# CSOL520 Module 2 Assignment 2.1: Business Risk Model

John C. McGovern

University of San Diego

Table of Contents

## Summary

Below is a Business Risk Model based on the example provided in figure 9-8 of Enterprise Security Architecture: A Business-Driven Approach (2019). The example used for this model is based on the well-known and documented Target Corporation data breach (Krebs, 2015).

**Figure 1: Target Business Risk Model (Contextual Security Architecture)**

| 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 Vulnerability** | **Green Field Vuln Value** | **Green Field Risk Cat** |
| BD001 | Rise of Digital Business as a major means of customer engagement and revenue. | Revenue | Security in support of important and competitive digital business properties (i.e., target.com and Target Mobile App). | Digital Storefront and app-based purchases must be seamless, performant, and reliable while meeting industry security requirements. | Short-term cart abandonment. Loss of revenue.<br><br>Long-term customer attrition to competitors. | H | Client-side and server-side exploitation of web and mobile platform vulnerabilities. | H | A<br><br>(Red) |
| BD002 | Modernized storefront experience. | Experience | Target is building digital selling kiosks into modern storefront experience. These various kiosks use different platform and require storewide connectivity. | Vendor highlight kiosks require implementation of a variety of technologies and require store-wide connectivity and standardization between locations. | Loss of revenue.<br><br>Inability to leverage vendor partnerships and brand promotions. | M | Introduction of potentially untrusted third-party kiosk and display platforms into store environment. | M | B<br><br>(Amber) |
| BD003 | Real-estate management infrastructure modernization and Green initiative. | Infrastructure<br><br>Experience | Corporate real estate and infrastructure systems should be managed centrally and consistently across properties and geographies. | Need to integrate multiple infrastructure technology management technologies into stores and provide 3rd party vendor remote access. | Additional costs due to inefficient energy utilization.<br><br>Wide variety of management systems with required 3rd party access. | H | 3rd party contractors require access into energy management, HVAC, plumbing, and mechanical systems using their own systems from a variety of remote locations. | H | A<br><br>(Red) |
| BD004 | Uptime and business continuity in regard to core payment and register infrastructure. | Continuity<br><br>Trust | Stores must have payment stream / register redundancy to mitigate against loss of revenue. | Payment/transaction capabilities must support high levels of security as well as availability across stores in various regions. | Loss of revenue due to downtime. | H | Distributed register infrastructure.<br><br>Difficult to physically secure and patch in a timely manner. High criticality. | H | A<br><br>(Red) |
| BD005 | PCI regulatory compliance. | Compliance<br><br>Privacy<br><br>Trust | Required compliance with Payment Card Industry regulations and audit. | Payment card data must be stored and transmitted securely and meet compliance requirements. | PCI fines.<br><br>Loss of customer trust.<br><br>Revenue impact. | H | Customer card data must be collected, stored, and processed from thousands of locations securely and is a highly prized attack target. | H | A<br><br>(Red) |

# References

Krebs, B. (2015, September 21). *Inside Target Corp., Days After 2013 Breach*. Krebs on Security. https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Sherwood, J., Clark, A., & Lynas, D. (2019). Enterprise Security Architecture: A Business-Driven Approach. Routledge.