The Future of Retail Security
In the Eyes of Security Professionals

White Paper

Retail companies face a landscape filled with growing and increasingly complex threats. And the financial impact of these breaches is soaring. Just check the headlines. President Obama's call for a 30-day mandatory disclosure of retail data breaches in his 2015 State of the Union address illustrates the gravity of such security failures, felt even at the highest levels of government.[1]

Paradigm shifts involving mobile payments make security more complex, and in an increasingly connected world, security vulnerabilities involving vendors, partners, and others along your supply chain can impact your organization in unexpected ways. Perhaps even more compelling than the increased external scrutiny, security officers continue to tell Cisco® that internal risks present some of the most challenging security threats. For example, employees continue to click on phishing scams, opening organizations to additional risk. Security breaches are not a matter of "if" but "when." And when an incident takes place, merely fixing the problem isn't enough. You have to move quickly, and remediate effectively, to minimize impact. This document outlines technological best practices for retail security that can help your organization make informed decisions when designing a comprehensive security solution.

There are obvious financial incentives for attacking retailers. They typically don't spend as much on security as financial institutions or government organizations, so they've become easy targets in recent years[2]. According to Gartner, retailers spend about four percent of their IT budgets on cybersecurity, while financial services and health organizations spend 5.5 percent and 5.6 percent respectively.[2] This contrast

1. Remarks by the President in *State of the Union Address*, January 20, 2015
2. *Retail Spends Less on Cybersecurity than Banking, Healthcare,* Wall Street Journal, September 2, 2014

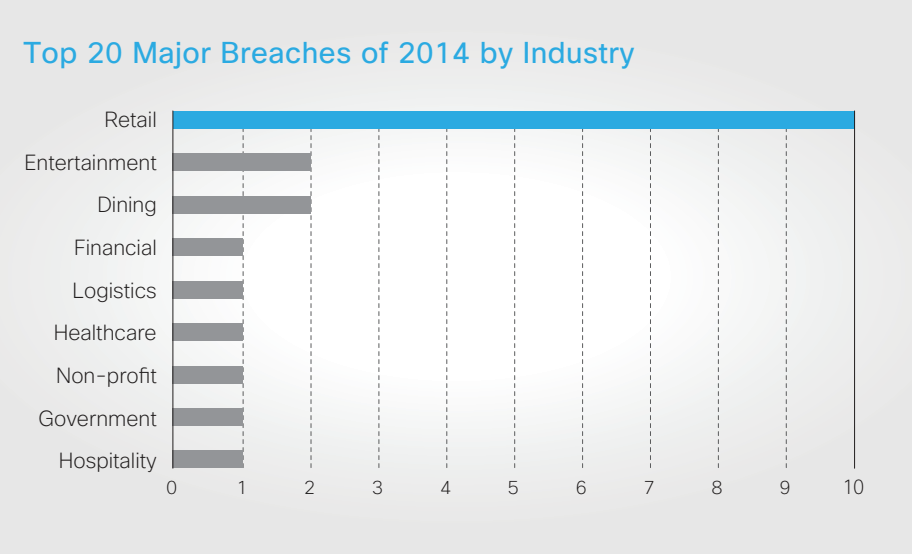
Financial organizations spent as much as $2,500 per employee on cybersecurity in 2014 while retail organizations only spent about $400 per employee.[3]

becomes even starker when you consider security spending on a per-employee basis. Financial organizations spent as much as $2,500 per employee on cybersecurity in 2014 while retail organizations only spent about $400 per employee.[3]

The dramatic news stories of the past year involving point-of-sale (POS) attacks are a symptom of the problem facing retailers. Criminals now believe that stealing from POS systems is more effective than stealing directly from e-commerce merchants because banks have become more skilled at detecting and stopping the latter. Without a comprehensive security framework, spotting, stopping, and remediating bad actors or malware is an impossible challenge.

In spite of the growing concerns, Cisco has an answer. Cisco designs its solutions to work in conjunction with partner solutions so that, together, they transform the network infrastructure into a security sensor. Doing this provides customers with greater network visibility and more effective detection, containment, and remediation. There is a long list of best practices that work independently (in silos), and they continue to leave organizations vulnerable. Mitigating sophisticated threats requires visibility, intelligence, and capability. This can only be accomplished when organizations utilize big data for predictive analytics and to detect anomalous patterns. Simply deploying best-of-breed solutions no longer works. Retail organizations must empower their networks to share security information with all security products and solutions in order for detection, containment, and mitigation to be successful.

