# Analysis of Enterprise Risk Management of Two Retail Industry Competitors

Christopher Furton

Syracuse University

Author Note:

Information provided in this report was gathered from publicly available reports, news articles, and press releases.  Analysis and assumptions are based off information available which may or may not adequately reflect present day corporate practices and processes.

# Abstract

The purpose of this report is to investigate the Enterprise Risk Management (ERM) programs of two retail industry competitors: Wal-Mart Stores, Inc. and Target Corporation. Through in-depth research on the overall retail industry as well as each individual company, this paper explores the fundamental bases for each ERM program including risk governance, risk identification, risk analysis and evaluation, risk treatment, business continuity planning, and disaster recovery.

Two specific risks, reputation degradation and cyber threats, are further investigated from the perspective of each company and a comparison is made analyzing the similarities and differences in respect to ERM. Furthermore, a review of the history of incidents for each company and each risk highlights several positive and negative aspects contributing to the evolution of the ERM programs. Additional analysis comparing both companies' ERM programs and history is provided culminating in three significant lessons learned.

Lastly, this paper introduces a hypothetical small to medium-sized retail company, develops an ERM program applying many of the lessons learned, and identifies some potential challenges. Both reputation degradation and cyber threat risks are incorporated into this company's ERM program and recommendations are made on best treatment options. Also, business continuity plans and disaster recovery is addressed particularly in response to the two identified risks.

Analysis of Enterprise Risk Management of Two Retail Industry Competitors

## Executive Summary

Enterprise Risk Management (ERM) is critical for companies within the US$22 trillion dollar global retail industry regardless of market position. Target Corporation, a 113 year old US-based and operated company, generated US$72,596 million of the industry total. Wal-Mart Stores, Inc., a 53 year old multinational giant, generated US$469,162 million of the industry total. Despite the different business strategies, both retailers face similar risks and, in some cases, employ similar mitigation. Conversely, the retailers have somewhat different ERM governance and risk identification processes. Either way, both retailers continue to evolve their risk programs based off history of incidents, risk exposure and an ever evolving risk appetite.

## Purpose

The purpose of this report is to investigate the Enterprise Risk Management programs of two retail industry competitors: Wal-Mart Stores, Inc. and Target Corporation. Through in-depth research on the overall retail industry as well as each individual company, this paper explores the fundamental bases for each ERM program including risk governance, risk identification, risk analysis and evaluation, risk treatment, business continuity planning, and disaster recovery.

Two specific risks, reputation degradation and cyber threats, are further investigated from the perspective of each company and a comparison is made analyzing the similarities and differences in respect to ERM. Furthermore, a review of the history of incidents for each company and each risk highlights several positive and negative aspects contributing to the evolution of the ERM programs. Additional analysis comparing both companies' ERM programs and history is provided culminating in three significant lessons learned.

Lastly, this paper introduces a hypothetical small to medium-sized retail company, develops an ERM program applying many of the lessons learned, and identifies some potential challenges. Both reputation degradation and cyber threat risks are incorporated into this company's ERM program and recommendations are made on best treatment options. Also, business continuity plans and disaster recovery is addressed particularly in response to the two identified risks.

**Key Findings**

- Wal-Mart and Target have significantly different business strategies and histories, but many of the same risks.
- Wal-Mart and Target employ different ERM governance structures with one having a bottom-up and the other a top-down approach.
- Risk leadership roles have evolved with each company throughout their history of incidents resulting in Target having a Chief Risk Officer and Wal-Mart assigning that duty to their Chief Financial Officer.
- Risk identification and analysis is different between the companies where Target relies heavily on executives and Wal-Mart utilizes a committee and identification workshops.
- Target and Wal-Mart define reputation risk in two different ways. Target identifies a standalone reputation risk and recognizes several other risks that are contributing factors. Walmart joins reputation risk with competitive risk creating a combined category.
- Despite *differences* in the definition of reputation risk, both companies employ *similar* risk treatment strategies involving public relation campaigns in proactive and reactive ways.

- Target and Wal-Mart define cyber threat risk as two separate risks: loss of information systems that support business functions and the loss of private customer and employee information.
- Despite *similarities* in the definition of cyber threat risk, both companies employ *different* risk treatment strategies including data segregation through redundant duplicate systems or risk transference via insurance.
- Both companies have experienced reputation risk throughout their histories; however, Wal-Mart’s risk is persistent requiring ongoing and innovative public relations treatment. Conversely, Target’s risk is more recent and in response to a specific incident: the 2013 Data Breach.
- Both companies have experienced cyber threat risks; however, Wal-Mart’s security breach in 2005/2006 did not trigger reporting requirements.  Target’s security breach in 2013 received unprecedented publicity highlighting a connection between cyber threat risks and reputation risks.
- After the 2005/2006 security breach, Wal-Mart implemented many of the same cyber threat responses that Target is now implementing in 2015.
- Three significant Lessons Learned:
    - It is critical for companies, particularly those within the same industry, to learn and grow from the mistakes and incidents of others.
    - Enterprise Risk Management programs can vary greatly from company to company often based on organizational culture and leadership styles.  There is no “one size fits all” solution to risk management.

- A company's perspective on ERM and appetite for risk comes in part from their historic risk exposure and serious risk-related catastrophes.

## Background

Companies in the retail sector sell a wide range of products to include food, apparel, hardware, household goods, and office supplies. Many companies operate under a business-to-consumer (B2C) model as well as a business-to-business (B2B) model on both National and International settings. Currently, a third of the 250 largest retail companies in the world are based in the United States followed by Europe and then Japan. Globally, the retail industry exceeded US$22 trillion in 2014 with projections up to US$28 trillion in 2018 (FirstResearch, 2015, p. 2).

Within the retail industry, demand is driven by three main factors: personal income, consumer confidence, and interest rates. Profitability often depends on efficient supply chain management and effective merchandising. Marketing is also a significant factor affecting profitability (FirstResearch, 2015, p. 2).

Information Technology supports most operations within the retail industry where point-of-sale (POS) systems records sales transaction and processes payments. These POS systems fully integrate with inventory, forecasting, purchasing, payroll, finance and accounting functions. Some retailers place orders with manufacturers electronically using the Electronic Data Interchange (EDI) format which is sometimes accomplished automatically using replenishment systems. These systems are often linked from individual stores up to corporate offices to access real-time sales data. Furthermore, Enterprise Resource Planning (ERP) systems connect retailers to manufacturors, distributors, and transportors enabling Just-in-Time merchandising (FirstResearch, 2015, p. 3).

According to First Research (2015), one of the top issues facing the retail industry is data security (p. 4). Retailers are focused on security flaws within Information Technology after several major retailers fell victim to malicious hackers stealing customer information and financial records. These breaches have had a secondary impact on retailers' reputations causing major companies to focus on winning back the trust of consumers (FirstResearch, 2015, p. 4).

In a survey by Accenture (2011) of 397 companies, a growing concern has been identified about the broad spectrum of risks facing the retail industry: reputational risk, particular due to supplier ethics and quality, being one of the major concerns (p. 6). Additional risks include managing credit risk and integrating market risk with finance. Lastly, regulatory risk regarding privacy issues and protection of customer databases rated amongst the top areas of concern for retail companies (Accenture, 2011, p. 6). One of the business challenges for companies in the retail industry is protecting customer information, especially for retailers using older technology. Retailers often access and store confidential customer information using loyalty programs or company-issued credit cards which introduces substantial risk from crime-related losses (FirstResearch, 2015, p. 8).

Retail industry wide, Enterprise Resource Management adoption is high compared to other industries. "Fifty-seven percent of retail survey respondents described risk management as a source of competitive advantage … compared with 44 percent for the average of all industries and just 37 percent for consumer goods and services. Retailers are also more likely than the survey average (86 percent versus 76 percent) to indicate that risk capabilities have helped achieve sustainable profit growth" (Accenture, 2011, p. 6).

