
SecurityScorecard
2018 Retail Cybersecurity Report
securityscorecard.com
[800] 682 1707

SecurityScorecard

Introduction

Despite the prediction in the early 2000s that online retail sales would die out rapidly, they continue to increase as consumers embrace ease of purchasing using the internet and mobile phone applications. In fact, 2017 holiday retail sales increased at a higher percentage than originally predicted. Although the National Retail Foundation predicted a 4% increase over the 2016 numbers[1], their finalized January 2018 statistics showed that online retail sales reached $691.9 billion during the November and December 2017 period, a 5.5% increase from the same period in 2016[2]. With this increased convenience comes an increased risk of credit card data being stolen. During the 2017 holiday season, experts argued that the greatest threats to cardholder data came from worms, buffer overflow, POS malware, brute force tools, account checkers, web injects, and mobile malware.[3]

SecurityScorecard analyzed 1444 domains in the retail industry 2017-10-01 to 2018-03-01 analyzing domains with an IP footprint of 100 or more.

- We compared the average SSC grade of the retail industry to all other industries and by factor.
- Best and worst 100 retail domains.
- The percentage of retail domains that had malware emanating.
- The percentage of retail domains had an issue associated to it.
- Domains that were breached, and a time analys to show how their grades compared to the industry average.
- Compliance analysis. How many domains were non-compliant by question and sub-question. As well as the total number of non-compliant question and sub-questions per domain.

The results display that although hackers have become increasingly clever with stealing credit card data, the retail industry is no better prepared to deal with the threat.

[1]Retail Cybersecurity Report 2017. (n.d.). Retrieved from https://www.boozallen.com/s/insight/publication/retail-cybersecurity-report-2017.html

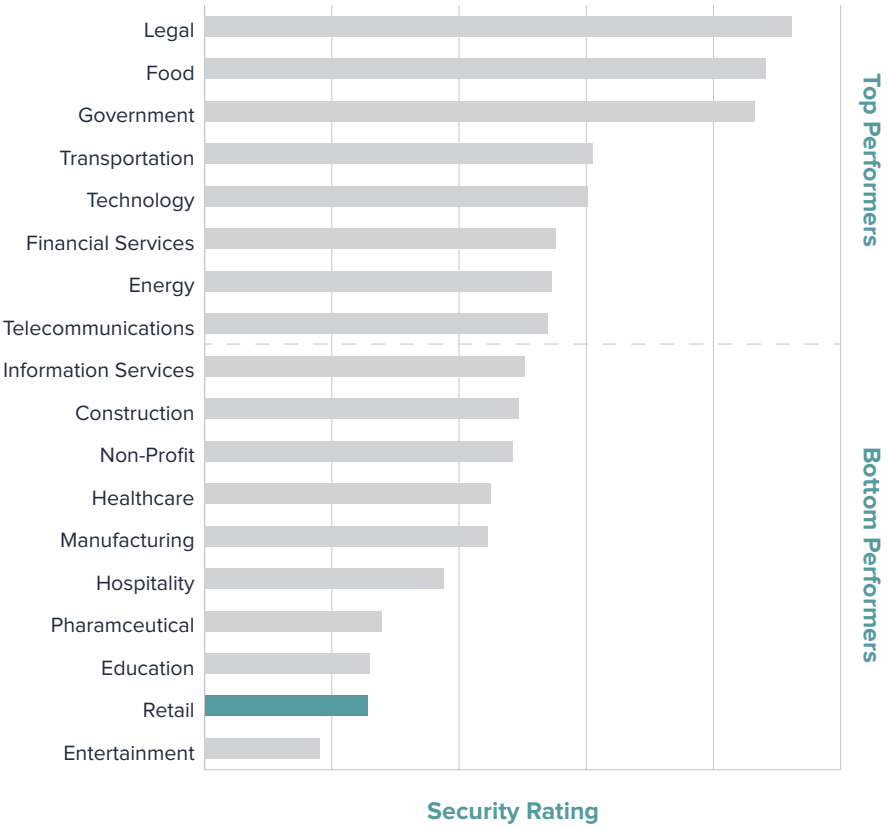
[2]Holiday Retail Sales Increased 5.5 Percent in 2017, Exceeding NRF Forecast and Showing Strongest Gain Since Great Recession. (January 12, 2018). Retrieved from https://nrf.com/media/press-releases/holiday-retail-sales-increased-55-percent-2017-exceeding-nrf-forecast-and

[3]Retail Cybersecurity Report 2017. (n.d.). Retrieved from https://www.boozallen.com/s/insight/publication/retail-cybersecurity-report-2017.html

SecurityScorecard

Retail Industry Neglects Application Security

The retail industry is the second lowest performer in terms of application security, indicating a decrease from 2017's Retail Report where they were the fourth lowest performer.



