SecurityScorecard


# 2017 Retail & E-Commerce Report

**SecurityScorecard | Security Research Team |** August 24th, 2017

SecurityScorecard

## Overview

As Black Friday and Cyber Monday approach, retailers prepare for what has become an over $650 billion dollar holiday shopping season, according to the National Retail Federation. But for retailers who are not paying enough attention to their cybersecurity health, this weekend could mean the start of a slippery slope from cyberattacks to reduced sales and eventually to store closures.

With IoT innovations being used to streamline inventory and transactions in stores and with more and more shoppers opting to make online purchases  instead of braving the cold weather and long lines to get a deal, focusing on cybersecurity is increasingly important. The impact of poor security for consumers can range from fraudulent charges to identify left. For retailers, who engage in this trust-based industry, a failure in security can result in a business losing its customers – 19 percent of whom would prefer to stop shopping at a recently hacked retailer and 33 percent of whom would stay away from the retailer for at least three months, according to the 2016 KPMG Consumer Loss Barometer.

Using our proprietary data, SecurityScorecard analyzed 1924 companies in the retail industry from January to October of this year, looking at this industry as compared to other major U.S. industries and at the cybersecurity indicators of the best and worst cybersecurity performers.

SecurityScorecard

## Key Findings

- The retail industry ranks fifth compared to 17 other major U.S. industries.
- The retail industry struggles with application security, DNS Health, and social engineering when compared to other industries.
- With respect to cybersecurity health, 100 percent of top performing companies had an A as an overall score.
- The top five retailer in terms of cybersecurity performance were: a store that sells razors, a car dealership, a store that sells pens, a magic store, and a store that sells plumbing supplies.
- Thirty percent of the bottom cybersecurity performers in the retail industry were clothing stores.
- With respect to cyberhealth, 100 percent of bottom performers in the retail industry had a C grade or lower, indicating a need for substantial improvements to cybersecurity practices.
- On average, bottom cybersecurity performers in the retail industry scored a C or lower in five out of 10 risk factors.

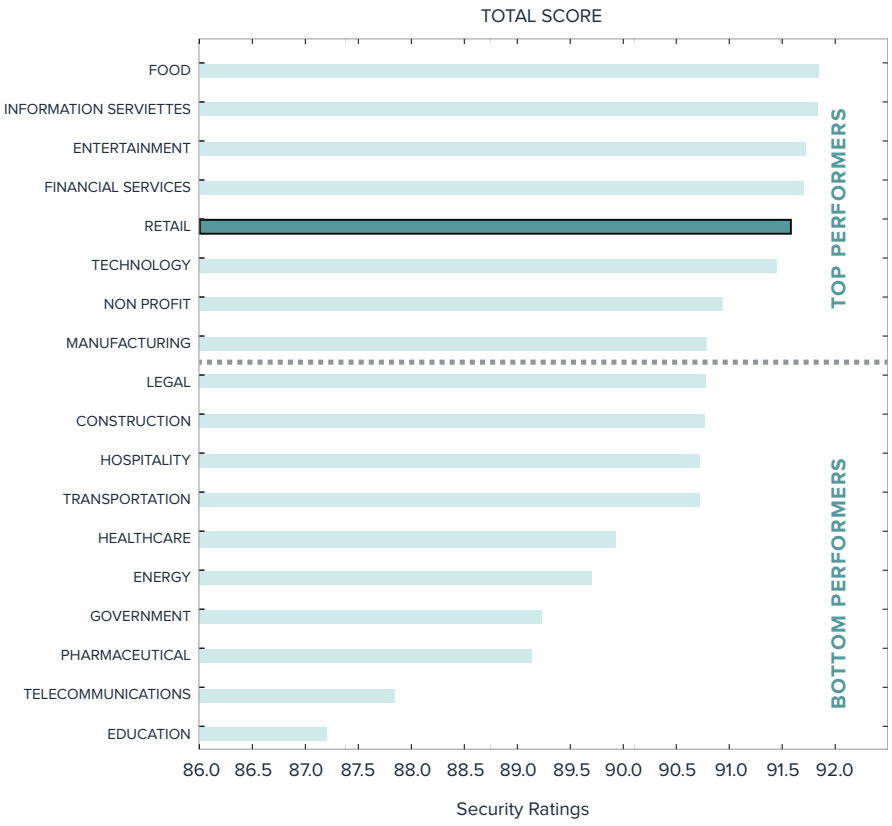
1. https://nrf.com/media/press-releases/nrf-forecasts-holiday-sales-increase-between-36-and-4-percent
2. https://www.forbes.com/sites/forbescommunicationscouncil/2017/11/07/black-friday-and-cyber-monday-trends-for-2017/#5db660a67397
3. https://www.retaildive.com/news/5-numbers-to-know-about-retail-cybersecurity/435682/