## Target Corporation

Target, headquartered in Minnesota and founded in 1902, is significantly smaller than Wal-Mart. It operates 1,917 large-format general merchandise and food discount stores in the United States and Canada including 289 Target general merchandise stores, 251 SuperTarget stores, and 8 CityTarget stores. Target operates 40 distribution centers, with 37 in the US and 3 in Canada, through which food and general merchandise passes for both supply chain functions and e-commerce shipments to customers. Target undertakes international sourcing operations as part of its supply chain including several private-label product lines (Canadean, 2015, p. 24). During fiscal year 2014, Target reported revenue of US$72,596 million with annual decline of .96% and operating margins of 5.21% (Canadean, 2015, p. 6)

Target is broken down into two divisions: US Retail and Target Canada. In 2014, the US retail division accounted for 98.2% of the company's total revenue. The company classifies product offerings into five categories: Household Essentials, Hardlines, Apparel and Accessories, Food and Pet Supplies, and Home Furnishings and Décor. The company offers products from private-labels as well as exclusive brands. In 2014, the Household Essentials accounted for 25% of total sales followed by Food and Pet Supplies at 21%. As part of the US Retail division, Target operates a fully integrated online business as well as a credit card servicing segment through its branded proprietary credit cards. The US Credit Card segment accounted for 1.83% of total revenue for the company (Canadean, 2015, pp. 24-25).

Target Canada was classified as its own separate segment in FY2011 with a startup investment of US$74 million (World Market Intelligence, 2014, p. 6). In August of 2013, this division operated 68 stores in Canada but quickly grew to 133 by 2015 with a total of US$932 capital expenditure (Canadean, 2015, pp. 24-25; Target Public Affairs, 2015, p. 1). However, according to a press release from Target Public Affairs (2015), Target plans to discontinue Canadian operations and has filed for protection under the Companies' Creditors Arrangement Act with the Ontario Superior Court of Justice (p. 1).

An assessment of Target's Strengths, Weaknesses, Opportunities, and Threats (SWOT) identifies three weaknesses: limited financial leverage, product recalls, and patent infringements. Product recalls may affect the company's brand image and reputation especially when the recall affects a private-label product. Also, lawsuits over intellectual property and discriminatory hiring practices have the potential to hurt both the company's cost structure but also its image. In addition to weaknesses, several threats were identified relating to changing consumer preferences, expansion by competitor, and the counterfeit goods market (Canadean, 2015, pp. 27-29). Figure 1 shows the full SWOT analysis.

Target Corporation has a unique culture that can be both a strength and a weakness. The company's strong heritage has arguably made it one of the most trusted brands in the north-eastern states of the US. It has strong insight into the retail industry with ties to suppliers facilitating procurement of merchandise on reasonable terms. All this helps Target achieve a loyal customer base built on trust (Canadean, 2015, p. 27). However, the culture is being challenged due to recent incidents discussed later in this paper. As reported by USA Today (2014), a Target corporate employee went public with an anonymous letter emphasizing the need for serious change in leadership and culture (p. 1).

**Wal-Mart Stores, Inc.**

Wal-Mart is considered the world's largest retailer (FirstResearch, 2015, p. 5). Headquartered in Bentonville, Arkansas and founded in 1962, Wal-Mart operates discount stores, supercenters, neighborhood markets, and club stores totaling 245 million customers every week. Globally, Wal-Mart operates 10,733 stores under 69 different banners in 27 countries. In the United States, Wal-Mart operates 4,625 locations. Wal-Mart operates 318 distribution facilities worldwide with 158 in the United States (World Market Intelligence, 2015, p. 5). In 2013, the company reported revenue of US$469,162 million dollars with annual growth of 4.97% and operating margins of 5.93% (World Market Intelligence, 2015, p. 1).

Wal-Mart is broken down into three business segments: Wal-Mart US, Wal-Mart International, and Sam's Club. In 2013, the US segment generated 58.89% of Wal-Mart total revenue. The US segment classifies product offerings into merchandise units consisting of Grocery, Entertainment, Health and Wellness, Hardlines, Apparel, and Home with the Grocery Unit generating 55% of total revenue for that segment and 11% each from Entertainment and Health (World Market Intelligence, 2015, p. 6).

Wal-Mart International generated significantly less revenue in 2013 for a total of 29.01% despite operating a larger number of locations. This segment operates through subsidiaries in Americas, Europe, Africa, and Asia and its joint ventures in Asia. Operations within Wal-Mart International fit within three segments: Retail, Wholesale, and Other. These units are further broken down into formats including discount stores, supermarkets, hypermarkets, warehouse clubs, apparel stores, and even restaurants that operate in Chili, Japan, and Mexico (World Market Intelligence, 2015, p. 6).

Wal-Mart's last business segment, Sam's Club, accounted for 12.10% of the company's total revenue in 2013. This business segment operates members' only warehouse clubs serving both individuals and businesses. It operates 621 stores in 47 of the US states and Puerto Rico. Its products are classified into five categories: Grocery and Consumables; Fuel and Other; Technology, Office and Entertainment; Home and apparel; and Health and Wellness. Similar to the Wal-Mart US, Grocery and Consumables accounted for 55% of revenue for this segment (World Market Intelligence, 2015, p. 6).

An assessment of Wal-Mart's Strengths, Weaknesses, Opportunities, and Threats (SWOT) identifies legal proceedings as one of only two weakness concern areas. The other weakness involves lobbying efforts in the Indian market and allegations of violating the Foreign Exchange Management Act. Both of the two identified weaknesses have potential to impact the brand image and reputation of the company. In addition to weaknesses, several threats were identified relating to manpower costs, foreign exchange rates, intense competition, and organized retail crime. Figure 2 shows the full SWOT analysis.

## ERM Governance

### Target Corporation

Target Corporation has an enterprise-wide risk program; however, it is currently undergoing an overhauling process. With the assistance of a consulting firm, Target is currently evaluating their "technology, structure, processes and talent" as part of a transformation (Wallace, 2014, p. 1). This transformation resulted in the creation of two new executive positions: Chief Information Security Officer and a Chief Risk and Compliance Officer. According to Target Public Affairs (2014a, 2014b), both positions have been filled with former executives from General Motors. Due to a recent incident (see: History of Incidents), Target decided to elevate the role of key positions involving risk management (Target Public Affairs, 2014a, p. 1).

In 2009, Target Corporation strengthened its efforts to create an enterprise-wide risk program with a top-down perspective for its most strategic risks. At the time, Target found that the majority of its current risk efforts were being spent on compliance, operations, and financial stability and not focused on integration of strategy and risk. Under this program, Target separated the ERM function from the internal audit and finance functions and collocating it with legal, compliance, sustainability, and fraud investigation functions underneath the Corporate Risk and Responsibility (CR&R) division. The CR&R division reported through the Executive Vice President of General Counsel to the Chief Executive Officer.

Target's ERM program identified four main objectives: "1. Enhance Risk Awareness and Dialogue, 2. Reduce Operational Surprises and Losses, 3. Align Risk Appetite and Strategy, 4. Anticipate and Manage Cross-Company Risks." These high-level objectives had to fit into Target's unique culture prompting target to take pre-planned steps to achieve that integration (NC State University, 2010, p. 2).

When Target first developed their ERM program in 2009, the ERM staff compiled a summary of major risk exposures facing the company. This resulted in a listing of the top 20 risks that were reviewed and reduced to the top ten through executive committee dialogue. Those ten risks were then sorted into three risk themes: market related (5 risks), internal drivers (3 risks), and external drivers (2 risks). It was Target's belief that the external driver risks could only be monitored so the focus was on the internal driver and market-related risks. Finally, if the risk was adequately addressed by existing processes, it was assigned an inactive category while those not addressed at all were assigned an active category. The purpose of this was to allow prioritization of high risks (NC State University, 2010, pp. 2-3).