The increased use of new technologies that have not yet been subject to standardization along with the integration of pre-existing technology leads to application security issues in the retail industry. In fact, the PCI SSC only recently released a core standard for mobile point-of-sales (mPOS) in April 2018.[4]

Retailer use of mPOS increased exponentially over the last few years. According to STAR PoS, consumer mobile wallet use increased significantly in 2017. A Capital One report noted that 63% of respondents had been using mobile wallets for less than a year. The same article noted that in February 2017 almost half of the retailers interviewed by Boston Retail Partners, 49%, were using mPOS.[5] Additionally, to better integrate online sales, many retailers are integrating their in-store mPOS with their online ecommerce platform.

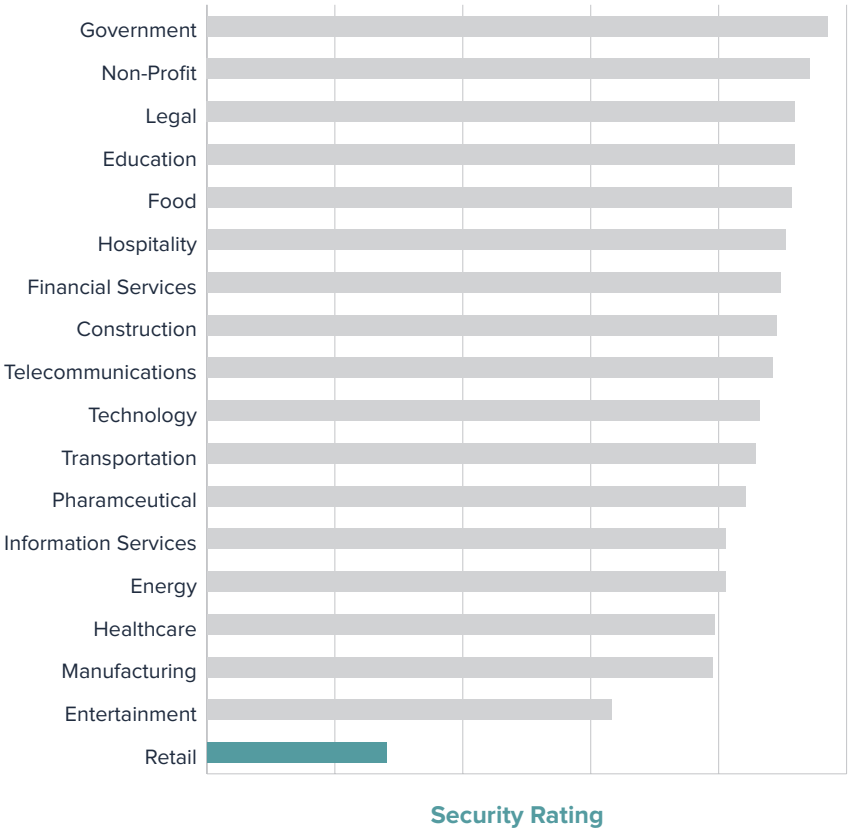
[4] What is included in the mPOS security standard from PCI SSC? (April 30, 2018). Retrieved from https://searchsecurity.techtarget.com/answer/What-is-included-in-the-mPOS-security-standard-from-PCI-SSC

[3] Critical Payment Trends to Watch This Year. (February 15, 2017). Retrieved from http://www.starmicronics.com/blog/3-critical-payment-trends-to-watch-this-year/

SecurityScorecard

Social Engineering Rampant in Retail Industry

When it comes to social engineering vulnerabilities, the retail industry ranks dead last. More importantly, the SecurityScorecard 2017 Retail Report noted that the industry was seventh from last. Social engineering that leads to data breaches in the retail industry shows a disturbing trend.



