# Cyber Breach at Target Case Analysis

Helen Le

3/1/2026

# Table of Contents

## Executive Summary

In November 2013, Target suffered one of the largest retail cyberattacks in history. Hackers exploited stolen credentials from Fazio Mechanical Services, a third-party HVAC vendor, to infiltrate Target's network and install RAM-scraping malware on point-of-sale systems across stores. The attack compromised payment card data for 40 million customers and personal information for an additional 70 million. Despite detection tools alerting the intrusion twice, Target's security team failed to act. The breach cost Target at least $162 million in direct expenses, a 46% drop in fourth-quarter net earnings, over 100 lawsuits, and the resignations of both CEO and CIO.

This analysis examines the breach through SWOT and PEST analysess, Porter's Five Forces, and organizational structure analysis. Target's differentiation strategy depends on customer trust, which the breach and following communication damaged. The organizational analysis revealed a fragmented security governance structure with three reporting pipelines, no dedicated CISO, and 200+ daily alerts causing alert fatigue and dispersing accountability. The stakeholder analysis identifies customers, the board, banks, shareholders, employees, and third-party vendors as all negatively impacted, demanding a change beyond technical fixes.

Three alternatives were considered: a technical-only fix, a governance-only, and a comprehensive cybersecurity overhaul combining both with stricter vendor oversight and incident response protocols. The comprehensive overhaul is recommended as the only solution addressing all dimensions of failure – pairing detection tools with accountable leadership, segmenting network architecture, holding vendors to stricter standards and monitoring them, and established defined response and communication protocols to preserve customer trust.

## Introduction

George Dayton built Target around a "Pay Less, Expect More" differentiation strategy, offering high-quality products at low prices across 1,919 stores with over $72 billion in fiscal 2013 revenue. The Thanksgiving-to-Christmas season accounted for 30% of annual revenue from 2010-2013, making it the most critical sales period (Srinivasan et al. 2).

In November 2013, Target faced one of the largest cyberattacks in history. Hackers used stolen credentials obtained from a phishing email to Fazio Mechanical Services, a third-party HVAC vendor, to infiltrate Target's network and install RAM-scraping malware across nearly all of its U.S. point-of-sale (POS) systems. From November 15 to December 15, which is holiday shopping season, cybercriminals breached Target's systems and obtained payment card details from approximately 40 million shoppers. The attack also exposed the personal information – including names, mailing addresses, and emails – of approximately 70 million additional customers (Srinivasan et al. 1). This breach cost Target at least $162 million in direct breach-related costs by end of 2014 with total costs continuing to rise; a 46% decline in net earnings for the fourth quarter; over 100 lawsuits from consumers, banks, and shareholders; and the resignations of CIO Beth Jacob and CEO Gregg Steinhafel. (Srinivasan et al. 7-8).

However, the core issue is not that Target was hacked – it was the lack of governance and accountability. Cyber breaches were a growing threat with 471 reported across all industries in 2012 alone (Srinivasan et al. 25). Target had measures in place to detect and stop the attack but failed to act. Cybersecurity monitoring was outsourced to FireEye, Inc., who provided a team of security specialists and malware detection tools. A series of security alerts were sent throughout November 30-December 2, that flagged malware, which was after the systems were infected but before data was sent to attackers' servers. Despite multiple alerts, no action was taken by the

security team in Minnesota to resolve the issue (Westervelt). The FireEye system also included an automatic malware deletion function that could have eliminated the threat without human intervention, but Target's security team had turned it off. Furthermore, at least two months before the attacks, vulnerabilities in the POS system were found and a review was requested, but this was ignored to instead prepare for Black Friday. Visa published their own alerts of RAM scraper malware and recommended firewall configuration, segregated payment processing, and hardware-based point-to-point encryption. While Target escalated the alert, no action was taken (Srinivasan et al. 9). Ultimately, this was not a failure of technology, but a failure of governance, vendor oversight, and organizational accountability that permanently damaged customer trust.

