Target Corporation: A business risk model based on the 2013 data breach

Daniel Cordeiro Marques

University of San Diego

CSOL-520-03-FA20 - Secure Systems Architecture

Dr. Michelle Moore

November 8, 2020

Target Corporation: A business risk model based on the 2013 data breach

In 2013, the retailer Target suffered a data breach that exposed credit and card information from approximately 40 million clients (Target Corporation, 2013). According to Committee on Commerce, Science, and Transportation (2014), threat agents gained initial access to the Target network through a third-party, exploited ineffective security controls on point-of-sale systems, retrieved payment data from the environment, and remained undetected for at least one month. The assets affected by the incident, including the compromised systems and data, are essential to support critical business functions. The weak controls defending those assets may indicate a lack of alignment between the security strategy and the business requirements.

Target recognizes the importance of an effective security strategy by highlighting information security, cybersecurity and data privacy risks in their 2019 annual report and stating that “based on the prominence and notoriety of the 2013 data breach, even minor additional data security incidents could draw greater scrutiny” (Target Corporation, 2020, p. 6). Therefore, as one of the largest retailers in the United States (Schulz, 2020), Target can benefit from a business-driven security strategy. To achieve this objective, the SABSA architecture proposed by Sherwood et al. (2005) provides a framework to position security as a business enabler.

In the contextual architecture layer of the SABSA model, business drivers serve as initial input to establish Business Attributes and, consequently, the Business Risk Model. Leveraging the Business Risk Model, the security practitioner can, for instance, establish control objectives aligned to the business goals. This paper uses the methodology described by Sherwood et al. (2005) to create a Business Risk Model for the company. It leverages publicly available information regarding Target and the 2013 breach to derive business drivers, requirements and impact, and potential vulnerabilities.

Method

SABSA Risk Assessment Method Applied to The Target Case

Sherwood et al. (2005) adopted a "qualitative measurement method that classifies risks into a series of bands"(p. 205). This risk assessment method encompasses five steps that result in a Business Risk Model for the company.

Step 1: Business Drivers and Business Attributes (Sherwood et al., 2005, p. 205). The first step identifies what is essential to the business and the primary concern of the security strategy. On a typical risk assessment, the security professional obtains this information from interviews with key stakeholders; however, this option is not feasible. As an alternative, Target's annual report (Target Corporation, 2020) can provide enough details on the company's business goals and concerns to derive at least the five Business Drivers (BD) below.

BD01 - Maintaining the continuity of services, especially during the holiday period. Continuity of services and systems is paramount for the company's overall business strategy. It allows Target to offer clients a consistent and timely retail experience. A significant portion of Target's revenue occurs during the holiday period (Target Corporation, 2020, p. 2); therefore, services should consider peak activity during that period.

BD02 - Ensuring that information is accurate and available when needed. Target relies heavily on customer data to remain competitive and provide an engaging retail experience. Timely and accurate delivery of information to meet order fulfillment expectations and maintain low costs (Target Corporation, 2020).

BD03 - Protecting Target's reputation. After the 2013 incident, the brand's reputation became a significant concern for Target. Losing clients' confidence may directly impact the company's ability to generate revenue (Target Corporation, 2020, p. 4).

BD04 - Maintaining privacy and security of data stored, processed, and communicated by Target's systems related to customers, intellectual property, and third-parties. As mentioned before, customer information is a pillar of Target's business strategy. Additionally, one-third of the company's revenue in 2019 came from Target-owned brands (Target Corporation, 2020, p. 2); therefore, protecting their intellectual property is critical for its success.

BD05 - Ensuring that system security solutions comply with applicable law, standards, and best practices. Target has a workforce distributed over multiple states and countries and is continually pursuing certification on standards such as the Payment Card Industry Data Security Standard (PCI DSS). Failing to comply with the applicable law may impact its operational ability (Target Corporation, 2020, p. 6).

The output from this step is used as an input to define potential threat scenarios.