SecurityScorecard

# Industry Comparison

The retail industry ranks fifth compared to 17 other major US industries, but as a trust-based industry the retail industry has a compelling reason to move up within the ranks.

**FIGURE 1 :** Cybersecurity Performance: Retail & E-Commerce




According to PwC's annual Global State of Information Security Survey 2017, there were over 4000 security incidents suffered by the retail and consumer sector over the last year. Compounded with the fact that a cyberattack may increase a company's churn by 2.9 percent, having poor cybersecurity health can be a real threat to the financial viability of companies in this industry.

Specific areas of weakness that the retail industry include: Application Security, DNS Health, and Social Engineering.

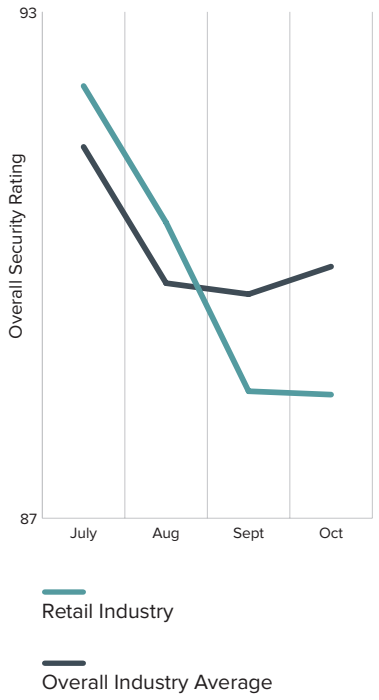
4. http://pwc.blogs.com/industry_perspectives/2017/05/cyber-security-the-retail-sector-under-attack.html