The last step in Target's risk identification and analysis stage involved review by the nine executives and the Chief Executive Officer. The executives were divided into teams to determine how important each risk is to the future of Target and to assign a level rating for discomfort with current controls, strategy, and management approach for that risk. The outcome highlighted the different views amongst the executive staff and the Chief Executive but provided needed insight ultimately reassuring executives that an enterprise-wide risk management program was in the best interest of the company (NC State University, 2010, p. 3).

### Wal-Mart Stores, Inc.

Wal-Mart's Enterprise Risk Management dates back to the 1990s when then Chief Financial Officer John Menzer recommended creation of the program. Throughout the early 2000s, the ERM program utilized a bottom-up, grassroots approach without a company-wide mandate from senior management directing everyone to adopt ERM (Atkinson, 2003, pp. 36-38). As of 2007, the ERM program is part of the audit group with support from the treasury. A risk management committee makes recommendations to the board of directors concerning policy options (Gamble, 2007, p. 42).

At Wal-Mart, the ERM process is broken down into five steps. The first step, Risk Identification, begins with clearly identified business objectives. Information is gathered from senior leadership identifying the top five risks that will keep them from meeting those business objectives over the next 18 to 24 months. This results in a listing of 20 to 30 risks which are taken into a four- to five-hour risk identification workshop where consensus is achieved on the top four or five risks (Atkinson, 2003, p. 36).

During the risk identification workshops, risks are based on seven categories broken down into either internal or external risk subcategories. External risk categories are identified as legal/regulatory, political and business environment. Internal risk categories are identified as financial, strategic, operational, and integrity. Wal-Mart then utilizes a risk map to evaluate risks on an XY-axis charting probability and impact in order to prioritize what are seen as Wal-Mart's biggest risks (Atkinson, 2003, p. 36).

After risks are identified, the second step of the five-step process, Risk Mitigation, begins with another facilitated workshop. Here, the three to five most important risks are further defined and quantified. A project team is created that conducts an initiative inventory of the procedures already in place that may address the specific risk and evaluates those mechanisms (Atkinson, 2003, p. 38).

The third step of the five-step process, Action Planning, occurs within the project teams for each risk. These teams meet and create simple project plans that assign responsibility and actions to people to mitigate those risks. Those project plans assign metrics, which is identified as the fourth step, that measure results as having either a positive or negative impact on the identified risks. This is achieved by identifying the target performance compared to the actual performance over time (Atkinson, 2003, p. 38).

The final step of the five-step process, Shareholder Value/Return on Investment, is to evaluate whether or not the project increased shareholder value through an increase in sales or a decrease in expenses. Through this overall five-step process, Wal-Mart believes that they are more focused on what major risks exist and what they can do about them. Wal-Mart feels their ERM program is not an "enlightenment process" where ERM professionals go into business units and identify risks that they are not familiar with. Rather, the ERM professionals help them identify and focus on the few that are most important to address (Atkinson, 2003, pp. 38-39).

## High Impact Risks – Cyber and Reputation

Although retail companies, including Wal-Mart and Target, face many risks, this paper will analyze two that affect both companies in similar yet different ways. First, this paper will review risks related to reputation degradation caused by a range of situations. Then, this paper will look further into cybercrime risks, including cyber intrusion or hacking, as well as protection of personal private information. Finally, a compare and contrast will show how each company addresses these risks.

## Reputation Degradation at Target Corporation

"It takes years to build a first-class corporate reputation and image in the marketplace" (Parekh, 2007, p. 26). According to Target's director of risk management in 2007, risk managers ought to engage staff throughout the company for reputational risk management since threats to a company's reputation come from a variety of sources including product recalls, privacy breaches, and executive misconduct (Parekh, 2007, p. 26). Eight years later, both Target and Wal-Mart have seen instances of those risks affect business operations.

At Target, reputational risk has the attention of the Board of Directors through the Corporate Responsibility Committee. Within this committee, the members review and evaluate the company's public affairs, community relations, corporate social responsibility, and reputation management programs. This committee, chaired by a member of the Board of Directors Mr. Kenneth Salazar, is primarily responsible for reputational risk (Target Corporation, 2014a, p. 11). This shows high level involvement at the board level specifically in reference to reputational risks.

In a 2014 filing with the Security and Exchange Commission, Target identified reputational risk as a standalone risk but also recognizes that reputational risk should be looked at as having many contributing factors that could be monitored and mitigated. As a standalone, Target identified positive perceptions as critical for continued success, stating that, if eroded, those perceptions could affect business and relationships with guests (customers) and team members (employees). Particularly, Target identified three signpost indicators to observe: adverse mainstream media publicity, adverse social media publicity, and governmental investigations or litigation. An increase in these indicators could lead to tangible adverse effects, namely boycotts, lost sales, loss of new store development opportunities, or team member retention and recruiting difficulties (Target Corporation, 2014b, p. 5).

One contributing factor for Target's reputation risk is to "successfully develop and maintain a relevant and reliable multichannel experience for our guests" (Target Corporation, 2014b, p. 5). With this risk, Target is concerned about keeping pace with evolving technologies to provide the desired multichannel customer experience. Failure within this risk results in a chain of events leading to loss of guest confidence, loss of sales, and exposure to fraudulent purchases that culminates in adverse impact on reputation (Target Corporation, 2014b, pp. 5-6).

Another contributing factor for Target's reputation risk is the "failure to address product safety concerns [that] could adversely affect [their] sales and results of operations" (Target Corporation, 2014b, p. 7). As shown in Figure 2, a SWOT analysis identified a weakness involving product recalls. Target developed mitigation strategies by requiring vendors to comply with product safety laws but are dependent on vendors to ensure product safety.

The last contributing factor for Target's reputation risk is their "efforts to protect the security of information about [their] guests and team members" from cybersecurity data breaches (Target Corporation, 2014b, p. 7). Although more information on this risk is provided later in this section, Target risk managers identify this risk as directly impacting reputational risk. According to Target Corporation's 2014 Annual Report, the company believes the greatest risk to their business arising out of the data breach in 2013 is the negative impact on reputation and loss of confidence of the guests (Target Corporation, 2014b, p. 10).

As expected, Target does utilize mitigation strategies to minimize residual risk associated with reputational damage. Actions directly related to mitigating the standalone reputation risk can be seen through programs designed to reinforce the company’s commitment to integrity and ethical culture. The Corporate Responsibility Report (2013) identifies the need to maintain reputation with team members, guests, communities, and shareholders and stresses the importance of “uncompromising ethics” (p. 83). Additional reputation-enhancing risk mitigation activities are evident through Target’s recent effort to publicize corporate volunteer efforts and giving back to the community through headline articles like “Target Donates $100,000 for Tornado and Flood Relief in the South” and “Target and Major League Baseball Team Up For Education” (Target Public Affairs, 2014e, 2014c). As states in Canadean (2015), Target is “committed to, and actively engaged in, activities to restore [customer] confidence” (p. 20).

## Reputation Degradation at Wal-Mart Stores, Inc.

Wal-Mart identifies reputational risk similar to Target; however, the company groups reputational risk with competitive risks. This method of defining reputation and linking it to competitiveness results in defining a couple specific risks that, if handled properly, can result in a net positive reputational gain. For example, Wal-Mart’s first risk is the “failure to attract and retain qualified associates, increases in wage and benefits costs, changes in laws and other labor issues could materially adversely affect [their] financial performance” (Wal-Mart Stores, Inc., 2014, p. 22). With this risk, Wal-Mart identifies that qualified employees have a direct correlation to reputational risk where, in essence, the qualified employee risk becomes a contributing factor to reputational risk. Furthermore, Wal-Mart identifies several external factors that can be monitored for gauging risk associated with quality employees: “the availability of a sufficient number of qualified persons in the work force of the markets in which we are located, unemployment levels within those markets, prevailing wage rates, changing demographics, health and other insurance costs, and adoption of new or revised employment and labor laws and regulations" (Wal-Mart Stores, Inc., 2014, p. 22). Having these correlations allows Wal-Mart to monitor many different external factors, some of which are controllable and others are not, that ultimately impact the company's Competitive and Reputational risk.

