. This confidence is probably misplaced, considering that almost half (49 percent) of security professionals said their organizations have had to manage public scrutiny following a security breach.
>
> – Cisco 2017 Security Capabilities Benchmark Study

Cisco SAFE and the Next-Gen Network

The SAFE approach encompasses the Cisco® Digital Network Architecture (Cisco DNA™) for Retail, the foundation technology that enables digital transformation of your stores and corporate offices. Supporting comprehensive network automation, assurance, and security, Cisco DNA makes it simple to manage your store and corporate networks while protecting customer and business data, reducing TCO, and providing deeper business insights.

Security, cloud, and the Internet of Things (IoT) are fueling today's digital transformation in retail, driving the need for better business and security data and analytics, operational simplicity, and business speed. Retailers gain:

- **More effective security** – You can rely on the network as an extended data source for threat visibility (network as a sensor) and accelerate threat mitigation (network as an enforcer)
- **Better cloud applications experience** – A network that automatically adapts to new traffic patterns and optimizes the secure delivery of cloud applications
- **Operational cost savings** – Centrally managed, policy-based automation of IT across the entire network
- **Business agility** – Greater business efficiency that speeds tasks that used to take weeks and require wide IT staff, and now only take minutes and involve fewer people
- **IoT scale** – A network that connects and secures any IoT device through device profiles, on a massive scale
- **Business innovation** – Data and analytics on users, devices, applications, and locations that enable creation and protection of new customer applications and experiences

Designing the Secure Store Branch

To address these existing and emerging challenges, SAFE helps you design a powerful security solution for each store branch. It includes support for your employees using devices (smartphones, laptops, tablets) that require secure access to the Internet, collaboration services such as email and voice, and branch-critical applications. It also encompasses third parties, such as service providers and partners, to provide secure remote access to apps and devices. Most important of all, it offers secure connectivity for shoppers who need guest Internet access within the store and across channels on their phones or tablets.

This methodology maps the security capability to the threat, helping you design a secure infrastructure for the edge, branch, data center, campus, cloud, and WAN. It encompasses operational domains such as management, security intelligence, compliance, segmentation, threat defense, and secure services. SAFE solutions have been deployed, tested, and validated to provide guidance, best practices, and configuration steps.

Understanding the “Attack Surface”

For a true security solution, your store needs to be protected on a number of different fronts, or “attack surfaces.” The SAFE methodology breaks these down into five layers: Human, Devices, Access, Distribution/Core, and Services. It is also necessary to consider the greatly increased number of–and risks created by–apps.

For a more detailed description of the SAFE methodology in the branch, please see the SAFE Architecture Guide.

