Journal of Comparative International Management
2020, Vol. 23, No. 1, 35–54

Surviving Data Breaches: A Multiple Case Study Analysis

by

Nithya Shankar
State University of New York at Plattsburgh, U.S.A.

Zareef Mohammed
State University of New York at Plattsburgh, U.S.A.

This study examines how organizations could potentially overcome the fallout of data breaches and achieve competitive advantage, by enhancing key firm capabilities through the process of sensing threats, seizing opportunities, and transforming/reconfiguring their existing resource base. We use the dynamic capabilities framework as the theoretical basis for this study. A multiple case study approach is applied to this study, using secondary data from the case studies of Target, Anthem, and Yahoo data breaches. Our findings indicate that utilizing the dynamic capability framework and its orchestration processes of sensing, seizing, and transforming/reconfiguring the resource base worked favorably in the case of Target and Anthem. However, for Yahoo, failure to utilize the aforementioned framework and orchestration processes had negative impacts on the firm. Our findings have implications for organizations regarding how they could restructure their internal practices and contain the fallout after a data breach.

1. Introduction

Data breaches are defined as unauthorized or unintentional disclosures by organizations that result in the loss of customers' personally identifiable information (PII), such as social security numbers (SSN) and credit card information (Peretti, 2008). The consequences of suffering a data breach are severe for an organization, with several negative effects such as falling market value and high penalty costs (Gatzlaff & McCullough, 2010; Ponemon, 2017). To survive a data breach and combat its negative effects, it is crucial that organizations implement a better security and privacy program from both an accountability perspective and as a preventative measure against future incidents. Research in the area of data breach recovery has shown how organizations can recover customers' confidence and continued business (Bansal & Zahedi, 2015; Choi, Kim, & Jiang, 2016; Goode et al., 2017), but little emphasis is given on the internal operations of the organization itself in the data breach recovery phase. Specifically, an organization that suffers a data breach is in a more precarious position than one that has not, and is required to not only recover their customers, but also restructure the organization, which includes their security and privacy practices, to better address the negative impact of the data breach. This study focuses on examining the necessary organizational changes – which also includes security and privacy practices, required for surviving the impacts of data breaches. Specifically, the following research questions were developed to guide the investigation of this study: (1) How do organizations recover from the aftermath of a data breach, and (2) What strategies do they undertake to achieve a competitive advantage?

In order to identify what potential practices could help organizations recover from data breaches, our study uses a multiple case study approach based on three recent data breaches – Target, Anthem, and Yahoo. We adopt the approach of Breznik et al. (2019) in focusing on how six key firm capabilities could be redeployed and enhanced as dynamic capabilities, through the process of sensing threats, seizing opportunities, and reconfiguring existing capabilities. Our findings provide evidence that integrating the dynamic capabilities framework was beneficial in the case of Target and partially in the case of Anthem. However, in the case of Yahoo, findings demonstrate that Yahoo as an organization did not readapt their

organizational practices and as a result lost both their reputation and market value in the acquisition process by Verizon.

This study contributes to information privacy and security literature, as well as the strategic management/marketing literature by primarily exploring how organizations handle the fallout from data breaches from an internal change process and regain/lose their market value and brand name. Furthermore, this study opens dialogue among multidisciplinary scholars in the scarcely studied phenomenon of the organizational practices adapted following data breaches. In addition to theoretical contributions, the study provides managerial principles that may be useful for organizations for both avoiding data breaches and recovering from them.

2. Literature Review

With rapid advancements in technology and information storage going digital, organizations are increasingly transitioning from a supply-and-demand model to a value-based model, while keeping the needs of the customers in mind. Organizations are known to collect and analyze personally identifiable information (PII) from customers such as their shopping habits, browsing patterns, credit card details, social security numbers (SSNs); subsequently, this information is used to offer customized promotions to customers (Culnan & Armstrong, 1999). Furthermore, some organizations go the extra mile to convince customers that their PII is safe and secure with them. An experimental study by Tsai et al. (2011) provided evidence that in an online environment, customers are likely to purchase from those online vendors who had clear privacy policies displayed on their website. In the healthcare context, Huang et al (2009) showed that adopting de-identification, pseudonymity, and de-encryption methods could potentially help patients keep their PII private, while allowing them the ability to access their records without worrying about their information being compromised.

As organizations are required to protect and preserve customers' privacy in the electronic space, the United States Federal Trade Commission (FTC) came up with a set of guidelines known as Fair Information Practices (FIP). Extant research, however, established that many organizations do not always comply with all the guidelines of the FIP. Peslak (2006) provided evidence that among the top 100 Forbes corporations FIP and customer-centric privacy policies were not being adhered to, while Schwaig et. al (2006) developed a privacy policy assessment matrix to analyze whether Fortune 500 firms strictly complied with FIP. In reality, in a quest to achieve competitive advantage, organizations were found to reuse customers' PII without disclosing how their sensitive information is being reused; these firms exhibited unethical behavior by failing to disclose to customers how their PII might be reused, while giving unauthorized access privileges to internal employees and external entities (Culnan & Armstrong, 1999). Consequently, customers' PII were exposed to data breaches.