Another risk that Wal-Mart identifies as a Competitive and Reputational risk is the failure of technology-based systems preventing customers from effectively shopping online impacting e-commerce operations. In this instance, Wal-Mart identifies the multi-channel retail environment as critical to maintaining competitive advantage; however, the company takes it one step further identifying the loss of e-commerce functionality as having a direct impact to the company's reputation beyond the loss of sales revenue. This distinction is important as it shows that the company recognizes how interconnected their reputation in is with online communities which includes the company identifying social media as an area of focus where the company can "interact with customers and as a means to enhance their shopping experience" (Wal-Mart Stores, Inc., 2014, p. 23).

In addition to risks identified as Competitive and Reputational, the company also identifies several contributing factors or other risks that has an effect on Wal-Mart's reputation. Data and Privacy risks are highlighted as having an impact on reputation. Although this risk is not categorized as reputational, the company recognizes the correlation which opens up a realm of potential opportunities. For example, the company can use risk indicators associated with heightened cyber activity – an easily quantifiable metric – as a signal to a potential reputational risk event.

Like Target, Wal-Mart employs reputational risk mitigation strategies in the form of public relations campaigns. One notable campaign from Wal-Mart is known as the "Made in America" campaign that serves as a reminder of the retailer's commitment to American jobs and manufacturing to counteract negative publicity over imported products and poor working conditions at Wal-Mart-contracted manufacturing companies (Sherman, 2013).

Wal-Mart also publishes a “Global Statement of Ethics” report, conveniently available through the company’s Wal-MartEthics.com website, that indicates that the Wal-Mart board of directors and all associates at every level of the organization are committed to “upholding ethical behavior” and “willingness to speak up for the highest standards” because it “demonstrates [they] care about Wal-Mart, [their] reputation and [their] customers” (Wal-Mart Stores, Inc., 2015, p. 2). The statement of ethics specifically identifies two “Global Corporate Brand Reputation Risk” conditions that meet immediately reportable criteria to the company’s Global Ethics organization: “threats to human life, slave or forced labor, human trafficking, or child labor” and “serious criminal misconduct” including price fixing, insider trading, money laundering, and export violations (Wal-Mart Stores, Inc., 2015, p. 9).

## Cyber Risks at Target Corporation

Target identifies efforts to “protect the security of information about [their] guests and team members” as a top 20 risk. The identification of this risk is broad in nature not limiting to cyber-related data breaches; however, the wording focuses on techniques used “to obtain unauthorized access, disable or degrade service, or sabotage systems.” Target corporation further identifies this risk as being difficult to detect for long periods of time and that the company may be unable to “anticipate these techniques or implement adequate preventative measures” (Target Corporation, 2014b, p. 7).

Target also identifies a second risk, the “significant disruption in [their] computer systems and [their] ability to adequately maintain and update those systems could adversely affect [their] operations and [their] ability to maintain guest confidence” (Target Corporation, 2014b, p. 8). With this risk, Target distinguishes the loss of system functionality for core services such as servicing credit card accounts, processing guest transactions, communication with vendors, as well as unimpeded access to the Internet from the previous risk of loss of guest and employee information (Target Corporation, 2014b, p. 9). This is an important distinction as the two risks may be triggered by the same event or they could be mutually exclusive.

To mitigate the second risk, Target acknowledges making significant technology investments that help maintain and update existing systems; however, those mitigation steps also introduce the possibility of further system disruption, potential problems, and reduced operational efficiency. Related to this, Target identifies another risk associated with outsourcing of information technology to India where socio-political factors such as political, environmental and health may adversely affect operations for stability and maintenance of digital channels and IT development (Target Corporation, 2014b, pp. 6,8-9).

One significant cyber risk mitigation strategy the Target implemented in 2014 was the creation of a new C-level position responsible for cyber security. This position, the Chief Information Security Officer, is responsible for the company’s “information security and technology risk strategy helping to ensure that the company, its guests and team members are protected from internal and external information security threats” (Target Public Affairs, 2014b, p. 1). This position reports directly to the Chief Information Officer (CIO).

Target identifies several risk mitigation measures currently in place including “enhanced monitoring, segmentation, logging, and security of accounts and installation of application whitelisting on point-of-sale systems” (Target Public Affairs, 2014b, p. 1). Additionally, Target maintains $100 million of network-security insurance coverage with a $10 million deductible (Canadean, 2015, p. 20). Lastly, Target plans to make capital investment to equip proprietary credit cards and US store card readers with chip-enabled technology by first quarter 2015 (Canadean, 2015, p. 20)

**Cyber Risks at Wal-Mart Stores, Inc.**

Like Target, Wal-Mart separates cyber risks into two distinct categories: one for data privacy and the other for loss of systems. The first risk, Data and Privacy, is defined as any “failure to maintain the security of the information relating to our company, customers, associates and vendors that [they] hold” could incur substantial additional costs and subject them to litigation (Wal-Mart Stores, Inc., 2014, p. 23). Wal-Mart recognizes the rapidly evolving and increasing sophistication of hackers stating that Wal-Mart may not be able to adequately anticipate those threats. Furthermore, Wal-Mart acknowledges that “computer hackers, cyber terrorists, and others make numerous attempts to access the information stored in [their] systems” (Wal-Mart Stores, Inc., 2014, p. 23).

In defining Data and Privacy risk, Wal-Mart makes an important distinction by including not just internal systems, but also third-party service providers, vendors, and employee malfeasance as potential sources of exposure. Because the company operates globally, additional factors are considered; specifically, secure transmission of confidential information over public networks and cashless payments (Wal-Mart Stores, Inc., 2014, p. 23).

The second risk, Information System Risk, is defined as the disruption of both primary and secondary (back-up) systems that affect their ability to process transactions, summarize results, and manage the business. Wal-Mart recognizes several factors that could contribute to this risk including power outages, telecommunication failures, malware, offensive cyberattacks, as well as catastrophic events such as fires and earthquakes (Wal-Mart Stores, Inc., 2014, p. 21).

However, Wal-Mart's usage of a primary and secondary system greatly reduces the probability of complete system outage.

As a related risk, Wal-Mart identifies a risk associated with system upgrades as part of their initiatives to transform IT processes and systems and establish common processes across lines of business. The company acknowledges a potential increase in risk caused by system disruption during these upgrades; however, this risk is mitigated by through use of a change management system (Wal-Mart Stores, Inc., 2014, p. 22).

To mitigate the overall cyber risks, Wal-Mart acknowledges having "substantial security measures to protect, and to prevent unauthorized access to, such information and have security processes, protocols and standards that are applicable to [their] third-party service providers to protect information from our systems to which they have access." Additionally, Wal-Mart utilizes several technical risk reduction strategies such as operating a secondary independent, redundant, and physically separate information system for back-up purposes (Wal-Mart Stores, Inc., 2014, pp. 21,23). This risk reduction strategy protects Wal-Mart from the second risk related to loss of information systems but not data privacy risk.

## Compare and Contrast

Both Target and Wal-Mart identify reputational and cyber risks within their Securities and Exchange Commission 10-K Annual Reports; however, there are some differences in how each company defines these risks and their treatment strategies.

One significant difference is how the companies define and analyze reputational risk. Target lists reputation as a standalone risk but also makes connections with other risks that will have a secondary effect on brand reputation. In contrast, Wal-Mart combines reputation risk with competitive risk resulting in a more distinctive connection between loss of competitiveness and a negative impact on reputation. On a more micro-level, both companies have similar concerns over reputation; specifically, protecting customer data and ensuring successful multi-channel customer experience. However, there are some differences; namely, Target identifies product recalls as a factor affecting reputational risk whereas Wal-Mart identifies qualified employees as a factor.