Figure 1 Top 20 Major Breaches of 2014 by Industry[4]



3. *US cybercrime: Rising risks, reduced readiness,* Key findings from the 2014 US State of Cybercrime Survey, June 2014
4. AppRiver Global Security Report: *End-of-year Report* 2014

The Future of Retail Security In the Eyes of Security Professionals

Big data is the key to security today, and its importance will grow larger in the future.

Insight 1: Analyze data to identify actionable insights

Big data is the key to security today, and its importance will grow larger in the future. Security Information Event Management (SIEM) has been the traditional solution used in data centers. However, these database systems, and the connectors that draw data in from other systems, are only as good as the often undertrained people who operate them. In addition, these databases are being overwhelmed by large amounts of incoming data. Traditional databases simply aren't designed to handle such large amounts of unstructured data. These mountains of data, without intelligent analytics and knowledgeable security professionals, are fundamentally useless.

Using predictive analytics allows security professionals to analyze data quickly, identify actionable insights, and keep attackers in check. Predictive analytics are absolutely necessary for combatting adversaries because cyber criminals are constantly probing to discover which security solutions are being deployed and then shifting their focus to less visible, less content-detectable behavior patterns to conceal the threats they present. Big data with analytics convert SIEM and the large volumes of unstructured data into a structure that enables informed, strategic decision-making.

Insight 2: Protect any and all data around processing of cards

- **Integrity of Key Data:** Prevent theft, corruption, or modifications of key data.
- **Privilege Escalation Monitoring:** Monitor this important area, since 85 percent of breaches involve privilege escalation.
- **Penetration Testing:** Have internal and external penetration tests done. Monitor PCI activity and watch the Pastebin site for your customers' credit cards.
- **Outgoing Data Monitoring:** Conduct a quarterly analysis of your large data ex-flows to see whom you are talking to besides your vendors and suppliers. Understand whom you really are doing business with.
- **DLP Scanning:** Know where your key IP is sitting in your infrastructure. Regular data loss prevention (DLP) scanning for PCI or SA database SAD information is important (in rest or in motion).
- **Database protection:** Don't skimp on this key area. Oracle, IBM, and others have solutions.

Insight 3: Use your network infrastructure as a security sensor

Let's look at a new paradigm shift—Cisco's Managed Threat Defense (MTD). MTD supplements companies' existing infrastructures using traditional managed security services solutions. By using Hadoop, Hortonworks (to inject your unstructured data), and a number of Cisco products like Advanced Malware Platform (uses Analytics) and ThreatGRID (malware analysis and threat intelligence), Cisco can provide in-depth insights and actionable intelligence about cyber attacks and activity that go undetected by managed security solutions (MSS).

By approaching the problem in this manner, Cisco uses the customers' own networks to spot, stop, and mitigate attackers. When implemented correctly, customers can determine if malware gained access, where it entered, how it advanced, and to which parts of the network it was able to spread. This approach also enables customers to trace the malware's path back to its point of origin and remove it from the source. Additional components will even allow customers to establish their own forensics capabilities.

Hackers are targeting retailers with progressively more sophisticated DDoS attacks, resulting in significant downtime, lost revenue, and increased mitigation costs.

Insight 4: Identify internal indicators of compromise

Traditional security measures are very good at identifying a company's risky inbound traffic. But they're not as effective at identifying the risky outbound traffic. For a retailer, leaks initiated from within the enterprise can be extremely damaging. Only by analyzing outbound traffic can a company discover whom it is talking to besides suppliers, vendors, partners, employees, and customers. Such analysis will help neutralize unknown breaches and keep uninvited guests at bay.

Insight 5: DDoS attacks are still important to the retail industry

According to a 2014 poll of nearly 450 North American organizations, 91 percent of companies feel Distributed Denial of Service (DDoS) attacks are as serious as, or more serious than, in previous years.[5] Hackers are targeting retailers with progressively more sophisticated DDoS attacks, resulting in significant downtime, lost revenue, and increased mitigation costs. DDoS attacks can also be used as a diversionary tactic to draw attention away from an actual malware attack or data theft.