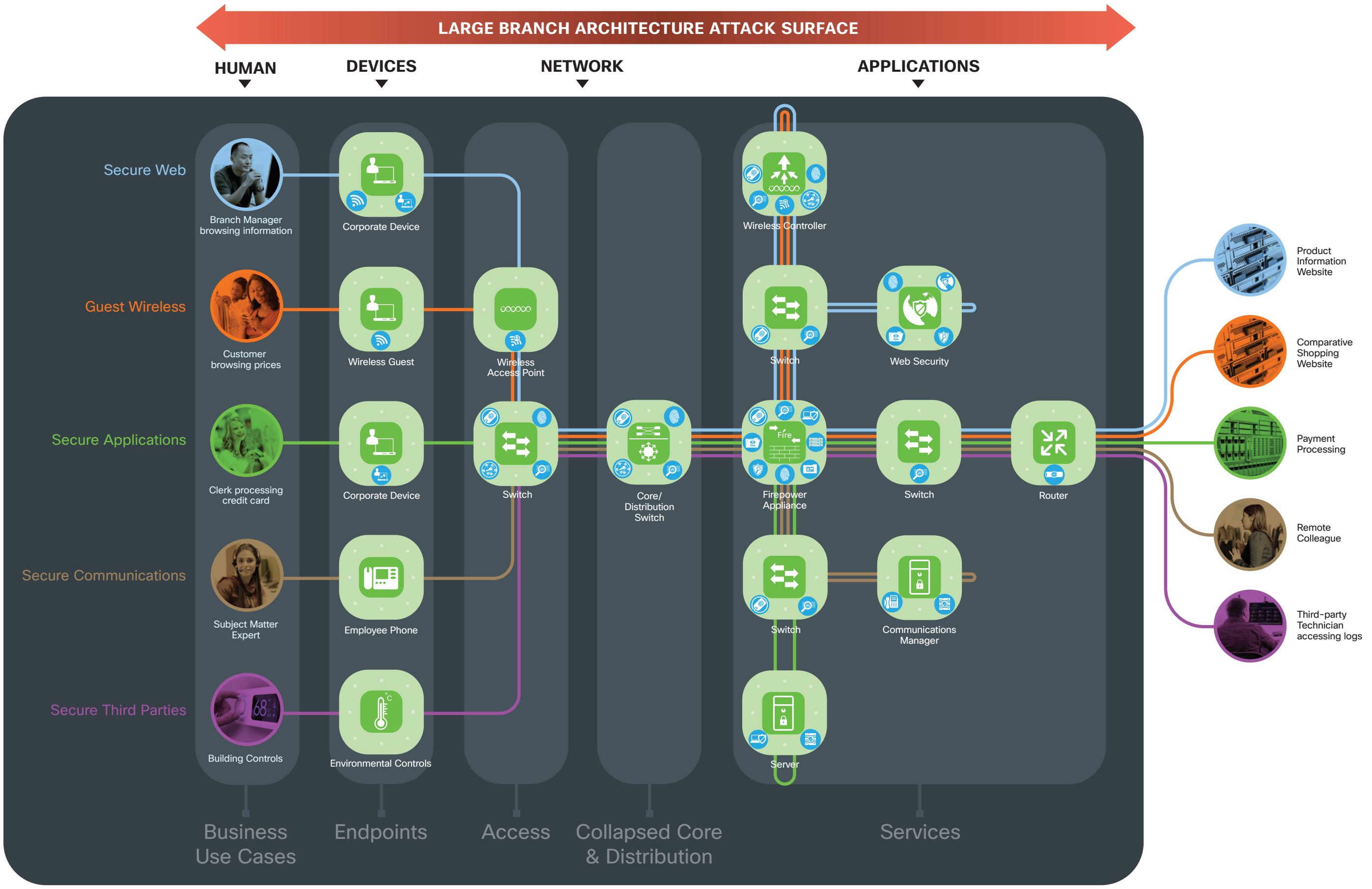
1. Human

The humans in the physical store are usually employees and remote access users such as partners (increasingly, supply chain partners). They are the greatest risk to any organization–whether through human error, sloppy security, or even malicious intent. No amount of technology can prevent successful attacks if humans in your company, both internal and partner users, are not trained to keep security in mind.

Security technology should therefore be augmented with regular security awareness training and acceptable use policies for internal, partner, and customer users–in other words, security is also a change management responsibility.

2. Devices

Mobile devices such as tablets and phones are another part of the security architecture. This means that, if you are not using the network as a sensor, you are not secure. Such visibility allows for effective containment through intelligent architectural design. It is equally important to ensure that client devices are secured and malicious devices are quarantined.



The Cisco SAFE methodology enables retailers to address the specific threats to their network. Security capabilities (blue icons) are mapped to business use cases and arranged in a logical architecture (green icons).

3. Access

The access layer is where users and devices connect to the company network. As you can imagine, this is a major target for hackers and should therefore be the first line of defense within the Secure Branch architecture. The network as a sensor uses flow analytics to capture anomalies and provide visibility to attacks. Its purpose is to identify the users, to assess whether devices seeking access to the network comply to policy, and to respond appropriately. It therefore helps you to quickly respond to violations of posture or identity, or to anomalous behavior.

4. Distribution/Core

In-store networks have commonly been built with the singular purpose of connecting point-of-sale (POS) systems to the corporate network. These solutions are typically deployed inside the security perimeter of the organization. Recent security breaches in retail organizations involving POS systems, however, suggest that this network architecture is no longer viable for building or operating in-store networks.[13]

Recommended for the branch is a classic network architecture, but usually collapsed into a single functionality because the branch is smaller. With the access layer segregated from the services layer, the services layer provides distribution of services that discretely separates business traffic into flows, helping assure the security of cardholder and other data.

