VENBROOK
INSURANCE SERVICES

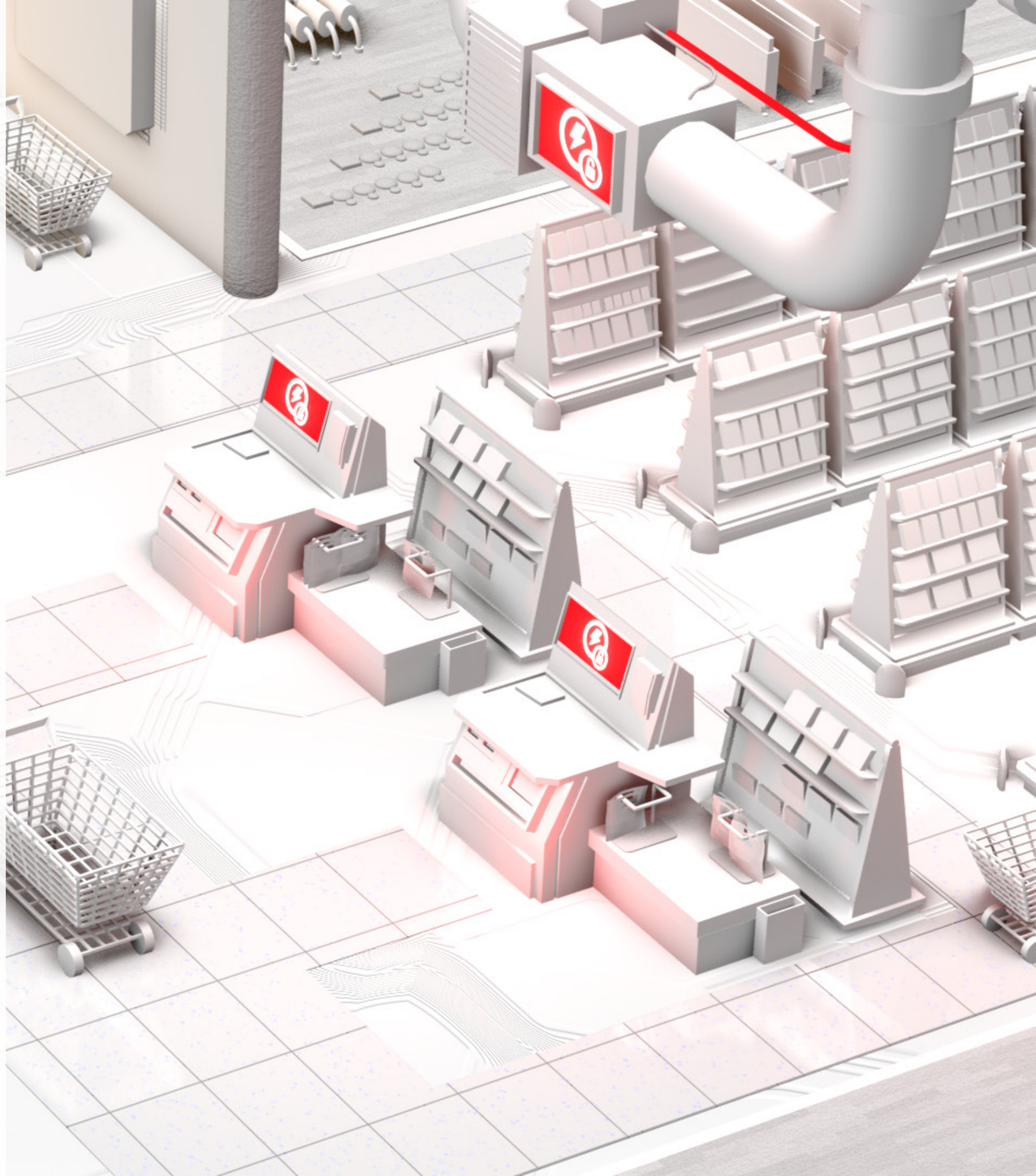
Cyber Case Study

provided by Venbrook Insurance Services

Target Data Breach

During the final months of 2013, Target—the well-known American retailer—experienced a large-scale security breach. This breach led to several point-of-sale systems being compromised by malware, giving cybercriminals access to millions of customers' personal and financial data. The incident became one of the most high-profile data breaches of the decade, impacting customers across the country.

Target faced numerous consequences in the aftermath of the breach—including a range of recovery expenses, hundreds of lawsuits, decreased customer confidence, lost profits and widespread criticism related to the company's initial response. In hindsight, organizations can learn many lessons by analyzing the details of this breach, its impact and Target's mistakes along the way. Here's what your organization needs to know.