As expected, both companies utilize public relation campaigns to mitigate reputation risk. Those campaigns are both risk reduction efforts as well as disaster recovery initiatives in direct response to an incident. For example, Wal-Mart led a pre-emptive public relation initiative to improve the brand image called “The Real Wal-Mart” that highlights how Wal-Mart helps customers, associates, and communities (Heller, 2013). In response to negative publicity over data protection measures, Target launched a campaign after its 2013 data breach (see History of Incidents section) that included full page newspaper advertisements apologizing for the attack and public interviews with then CEO Gregg Steinhafel (Kerber, Wahba, & Finkle, 2014).

In terms of cybersecurity, both companies identify two different risks: protection of private data and loss or degradation of information technology systems. With these risks, the differences come down to the companies’ risk treatments. Wal-Mart has implemented a secondary information technology architecture that is physically separated from the primary which, if properly architected and administered, adds substantial redundancy and protection from system outages. In contrast, Target acknowledges having recently added network segmentation but does not identify a complete secondary back-up system.

Another risk treatment, transference, is discussed by Target. Through the use of a cyber-insurance policy, Target financially protects itself against loss caused by data breach or network disturbances. Coverage amounts between US$300 and US$350 million were possible; however, due to increase in incidents, coverage amounts have dropped and premiums have increased. According to Greenwald (2014), retailers often obtain policies from several insurers to obtain the capacity needed; however, the cost dynamics are in flux with increases in retention and higher rates (p. 1).

## History of Incidents

Both Target and Wal-Mart have a history of Enterprise Risk Management that initiated in response to an adverse situation or event. Target's initial push into ERM back in 2009 was the result of a "proxy contest" that caught the organization somewhat by surprise. The Board of Directors and Management realized that a "more explicit and focused effort on identifying emerging risks would be valuable and strategic for the organization." This event led to the realization that there was a lack of dedicated resources assigned to evaluate potential emerging risks and that management needed better risk indicators signaling potential problems on the horizon (NC State University, 2010, p. 1).

In addition to the "proxy contest" event, the 2008-2009 economic recession caused Target to evaluated and modify its current business model. Previously, it depended on purchasing land near neighborhoods, building stores, and collecting revenue leaning heavily on previously established reputation. This model was modified during the recession which introduced new and different risk exposures not seen with the previous business model. This change, along with SEC regulation and external drivers, such as the Standard and Poor's evaluation of risk oversight practices, led Target to create a formalized ERM program (NC State University, 2010, p. 1).

In 2012, three years after Target assembled the ERM program, a Senior Architect evaluated the progress that Target made with risk management specifically from an information architecture perspective and assigned a maturity value of 2.5 out of 5. Furthermore, he identified challenges obtaining executive buy-in and issues involving communication of IT risk management concepts to business leaders (Parizo, 2012, pp. 1-2). These issues could have been indicators that Target's enterprise risk program was not performing well.

One year later in late 2013, Target experienced two of their top risk in what later became known as "The Data Breach." This single event went undetected for several weeks resulting in a loss of private data as well as an adverse impact to system availability during disaster recovery. Additionally, the company faced more than 80 civil lawsuits filed by customers, employees, and shareholders. Lastly, state and federal authorities are still investigating the source of the attack as well as Target's contingency planning and response (Target Corporation, 2014b, p. 7).

Target was heavily scrutinized for the response to the 2013 Data Breach. Target received advance warning of a potential data breach from a malware detection tool developed by the security research company FireEye. "Target apparently didn't have an incident response plan, so it was unprepared to act quickly when presented with a critical event" (Verschoor, 2014, p. 12). Although Target does not publicly acknowledge the lack of a contingency plan for cyber risks, in the months following, the company detailed significant steps it took to enhance its information security systems and processes while transforming its security and compliance structure and practices. Examples of this included enhancing monitoring, segmentation, logging, and security of accounts and installation of application whitelisting on point-of-sale systems (Target Public Affairs, 2014b).

Although Target's actions leading up to and during the Data Breach were heavily scrutinized, Target's response afterwards met industry expectations. Target contacted law enforcement including both the Federal Bureau of Investigation and the Secret Service (Target Corporation, 2014b, p. 17). Additionally, Target notified customers of the breach and, considering the company was involved in an ongoing criminal investigation, it still provided relevant information when possible through press releases and full-page newspaper announcements (Kerber, Wahba, & Finkle, 2014). Also, Target offered 12 months of identity protection through Experian for affected customers (Target Public Affairs, 2014d). Lastly, further reducing residual risk, Target had several insurance policies in place for cyber-related mishaps (Greenwald, 2014, p. 1).

Target's reputation was also affected due to the 2013 Data Beach. Target experienced significant negative comparable sales; however, precise quantification is infeasible due to a broad array of competitive, consumer behavior, and weather factors (Canadean, 2015, p. 20). Now 18 months later, Target is still fighting to re-polish the corporate brand and regain the trust of consumers. Unfortunately for Target, smaller instances keep reaching the media making the process more difficult. For example, a mid-level corporate employee published an "anonymous rant" that achieved significant publicity detailing failures within Target's management practices and culture (Malcolm, 2014). Also, Target received negative publicity that impacted reputation during a corporate restructuring where 40 new employees were terminated two weeks before their expected start dates (Mudd, 2015). Regardless, Target's Chief Marketing Officer, Jeff Jones, best addressed these issues with this statement: "Target is not the first brand in history to hit a rough patch, and we won't be the last brand to do what it takes to recover" (Malcolm, 2014).

In Summary, Target has experienced several incidents where identified risks became reality for both cyber situations and reputational impact. Although details over exact business continuity plans or disaster recovery plans are not known, analyzing the company's actions in response to these risks indicates the existence of some level of formal planning particular with respect to cyber-incident insurance coverage. Unfortunately for the company, media coverage has continued to plague their return to stasis.

Like Target, Wal-Mart's ERM program developed in response to incidents. One particular incident in 2005/2006 is one of the earliest reported cyber events against retailers. Wal-Mart acknowledged being hacked in what it called an "internal issue," but was fortunate that no sensitive consumer data had been stolen. In this case, cybercriminals attempted to access Wal-Mart's point-of-sale systems but were identified when one of them accidentally crashed a critical server. At the time, Wal-Mart had a number of security vulnerabilities including unencrypted credit card data and customer purchasing data, all stored on inter-connected networks (Zetter, 2009, pp. 1-2).

Based off limited public information, one could assume that Wal-Mart was not prepared for this type of risk. Several administrative and procedural errors were identified including failure to terminate system access to former employees and inadequate system audit logs. In response, Wal-Mart initiated major system upgrades to "segregate the data, to make separate networks, to encrypt it fully from start to finish through the transmission" (Zetter, 2009, p. 1). Wal-Mart's early cybersecurity breach likely resulted in the current design of their systems that provides robust cyber risk mitigation. As of 2014, Wal-Mart acknowledges that their network systems have faced numerous hacking attempts but unauthorized access was prevented (Wal-Mart Stores, Inc., 2014).

Although Wal-Mart is well-positioned to handle cyber risks, the company struggles with reputational risk. In 2005, two advocacy groups formed to unite against Wal-Mart: Wake-Up Wal-Mart and Wal-Mart Watch. These two groups leaked internal documents, setup smear campaigns through their websites, and highlighted unethical business practices and policies (Arthur W. Page Society, 2011, pp. 7-8). Highly publicized criticisms gained media attention over gender discrimination, employee relations and workers' rights, and blamed the company for leading an "assault on families and American values" (Arthur W. Page Society, 2011, p. 13).

In response to this reputational risk, in 2005, Wal-Mart hired a team of 35 consultants from New-York-based Edelman Public Relations along with political advisors and lobbyists aimed at three functions: promote, respond, and pressure. This began Wal-Mart's ongoing efforts to reverse the negative reputation and mitigate future brand-reputation attacks (Arthur W. Page Society, 2011, pp. 15-16).