Hackers target retailers through social engineering in three ways: baiting, phishing, and vishing[6]. In the retail industry, phishing and vishing may be the most important. Phishing can often look like an official email from management. Many employees believe that their IT department will not lie to them. If they receive an email asking to reset their password, they intend to do what's right to protect their employer. Unfortunately, a malicious actor engaging in social engineering may have hacked the IT department's email address. By resetting their password using the link in the email, the employee accidentally gives out their information allowing access to the company's systems.

Similarly, vishing is when a social engineer calls employees. The social engineer sounds like a reasonable customer. Since good retailers assume the customer is always right, they try to work with the social engineer

[6]Three Types of Social Engineering That Keep Coming after Retailers. (December 1, 2017). Retreived from https://www.controltekusa.com/three-types-of-social-engineering-that-keep-coming-after-retailers/

for a resolution. In the process, they may give out cardholder data or employee access information accidentally.

Since the retail industry employs younger, less experienced people at a higher rate than other industries, these employees may be less aware of these attack vectors. Additionally, small retailers were more likely to be subjects of cyber attacks. Small business accounted for 43% of attacks with 62% of those arising out of phishing and social engineering.

This in combination with the fact that hackers are employing increasingly clever techniques to get sensitive information--we previously wrote about hackers leveraging MiTB attacks to target cryptocurrency sites. That method of attack is also used to target online, resulting in a dangerous combination.

What is PCI DSS?

Concerns over cardholder data drove American Express, Discover Financial Services, JCB International, MasterCard, and Visa, Inc. to create standards that would protect themselves and their customers from data breaches–the Payment Card Industry Data Security Standard (PCI DSS). The twelve requirements in this standard are:

1. Install and maintain a firewall
2. Change vendor-supplied system passwords and other security parameters
3. Protect cardholder data
4. Encryption cardholder data transmitted across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholdholder data on a need-to-know basis
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to networks and cardholder data
11. Regularly test security systems and processes
12. Maintain an Information Security policy

Aside from being a helpful tool to guide organizations that transmit, process, and/or store cardholder data, noncompliance with PCI DSS comes with severe penalties from the individual payment brands including that payment brands and banks may discretionarily fine merchants anywhere from $5,000 to $100,000 per month These fines can bankrupt a a small businesses and cripple larger merchants.

SecurityScorecard

Point-In-Time PCI Compliance Creates Opportunities for Hackers

Isn't there guidance for retailers that could help prevent these weaknesses in cybersecurity posture? The short answer is yes, but they aren't being adequately followed and certainly aren't being followed continuously. [Read more in What is PCI DSS?]

Retailers are failing dismally at adhering to this standard across the board:

- **90.72% of the domains** analyzed had issues indicating the organization may have been **non-compliant with PCI DSS standards in four or more requirements.**
- Retail organizations struggled most with Requirement 6 (Develop and maintain secure systems and applications)–with **97.5% of the domains analyzed presenting at least one issue indicating potential non-compliance.**
- **90.92% of domains analyzed had issues indicating the organization may have been non-compliant with Requirement 6.2.**

Requirement 6.2 as an Example

The PCI DSS Requirement 6 focuses on requiring organizations to develop and maintain secure systems and applications. A primary problem for retailers in patching regularly lies with security updates being released on a regular basis.

As a whole, Requirement 6 focuses on maintaining and securing systems and applications. Protecting information from outsiders forms the basis of any information security program. PCI DSS requires that merchants install and maintain firewall configurations that control access to the company's networks. When seeking to create a compliant configuration, merchants need to review both the firewalls and routers that connect to the CDE.

The first step to compliance lies in identifying where customer data resides and where it travels. To do this, organizations need to review not just their systems and servers but also their wireless networks. Once identified, the systems, servers, and networks need to be documented and diagrammed to show how the information flows.

As part of the process, organizations need to build firewall and router rules that restrict inbound and outbound traffic. These restrictions need to specify all "untrusted" networks and hosts, especially wireless ones. As part of this restriction, no public access can occur between the internet and system components in the CDE. Adding firewall software to individual devices - both corporate and personal - that connect to the internet outside of the company network is one suggested solution. This solution specifically notes the importance of mobile devices like laptops that can access networks from remote locations.