## Industry & Competitive Analysis

### *Mission & Generic Strategy*

Target's mission has been rooted in offering quality products at affordable prices in an upscale environment. It aimed to be a store customers would be proud, confident, and fun and exciting to shop in (Srinivasan et al. 1). This vision was then put into words: "Pay Less, Expect More," which captures Target's core value proposition: people don't have to sacrifice quality for affordability. Through a differentiation strategy, it distinguishes itself from competitors through not only low prices, but also a unique shopping experience. Competitors like Walmart and Kmart focused on selling goods as cheaply as possible. Instead, Target considered trends, collaborated with designer labels to cultivate their brand image as an affordable but quality retailer, and "displays a creative and fashionable ambience which appeals to middle class customers who look down on cheap discount stores" (Alshakhoori, 30). By offering higher quality goods, they can sell at higher price points than competitors while still maintaining strong customer loyalty.

Consumer trust then lies at the foundation of their differentiation strategy. Unlike a cost leader whose competitive advantage relies on prices remaining low, a differentiator depends on providing unique products and experiences of a high quality, building customer loyalty to their brand (Kennedy). The REDcard program deepened this relationship by collecting Social Security numbers, making data protection tied to brand promise. However, the 2013 breach violated this trust, striking directly at the foundation. Target "reached its lowest consumer perception point since at least June 2007" with customers describing the response as disheartening.

***Porter's Five Forces***

Porter's Five Forces framework examines the competitive pressures shaping an industry and a firm's strategic position.

**Competitive Rivalry (High):** The U.S. general merchandise retail market is incredibly competitive, with Target competing with Walmart and Kmart. Target's differentiation strategy provided a buffer against price competition, but the breach eroded this during the most critical sales period of the year. Competitors didn't need to change to consume Target's audience – Target's own crisis drove customers away (6.6% sales decline and 46% drop in net earnings). In an environment with high rivalry, losing customer trust means losing customers to competitors. Any solution Target pursues must rebuild that trust, not just fix the technical vulnerability.

**Bargaining Power of Customers (High Post-Breach):** Before the breach, Target managed buyer power effectively through loyalty programs, a curated brand experience, and high-quality products at a low price. After the breach, customers gained significant leverage as Target was forced to offer a 10% discount if they shopped December 21-22. Customers boycotted Target and canceled REDcards. This power was then amplified by the "disheartening" response from Target, showing how the perception of disclosure efforts is crucial in choosing a solution.

**Bargaining Power of Suppliers (High for IT Vendors):** Target sourced 80.6% of internationally sourced goods from China (Banker), but the critical supplier vulnerability was in IT vendor relationships. Fazio Mechanical Services held network credentials reaching Target's most sensitive systems without two-factor authentication – a PCI standard – and used a prohibited security product license (Srinivasan et al. 2). Trustwave Holdings, a firm with clients suffering large cyberattacks soon after receiving certifications, certified Target as PCI-compliant just two months prior – this raises liability questions of auditors when the attack was able to advance for 18 days (Srinivasan et al. 7). Post-breach, supplier power shifted against Target – the breach left the company in a reactive position, dependent on cybersecurity firms and new technology vendors who could upcharge a retailer facing immense public scrutiny.

**Threat of Substitutes (Moderate):** The breach didn't create substitutes for discount retail, but it did increase customer migration towards online retailers like Amazon, who had secure payment systems that used encryption for data in transit and had 'A-z Guarantee' that offered buyers purchase protection (Panzarino). Customers could also switch to similar retailers like Walmart or Kmart with minimal switching costs, which likely occurred as reflected in the 6.6% decline in quarterly sales. The threat of substitution then reinforces how Target's response must go beyond simply repairing security vulnerabilities and give customers a true reason to return.