For over the past decade, Wal-Mart has been consistently under attack by those trying to destroy the company's reputation. In respect to the company's ERM program and reputational risk, this likely places the company in a continual monitoring mode where reputational risk indicators are identified and quickly responded too through use of PR campaigns or other response plans. Although specific company documents are not available documenting these actions, one can observe the various efforts made by the company in response to attacks and conclude that Wal-Mart does have sufficient continuity plans and likely incorporates reputational risk into everyday strategic business plans.

## Personal Reflection and Lessons Learned

Target and Wal-Mart are two rather different companies that face many of the same risks. Despite this, each company has built an Enterprise Risk Management program in response to incidents with many factors affecting governance, risk identification, risk analysis, risk treatment, contingency planning and disaster recovery. This section will break down specific similarities and differences identified throughout the first sections of this report. Lastly, this section will discuss some personal lessons learned.

## ERM Differences between Target and Wal-Mart

Wal-Mart and Target are both well-established companies; however, Target has been around for nearly twice as long. Formed in 1902, Target slowly expanded throughout the United States and eventually into Canada – although the company has recently ceased Canadian efforts (World Market Intelligence, 2014; Target Public Affairs, 2015). In contrast, Wal-Mart was founded in 1962 and quickly expanded throughout the United States and grew internationally (World Market Intelligence, 2015). The scope of the companies, combined with rates of growth, can be seen within their ERM programs. See Figure 3 for a review of differences in ERM programs identified throughout this paper.

With Wal-Mart's rapid expansion, despite the company's younger age, the it started an ERM program almost two decades before Target. This is evident when analyzing the maturity of each program in terms of risk identification and analysis, risk treatment, and history of events. When Wal-Mart identifies risks, the company relies heavily on risk workshops where company managers contribute to the identification and analysis process. In contrast, Target relies heavily on executive level staff to decide which risks are most important. Using employees throughout the organization, as Wal-Mart does, breaks down silos and embraces risk as an enterprise program.

Another substantial difference between the companies' risk programs involves overall risk governance. Wal-Mart's program is designed to push information from the bottom-up as opposed to Target's top-down approach. In response to the 2013 Data Breach, Target has a newly created Chief Risk Officer position.  In contrast, Wal-Mart incorporates the Chief Risk Officer responsibilities with the Chief Financial Officer (Wal-Mart Stores, Inc., n.d.).

In terms of risk treatment, Wal-Mart's strategy for reputation management appears more proactive than Target's approach.  Due to history of public scrutiny of Wal-Mart's operations, the company developed a proactive, non-stop campaign to improve the brand image.  While both companies use public relation campaigns in response to an incident, it is clear that Wal-Mart has a continual program in place.  Conversely, Target's reputation and brand image has been relatively solid over the past 100 years so the need for constant reputation management may be new to the company.

## ERM Similarities between Target and Wal-Mart

Despite having very different origins and business strategy, Target and Wal-Mart have many similarities in their Enterprise Risk Programs.  Both companies utilize primarily qualitative measures to identify risks and focus on the top 20 risks with efforts to reduce down to the top 5 to 10.  Of those, the companies identify many of the same risks: multi-channel retail strategy with respect to reputational risk, protection of customer and employee private information, and system disruption that affects business operations.  See Figure 4 for a review of similarities in ERM programs identified throughout this paper.

Risk treatments for reputational risks are also very similar with heavy reliance on public relation campaigns.  Generally speaking, Wal-Mart appears to be slightly ahead compared to Target but both companies have similar processes in place.  Wal-Mart's use of consultants has proven helpful in the past whereas Target may need to follow suit to help cope with Data Breach reputation problems.

Risk treatment of cyber risks further highlights the similarities between Wal-Mart and Target ERM programs; however, Wal-Mart learned many of the lessons in 2006 that Target is presently facing. For example, both companies have now segregated network infrastructures isolating data warehouses and increasing security measures. Wal-Mart recognized this as necessary after a data breach in 2006, whereas Target has just implemented those mitigating steps. Generally, Target's cyber risk treatment strategy is similar to Wal-Mart's strategy but slightly behind, particularly in terms of operating a completely redundant information system.

## Lessons Learned

There are many lessons learned during research; however, three will be mentioned. First, it is critical for companies, particularly those within the same industry, to learn and grow from the mistakes and incidents of others. This can be seen with Target's 2013 Data Breach and Wal-Mart's 2006 security incident. After hackers exploited Wal-Mart's networks, the company underwent substantial efforts to encrypt, segregate, and generally improve network security posture resulting in a duplicate, redundant infrastructure. Seven years later, Target experienced a similar incident and is now learning those same lessons. Sharing information and learning from past mistakes can help companies prevent following negative historical patterns.

Second, Enterprise Risk Management programs can vary greatly from company to company often based on organizational culture and leadership styles. This is seen with the differences in the Top-Down vs Bottom-Up approaches by Target and Wal-Mart. Both strategies are successful but have different implications. This is also reflected in the companies' decisions with top-level executive positions. Target's top-down approach is reflected in the creation of a senior Chief Risk Officer position compared with Wal-Mart tasking the Chief Financial Officer with those duties.

Lastly, the history of a company is often reflected in its corporate policies and programs. Historically, Target, as a 100+ year old company, has expanded slowly and relied heavily on brand to succeed. It has a well-established culture that helps it achieve such high levels of success. Over the company's history, it has undergone several challenges from proxy contests to large-scale cybersecurity problems. After each incident, the company reassesses policies and modified organizational structures and processes to adapt. The same is seen with Wal-Mart during attacks on reputation and brand image over vendors and employee working conditions. Although reactive in nature, those historic events, or incidents, shape and form the company guiding it towards the future.

## Moving Forward – Applying Lessons Learned to Sweet Tooth Bakery

In today's interconnected society, user-generated content provides unlimited avenues for consumers to express criticism regardless of accuracy or bias. With this capability, retailers of all sizes or market positions must consider reputation risk and develop plans to reduce the probability of negative publicity and lessen the impact severity. Additionally, the interconnected society offers benefits to companies through cyber-powered business processes. With this comes the need to secure infrastructure and protect information entrusted to retailers by their employees and customers. Historically, cyber threats have been focused on large institutions; however, the trend is shifting and small/medium sized businesses must be just as vigilant as the large ones (Berr, 2014, p. 1).

Sweet Tooth Bakery, a hypothetic small to medium-sized enterprise, consists of 10 bakeries dispersed throughout a 500 mile area within Southern California. This highly successful business, founded 10 years ago, has experienced rapid growth and has plans to continue to expand throughout the region. The company's success stems from super-low prices on innovative bakery products as well as commanding a near cult-like following with customers. Sweet Tooth Bakery introduced a customer loyalty program, accessible via their webpage or mobile app, which tracks customer purchases and offers discounts on new items when purchased using rechargeable gift cards linked to a major credit card.

Leadership at Sweet Tooth Bakery implemented a small-scale enterprise risk management program and included cyber threat and reputation risks. This risk program was flexible to adjust to the turbulent environment, yet scalable so that it can support the rate of growth. Hiring a Chief Risk Officer would not be efficient for this situation, opting instead to form a cross-functional risk committee with employees from each location. The Corporate Office, located in a tiny building within an industrial park, identified an existing manager to lead the effort. While the program was top-down in design, it utilized a committee of employees that met quarterly for risk workshops.

During the last workshop, the committee added reputation decay as a stand-alone risk to their risk register and rated it as having moderate probability (6 out of 10) with moderate severity (7 out of 10). With the assistance of Corporate Office's marketing person, the committee decided to proactively build an online reputation using Yelp and several other social media websites. Although other options were available, the committee felt the cost of large public relations campaigns would be greater than the risk of an occasional upset customer; however, they developed a disaster recovery plan that included billboards, radio spots, and newspaper advertisements just in case a major negative publicity event occurred. Lastly, following in the footsteps of other major retailers, the committee identified several reputation indicators that could be tracked and monitored providing advance warning that problems are in the near future. Those indicators were Yelp's star rating, customer comment card statistics, employee turnover rates, Better Business Bureau complaints, and change in return customer percentage based off loyalty card data.