5. Services

Services connect the Secure Store to the outside data center, cloud, and Internet via service providers. It connects the access and distribution layers inside the branch to the security and inspection capabilities as well.

For more information on SAFE, see www.cisco.com/go/SAFE.

A Word About Applications

The Cisco security study found that 27 percent of connected third-party cloud apps introduced by employees into enterprise environments in 2016 posed a high security risk. Open authentication connections touch the corporate infrastructure and can communicate freely with corporate cloud and software-as-a-service (SaaS) platforms after users grant access—for good or evil.[14]

However, the Ponemon Institute found that companies using application security controls can reduce the cost of cybercrime. Companies that deployed eight to nine application controls saved almost US$2 million on total cybercrime cost. However, if only one to three controls are used, the cost increases by an average of US$2 million. Building security into application and data protection, in addition to a layered approach with multiple tools, can also reduce risk. Dynamic testing, static testing, and run-time application self-protection were also shown to reduce costs and support innovation.

Overall, a strong security profile enables companies to innovate while still controlling the cost of cybercrime. Improved deployment of security, backup, recovery, and formal governance capabilities (such as advanced access and encryption) can reduce the total average cost of cybercrimes by nearly US$3 million.[15]

And, in comparison to the average time of up to 200 days to detect an advanced threat, a fully realized Cisco security solution can reduce time to detection to just nine hours.

Use Case: Retail Security

SCHEELS is a sporting goods chain with 26 locations in 11 states, including the largest all-sports store in the world. For years, the company relied on a vendor-managed security solution that had become costly and difficult to manage. The company realized it needed to ensure that its infrastructure could scale and keep pace with the dynamic threat landscape and its growing business.

Cisco provided a roadmap for SCHEELS, recommending a security appliance with Cisco FirePOWER™ Services and the Cisco FireSIGHT® Management Center. This solution provided the centralized visibility and intelligence SCHEELS needed to manage security with better results and lower cost. Today, the company:

- Has cut response time from hours to minutes
- Can detect and stop threats that evade the initial anti-virus solutions and training preventions
- Can deploy devices at new stores in a couple of hours versus more than a month

Read the full use case here.

Conclusion

Today's companies are threatened by increasingly sophisticated attacks. Retailers are commonly targeted because they are susceptible to physical access and have a large mix of services across increasingly complicated devices. With the emergence of such capabilities as in-store mobile apps, omnichannel and unified commerce, and alternate and mobile payment solutions, security and risk management are more critical than ever.

Cisco takes an approach to cybersecurity that deploys multiple networked solutions to increase visibility and preparedness before, during, and after an attack. This strategy enables a stance of constant readiness, response, and resiliency, and is designed to address threats throughout every business operation, process, and interaction. SAFE is Cisco's security reference architecture that simplifies the security challenges of today and prepares for the threats of tomorrow.

For More Information

To learn more, please contact your Cisco representative and visit our website at cisco.com/go/retail.

Follow us at @CiscoRetail.

[1] "Retailers Now Leading Cyberattack Target, Eclipsing Financial Services," *RetailDive* (April 20, 2016).
[2] "Advanced Threats in Retail – A Study of North America & EMEA," Ponemon Institute (2015).
[3] "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," Ponemon Institute (2016).
[4] "2017 Annual Cybersecurity Report," Cisco.
[5] "Cybersecurity as a Growth Advantage," Cisco (2016).
[6] Ibid.
[7] "2017 Annual Cybersecurity Report," Cisco.
[8] "Advanced Threats in Retail," Ponemon Institute.
[9] Bloomberg *BusinessWeek* (2014).
[10] "2017 Annual Cybersecurity Report," Cisco.
[11] Ibid.
[12] "Ransomware Defense Validated Design Guide: SAFE Design Guide," Cisco (2017).
[13] "Retail Security: Protect Customer Data While Saving Money and Time," Cisco (2016).
[14] "2017 Annual Cybersecurity Report," Cisco.
[15] "Cost of Cyber Crime Study & the Risk of Business Innovation," Ponemon Institute (2016).

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.