**Threat of New Entrants (Low, Still Impacted by Crisis):** Barriers to entry remain high due to capital requirements and supply chain complexity to sell a broad catalog – the breach did not change this. However, it transformed industry-wide expectations for cybersecurity investment, increasing costs for cybersecurity for all. Target responded by conducting end-to-end reviews of network security, adopting chip and PIN technology for credit cards, hiring a new CIO, and elevating the Chief Information Security Officer and Chief Compliance Officer roles to

demonstrate the steps Target is taking towards IT security and governance (Srinivasan et al. 22). While new entrants aren't a primary concern, the breach established that cybersecurity investment is a baseline cost of competing in retail, not an optional investment.

### *Organizational Structure*

Target's pre-breach security responsibilities were split across three teams: Target Information Protection (TIP) reported to the President of Financial and Retail Services who then reported to the CFO, Target Technology Services (TTS) reported through the CIO to the CEO, and Information Security Investigations (ISI) reported to Corporate Security who then reported to the General Counsel (Srinivasan et al. 16). No single group controlled cybersecurity. The Cyber Executive Committee, composed of leaders from all three teams, provided overall governance but only met quarterly. TTS also operated a 24-hour Security Operations Center and a Red team of white hat hackers, but with approximately 200 alerts generated daily, the volume combined with the unclear ownership across three reporting chains led to alert fatigue and scattered accountability. While the FireEye alerts may have been dismissed as false positives due to generic naming like "malware.binary," the underlying problem is that Target had the effective tools but an organizational structure that failed to act on them.

### *SWOT Analysis*

| Strengths | Weaknesses |
|---|---|
| - Strong brand identity respected by consumers, earning over $72 billion in revenue<br>- Existing FireEye investment with 24/7 SOC and 300 employees dedicated to IS<br>- PCI DSS compliance certification in September 2013 | - Fragmented security governance across three teams with different reporting pipelines and no CISO<br>- Unsegmented network that allows hackers to gain access to payment data network from outside contractor network<br>- No two-factor authentication for third-party vendors → missing monitoring |

| | |
|---|---|
| | - FireEye's 'automatically delete malware' was disabled<br>- CIO lacked an IT and security background (Srinivasan et al. 11) |
| **Opportunities** | **Threats** |
| - Implement a Zero Trust architecture and network segmentation<br>- Create a dedicated CISO role with board-level reporting and clearer pipelines for cybersecurity teams<br>- Ensure vendors follow compliance standards<br>- Implement chip readers for stores and REDcard program | - Increasing volumes of cyber threats in all industries<br>- Ongoing lawsuits from consumers, banks, and shareholders<br>- Extensive scrutiny from Congress, SEC, DOJ, and FTC<br>- Competitors taking in former Target loyal customers who switched post-breach |

The SWOT analysis shows that Target's strengths in security investment, brand reputation, and operational scale were undermined by structural flaws in governance and network architecture. Each opportunity directly addresses a specific weakness: Zero Trust architecture combats the unsegmented network, a dedicated CISO resolves fragmented governance, vendor compliance standards address the lack of vendor oversight, and chip readers fix the vulnerable POS infrastructure. The external threats represent the damage that continues to grow with a lack of action. A solution that addresses all is necessary for Target's success.

***PEST Analysis***

A PEST analysis deepens the severity of the breach. Politically, congressional hearings and investigations from the DOJ, SEC, and FTC indicated increasing regulatory pressure to protect consumer data. Economically, the $290 million in total breach-related expenses demonstrated how cybersecurity failures can quickly grow into detrimental financial damage. Socially, consumers hold retailers more accountable for taking the necessary standards to prevent breaches or else, there is a loss of trust. Technologically, Target must shift away from magnetic stripe to chip-and-PIN and Zero Trust architecture in order to meet the evolving security landscape and protect customers as threats grow.