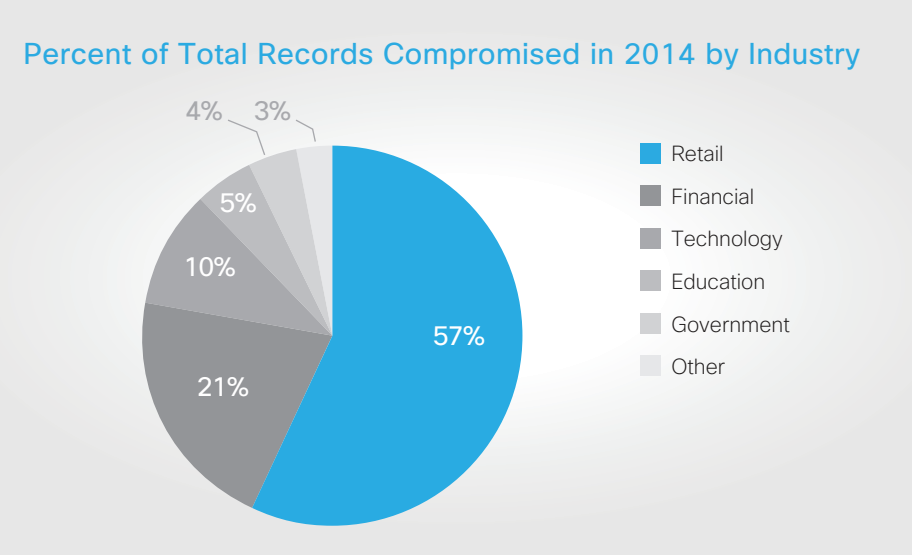
In 2014, Cisco researchers looked at 16 large multinational companies and found that more than 90 percent of selected customer networks have been identified as issuing Domain Name System (DNS) requests for host names associated with the distribution of malware.[6] Seventy percent of the customer networks had been used in issuing DNS queries for DDNS. In short, these customers were unwittingly helping with DDoS attacks.

5. *2014 The Danger Deepens: Neustar Annual DDoS Attacks and Impact Report*
6. *Cisco 2014 Midyear Security Report*

Insight 6: Seven steps to reduce your cybersecurity attack surface

1. Assume your employees will click on anything. Put in a strong secure email gateway so end users don't have the opportunity to click email spam. Make sure this email gateway passes on its findings to your security infrastructure.
2. Know what your key intellectual property is, where it's located, and design your security around it through authentication, policies, segmentation, and zoning.
3. Use authentication, endpoint, network, and gateway controls that share findings and provide an orchestrated reduction in attack surface.
4. Implement a solid supply chain and vendor management system.
5. Promote education training awareness that makes your employees smarter.
6. Using ACLs, virtualization or TrustSec reduces the number of locations where PCI data is touched so that the rest of your headquarters, data center, and store infrastructure don't have to be audited.
7. Install a strong web security gateway to stop users from clicking on poison well sites. Again, make sure the gateway passes along it findings to your security infrastructure.

Figure 2 Percent of Total Records Compromised in 2014 by Industry[7]



7. Breach Level Index

According to studies by Cisco, 75 percent of all attacks, despite taking only minutes to initiate data exfiltration, take much longer to detect.[8]

Insight 7: Develop an incident response plan

"Even the best plan goes out the window as soon as the first shot is fired." The author of this quote certainly wasn't talking about security incident response plans. A plan that is simple enough to provide guidance to first responders, and is vertically integrated into a retail organization's overall security policy charter, as well its disaster recovery document, will withstand even the most advanced threats. According to studies by Cisco, 75 percent of all attacks, despite taking only minutes to initiate data exfiltration, take much longer to detect.[8] More than 50 percent of them manage go undetected for months, or even years. After being discovered, it takes several weeks before they are fully contained and remediated.[8]

Many attacks result from a company not knowing its own assets (databases, homegrown and off-the-shelf applications, servers, and end points) and how these assets communicate with its suppliers, customers, and financial systems. Developing an incident response plan around asset inventories, and understanding staff, partner, and supplier capabilities, goes a long way toward creating an actionable and current plan.

Inclusive incident management planning helps to create meaningful partnerships with IT, legal, HR, store operations, and distribution. An incident response plan is not a document shown once each year to auditors. It is a document that needs to be refined quarterly, or upon discovery of new threats. It is a document an organization runs through during various tabletop scenarios and tests its own response to real threat scenarios. Incident response plans present a process for dealing with successful attacks and learning from mistakes.

Find out more about security within the retail industry and Cisco Security Services at www.cisco.com/go/securityservices.

8. *Cisco 2015 Annual Security Report*

DEC15CS4717 04/15