Target Corporation: Control objectives and mock security strategy

Daniel Cordeiro Marques

University of San Diego

CSOL-520-03-FA20 - Secure Systems Architecture

Dr. Michelle Moore

November 15, 2020

Target Corporation: Control objectives and mock security strategy

In the conceptual security architecture proposed by Sherwood et al. (2005), security practitioners can derive an overall security strategy using the contextual layer's business information. Leveraging the business attribute profiles as a starting point, the security practitioner can define control objectives to mitigate the business risks.

Cordeiro Marques (2020) defines five business drivers from Target's 2019 annual report (Target Corporation, 2020), along with potential vulnerabilities and associated impacts. Committee on Commerce, Science, and Transportation (2014) and Shu et al. (2017) provide additional insights on potential gaps that should be considered by a successful security strategy implemented by Target. This paper expands on the previous works by applying the SABSA conceptual security architecture to develop a mock security strategy that addresses the risks outlined in Cordeiro Marques (2020).

Method

Business Attributes and Control Objectives

The definition of control objectives for Target starts by establishing the Business Attribute Profile (BPA) for the company. The previous paper (Cordeiro Marques, 2020) defines a Business Risk Model (BRM) based on five business drivers (BD) and associated business attributes (BA) according to the information provided by Target's annual report (Target Corporation, 2020):

- BD01 - Maintaining the continuity of services, especially during the holiday period (BAs: Accessible, continuous, responsive, available, recoverable, and scalable).

- BD02 - Ensuring that information is accurate and available when needed (BAs: accessible, accurate, consistent, current, duty segregated, reliable, timely, usable, continuous, and private).
- BD03 - Protecting Target's reputation (BAs: trustworthy, consistent, competent, confident, compliant, and credible).
- BD04 - Maintaining privacy and security of data stored, processed, and communicated by Target's systems related to customers, intellectual property, and third-parties (BAs: protected, compliant, confidential, and private).
- BD05 - Ensuring that system security solutions comply with applicable law, standards, and best practices (BAs: protected, consistent, continuous, and compliant).

The BRM also established potential vulnerability and risks that could affect the company's ability to achieve its goals. Leveraging that information, Table 1 defines six control objectives derived from the Business Attribute Profile to mitigate the risks and address Target's business drivers' security needs.

Table 1.

Control objectives based on the BAP and the BRM proposed by Cordeiro Marques (2020, p. 7).

High-level control objectives	Business driver	Business attributes
Establish consistent business continuity and disaster recovery plans and procedures around sales-supporting services.	BD01, BD02, BD03	Accessible, available, competent, confident, consistent, continuous, credible, current, recoverable, reliable, responsive, scalable, timely, trustworthy, usable

Table 1 (continued).

Establish strong physical security around sales-supporting services, such as point-of-sales and backend servers.	BD01, BD02, BD03, BD04, BD05	Accurate, available, competent, compliant, confidential, consistent, continuous, credible, duty segregated, private, protected, reliable, responsive, timely, trustworthy, usable
Establish strong logical security around sales-supporting services, such as point-of-sales and backend servers.	BD01, BD02, BD03	Accurate, available, competent, compliant, confidential, consistent, continuous, credible, duty segregated, private, protected, reliable, responsive, timely, trustworthy, usable
Establish strong authentication and authorization processes and protocols to access systems supporting sales and storing customer data.	BD01, BD02, BD03, BD04, BD05	Accurate, available, competent, compliant, confidential, consistent, continuous, credible, duty segregated, private, protected, reliable, responsive, timely, trustworthy, usable
Establish consistent incident response procedures.	BD01, BD02, BD03, BD04, BD05	Accurate, available, competent, compliant, confidential, consistent, continuous, credible, private, protected, reliable, responsive, trustworthy
Establish a mechanism to monitor compliance with applicable laws, standards, and regulations.	BD03, BD04, BD05	Competent, compliant, confidential, consistent, credible, duty segregated, private, protected, reliable, trustworthy

The next step in developing a conceptual security strategy is assessing the current state of Target's security.

Current Security Status

A comprehensive security assessment requires a review of Target's processes, documentation, and technologies. However, as this information is not readily available, to assess the current security status, this paper uses publicly available information regarding the 2013 Target incident provided by Shu et al. (2017) and Committee on Commerce, Science, and

Transportation (2014) along with the BRM proposed by Cordeiro Marques (2020, p. 7) to derive opportunities for improvement that will guide the mock security strategy. The three topics below summarize the gaps identified when analyzing the references:

Security of point-of-sale systems. Attackers compromised point-of-sale systems and exfiltrated customer data from the Target environment, directly impacting business drivers BD03, BD04, and BD05. The security strategy must address the potential vulnerabilities affecting point-of-sale systems.

