Retail: Security Challenges

Cybersecurity for retail companies needs to be a priority.

Retailers are stores that resell consumer goods or services through different channels to gain a profit. The retail industry includes grocery, technology, pharmaceutical, and convenient stores. Walmart, Target, and Amazon are the top retail companies, but a local convenience store fits on the same category. All of these stores have one thing in common, they are all susceptible to cyberattacks.

The retail industry has experienced a lot of crime, not only in physical robberies but also through cyber-related means. Every 1 out of 3 retailers lose revenue over cyber attacks, and 16% of all retail companies suffer the loss of more than $1 million.

Retailers recognize that they are a massive target to cybercrime, yet only 52% of companies feel their security infrastructure is updated, and 61% of companies feel that they are compliant with security standards.

Data breaches cost companies millions of dollars cause them to lose customers and can cause irreconcilable damage to the brand. Studies have proven that the majority of data breaches start with "one compromised password."

The problem for the retail industry is that not only do they have to fend off against cybercrime and organized crime, but also, they must be compliant or be subject to consequences.

Organized Crime Statistics:

These are the crime statistics against retailers in recent years.

- Organized crime costs the retail industry around $30 billion each year.
- 91.6% of retail companies witnessed organized retail crime in the past year.
- 71.3% of retailers surveyed reported an increase in organized crime year over year.
- 55.2% of management responded that none of the employees have organized crime as their primary job responsibility.
- Robberies and burglaries are up 8.6% since 2016.
- The reported value of organized crime cases in 2016 exceeded $200 million.

Even though crime is a significant issue in retailers, not many companies plan to make a change to these numbers. With crime increasing steadily and more money being stolen year after year, retailers play the bystander and only report the action instead of trying to protect the business better.

Besides organized crime, retailers experience other forms of stealing.

- Average cost per shoplifting incident doubled to $559.
- Average costs of return fraud were $1,766.27.

Top Threats

The top threats from organized crime are:

POS or point-of-sale breaches are of the top threats to retail cybersecurity. Many retailers fail to maintain their POS Systems due to outdated systems. POS is without point-to-point encryption (P2PE) which enables the secure process of transferring encrypted data from devices to the local network, which means that a point of sales such as a register or a card reader can be the hacker's main priority since there is no protection on the card reader. Without a point to point encryption, hackers can target the device with the lowest security and retrieve cardholder data from there.

DDOS also was known as disrupted denial of service attacks are top threats because of the rise of the Internet of Things which leads to an increase of DDoS attacks. The purpose of a DDoS attack is to disrupt the site from making any sales. Although there is no stealing of information in a DDoS attack, it does prevent the company from operating, and in turn, cost hundreds of thousands of dollars in repair and potentially lost revenue. Companies are trying to add security to their cloud which allows companies to operate still even if a DDoS attack occurs in a targeted area of the network to solve this issue.

Ransomware is still a top threat in retailers. While it is an old threat, its numbers jumped from 3.8 million to 638 million within the last year. Ransomware is malicious software that employees download on their devices which can steal company data, cause viruses, and cause a considerable break in the company if not prevented immediately. Although many retail companies are aware that ransomware exists, some employees still accidentally download it, and they are not educated against manipulative emails that contain ransomware.

Retail Threats:

Network intrusion is any unauthorized activity on a computer network. Network intrusion takes network resources that were intended for other purposes, and it threatens the security of the system. A well-known type of network intrusion is a Trojan which appears harmless, but Trojans act the complete opposite. They can erase stored data and open security channels to allow outside hackers into the network. Another type of network intrusion is a Worm which is pieces of computer code that replicate itself without affecting program files. Worms actively seek confidential data such as cardholder information and send that data back to the attackers who sent the worm. Both Trojans and Worms are transmitted and breach the network through emails, meaning human error can accidentally break down a company.

Unauthorized system access is when someone outside the network gains access to the network using someone else's account information. Although there are extreme measures where viruses can track your computer and formulate your passwords through multiple algorithms, hackers can log in through a user's account if that user has a simple password. Hackers target users with important passwords saved on password managers because a password can open access to the hacker.

Data leakage and theft is the unauthorized transfer of classified information from a network to the outside world. Hackers can purchase physical data saved onto a USB or hackers can steal physical laptops from company executives to access financial records or other confidential data.

Payment card system vulnerabilities are substantial retail threats. Point-to-point encryption is essential because, without it, payment card systems are vulnerable to outside attackers. Another weakness is buffering error in online payment systems when the consumer is charged, but the order is never confirmed.