Step 2: Threat Assessment (Sherwood et al., 2005, p. 205-206). This step establishes potential high-level threats and threat scenarios relevant to the requirements defined in the first step. After establishing potential threats to the Business Attributes, the Business Risk Model must consider their impact on the business requirement. Table 1 documents high-level threats for each business requirement previously defined.

Step 3: Impact Assessment (Sherwood et al., 2005, p. 206). Next, the business model identifies "what would be the business impact that would result from each threat materializing"

(Sherwood et al., 2005, p. 206). Target Corporation (2020) provides high-level information that can support the understanding of business impacts. The impact value uses following the scale proposed by Sherwood et al. (2005, p. 207):

- High impact (H): Could potentially do significant damage to the business
- Medium impact (M): This could cause a moderate impact on the business
- Low impact (L): This could cause minimal damage to the business

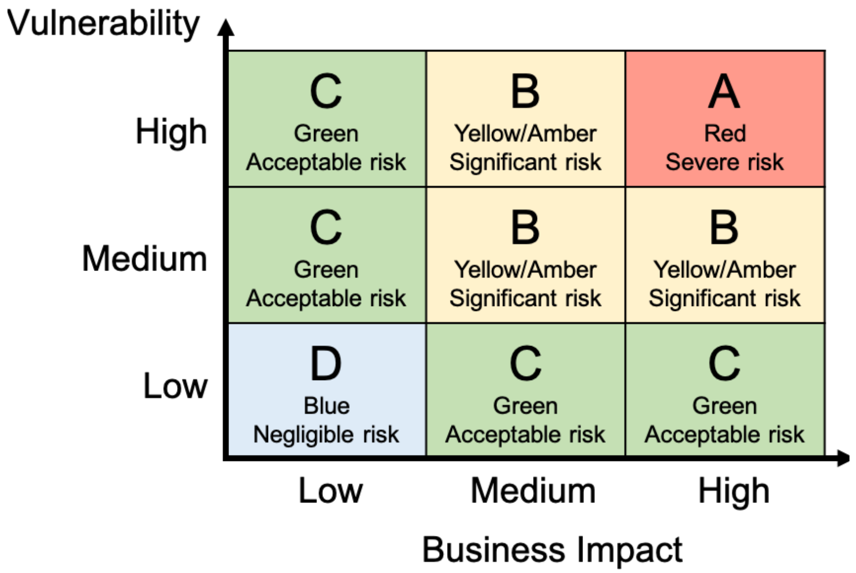
Step 4: Vulnerability Assessment (Sherwood et al., 2005, p. 207-208). Assessment of potential weaknesses in the environment, including people, processes, and technology. Committee on Commerce, Science, and Transportation (2014) and Shu et al. (2017) provide insights on vulnerabilities previously exploited by threat agents that might still be present in the environment. Sherwood et al. (2005, p. 208) propose the following scale to rate vulnerabilities:

- High vulnerability (H): Easily exploited by the threat
- Medium vulnerability (M): Possible for the threat to exploit
- Low vulnerability (L): Complex for the threat to exploit

Step 5: Risk Category (Sherwood et al., 2005, p. 208). This step focuses on prioritizing risk, based on four categories calculated by the combination of vulnerabilities and impacts. Sherwood et al. (2005, p. 209) propose a matrix of four risk categories illustrated in figure 1.

Figure 1

Risk Category Matrix based on the mapping proposed by Sherwood et al. (2005, p. 208)



Vulnerability	Low	Medium	High
High	C Green Acceptable risk	B Yellow/Amber Significant risk	A Red Severe risk
Medium	C Green Acceptable risk	B Yellow/Amber Significant risk	B Yellow/Amber Significant risk
Low	D Blue Negligible risk	C Green Acceptable risk	C Green Acceptable risk
	Business Impact		

Finally, the Business Risk Model combines the information from each step and classifies business risks according to each business driver.

Target's Business Risk Model

Table 1 represents the Business Risk Model for Target, based on publicly available information. The Business Attribute column follows the list proposed by Sherwood et al. (2005, p. 88), which lists and defines 85 different attributes grouped into seven classes (user, management, operational, risk management, legal and regulatory, technical strategy, and business strategy).

Table 1.