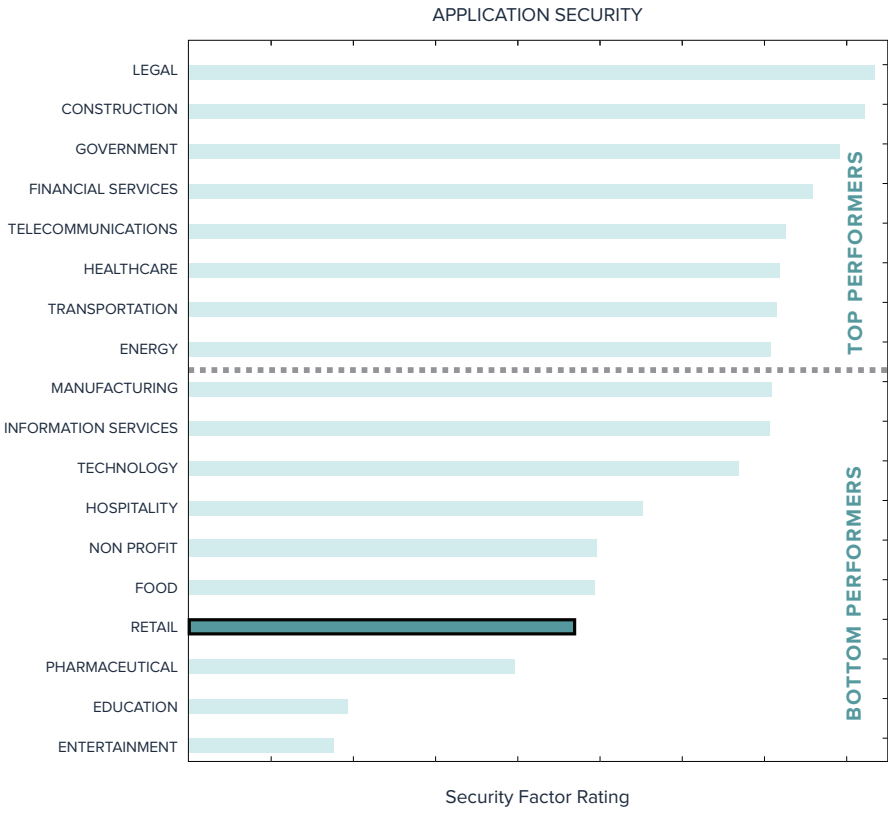
SecurityScorecard

# A Spotlight on Application Security

The retail and e-commerce industry ranks near the bottom in terms of cybersecurity performance in the area of application security, and since July, performance in this area is getting worse. This might explain why, this year, web application exploits were one of the most common cybersecurity attacks against e-commerce retailers, accounting for 13 percent of all attacks.

**FIGURE 2 :** Retail & E-Commerce Industry Cybersecurity: Application Security



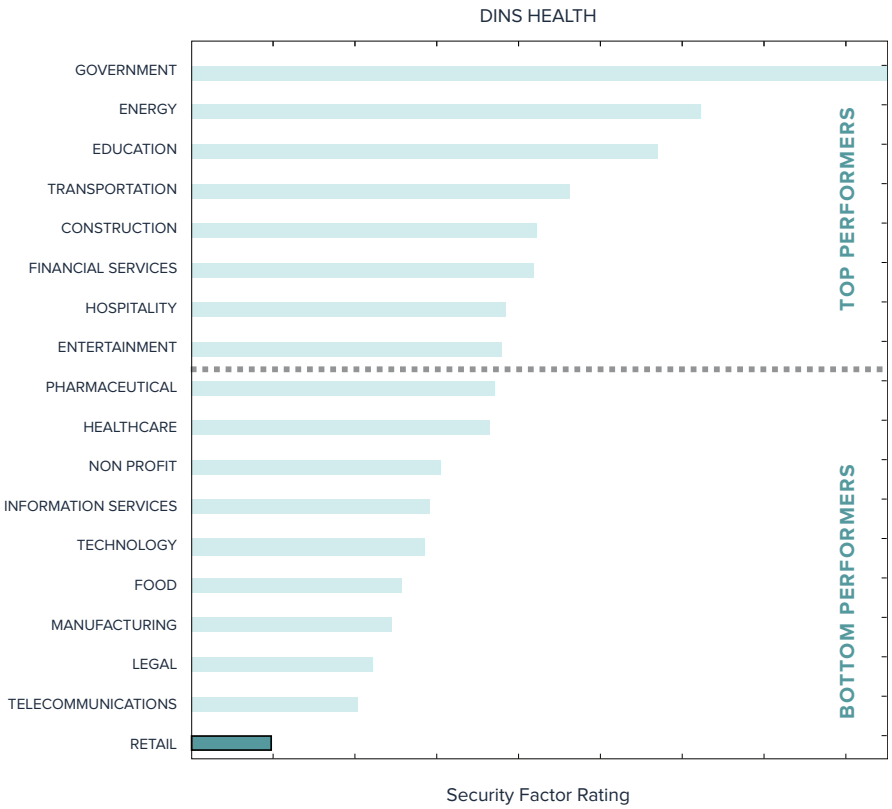

As to what is causing poor web application security, in some cases the root problem traces back to the potentially decentralized ownership of technology in brick-and-mortar shops. For these stores, it's a very real possibility that an electrician and not a dedicated IT Security resource is setting up the wifi networks and other technology. As a result, there can be rampant misconfigurations that go undetected until it's too late.

With the average cost of a data breach to an e-commerce retailer now at $172 dollars per record, hackers are targeting retailers, and they know that web applications are often a vulnerable entry point that can be exploited to gain access to sensitive cardholder information. And attacks on web applications have increased since July.

