CIS410-50-4238

Case 2 – Target James Cook

Summary

Target’s security breach resulted from multiple negligent behaviors that accumulated into one big problem despite having precautions. The risks were internal and external components overlooked throughout the audits and operations. Proper access management of third-party vendors could have prevented this issue. However, one should also consider that the nature of these attacks is challenging to discover, which the text mentions taking more than 200 days on average.

Business Issue

Target’s issue with their structure was allowing a third-party vendor, Fazio Mechanical Services, to directly access the internal system. While vendors with external access may enable swift business operations, it may also introduce security-related risks or vulnerabilities like the one that happened with Target. Regardless of how strictly one manages and audits the organization, more doors will increase the chances of loopholes. Furthermore, countless accidents across all industries typically result from managers ignoring the initial warning or the signs of failure. Target’s case was the same, since the people who were supposed to stay alert and prevent security attacks remained off guard and did not take proper action.

Analysis

Surprisingly, Target was known to invest a lot of money into security, achieving one of the highest standards at that time, on par with some government agencies. FireEye allowed them to gain an advantage in cyber security. Target’s goal was to provide the best shopping experience to the customers which they took multiple measures to protect their customers’ personal information. As a result, Target was considered “well protected.” Recurring security checks and various tools allowed Target to pass the test, but this may have made the managers to over-trust the system and underestimate the situation.

The time breach occurred was to be the worst time to happen. Since it was around holiday season, banks and credit card companies could not simply lock down the affected accounts. Instead, one of their solutions was to allow limited transactions per time, so that no unauthorized activities may quickly get out of control. As it could not fundamentally prevent the fraudulent activities, new cards had to be issued, and it came back to Target as a financial burden.

Stakeholder Groups

Customers are the victims of this incident, losing private data and facing potential threats of identity theft and financial fraud. Many customers experienced trouble reaching Target due to poor customer service. The delayed public announcement of the breach worsened their concerns. Customers wanted to secure their personal information and have a smooth shopping experience during the holiday season.

Banks and credit card companies are indirect victims of the incident, as they took the financial loss as an aftermath of the breach. Millions of new cards had to be reissued, which was more money to cover. They had to take preventive measures to discourage financial fraud in the customer's accounts, such as minimizing the ability to spend money at once. Financial institutions may want to agree on a settlement with Target to reduce the burden.

Investors were affected by this incident due to a loss in sales and a decrease in stock value. Low stock value translates to the loss of the investor group, affecting their profitability. Investors may want an active resolution from Target to recover their way back to normal.

Third-party vendors such as Fazio were the starting point of this breach. A security breach within the vendor spread across the network, allowing the attackers to reach Target's internal system through authorized vendor access. Third-party vendors may worry about the future relationship with Target after this incident because they have contributed to the breach.

Employee and manager groups were affected heavily by this incident. The CIO and CEO left Target after the breach while the company managed through structural changes. Apart from recovering from the breach, the employees had to adjust to the changing environment.

Government agencies told Target about the breach and led the investigation. Their goals were to prevent further malicious activities and identify the attackers. They worked on improving laws related to data protection, as there needed to be an industry-wide regulation to handle such attacks.

Alternatives and impact of alternatives on stakeholders

1. The first alternative to the case is straightforward. If the managers had stayed high alert and taken proper actions during the early stages of the suspicious activity, the outcome may have been different. The same thing happened in Pearl Harbor. Early suspicions on the radar were underestimated or ignored, just like Target. This phenomenon appears across various places and often becomes the cause of a disaster. Instead of repeating the cycle of history, if Target had been able to eliminate such human error, the attackers would have failed.

2. The second alternative to the case is to trust FireEye. Although they had access to one of the most advanced security systems, the managers did not want to rely on its features because it was new to them. This norm of following the tradition can quickly turn unsafe in the cyber security scene. Sticking to something they feel comfortable with is not a viable protection strategy against attacks that may take advantage of a zero-day.

3. The third alternative to the case is to limit third-party access. Frontegg states that access management can reduce the dangers of data breaches through a controlled environment. Even though the managers at Target continuously ignored warnings, they had a reason for their behavior - a state-of-the-art security system. The point of failure from the technical perspective was the vendor access. A general person would find it difficult to suspect malicious activity through one of their trusted vendors. This "whitelisting" could lead to overlooking tiny details. Adding a simple step of approval from Target for all the changes vendors make could have detected the injection of BlackPOS.

I believe all three solutions are effective practices to prevent the data breach at Target. Unfortunately, all of them failed. To rule out the best among all, permission management of the third-party vendors is the most effective solution. It is the only technical point of failure that Target experienced. Other problems were related to human error, which the managers ignored and relied more on their habits.

Reference:

*The radar warning that went unheeded | PearlHarbor.org*. (n.d.). PearlHarbor.org. <https://pearlharbor.org/blog/warning-went-unheeded/>

*What is access Management? Risks, technology & best practices*. (2024, October 3). Frontegg. <https://frontegg.com/guides/access-management>