### *Stakeholder Impact Analysis*

| Stakeholder | Interest | Influence |
|---|---|---|
| **Customers** | **High:** up to 110M customers impacted with financial fraud and credit damage | **High:** customers make up revenue; boycotts and REDcard cancellations led to sales decline |
| **Board of Directors (BoD)** | **High:** facing lawsuits and ISS states 7 of 10 members should be removed | **High:** responsible for disclosure procedures and risk assessment |
| **Shareholders** | **High:** stock is down 8.8%, 20% less earnings per share, and incurring class-action settlements, legal investigations and fines, and costs for customer-retention efforts → erodes shareholder value | **High:** filing derivative lawsuits against BoD, CFO, and CIO |
| **Banks/Financial Institutions** | **High:** spending $11-$12 per customer to reissue cards, providing relief to reimburse fraud, and hiring more staff to handle customers; Visa issued an alert to retailers with recommended steps for protection that Target did not act upon | **High:** Visa, MasterCard, and more are filing lawsuits for over $100 million |
| **Employees** | **High:** 350,000 data security staff impacted by brand damage, temporarily left with CEO and CIO | **Moderate:** contracted team in Bangalore did their job, but team in Minneapolis did not |
| **Third-Party Vendors** | **Moderate:** Fazio employees not trained to properly handle phishing emails; Fazio exposed for using free version of security product "whose license explicitly prohibited corporate use" (Srinivasan et al. 2) | **Low:** no leverage in security decisions but still played a role as the attacker's entry route |

This influence-interest table shows how the highest-priority stakeholders (customers, the board, banks, and shareholders) require a change extending beyond technical fixes and into governance reform, vendor oversight, and defined response and communication protocols.

## Proposed Alternatives

### *Alternative 1: Technical-Only Fix*

This alternative would upgrade Target's security infrastructure by enabling FireEye's auto-delete function to remove malware as it is detected, implementing network segmentation to

limit lateral movement for attackers, requiring two-factor authentication for all third-party vendors connected to Target (a PCI standard), and implementing firewalls and hardware-based point-to-point encryption like Visa recommended. While these fix the physical causes of the breach, they ignore the root cause. Target already had detection tools and a security team in place to alert of suspicious activity – these alerts went unanswered due to the unclear ownership of cybersecurity. Customers receive improved protection but no assurance that Target will respond differently, which was a main disappointment. The board avoids accountability and the fragmented reporting structure remains, leaving unclear disclosure procedures. Banks and shareholders see only a small decrease in risk, but ultimately no structural changes are being made to prevent a repeat. Employees are responsible for upgrading infrastructure, but no culture of clear procedures, accountability, and disclosure is created. Vendors implement regulations like two-factor authentication, but oversight is not guaranteed. This alternative addresses SWOT weaknesses but fails to capitalize on governance opportunities or mitigate threats.

***Alternative 2: Governance-Only Fix***

This solution solely addresses the root cause of the issue – a lack of governance – without rebuilding the technical infrastructure. A dedicated CISO role reporting to the CEO and board would unite the three fragmented security teams under one leadership, establishing mandatory automated escalation protocols so critical alerts are taken seriously, and implementing proper incident response protocols. This directly addresses the organizational failures identified in the SWOT and organizational structure analyses. The current CIO had also lacked IT or security expertise, so the CISO would bring in formal security governance, stronger policy enforcement, and clearer accountability for protecting customer data. The board would approve of clearer oversight and more awareness of information security concerns. Customers benefit from honest

communication and faster incident response times. However, without technical cases, the physical causes of the crisis remain. The leadership team would respond faster to breaches that proper segmentation could have prevented entirely. Banks and shareholders then gain confidence in governance but still remain wary of the technical vulnerabilities. Third-party vendors remain unaffected by this alternative. While this alternative capitalizes on governance opportunities, it leaves the technical vulnerabilities that physically allowed the breach to occur stay unresolved and leaves no change to vendor management.