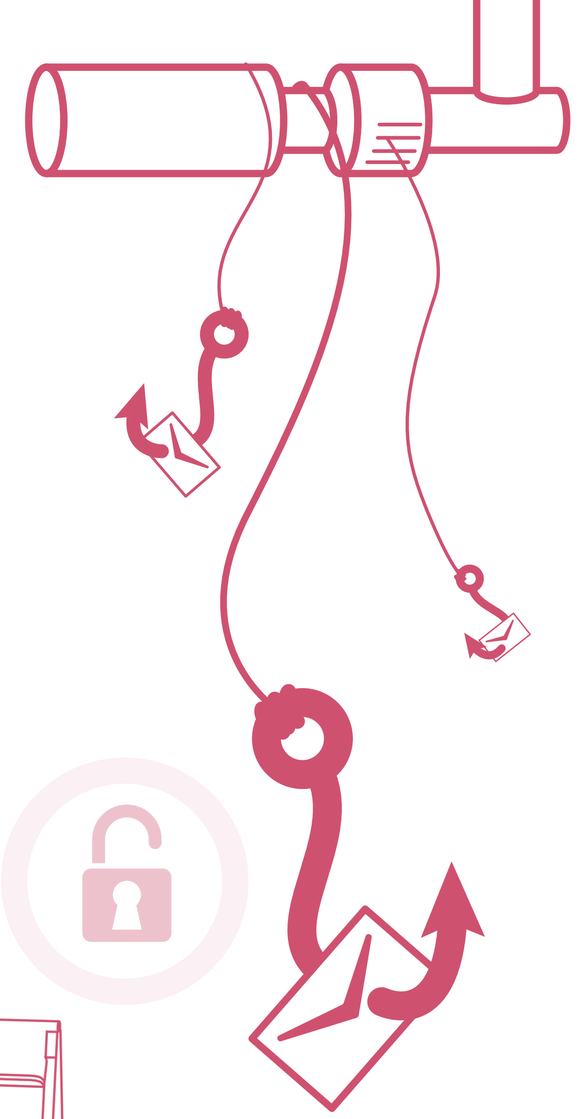


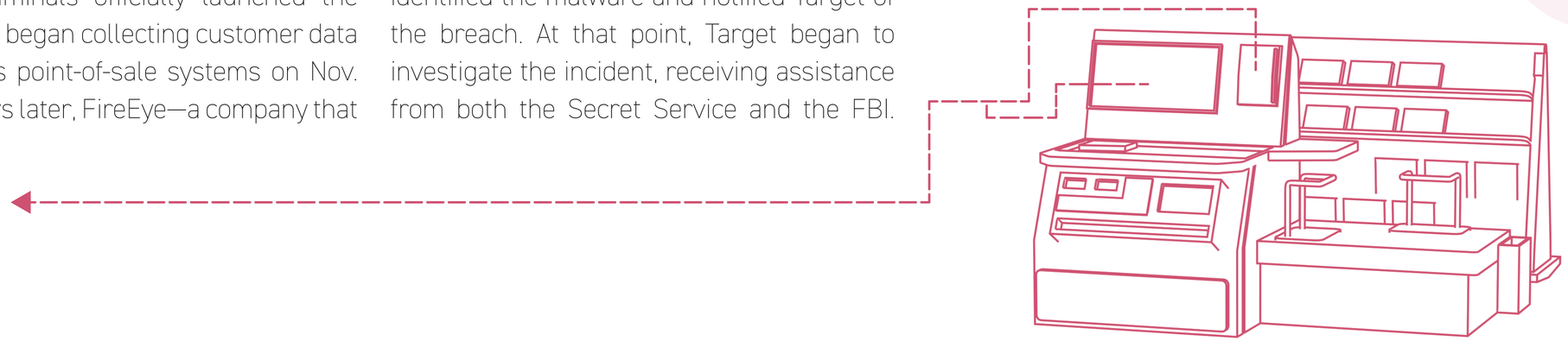
The Details

In September 2013, cybercriminals utilized an email-based phishing scam to trick an employee from Fazio Mechanical—an HVAC contractor and one of Target's third-party vendors—into providing their credentials. From there, the cybercriminals used these stolen credentials to infiltrate Target's network and install malware on a number of point-of-sale systems on Nov. 15. Even though Target had various cybersecurity measures in place to help avoid such an incident, Fazio Mechanical's lack of malware detection software and both companies' failure to properly segment their networks permitted the cybercriminals to execute their plan successfully.

The cybercriminals officially launched the malware and began collecting customer data from Target's point-of-sale systems on Nov. 27. Three days later, FireEye—a company that Target had purchased security software from earlier that year—detected the malware and reported the issue to Target's headquarters. Despite receiving this report, Target did not take steps to stop the malware. After Target's inadequate response, the cybercriminals were then able to implement exfiltration malware on the point-of-sale systems to transport customer data out of the company's network. In the coming days, the cybercriminals began moving the data. This activity triggered another report from FireEye on Dec. 2. However, Target still did not respond to the malware.