5. https://smallbiztrends.com/2017/02/cost-of-a-data-breach.html
6. https://smallbiztrends.com/2017/02/cost-of-a-data-breach.html

# A Spotlight on DNS Health and Social Engineering

**FIGURE 3 :** DNS Health of Retail vs. Other Industries



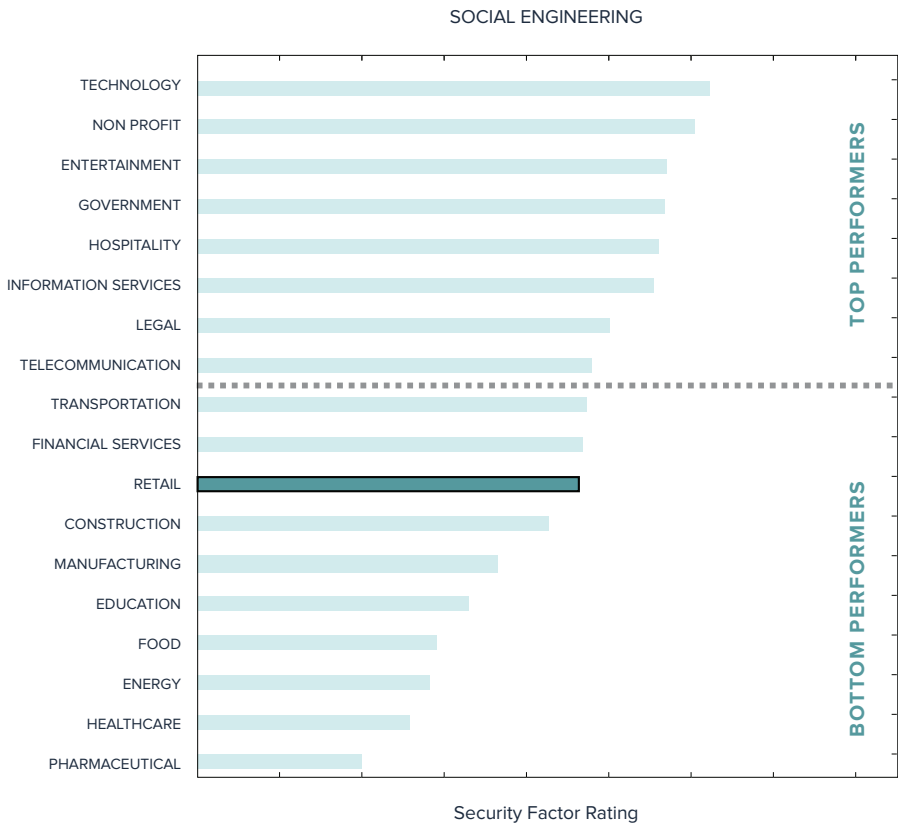

One poor cybersecurity practice that can result in low DNS health score is failing set up SPF policies, which indicate where mail can be sent from.

Not having that layer of protection can lead to an increased potential for phishing attacks – a type of attack where a hacker tricks consumers to visit a fraudulent site and attempts to steal login credentials or credit card information.

The retail industry currently ranks lower than 10 other industries in social engineering, and this number is only expected to get worse as the holiday shopping season ramps up.

7. https://smallbiztrends.com/2017/02/cost-of-a-data-breach.html

**FIGURE 4 :** Social Engineering of Retail vs. Other Industries




During the heavy shopping months of November and December, prior studies have shown that the prevalence of phishing and other social engineering schemes go up as much as 336 percent.

## Top Cybersecurity Performers in the Retail Industry

For retailers motivated to improve their cybersecurity and wondering what the view from the top looks like, the average score of the top 50 retailers, in terms of overall cybersecurity performance, is a mid-A. Furthermore, on average, top cybersecurity performers in the retail industry score an A in every single category, except DNS Health, where they score a high B.

8. https://www.recordedfuture.com/black-friday-threats/
9 https://www.zerofox.com/blog/cyber-monday-breeds-cyber-crime-infographic/