***Alternative 3: Comprehensive Overhaul***

This alternative combines the technical fixes of Alternative 1 with the governance reforms of Alternative 2 into an all-encompassing solution that addresses both the physical and root causes. On top of those, vendor risk management and communication protocols are created to address all areas of improvement. On a technical level, Target would implement Zero Trust architecture with network segmentation to isolate POS systems from vendor access, require two-factor authentication for all third-party connections, enable auto-delete on detection tools, and adopt chip-and-PIN for stores and REDcards. A Zero Trust architecture relies on the principle that “trust is never granted implicitly but must be continually evaluated” (Rose et al. 4). This reduces the attack surface and prevents lateral movement by attackers. While implementing Zero Trust across 1,919 stores with the existing POS infrastructure presents logistical challenges like fitting network segmentation into a flat architecture, upgrading all POS terminals, and training employees on new protocols, Target’s post-breach end-to-end security review can guide a phased rollout to prioritize busy stores first. On a governance level, a dedicated CISO with direct board reporting would lead a more consolidated security structure, with automated alert escalation activated for critical threats. This replaces security oversight within the Cyber Executive

Committee. To better handle vendor management, Target should perform risk assessments based on the sensitivity of the systems accessed. For example, a vendor like Fazio Mechanical Services whose role is limited to HVAC billing, project management, and contract submission, should never have credentials that can log into payment processing systems with sensitive customer data. Fazio would be deemed low sensitivity as access is limited to billing. However, a vendor that needs confidential data would need stricter guidelines of encryption, two-factor authentication, and mandatory security audits. Additionally, continuous monitoring rather than one-time checks would be conducted to ensure third-party vendors consistently follow PCI standards and use comprehensive security products unlike Fazio's free Malwarebytes license. Lastly, employees gain clear escalation paths so that alerts are actually addressed rather than brushed aside. Disclosure timelines would be established to ensure the breach is heard from Target first and not an online security blog. For customers, this alternative provides improved protection and the honest communication that was missing, directly addressing the amplified buyer power in the Five Forces analysis. The board then gains a strong governance structure with clear responsibility and accountability, reducing risk of shareholder litigation and ISS backlash. Banks benefit from faster notification of a potential crisis and reduced fraud exposure that they had to bear the burden for. Vendors face stricter expectations and standards. Shareholders see careful efforts to reduce the crisis from repeating.

## Recommended Alternative

Alternative 3 is the recommended solution because it addresses all areas of the failure simultaneously. The Senate Committee performed a "Kill Chain" analysis to identify steps Target and Fazio could have taken to prevent the attack but didn't. It is important for all of these steps to be addressed, which a sole technical or sole governance solution wouldn't accomplish.

Using the SWOT analysis, Alternative 1 is able to correct weaknesses like an unsegmented network that allowed for lateral movement and a disabled auto-delete malware option. However, it does not capitalize on the opportunities in place like the creation of a dedicated CISO role or continuous monitoring of compliance for vendors. In contrast, Alternative 2 does capitalize on these opportunities but leaves the technical vulnerabilities that allowed the breach to physically happen. Alternative 3 is the only option that can address all identified weaknesses and take advantage of every opportunity. It directly mitigates the threats of increasing cyber threats, ongoing lawsuits, extensive scrutiny, and competition by demonstrating comprehensive efforts to prevent the breach from reoccurring.

The Porter's Five Forces analysis also supports this recommendation. High competitive rivalry means that rebuilding customer trust is crucial in order to prevent customers from switching. Neither Alternatives 1 nor 2 can fully achieve this. The amplified bargaining power of customers post-breach requires accountability and honest disclosure of the crisis, not just firewalls. High IT supplier power requires structured vendor oversight, so Target isn't vulnerable to a third-party's failure. The threat of substitution requires giving customers a reason to return, something a solution addressing technical change *and* governance reform can provide.

The PEST analysis then reinforces this recommendation – political pressure from federal agencies demands governance reform and technological advancements with ongoing compliance monitoring, economic losses justify the need for a comprehensive overhaul to prevent a repeat, rising social expectations from consumers around data privacy require transparent disclosure protocols, and upgrading technology is a must for Target to meet the changing landscape.