Requirement 6.2 states:

- "Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release."

Enacting controls and protections to the CDE environment acts as a first step. However, maintenance proves more difficult. To ensure ongoing protection of the CDE, PCI SSC explains that Requirement 6.2 intends to protect retailers from the constant stream of "Zero Day" attacks, ones that exploit previously unknown vulnerabilities. Once software, systems, and network vendors learn of the vulnerability, they rapidly push out updates. Updating software quickly enables better protection against intrusions.

- 6.2.a Examine policies and procedures related to security patch installation to verify processes are defined for:
  - Installation of applicable critical vendor-supplied security patches within one month of release.
  - Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).

Based on the analysis, reasons for non-compliance could be due to a CVE vulnerability that was open longer than 30 days after the CVE was published, the presence of vulnerabilities in the company's technology stack, or the presence of obsolete browsers and operating systems as well as for products whose manufacturers have declared them as end-of-service or end-of-life.

SecurityScorecard

SecurityScorecard enables better compliance with Requirement 6.2 by scanning a company's digital footprint externally and reviewing systems and software for recent updates. A low security rating for patching cadence means that a company may not be updating within the 30 Day PCI DSS time period.

- 6.2.b For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:
  - That applicable critical vendor-supplied security patches are installed within one month of release.
  - All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).

A reason many retailers lack compliance with Requirement 6.2 is that the increased number of vendors makes mapping updates more time-consuming. A retailer that uses different vendors for cloud storage, operating systems, data backup, mPOS, and POS may have a hard time following every update for each of these. In addition, some updates may be critical security updates while others focus on better usability.

Requirement 11.2 and Beyond

This approach to point-in-time compliance create vulnerabilities extends even beyond the literal text of PCI. Organizations looking to secure cardholder data should shoot to not approach PCI as a punch list but strive to fulfill the standard's goal to truly secure this data. For example, PCI DSS requirement 11.2 specifies that external vulnerability scans be conducted at least quarterly to help identify these security gaps. Many organizations demonstrate reasonable security of their own domain and of their supply chain at least quarterly. However, given that the concept of continuous monitoring is relatively recent, practicing reasonable security between scans is not as common. Failing to continuously monitor leaves organizations open to having cardholder data compromised.

As organizations consider all the regulatory changes even beyond PCI (GDPR, NIST 800-171, CA privacy law, SOX cybersecurity attestation requirements and so on), monitoring the third party ecosystem continuously is increasingly critical. Security ratings provide a critical component of near real-time visibility of cyber threats and vulnerabilities; early identification can yield to quicker resolution of potential risk, which may ultimately impact card-holder data for the better.

SecurityScorecard

Conclusion

In 2018, the Retail Industry's security posture fell lower than ever in both application security and social engineering. Increased technology use across the enterprise and a lack of security standards to help enable protection place retailers at a higher risk of data breaches. Moreover, while teenagers often comprise a large percentage of the retail industry's workforce, they often have less training and general awareness of of social engineering threats.

PCI DSS compliance enables security by prescribing security measures related to the storage and transmission of data within the cardholder data environment to help mitigate as many risks to information as possible. SecurityScorecard's scanning of the external environment enables retailers to streamline their PCI DSS compliance to mitigate fines and intrusions from malicious actors. Whittling down potential external intrusions using automation saves time which can then be used to focus on the human factor within the enterprise.

SecurityScorecard

About SecurityScorecard

SecurityScorecard helps enterprises gain operational command of their security posture and the security posture of their third-parties through continuous, non-intrusive monitoring. The company's approach to security focuses on identifying vulnerabilities from an outside perspective, the same way a hacker would. SecurityScorecard's proprietary SaaS platform offers an unmatched breadth and depth of critical data points including a broad range of risk categories such as Application Security, Malware, Patching Cadence, Network Security, Hacker Chatter, Social Engineering, and Leaked Information.

To receive an email with your company's current score, please visit instant.securityscorecard.com.

www.securityscorecard.com

1 (800) 682-1707

info@securityscorecard.com

@security_score

SecurityScorecard HQ

214 West 29th St

5th Floor

New York City, NY 10001