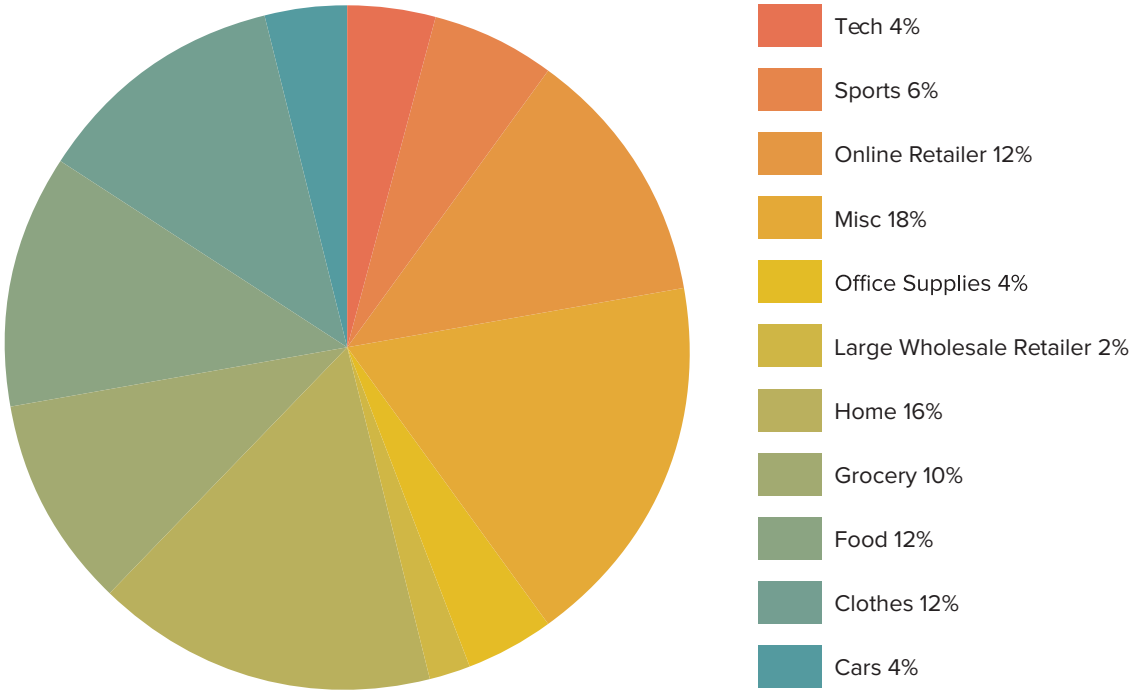
SecurityScorecard

## FIGURE 5: Top 50 Cybersecurity Performers in the Retail & E-Commerce

| Company | Total Score | Application Sec | Cubit Score | DNS Health | Endpoint Security | Hacker Chatter | IP Reputation | Network Security | Password Exposure | Patching Cadence | Social Engineering |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Grocery/Pharmacy - Razors | A | A | A | A | A | A | A | A | A | A | A |
| Cars | A | A | A | A | A | A | A | A | A | A | A |
| Office Supplies - Stationary | A | A | A | A | A | A | A | A | A | A | A |
| Misc-Magic Tricks Materials and DVD | A | A | A | B | A | A | A | A | A | A | A |
| Home - Plumbing Supplies | A | A | A | A | A | A | A | A | A | A | A |
| Food | A | A | A | B | A | A | A | A | A | A | A |
| Sports - Water Bottles | A | A | A | A | A | A | A | A | A | A | A |
| Online Retailer | A | A | A | B | A | A | A | A | A | A | B |
| Tech Related - Cable Service | A | A | A | B | A | A | A | A | A | A | A |
| Grocery | A | A | A | B | A | A | A | A | A | A | A |
| Cars | A | A | A | B | A | A | A | A | A | A | A |
| Misc - Gift Marketplace | A | A | A | B | A | A | A | A | A | A | A |
| Home - Outdoor Stuff | A | A | B | A | A | A | A | A | A | A | A |
| Online Retailer | A | A | A | B | A | A | A | A | A | A | A |
| Misc - Prescription Eyeglasses | A | A | B | A | A | A | A | A | A | A | A |
| Online Retailer | A | A | A | A | A | A | A | A | A | A | A |
| Online Retailer | A | A | A | A | A | A | A | A | A | A | A |
| Online Retailer | A | A | A | B | A | A | A | A | A | A | A |
| Office Supplies | A | A | A | B | A | A | A | A | A | A | A |
| Misc - Personal Branding Service | A | A | A | A | A | A | A | A | A | A | A |
| Misc - Safety Signs | A | A | A | B | A | A | A | A | A | A | A |
| Home Insurance | A | B | A | A | A | A | A | A | A | A | A |
| Grocery | A | B | A | A | A | A | A | A | A | A | A |
| Food- Water | A | A | A | B | A | A | A | A | A | A | A |
| Home - Power Equipment | A | B | A | A | A | A | A | A | A | A | A |
| Misc - Horse Classifieds | A | A | A | A | A | A | A | B | A | A | A |
| Sports Gear | A | A | A | A | A | A | A | A | A | A | A |
| Home Shopping Network | A | A | A | C | A | A | A | A | A | A | A |
| Clothes | A | A | A | B | A | A | A | A | A | A | A |
| Grocery - Pharmacy | A | A | A | B | A | A | A | A | A | B | A |
| Misc - Hotel Collection | A | B | A | A | A | A | A | A | A | A | A |
| Appliance Parts and Power Tools | A | A | A | B | A | A | A | A | A | A | A |
| Food | A | A | A | C | A | A | A | A | A | A | A |
| Misc - Baby Store | A | B | A | B | A | A | A | A | A | A | A |
| Clothes & Accessories Jewelry | A | A | A | A | A | A | A | B | A | A | A |