From an ethical standpoint, retailers who collect sensitive customer data have an obligation to protect that information. Target's lack of communication amplified the breach's

damage: on December 20, a statement was released saying PIN numbers weren't compromised, but on December 27, the statement was reversed to confirm they were compromised (Srinivasan et al. 6). The delay in disclosure allowed Krebs to report the breach before Target could control the narrative themselves. When customers were made aware of the breach, they called the hotline but did not receive a timely response. When the call finally went through, they received a pre-recorded message redirecting them to a website. An ethical framework demands proactive, honest, and timely communication even when the full scope is unknown. This principle is reflected in *The Adventures of an IT Leader* where CEO Carl Williams wants no disclosure, but the recommended decision is to provide limited but honest communication. Alternative 3 embeds this principle through a detailed incident response protocol to ensure future crises are properly disclosed.

Alternative 1 was ultimately rejected because Target's problem was never the lack of security tools – it was the failure to act on them. FireEye's team sent alerts and an auto-delete function existed. Upgrading the technology without reforming the security structure would repeat the same governance failures. This approach also failed to address the political and social pressures identified in the PEST analysis – congressional scrutiny and rising consumer expectations demands visible accountability, not just new firewalls. Alternative 2 was rejected because governance reform alone still leaves the unsegmented architecture that allowed hackers to move laterally, does not address the failure of the third-party vendor to meet PCI standards like two-factor authentication, and does not implement the recommendations from Visa to protect customer data from RAM scraper malware. It also ignores the technological aspect of the PEST analysis – without modernizing to Zero Trust and chip-and-PIN, Target falls behind the evolving security landscape.  A restructured security team might respond faster to preventable breaches,

but a technical fix could have prevented the attack entirely (Srinivasan et al. 4). Alternative 3 ensures technical infrastructure is in place to prevent what it can, governance structure responds to what gets through, vendors are held more accountable for following standards, and honest and timely communication exists to preserve the customer trust that Target relies on for success.

## Conclusion

The 2013 Target breach was a preventable crisis that occurred because of compounding failures across the dimensions of governance, technical infrastructure, vendor oversight, and crisis communication/disclosure. Target was aware of the risk of data security breaches, as shown in their 2012 10-K filing – just one year before the attack occurred (Srinivasan et al. 10). They were aware of the risk and properly invested in detection tools, but these investments were undermined by fragmented leadership, an unsegmented network that led to lateral vendor access, and a public response that worsened the damage. The comprehensive overhaul of Alternative 3 addresses all four dimensions, ensuring detection tools are paired with accountable leaders, network architecture prevents lateral movement, vendors are held to standards and regularly checked, and customers receive transparent communication that Target's differentiation strategy relies on. This case exemplifies how cybersecurity isn't just a technical matter, but a strategic function that impacts competitive positioning, customer trust, and value.

## References

Alshakhoori, N., et al. (2016). Business Strategies of Discount Retailers: A Comparative Study of Target Corporation and Costco Wholesale Corporation. *International Journal of Research in Management, Economics and Commerce*, *6*(6), 27–40.

Banker, S. (2013, October 29). *Sourcing Is A Competitive Differentiator At Target*. Forbes. https://www.forbes.com/sites/stevebanker/2013/10/29/sourcing-is-a-competitive-differentiator-at-target/

Kennedy, R. (2020, August 14). *6.4 differentiation*. Strategic Management. https://pressbooks.lib.vt.edu/strategicmanagement/chapter/6-4-differentiation/

Panzarino, M. (2013, October 8). *Amazon's "login and pay with Amazon" service challenges PayPal for the web's payment business*. TechCrunch. https://techcrunch.com/2013/10/08/amazons-pay-with-amazon-service-challenges-paypal-for-the-webs-payment-business/#:~:text=Amazon%20has%20been%20offering%20payment,they%20get%20on%20Amazon.com.

Rose, S., et al. (2020). *Zero Trust Architecture*. https://doi.org/10.6028/nist.sp.800-207

Srinivasan, S, et al. "Cyber Breach at Target." *Harvard Business School,* Jan., 2019, pp 1-32.

Westervelt, R. (2024, March 14). *Missed FireEye alerts reportedly warned of security lapse at Target*. CRN. https://www.crn.com/news/security/300072031/missed-fireeye-alerts-reportedly-warned-of-security-lapse-at-target