In addition to reputation risk, the committee also added two separate cyber threat risks: loss of system functionality and loss of private employee or customer data. The first, loss of system functionality, was rated as having moderate probability (5 out of 10) with moderate severity (6 out of 10). The second, loss of private employee or customer data, was rated as having low probability (3 out of 10) with high severity (9 out of 10). Several options were contemplated for treating the loss of system functionality risk including following the footsteps of retail giant Wal-Mart by creating a completely separate secondary information network; however, the committee determined the costs were prohibitive. Instead, the committee proposed leveraging the strategic benefit of having several physical locations and, with the help of the company's expert IT girl, developed a redundant network where each physical location provided backup services to another location in a decentralized manner. This highly redundant strategy was not fool-proof as it involved manual actions to recover from an outage or disaster; however, the Sweet Tooth Bakery, understanding that manual transactions were still possible, accepted that residual risk and approved the plan.

The second cyber threat risk, protection of employee and customer information, carried a higher severity and warranted more attention than the first risk. After conducting research, the company decided to contract a part-time computer security expert to implement the lessons learned from other major retailers who had already experienced a significant data breach. Despite this best effort, the company agreed with other retailers' assertions that data breaches are not completely preventable, so it decided to purchase an insurance policy that would minimally cover the cost of providing identity protection to every member of their loyalty program.

Identity protection services after a data breach is an emerging best practice and the company recognized that it would be costly and could potentially devastate their financial posture. In addition, a disaster recovery plan was developed that included sending the expert IT girl to a basic seminar teaching industry best practices for incident response, posting cyber emergency contact information for law enforcement next to the server room, and researching third-party cyber emergency response team companies to call in case of a breach.

Because the committee is intelligent, they quickly realized that many risks are interconnected. They decided to introduce risk scenarios to their ERM program particularly for areas involving cyber threats and reputation risk. One scenario involved the breach of private information from their servers. Through this scenario analysis, the committee realized that experiencing a data breach risk would trigger disaster recovery plans for that particular risk, but also for the severe negative publicity reputation risk. Because of this correlation, they decided to include quantitative metrics to their risk program regarding “information system health” such as vulnerability patching percentages and number of automated firewall-prevented attacks.

Although the risk program at Sweet Tooth Bakery has been an overall success, the committee has faced some problems that needed to be worked on. First, the culture of the company has fostered a level of competition between the individual stores. This became problematic as many of the risk treatment plans relied on one store helping another. Another challenge experienced was justifying the cost associated with risk treatment plans. For example, sending the expert IT girl to a training seminar was something out of the ordinary for a company of this size. Fortunately, Sweet Tooth Bakery’s senior leadership recognized that Enterprise Risk Management isn’t an expense, it is an opportunity.

## References

Accenture. (2011). *Global Risk Management Point of View: Retail.* Accenture. Retrieved from www.accenture.com/GlobalRiskManagementResearch2011

Arthur W. Page Society. (2011, September). Did Wal-Mart Wake Up? How Strategic Management Handled Wal-Mart's Reputation. Retrieved 04 15, 2014, from http://www.awpagesociety.com/wp-content/uploads/2011/09/Wal-Mart_CaseStudy.pdf

Atkinson, W. (2003, 12). Enterprise Risk at Wal-Mart. *Risk Management Magazine*, pp. 36-39.

Berr, J. (2014, September 08). A fast-growing threat to small business: Hackers. *CNBC*. Retrieved 04 17, 2014, from http://www.cnbc.com/id/101971980

Canadean. (2015). *Target Corporation Company Profile, SWOT & Financial Report.* New York: Progressive Digital Media. Retrieved from http://search.proquest.com.libezproxy2.syr.edu/docview/1652830396?accountid=14214

Chapman, R. J. (2011). *Simple Tools and Techniques for Enterprise Risk Management* (Second Edition ed.). John Wiley & Sons Ltd.

Davis, N. (2007). *Corporate Reputation Management, TheWal-Mart Way: Exploring Effective Strategies in the Global Market Place.* Texas A&M University. Retrieved 04 14, 2015, from http://repository.tamu.edu/bitstream/handle/1969.1/5687/Microsoft+Word+-+TEMPLATE.pdf?sequence=1

FirstResearch. (2015). *Retail Sector Industry Profile.* First Research. Retrieved from http://www.firstresearch.com/Industry-Research/Retail-Sector.html

Gamble, R. (2007, July/August). Steering A Giant. *Treasure & Risk*, pp. 41-43. Retrieved from www.treasuryandrisk.com

Greenwald, J. (2014). Insurers cut cyber capacity for retailers. *Business Insurance*, p. 1. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=95496540&site=ehost-live

Heller, L. (2013, May 06). New Ad Campaign Promotes 'The Real Walmart'. *Forbes Magazine*. Retrieved 04 14, 2014, from http://www.forbes.com/sites/lauraheller/2013/05/06/new-ad-campaign-promotes-the-real-walmart/

Kerber, R., Wahba, P., & Finkle, J. (2014, January 13). Target apologizes for data breach, retailers embrace security upgrade. *Reuters US*. Retrieved 04 14, 2015, from http://www.reuters.com/article/2014/01/13/us-target-databreach-retailers-idUSBREA0B01720140113

Malcolm, H. (2014, May 14). Target CMO responds to employee rant over culture. *USA Today*. Retrieved from http://www.usatoday.com/story/money/business/2014/05/14/target-cmo-response-employee-rant/9075327/

Mudd, J. (2015, January 14). Target's latest PR nightmare: The ripple effect of a bad business decision. *The Business Journals*. Retrieved from http://www.bizjournals.com/bizjournals/how-to/marketing/2015/01/targets-latest-pr-nightmare.html?page=all

NC State University. (2010). Enterprise Risk Management at Target. *ERM Roundtable Summit.* Poole College of Management, ERM Initiative. Retrieved from http://internalaudits.duke.edu/documents/articles_archive/ERMRoundtableSummit2_3_11.pdf

Parekh, R. (2007). Reputations on the line. *Business Insurance, 41*(20), p. 26.

Parizo, E. (2012). For Target, retailer's risk management program hinged on executive buy-in. *TechTarget*. Retrieved 04 03, 2015, from http://searchsecurity.techtarget.com/news/2240163008/For-Target-retailors-risk-management-program-hinged-on-executive-buy-in

Sherman, L. (2013, February 18). It's Cool Again to be 'Made in America'. *AdAge*. Retrieved 04 13, 2015, from http://adage.com/article/news/cool-made-america/239846/

Spoehr, W. D. (2012, 12). Consequences of Disconnects of 'Tone at the Top' at the Institutional and Operational Level. *Financial Executive,* pp. 68-69.