| Home Products, Parts & aAcessories | A | A | A | A | A | A | A | A | A | B | A |
| Food / Footwear | A | A | A | C | A | A | A | A | A | A | A |
| Home - Lighting | A | A | A | B | A | A | A | A | A | A | A |
| Food | A | A | A | B | A | A | A | A | A | B | A |
| Food Related | A | B | A | B | A | A | A | A | A | A | A |
| Clothes | A | A | A | B | A | A | A | A | A | A | A |
| Grocery | A | B | A | A | A | A | A | A | A | A | A |
| Tech Related Gadgets/Tech | A | B | A | B | A | A | A | A | A | A | A |
| Online Retailer | A | B | A | A | A | A | A | A | A | A | A |
| Clothes | A | A | A | B | A | A | A | A | A | A | A |
| Sports - Ski/Winter Stuff | A | A | A | A | A | A | A | A | A | B | A |
| Large Retailer | A | A | A | C | A | A | A | A | A | A | A |
| Clothes | A | B | A | A | A | A | A | A | A | B | A |
| Misc - Flag Maker | A | A | A | A | A | A | A | A | A | B | B |
| Clothes | A | A | A | C | A | A | A | A | A | A | A |

Most of the top 50 performers in terms of cybersecurity health in the retail industry are retailers that sell home-related products, food, or clothes, or are e-commerce sites . In the case of e-commerce, the simple fact that the average cost of a cybersecurity attack is a whopping $4 million dollars may be encouraging these companies to implement and practice better security than others in the retail industry.

**FIGURE 6:** Distribution of Top Performers by Retail Type



# How Safe is it to Swipe

In  a world in which outsourcing is an ordinary part of any business, consumers have to worry not only about the cybersecurity posture of retailers but also of their vendors and other companies involved in the payment process – which gives reason for retailers to worry about those other parties too.

To get a look at other potential risks to consumers, SecurityScorecard also analyzed nine major credit card issuers from January to October of this year, evaluating the state of cybersecurity health at these organizations.

With cardholder data being a number one concern for those tied to any part of the retail or e-commerce process, one might expect that cybersecurity is a top-of-mind issue for credit card issuers. That expectation could not be more wrong.

SecurityScorecard's analysis revealed that not a single credit card issuer received an 'A' grade, indicating that every single card issuer could take steps to mitigate cybersecurity risk. For the four of these nine credit card issues that scored a C or below overall, this could mean significant cybersecurity investments or changes in cybersecurity practices, especially in the areas of DNS Health (where 6 out of 9 issuers scored a C or below), Network Security (where 6 out of 9 issuers scored a C or below), and Patching Cadence (where 4 out of 9 issuers scored a C or below).