On Dec. 12, the U.S. Department of Justice identified the malware and notified Target of the breach. At that point, Target began to investigate the incident, receiving assistance from both the Secret Service and the FBI. By Dec. 15, most of the malware had been removed. On Dec. 18, a cybersecurity blogger became aware of the breach and publicly shared the incident's details. One day later, Target released an official statement on the matter, outlining what happened and confirming that the company was working with the proper authorities to resolve the incident. Nevertheless, severe damage had already been done. In total, the cybercriminals compromised approximately 40 million customers' credit and debit card information as well as 70 million customers' personal details (e.g., names, addresses and phone numbers).





The company was involved in over **140 lawsuits** throughout the country regarding the incident.

In 2017—four years after the breach occurred—Target finally reached an **$18.5 million** settlement spanning **47 states.**

The Impact

In addition to compromised customer data, Target encountered a series of ramifications after the breach.

Recovery costs

Target had to take several steps to recover from the breach and minimize the risk of future security incidents. Recovery efforts included obtaining assistance from a third-party forensics firm to investigate the breach, offering customers one year of free credit monitoring, setting up a call center for breach-related concerns, equipping point-of-sale systems with chip- and PIN-enabled technology, segmenting different company networks and implementing stricter access controls. The overall cost of these efforts totaled more than $250 million.

Legal expenses

Apart from recovery costs, Target also faced significant legal expenses from the breach. In particular, the company was involved in over 140 lawsuits throughout the country regarding the incident. In 2017—four years after the breach occurred—Target finally reached an $18.5 million settlement spanning 47 states. As part of the settlement, the company was required to consult a third party to help encrypt and further protect customer data as well as hire an executive responsible for leading a workplace cybersecurity program—thus compounding costs.

Reputational damages

Lastly, Target experienced a range of reputational issues due to the breach—namely, reduced customer confidence and distrust in senior leadership. The timing of the incident was especially detrimental, seeing as it took place during the holiday shopping season and negatively impacted year-end sales.

In fact, Target's profits dropped by a staggering 46% during the final quarter of 2013. Moving into January 2014, one-third (33%) of U.S. households reported shopping at Target—down 10% from the previous year. The company's prolonged response to the breach was also heavily criticized, causing stakeholders to hold senior leaders accountable for the delay and demand change. As a result, both Target's longstanding CEO and chief information officer stepped down in 2014, paving the way for significant transitions in executive leadership.

Lessons Learned

There are several cybersecurity takeaways from the Target data breach. Specifically, the incident emphasized these important lessons:

Investing in cybersecurity measures is worth it.

This large-scale breach could have been minimized or potentially avoided altogether if Target had additional cybersecurity precautions in place, such as network segmentation and more elaborate data encryption techniques. As such, this incident highlighted the value of investing in adequate cybersecurity procedures. The expense of implementing these measures is well worth the benefit of deterring even costlier incidents further down the road.

An effective cyber incident response plan is critical.

One of Target's greatest downfalls during the breach was the company's initial response. Although Target received multiple reports from FireEye about the malware, the company failed to act until the federal government got involved. By responding just days earlier, Target could have stopped the cybercriminals before they could transport customer data—significantly limiting the impact of the breach. What's more, the company also took extra time to inform the public of the incident, which upset many customers. Such concerns emphasize how critical it is to take reports seriously, act quickly and have an effective cyber incident response plan in place. This type of plan can help an organization establish timely response protocols for remaining operational and mitigating losses in a cyber incident. Generally speaking, an effective cyber incident response plan should outline:

- Who is part of the cyber incident response team (e.g., board members, department leaders, IT professionals, legal experts and HR specialists)
- What roles and responsibilities each member of the cyber incident response team must uphold during an attack
- What the organization's key functions are and how these operations will continue throughout an attack
- How any critical workplace decisions will be made during an attack
- When and how stakeholders should be informed of an attack (e.g., employees, customers, shareholders and suppliers)
- What federal, state and local regulations the organization must follow when responding to an attack (e.g., incident reporting protocols)
- When and how the organization should seek assistance from additional parties to help recover from an attack (e.g., law enforcement and insurance professionals)

Third-party exposures must be considered.

This breach also showcased the importance of promoting third-party security. After all, Fazio Mechanical's cyber vulnerabilities are what ultimately led to the onset of the breach. To prevent these exposures, it's vital to work with vendors, suppliers and other third parties to ensure they uphold effective cybersecurity practices. This collaboration may include incorporating cyber risk management within vendor contracts, restricting third parties' access to sensitive data and monitoring suppliers' compliance with applicable regulations—such as the Payment Card Industry Data Security Standard.

Proper coverage can make all the difference.

Finally, this breach made it evident that no organization—not even a successful, national retailer like Target—is immune to a data breach. What's worse, cyber incidents have only increased in cost and frequency since this event occurred. That's why it's crucial to ensure adequate protection against cyber-related losses by securing proper coverage. Make sure your organization works with a trusted insurance professional when navigating these coverage decisions.

For more risk management guidance and insurance solutions, contact us today.