Zettaset

WHITE PAPER

Shoplifting on Steroids: The Most Costly Retail Data Breaches of All Time

Thieves once targeted the retail industry for its physical goods, but the rise of the computer era proved cyber attacks to be more lucrative. Neither brick-and-mortar retail locations nor their online counterparts are safe from data breaches. Traditional storefronts are being attacked by payment card skimmers, while e-commerce predominantly faces denial of service (DoS) attacks intended to compromise the availability of networks and systems. In fact, these DoS hacks represent over 80 percent of all online retail incidents according to the 2017 Data Breach Investigations Report.[1]

While denial of service, web application attacks, and payment card skimmers (and, to a lesser extent, malware, misuse, and human error) wreak havoc and incur immediate costs, the retail industry faces many more expenses as a result of data breaches. First, an organization must notify customers of the breach. This is usually the least costly expense, since the outreach efforts tend to cost just a few dollars per compromised record. Regulatory fines weigh more heavily, however, if the organization is found to be non-compliant with current payment card industry data security standards (PCI DSS). Depending upon the size of the breach and the level of non-compliance, this fine can reach $500,000.[2]

Data breaches often require protection measures like credit monitoring for all affected customers, and this can add up. Providing identity theft repair and credit monitoring to affected individuals costs between $10 - $30 per compromised card.[3] Legal fees are a substantial cost, as well, which includes hiring third-party investigators to conduct the necessary forensic analysis, assembling a strong legal team for defense, and offering settlements where necessary. Lastly, and arguably most importantly,the incalculable loss of revenue and consumer trust cost the organization a considerable amount of money.

How much are we really talking about? Here are the top five most expensive data breaches in retail to-date:

5. Staples

Let's begin with Staples. From April to September of 2014, a cybercriminal gang known as both Anunak and Carbanak hacked into the office supply retailer's computer systems.[4] That October, Staples announced that it had learned of the potential data breach after several banks reported a pattern of payment card fraud. This suggested the company's systems were compromised. Data security experts within Staples confirmed that cybercriminals had deployed malware to point-of-sale (POS) systems at store locations throughout the US. In total, the breach affected 1.16 million customer credit cards used at stores in 35 states. The retail giant hired outside data security experts for the data theft investigation, and cooperated with law enforcement and credit card companies. However, it wasn't until May of 2017, more than two and a half years after the breach, that Staples hired its first-ever chief information security officer.[5]

---

1 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf
2 https://www.cimcor.com/blog/the-real-price-tag-of-retail-store-data-breaches
3 http://blog.securitymetrics.com/2016/10/-how-much-does-a-data-breach-cost.html
4 https://www.forbes.com/sites/thomasbrewster/2015/02/16/staples-hackers-made-one-billion-dollars/#541104ab37d0
5 https://www.bizjournals.com/boston/news/2017/05/08/two-years-after-massive-breach-staples-hires-first.html

The fallout was substantial. In the immediate aftermath, Staples announced that it would offer free identity protection services (including identity theft insurance, and credit monitoring and reporting) to any customer who used a credit or debit card at the affected stores during the breach. The incident cost Staples over $18 million in incremental expenses, and the company has admitted that it expects to incur further losses.[6] As of late 2017, Staples still faces ongoing legal action related to the event.

4. Home Depot

The timeline of Home Depot's breach was eerily similar to Staples, but the results were much more costly. Between April and September 2014, a malware infection designed to capture credit card information sat undetected in self-checkout machines across the US and Canada. Stolen credentials from one of the company's third party vendors were used to access the retailer's network, and eventually the POS system. Over 56 million credit and debit cards were compromised, 53 million customer email addresses were exposed, and the attack affected between 56 to 90 million accounts. This made it the largest reported retail data breach involving a POS system (although this distinction was short-lived).[7]

By September, large batches of these stolen credit and debit cards went on sale at rescator.cc, an underground cybercrime store.[8] Home Depot offered free credit protection services to any customer that visited the retailer around the time of its attack. In 2016, the company agreed to pay nearly $20 million to affected customers. This comes on top of an estimated $160 million arrangement with banks and credit card companies to cover damages suffered as a result of the data breach.[9] In total, the hack has cost Home Depot a staggering $179 million, not including costs associated with the long-term loss of customers and damage to the brand.

3. Sony

Sony has experienced two massive cyberattacks, one of which was sensationally referred to as "the hack of the century" and more closely followed Hollywood's dramatic portrayal of a data hack.[10] Cryptic notes, images of fiery skeletons appearing on employee computers, and threats of physical attacks on theaters showing Sony Pictures-produced movies contributed to the ensuing chaos in the 2014 data security breach.