**FIGURE 7:** A Look at the Cyberhealth of Nine Credit Card Issuers (Jan - Oct 2017)

| Company | Total Score | Application Sec | Cubit Score | DNS Health | Endpoint Security | Hacker Chatter | IP Reputation | Network Security | Password Exposure | Patching Cadence | Social Engineering |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Credit Provider #1 | B | A | A | B | A | A | A | D | B | A | F |
| Credit Provider #2 | D | C | B | C | C | C | D | F | B | F | D |
| Credit Provider #3 | B | A | A | B | C | B | C | A | B | A | C |
| Credit Provider #4 | B | A | A | C | A | C | B | F | A | D | A |
| Credit Provider #5 | C | C | A | C | A | C | A | D | A | F | A |
| Credit Provider #6 | B | A | A | B | B | C | A | A | A | A | C |
| Credit Provider #7 | C | B | A | F | C | A | A | D | A | B | B |
| Credit Provider #8 | B | A | A | C | A | A | C | A | A | B | A |
| Credit Provider #9 | C | A | B | F | D | A | B | C | A | C | A |
| Average | B | A | A | C | B | B | B | C | A | C | B |

10 Excluding the miscellaneous category.
11 https://smallbiztrends.com/2017/02/cost-of-a-data-breach.html

But consumer risk doesn't stop with credit card issuers, the retailer supply chain also includes the warehouses, distribution centers, data centers, payment processors, and more. Payment processors in particular are vendor with a high potential risk, especially considering the risks introduced by PoS terminals, which go over WiFi, can be modified, are running computers which could have malware, and so on. Consumer behavior reflects this awareness of supply chain risk too; 57 percent of consumers will only use payment providers they trust.

While it's true that adherence to the latest Payment Card Industry standards is one proofpoint that can help assuage those working to keep the supply chain accountable for cardholder security, it's only one part of a larger vetting process. Limitations on visibility include:

- The retail industry ranks 5th compared to 17 other major US industries.
- Attestations of Compliance alone don't provide a detailed level of information about the protections and vulnerabilities to cardholder data.
- While the PCI council may audit the full Records of Compliance, not every record is audited.
- Furthermore, audit evidence and adherence to compliance standards are generally point-in-time reflections that can change from month-to-month or even more often.
- There is a risk that companies may break PCI requirements and operate outside of the classification reflected within compliance documents.

A particularly ironic scenario is when a retailer, trying to protect consumers, uses a third-party fraud prevention solution that does not implement proper cybersecurity controls. By their nature, fraud prevention companies receive very sensitive and large amounts of consumer data. If those environments aren't secure, for example if transfer is happening across an unsecure FTP, piping that information to the third party can introduce risk.

12 http://pwc.blogs.com/industry_perspectives/2017/03/managing-cyber-risk-in-retail-a-winning-strategy.html

SecurityScorecard

# Bottom Cybersecurity Performers in the Retail Industry

As the holiday season approaches consumers are wondering what types of retailers they should they watch out for as they flock to stores and websites on Black Friday and Cyber Monday.

SecurityScorecard's analysis of the bottom 50 U.S. retail companies resulted in the following findings:

- **Thirty percent of the bottom cybersecurity performers in the retail industry were** clothing stores. There were more poor performing clothing stores than poor performing department stores, car dealerships, food stores, grocery/pharmacy stores, wholesale retailers, office supply stores, and stores selling sports good combined.
- While the top retailers received an overall mid-A grade across ten security factors collected and benchmarked by SecurityScorecard, **bottom retailers received an overall mid-C grade on average.**
- **Bottom cybersecurity performers in the retail industry struggle with half of the major cybersecurity risk factors.** Retailers score, on average, a C in application security, DNS Health, and IP Reputation and a D in Network Security and Patching Cadence.