Target Corporation. (2013). *Corporate Responsibility Report.* Retrieved 04 13, 2014, from https://corporate.target.com/_media/TargetCorp/csr/pdf/2013-corporate-responsibility-report.pdf

Target Corporation. (2014a). *Schedule 14A - Proxy Statement.* Security and Exchange Commission. Retrieved 04 13, 2014, from https://www.sec.gov/Archives/edgar/data/27419/000130817914000217/ltgt2014_def14a.htm

Target Corporation. (2014b). *10-K Annual Report.* Securities and Exchange Commission. Retrieved 04 13, 2014, from http://www.sec.gov/Archives/edgar/data/27419/000002741914000014/tgt-20140201x10k.htm

Target Public Affairs. (2014a, 11 06). *Target names Jacqueline Hourigan Rice as Senior Vice President, Chief Risk and Compliance Officer*. Retrieved from Target Corporation Press Releases: http://pressroom.target.com/news/target-names-jacqueline-hourigan-rice-as-senior-vice-president-chief-risk-and-compliance-officer

Target Public Affairs. (2014b, 06 10). *Target names Brad Maiorino Senior Vice President, Chief Information Security Officer*. Retrieved from Target Corporation Press Releases: http://pressroom.target.com/news/target-names-brad-maiorino-senior-vice-president-chief-information-security-officer

Target Public Affairs. (2014c, March 07). *Target and Major League Baseball Team Up For Education*. Retrieved from Target Corporation Press Releases: http://pressroom.target.com/news/target-and-major-league-baseball-team-up-for-education

Target Public Affairs. (2014d). *Free Credit Monitoring and Identity Theft Protection with Experian's ProtectMyID Now Available*. Retrieved from Target Corporation Press Releases: https://corporate.target.com/article/2014/01/free-credit-monitoring-and-identity-theft-protecti

Target Public Affairs. (2014e, May 08). *Target Donates $100,000 for Tornado and Flood Relief in the South*. Retrieved from Target Corporation Press Releases: http://pressroom.target.com/news/target-donates-100-000-for-tornado-and-flood-relief-in-the-south

Target Public Affairs. (2015, 01 15). *Target Corporation Announces Plans to Discontinue Canadian Operations*. Retrieved from Target Corporation Press Releases: http://pressroom.target.com/news/target-corporation-announces-plans-to-discontinue-canadian-operations

Verschoor, C. C. (2014, July). Ethics. *Strategic Finance*, pp. 12,61.

Wallace, G. (2014, 03 05). Target replaces officials in security overhaul. *CNN Money*, p. 1. Retrieved from http://money.cnn.com/2014/03/05/technology/target-breach-leadership/

Wal-Mart Stores, Inc. (2014). *10-K Annual Report.* Securities and Exchange Commission. Retrieved 04 14, 2014, from http://stock.walmart.com/financial-reporting/sec-filings/

Wal-Mart Stores, Inc. (2015). *Global Statement of Ethics.* Wal-Mart Stores, Inc. Retrieved 04 14, 2015, from https://walmartethics.com/uploadedFiles/Content/U.S.%20-%20English.pdf

Wal-Mart Stores, Inc. (n.d.). *Charles M. Holley, Jr. Biography*. Retrieved from Corporate @ Walmart.Com: http://corporate.walmart.com/our-story/leadership/executive-management/charles-holley/

World Market Intelligence. (2014). *Target Corporation Company Profile and SWOT Analysis.* San Francisco: World Market Intelligence Ltd.

World Market Intelligence. (2015). *Wal-Mart Stores, Inc. Company Profile and SWOT Analysis.* San Francisco: World Market Intelligence Ltd.

Zetter, K. (2009, October 13). Big-box Breach: The Inside Story of Wal-Mart's Hacker Attack. *Wired Magazine*. Retrieved 04 15, 2014, from http://www.wired.com/2009/10/walmart-hack/

**Target Corporation SWOT Analysis**

| | |
|---|---|
| Strengths | Operational Network |
| | Wide Product and Brand Portfolio |
| Weaknesses | Limited Financial Leverage |
| | Patent Infringements |
| | Product Recall |
| | Strong Heritage |
| Opportunities | Growth Prospects: E-Retail |
| | New Store Openings |
| | Private Labels Gaining Momentum |
| Threats | Changing Consumer Preferences |
| | Counterfeit Goods Market |
| | Expansion by Competitor |

Figure 1. Strength, Weaknesses, Opportunities, and Threats (SWOT) analysis of Target Corporation prepared by World Market Intelligence for first quarter 2014. Brand image risks are seen within the product recall weakness and the increase in counterfeit products (World Market Intelligence, 2014).

**Wal-Mart Stores, Inc. SWOT Analysis**

| | |
|---|---|
| Strengths | Constant revenue growth |
| | Diversified retail format |
| | Product and brand diversity |
| | Wide geographic presence |
| Weaknesses | Legal proceedings |
| | Lobbying in Indian market |
| Opportunities | Expansion into emerging markets |
| | Expansion of store network |
| | Growing e-retail industry |
| | Increase in consumer spending in the US |
| Threats | Foreign exchange risks |
| | Increase in organized retail crime |
| | Intense competition |
| | Rise in manpower costs |

Figure 2. Strength, Weaknesses, Opportunities, and Threats (SWOT) analysis of Wal-Mart Stores, Inc. prepared by World Market Intelligence for first quarter 2015. Recurring risk to brand image seen by both weaknesses as well as a threat of organized retail crime (World Market Intelligence, 2015, p. 1).

| **ERM Differences** | **Target Corporation** | **Wal-Mart Stores, Inc.** |
|---|---|---|
| ERM Program & Governance | Established in 2009 | Established in 1990s |
| | Currently US only | Global Implications |
| | Separate from Internal Audit | Part of Internal Audit |
| | Currently has Chief Risk and Compliance Position | Combined with Chief Financial Officer |
| | Top-Down | Bottom-up |
| Risk Analysis & Classification | Senior executives perform analysis | Use of Risk workshops |
| | 3 “Themes”: Internal, External and Market. Either inactive or active. | Risks are either Internal or External and then categorized into 7 different categories |
| Reputation Risk | Identifies single stand-alone risk as well as other risks that are contributing factors | Groups with Competitive Risk: Human Resource and System Failure risk |
| Cyber Risk | Compromised in 2013 | Compromised in 2005/2006 |
| | No mention of third-party or vendors | Includes third-party and vendors in planning |
| | General definition of system disruption | More granularity in defining system disruption to include fire and earthquake |
| | Chief Information Security Officer (CISO) position | No mentioned C-level Information Security position. |
| | Use of Insurance | No mention of use of insurance |
| Contingency Planning/Disaster Recovery | Reputation risk appears to be managed reactively. | Reputation risk appears to be managed both proactively and reactively. |

Figure 3. Differences between Target Corporation and Wal-Mart Stores, Inc. Enterprise Risk Management programs.

| **ERM Similarities** | **Target Corporation** | **Wal-Mart Stores, Inc.** |
|---|---|---|
| Risk Identification and Analysis | Start with top 20, reduce to top10 | Start with top 20-30, reduce to top 4 or 5 |
| | Qualitative in Nature | Qualitative in Nature |
| Reputation Risk | Identifies Multi-Channel strategy as critical to reputation | Identifies Multi-Channel strategy as critical to reputation |
| | Risk Treatment involves public relation efforts | Risk Treatment involves public relations efforts |
| | Focus on Ethics | Focus on Ethics |
| Cyber Risk | Difficult to prevent implying moderate to high probability | Difficult to prevent implying moderate to high probability |
| | Identifies two risks: Data Protection and System Disruption | Identifies two risks: Data Protection and System Disruption |
| History | ERM shaped by past incidents | ERM shaped by past incidents |
| Contingency Planning/Disaster Recovery | Cyber incident indicated lack of contingency planning; however, disaster recovery met industry expectations. | Cyber incident kept quiet so little is known about response. |

Figure 4. Similarities between Target Corporation and Wal-Mart Stores, Inc. Enterprise Risk Management programs.

# About the author

**Author: Christopher Furton**

***Website:*** Http://christopher.furton.net

Certified professional with over 12 years of Information Technology experience and 8 years of hands-on leadership. An expert in cyber security with both managerial and technical skills proven throughout a career with increasing responsibility and performance expectations. Known ability to translate complex information for universal understanding. Detail-driven, results-focused leader with superior analytical, multitasking, and communication skills. Well-versed in industry best practices including Project Management and IT Service Management. Currently holding active CISSP, CEH, ITIL Foundations, Security+, and Network+ certifications.

**Visit the auhor’s blog:**
*IT Management Perspectives* - https://christopherfurton.wordpress.com/

**Social Sphere:**

LinkedIn Twitter Google+ Quora Wordpress Flavors.me

Slide Share Tumblr YouTube Pinterest About.me Vimeo