Evolving information security policies and the challenge of sustained compliance affect retailers but different compared to cyber attacks. Instead of malicious attacks, retailers face fines and prison time when they are not compliant with changing security standards and policies.

Lack of reliable access refers to the weak passwords that employees have. Simple passwords are secure to crack, and more difficult passwords are hard for employees to remember. However, if an employee forgets a password, it costs the company approximately $70 to repair.

Top Compliance Standards

Payment Card Industry-Data Security Standard (PCI-DSS) is checkbox compliance. This compliance mandates the retailer on how to preserve and transmit credit card data after accepting and processing. Being non-compliant risks fines of $5,000 to $10,000 per month.

The Sarbanes-Oxley Act (SOX) is vital for publicly traded retail companies because it requires the company to deliver transparent financial reporting publicly. Additionally, the retailer must maintain a formal system of internal checks and balances for accurate reports, and if they are non-compliant, the company risks $5 million and prison time.

HIPAA, or the Health Insurance Portability and Accountability Act, affects retail pharmacies. HIPPA focuses on protecting patient information, and because retail pharmacies are in contact with physicians, the transfer of patient data must be secure. Therefore, it is a high-reward target for hackers.

Even if retailers are PCI-DSS compliant, retailers are a massive target. There is a lack of budget to deploy various security controls. For example, smaller retailers have the bare minimum: firewalls and anti-virus tech, and they think they are not a national/international chain so outside attackers would not target them. However, they are the most targeted because small retailers are less likely to have deployed advanced breach detection tools and have large IT teams which makes them an easy target.

Also, data not compliant with PCI-DSS increases credit card costs on every transaction. Then, data is at risk, and reportable data breaches have negative effects on sales and could cost the CEO their jobs.

Solutions

Several solutions would reinforce the security infrastructure of a retailer. First, retailers can encrypt data through integrated key management which makes data unreadable. Then, retailers will restrict access to encrypted data by changing who has access and user controls to the data. Thus, only authorized users can decrypt the data. Lastly, retailers should implement security intelligence that tracks the access attempts to the encrypted data which gives insight into how outside attackers are attempting to break the security.

Internet Security Upgrades

In 2013, big-box retailer Target failed to encrypt its credit card scanners costing them millions accurately. Since then, they began storing data in cloud security and encrypted their credit card swipers, meaning no credit card information is stored in any POS device, meaning hackers cannot access credit card information so quickly.

Biometric Solutions

Cybersecurity is continually improving, and with the use of biometric technology, security infrastructures are protecting confidential data. Biometric technologies such as fingerprint authentication and facial recognition have significantly secured data access. Not only are biometric solutions much safer, more secure, and faster to input than an employee pin, but they have resulted in useful statistics from retailers.

There is a 91% decrease in work-related injuries from violent assault using facial recognition.

There is a 34% decrease in shoplifting reported by retailers using face recognition.

Biometric solutions can also help as decryption from authorized users can be assisted with fingerprint authentication, so fingerprint authentication allows only authorized users to decrypt files without having to use their credentials.

One retail Point of Sale organization, NCR, recognized the value of fingerprint authentication. The company supports thousands of retail customers throughout the U.S. by providing the thoroughfare for all transactions. Their POS system is accessed by their IT team, administrators, executives, management along with full-time and part-time employees. Securing access and creating audit trails is critical in these types of environments. Passwords and swipe cards have proven to be vulnerable and costly to maintain. NCR integrated BIO-key's fingerprint authentication solutions with their POS system thus delivering strong one-touch authentication that raises the bar on security while promoting optimum workflow.

Whether your organization wants to secure access to the device, a POS system or a custom application, BIO-key has a product to suit your use case. We even have retailers that use our biometric technology to secure high end inventory.

If you're an IT leader with a retail organization, consider adding the Power of a Touch to your security platform.

Reference Links:

https://www.blackstratus.com/industries/cybersecurity-compliance-retail-industry

http://intigrow.com/retail.html

https://www.alienvault.com/solutions/retail

https://www.thalesesecurity.com/solutions/industry/retail

https://www.facefirst.com/blog/retail-loss-prevention-and-violent-crime-statistics/

https://losspreventionmedia.com/insider/shoplifting-organized-retail-crime/shedding-light-on-retail-theft-statistics/

https://www.mytotalretail.com/article/is-security-a-priority-for-your-retail-stores/

https://www.rsaconference.com/blogs/network-intrusion-methods-of-attack

https://dl.packetstormsecurity.net/papers/general/common-vulnerabilities.pdf