**FIGURE 8:** Bottom 50 Cybersecurity Performers in the Retail & E-Commerce Industry

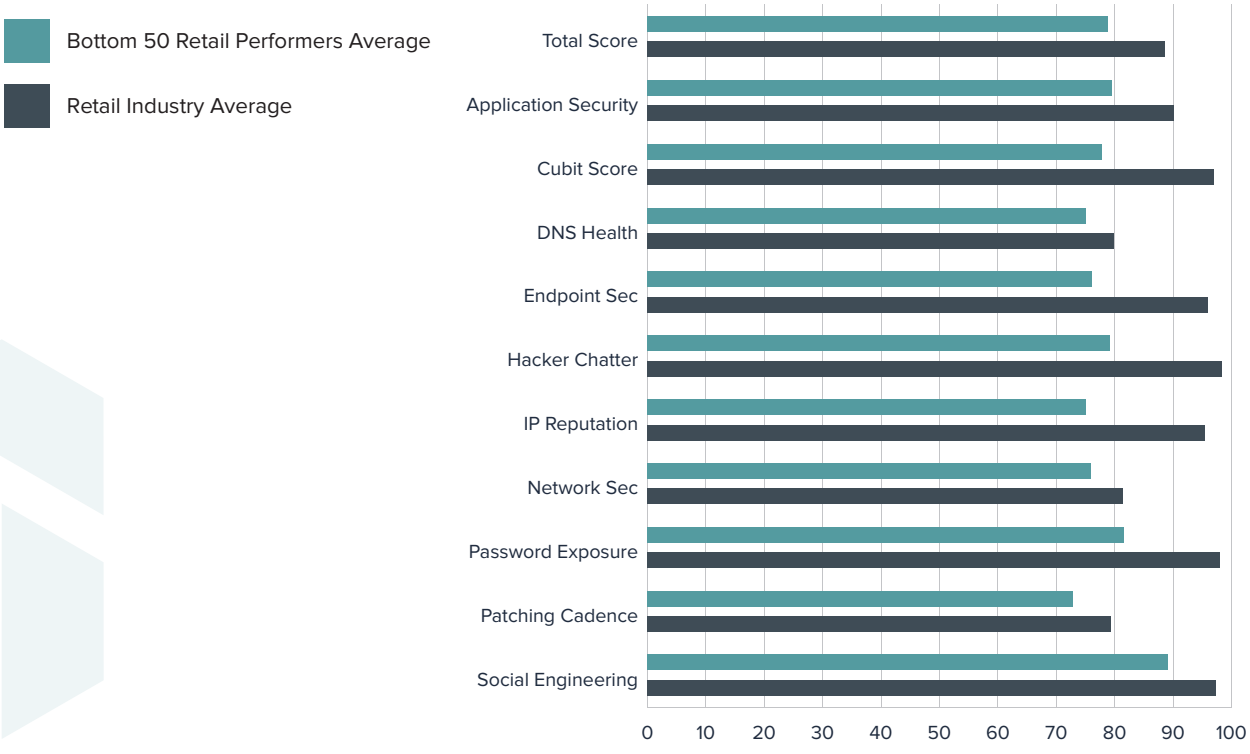


**FIGURE 9:** Types of Retailers With Poor Cybersecurity Performance

| Type of Store | Total Score | Application Sec | Cubit Score | DNS Health | Endpoint Security | Hacker Chatter | IP Reputation | Network Security | Password Exposure | Patching Cadence | Social Engineering |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Average - overall | C | C | A | C | B | A | C | D | A | D | A |
| Average - clothes | C | B | A | D | A | A | C | F | A | D | A |
| Average - dept | C | C | A | D | D | A | C | C | A | D | C |
| Average - food | C | C | A | D | B | A | C | D | A | D | A |
| Average - grocery | C | D | A | B | A | A | B | C | A | F | A |
| Average - home | C | B | A | C | B | A | C | D | A | D | A |
| Average - large whole saler | C | B | A | C | B | A | C | D | A | D | A |
| Average - misc | C | B | A | D | C | A | C | F | A | F | A |
| Average - online retailer | C | C | B | D | D | A | B | D | B | D | A |
| Average - sports | C | A | A | D | D | A | B | F | B | F | A |
| Average - tech | C | C | A | C | C | A | C | D | A | F | B |

- Of the bottom cybersecurity performers, **technology stores and department stores scored the lowest on average when compared to other types of stores.**

## Conclusion

Properly assessing vendor risk, implementing continuous monitoring, validating or supplementing compliance evidence, ensuring protection of the PoS system, and improving increased cybersecurity awareness are all examples of steps that retailers may consider when improving their cybersecurity posture. Ultimately, as cyberattacks continue to steal the headlines and consumers become more educated on the potential risks of poor cybersecurity performance, the retail industry, especially its bottom performers, will require significant investments in cybersecurity to keep its doors–physical or digital–open from this holiday season to the next.

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

NYC, NY 10001


SecurityScorecard
securityscorecard.com
sales@securityscorecard.com
214 West 29th St, 5th Floor
New York, NY 10001
1.800.682.1707
BUY