Target's Business Risk Model, based on Table 9-8 from Sherwood et al., (2005, p. 206-207)

1	2	3	4	5	6	7	8	9	10
ID	Business Driver	Business Attributes	Business Requirements	High-level Threat	Business Impact	Impact Value	Potential High-level Vuln	Green Filed Vuln Value	Green Field Risk Cat
BD01	Maintaining the continuity of services, especially during the holiday period	Accessible Continuos Responsive Available Recoverable Scalable	Services (inclduing the main website, point of sale, and inventory systems) must be available to customers and employees on time and without unplanned interruptions.	Customers fail to make a purchase.	Customers move to another retailer, reducing Target's earnings Lost of customer confidence	H	Inadequate Business continuity and disaster recovery planning	M	B (Yellow)
				Employees fail to access inventory and customer information.	Inconsistent inventory resulting in reduced stored efficiency Inability to provide a tailored customer experience	H	Inadequate Business continuity and disaster recovery planning	M	B (Yellow)

Table 1 (continued).

BD02	Ensuring that information is accurate and available when needed	Accessible Accurate Consistent Current Duty segregated Reliable Timely Usable Continuous Private	Accurate business information must be availale to the authorized personnel timely and consistently	Disruptions on critical systems	Inability to create a tailored customer experience Inability to positvely different Target from other competitors	M	Inadequate control over privacy of information	H	B (Yellow)
				Unauthorized modification of critical business data	Inability to create a tailored customer experience Inability to positvely different Target from other competitors	M	Inadequate Business continuity and disaster recovery planning	M	B (Yellow)

Table 1 (continued).

BD03	Protecting Target's reputation	Trustworthy Consistent Competent Confident Credible	Must ensure a positive perception from customers, employees and business partners.	Customer and business information leaked and publicly disclosed in the media.	Lost sales Lost of partner confidence Lost of customer confidence Team member retention and recruiting difficulties	H	Inadequate control over privacy of information	H	A (Red)
BD04	Maintaining privacy and security of data stored, processed, and communicated by Target's systems related to customers, intellectual property, and third-parties.	Protected Confidenial Private	Target must protect customer, third-party and intelectual property information from unauthorized access	Customer and business information leaked and publicly disclosed in the media	Lost of partner confidence Lost of customer confidence Inability to positvely different Target from other competitors	H	Inadequate control over privacy of information	H	A (Red)

Table 1 (continued).

BD05	Ensuring that system security solutions comply with applicable law, standards, and best practices	Protected Consistent Continuous Compliant	Must comply with privacy laws, data protection standards and, to the possible extend, industry best practices.	Customer and business information leaked and publicly disclosed in the media	Lost of partner and customer confidence Fines from regulators resulting in reduced earnings	H	Inadequate control over privacy of information	H	A (Red)

Conclusion

Target’s primary business drivers relate to brand reputation and their ability to differentiate from competitors in providing customer service through data collection. Therefore Information security plays an essential role in enabling Target’s business strategy.

The five Business drivers identified in this paper and used to define the Business Risk Model can support the definition of control objectives aligned with Target’s core business requirements. Maintaining this relationship will allow the security strategy to help the business move forward efficiently.

References

Committee on Commerce, Science, and Transportation. (2014). *A "kill chain" analysis of the 2013 Target data breach*. United States Senate. https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

Schulz, D. P. (2020, July 1). *2020 Top 100 Retailers*. National Retail Federation. Retrieved November 7, 2020, from https://nrf.com/resources/top-retailers/top-100-retailers/top-100-retailers-2020-list

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise security architecture: A business-driven approach* (1st ed.). CRC Press. https://doi.org/10.1201/b17776

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017, January 18). Breaking the target: An analysis of Target data breach and lessons learned. *arXiv preprint arXiv:1701.04940*. https://arxiv.org/pdf/1701.04940.pdf

Target Corporation. (2013, December 19). *Target confirms unauthorized access to payment card data in U.S. stores* [Press release]. A bullseye view. Retrieved November 7, 2020, from https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car

Target Corporation. (2020). *2019 Target annual report*. https://corporate.target.com/annual-reports/2019