Third-party access. The attack against the Target environment started from a trusted third-party. The attackers leveraged this access and gained access to Target's network and sales systems, impacting all five business drivers. The strategy must address third-party privileges and access and incident response procedures.

Network segmentation. With the initial access to the network, the attackers reused usernames and passwords to access multiple systems and expand their foothold in Target's environment and into the point of sale systems. A similar event may impact all five business drivers; therefore, the security strategy must consider the segmentation between the corporate and sales systems.

As a result of this analysis, these three topics provide an initial direction to develop the security domain model.

Security Domain and Trust Model

Sherwood et al. (2005) define security domains as "a set of security elements subject to a common security policy defined and enforced by a single security policy authority" (p. 266). Target's environment comprises five domains:

Corporate environment domain. The corporate environment aggregates the entities, functions, and processes that support the business. Elements include corporate network devices, corporate computers, finance employees, and related data.

Cardholder data environment domain. PCI Security Standard Council (n.d.) defines the Cardholder data environment (CDE) as "the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data." This domain includes the point-of-sale systems, other people, processes, and technologies supporting the sales process.

Third-party domain. The third-party domain covers people, processes, data, and technologies related to contractors, suppliers, and other partners that lease store space, such as CVS and Starbucks.

Store domain. The store domain relates to security entities supporting the store operations, including the store network, personnel, and processes.

Intellectual property domain. The intellectual property domain includes people, systems, and processes supporting the development of Target-owned products, brands, and trademarks.

The data flow between these domains should be limited only to shared services. For instance, users of the intellectual property domain might use the company directory to provide authentication and authorization services.

Security Time Model

As this paper focuses on the five business drivers and associated control objectives previously outlined, the strategy must address timing concerns that support the following

business attributes: available, competent, compliant, consistent, continuous, responsive, and timely.

Store data lifetimes. Data retention policies should respect the applicable privacy laws, electronic records regulation, and the PCI standard.

Disaster recovery. Systems must be live seven days a week, 24 hours a day. In case of a disaster, downtime should not exceed one hour on regular hours and 30 minutes during the holiday season.

Performance. Security measures should not impact system performance significantly. The response time for applications supporting sales processes should not exceed 20 seconds.

A Mock Security Strategy for Target

The security strategy combines the details from the business attributes, control objectives, security domains, time, and trust models to derive the elements that will protect the business. For the Target case, the "zero trust" model (National Institute of Standards and Technology, 2020) addresses the gaps previously identified by establishing three characteristics: entities are not implicitly trusted, enforcing authorization and authentication before granting granular access to assets, and flexibility to allow non-standard network devices.

Identity Management, Authentication, and Access Control

The strategy applies role-based access control (RBAC) to elements in each domain. This service leverages data and asset classification combined with information from a centralized directory to provide authentication and authorization for all domains. The directory should store details on identities, credentials, roles, and status for each object.

The systems must generate log events and send them to a centralized server for failed and successful attempts to log in, access granted and denied to elements, and attempts to traverse the boundaries established by the security domains.

Micro-segmentation

All security domains must be segmented, allowing limited access to shared services only. The use of micro-segmentation enables the creation of different zones that surround each domain, and dataflow is permitted or blocked according to security policies dynamically established; this allows overlapping elements of different domains (such as point-of-sale systems and barcode scanners in the stores) to coexist in the same physical environment.

In particular, micro-segmentation must ensure that third-parties cannot access the corporate environment, the cardholder data environment, and systems storing and processing intellectual property.

Encryption

The application must apply encryptions according to the classification of data. For instance, systems must encrypt data related to the intellectual property and cardholder data environment domains at rest, in transit, and in use. Additionally, systems must encrypt authentication material at all times.

Incident Response and Disaster Recovery

Incident response capabilities must consider the analysis of incidents according to the information obtained, a response and recovery time that fits the business's time constraints, and a communication plan demonstrating transparency while protecting the brand.

Compliance Monitoring

Periodic assessments should be performed to identify gaps in security implementation and opportunities for improvement. The assessments must include, for instance, verification of retention times for sensitive information and compliance with applicable standards.

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

Cordeiro Marques, D. (2020). *Target Corporation: A business risk model based on the 2013 data breach*. University of San Diego.

National Institute of Standards and Technology. (2020). *Zero trust architecture* (Special Publication 800-207 ed.). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

PCI Security Standard Council. (n.d.). *CDE*. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms. Retrieved November 15, 2020, from https://www.pcisecuritystandards.org/pci_security/glossary

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