The 2014 cyberattack was claimed by a group called "GOP," or Guardians of Peace, later identified by the FBI as operatives within the North Korean government. In order to access Sony's computer systems, the hackers stole a system administrator's computer credentials and planted a form of "wiper" malware on the network.[11] This cyberattack eventually involved not only the FBI but the CIA, the State Department, Homeland Security, Congress, and even President Barack

---

6 https://www.opi.net/business/large-resellers/staples-bolsters-it-controls-after-material-weaknesses-found/
7 https://www.webtitan.com/blog/cost-retail-data-breach-179-million-home-depot/
8 https://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/
9 https://www.webtitan.com/blog/cost-retail-data-breach-179-million-home-depot/
10 http://fortune.com/sony-hack-part-1/
11 http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12

Obama. Sony Pictures' network was shut down, and employees resorted to fax machines for communication and paper checks for payment processing. Valuable insider information was posted to the internet by the GOP, including yet-to-be-released movie files, sensitive personal information of over 4,000 employees, emails, and financial documents.[12] In total, the cost was projected to reach $100 million, including $35 million earmarked for IT repairs.[13,14]

Less theatric, but more easy to assign financial costs, was the 2011 data breach. This attack occurred three years prior and exposed sensitive information from over 77 million Playstation customer accounts. This breach compromised 14 million credit and debit cards and cost Sony $186 million.[15]

2. TJ Maxx

Back in 2005, TJ Maxx was hacked by a group of 11 men from the US, Ukraine, China, and Estonia. When it was discovered in 2007, it was called the "single largest and most complex hacking and identity theft that has ever been prosecuted."[16] The cybercriminals breached the Wired Equivalent Privacy (WEP) encryption protocol for a Minnesota store's WiFi network that transmitted data between price checkers, cash registers, and computers.[17] This enabled the hackers to access the company's central database, where they collected the sensitive information.

Court filings from October 2007 revealed that at least 94 million TJX customers were affected by the data breach that exposed credit card information and personal data.[18] As of November 2017, the breach has cost TJ Maxx over $256 million, though analysts in 2007 estimated the price tag at $1 billion for its failure to secure its WiFi.[19]

1. Target

Target experienced a large-scale data breach in 2013, and due to its reach and financial repercussions, it takes the number one spot on our list. As many as 110 million accounts were compromised in the attack on the retail giant, and data for nearly 40 million credit and debit cards were stolen. As a result of this attack, Target replaced Home Depot as the largest POS system-based retail data breach. Hackers accessed the sensitive data through stolen network credentials from a third party vendor. They then pushed malware to Target's POS devices.[20]

---

12 https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/
13 https://www.reuters.com/article/us-sony-cybersecurity-costs/cyber-attack-could-cost-sony-studio-as-much-as-100-million-idUSKBN0JN2L020141209
14 https://www.csoonline.com/article/2879444/data-breach/hack-to-cost-sony-35-million-in-it-repairs.html
15 https://www.csoonline.com/article/2128427/network-security/playstation-network-users-reporting-credit-card-fraud.html
16 https://nakedsecurity.sophos.com/2008/08/05/busted-gang-suspected-of-tj-maxx-credit-card-breach-charged/
17 http://www.zdnet.com/article/wi-fi-hack-caused-tk-maxx-security-breach/
18 http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/3.html
19 https://www.wired.com/2007/03/data_breach_wil/
20 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

While the costs associated with the data breach reached $300 million in November 2017,[21] some experts say that Target might be liable for nearly $3.6 billion in fines.[22] To date, 47 US states have filed lawsuits against the company, forcing the retailer to settle for nearly $20 million.[23] In total, the organization has paid $153.9 million in settlements. Additionally, Target's CFO admitted that upgrading the vulnerable technology to handle chip-and-PIN would cost $100 million.[24]

However, Target did hold a cybersecurity insurance policy at the time of attack that covered $100 million of the damage expenses.[25]

What the Retail Industry Can Learn

These five case studies in what not to do can teach the retail industry how to best prepare for and prevent cyberattacks and data breaches. Hackers were able to access private networks through stolen credentials from employees and third party vendors, as well as through weak security on WiFi networks. It's clear that comprehensive security vigilance must be constantly deployed, along with regular monitoring to detect early warning signs of an incident so that immediate action can be taken. Apart from the Sony Pictures hack, which occurred over the span of a few weeks, these devastating attacks gave hackers months of unfettered access to information. More importantly, you must use a proven data protection technology like encryption to secure your data from unauthorized access. Data encryption renders the information indecipherable to hackers, meaning they gain nothing from an attack. By recognizing the risks of distributed POS systems and other vulnerabilities, and encrypting sensitive data like customer records and personally identifiable information (PII), retail organizations can take positive steps to reduce the likelihood of an unexpected price tag reaching into the millions (or billions) of dollars.

Learn how XCrypt™ Full Disk can provide you with proven protection for your sensitive data.

[21] https://www.thesslstore.com/blog/2013-target-data-breach-settled/
[22] https://techcrunch.com/2013/12/23/target-may-be-liable-for-up-to-3-6-billion-from-credit-card-data-breach/
[23] https://consumerist.com/2017/05/23/target-will-pay-18-5m-to-47-states-to-close-investigations-into-2013-data-breach/
[24] http://www.businessinsider.com/target-may-have-to-spend-100-million-to-prevent-future-data-breaches-2014-2
[25] https://www.businessinsurance.com/article/20140119/NEWS07/301199973

465 Fairchild Drive, Suite 234, Mountain View, CA 94043
www.zettaset.com // +1.650.314.7920 // Fax: +1.650.314.7950 // sales@zettaset.com

About Zettaset

A leader in data protection, Zettaset's XCrypt™ line of encryption products are optimized for unmatched performance and infinite scalability to address the demanding data protection requirements of today's high-volume compute, storage, and cloud environments.