Evidence has documented that data breaches compromised the privacy of consumers and had a significant impact on their privacy related decisions. Affected customers echoed concerns that their PII was violated, thereby leading them to lose trust in the breached firm (Martin et al., 2017). Research also provided evidence that these affected customers switched to other competing companies as a consequence of loss of trust in the breached firm (Choi et al., 2016). In a survey conducted by the Ponemon Institute,[1] data breaches cost the affected organizations around $3.2 million and resulted in a stock price reduction of 5%, in addition to customers terminating their relationship with the organizations involved and switching to those firms with safer privacy practices. In short, misuse of customers' PII and the ensuing data breaches portended that the organizations involved were likely to face negative consequences. As evident in recent literature, when a data breach announcement was imminent, capital markets reacted negatively, thereby influencing the market value of the breached firm and subsequently, shareholder wealth (Cavusoglu et al., 2004; Goel & Shawky, 2009; Gatzlaff & McCullough, 2010).

Conditional on the magnitude of the breach, firms were known to be significantly impacted financially in the short term as well as the long-term, as a result of customer backlash, thereby motivating scholars to perceive data breaches as service failures rather than information system failures (Malhotra & Malhotra, 2011). When a service failure such as a data breach was detected, the natural course of action that had to be undertaken by the firm was to participate in service recovery efforts, in order to alleviate negative sentiments among customers and increase customer retention. Research by Goode et al (2017) used the context of the SONY Playstation breach to show that offering compensation to customers within expected limits as part of service recovery efforts positively influenced the customer recovery process. Furthermore, using an event study, Rasoulian et al (2017) provide evidence that after a data breach announcement, when firms offer compensation to customers and redefine organizational practices, capital markets are likely to view these firms in a positive light, thereby helping them achieve stable financial performance in the long-term. Additional research by Vaerenbergh et al (2019), discusses the three phases of the service recovery journey (i.e. pre-recovery, recovery, and post-recovery) and provides an overview on how organizations manage customer interactions in each of these phases.

While these aforementioned studies largely discuss steps that organizations could undertake take to remedy the aftermath of a data breach by viewing data breaches as service failures, another stream of literature rooted in information systems largely offers suggestions on how organizations could remedy their practices and processes to contain the fallout of a data breach. Using the example of Choicepoint and TJX, Culnan and Williams (2009) view data breaches as a privacy problem and provide suggestions that at an organizational level, firms should create a culture of privacy and implement rigid governance processes in order to ensure that these data breaches do not happen in the future. Rotvold (2008), provides a discussion on how having regular security awareness assessments within an organization could help create a culture of privacy, in order to prevent data breaches. Belanger and Crossler (2011), provide suggestions on how a culture of privacy should be analyzed at the organizational level across various geographic boundaries, while Gwebu et al (2018) demonstrate that highly reputed firms tend to recover better from a data breach while lower reputed firms require image renewal strategies to combat the negative effects of the data breach.

These aforementioned studies largely discuss how companies could potentially create a culture of privacy to contain the fallout of data breaches, participate in image restoration, or redefine organizational practices to prevent service failures and win back their customers. There is however, a dearth of research that specifically pays attention to what strategies firms could potentially undertake and how they could deploy their dynamic capabilities in order to bounce back from data breaches.

3. Theoretical Framework

We adopt the dynamic capabilities view and their influence/interaction on firm capabilities as proposed by Breznik et al. (2019) as the theoretical lens for better understanding the organizational data breach recovery processes. Dynamic Capabilities is defined as a firm's ability to integrate, build, and reconfigure their internal and external competencies so that they can achieve competitive advantage in rapidly changing business environments (Teece et al., 1997). It is rooted in three core factors, namely: *asset position, processes, and paths*. While "assets" refer to both the tangible and intangible assets an organization has, including information, skills, and knowledge, an organization must transform these existing assets into future dynamic assets for competitive gain (Teece & Pisano, 1994). In general, assets require processes for functionality within an organization; organizations in turn need to re-evaluate and change existing processes or create new processes to realize the future capabilities of these existing assets. Consequently, the capabilities of the *asset positions*, along with the right *processes* for achieving competitive advantage, require commitment to specific *paths* or events, for shaping the future organizational capabilities.

In the context of information systems (IS) research, the concept of enhancing dynamic capabilities has gained considerable traction. Sher and Lee (2004) provide empirical evidence that using information technology for the purpose of knowledge management helps enhance dynamic capabilities in an organization's IS. Desai et al. (2007) provide empirical support that resource-reconfigurability, social networking capability, and market orientation positively impacts dynamic capabilities in an organization's customer relationship management system, while Pavlou and El Sawy (2006) demonstrate that environmental turbulence enhances the positive impact of leveraging information technology as a dynamic capability in the new product development process.

From the perspective of Eisenhardt and Martin (2000), the consensus is that dynamic capabilities resemble routine processes in moderately dynamic markets, while in high velocity markets they are highly experiential and fragile processes that require constant innovation. Furthermore, they argue that firm competitive advantage largely rests with how resources are configured and not dynamic capabilities. Moreover, it is crucial that firms sustain their competitive advantage. As evident in the discussion by Wade and Hulland (2004), especially in the context of IS research, competitive advantage is sustained so long as organizational resources continue to add value, are difficult to acquire and imitate, and are unlikely to be impacted by the threat of substitutes.

The role of dynamic capabilities has been widely discussed from the perspective of crisis management as well. Witcher and Chau (2012), use the example of Nissan during the financial crisis to provide a discussion of how multinational corporations incorporate strategic prioritization and resource deployment as a dynamic capability for the purpose of crisis management. In light of disaster management, Battisti and Deakins (2017) provide empirical evidence that small firms require proactive efforts with regards to integrating resources from external networks as a dynamic capability for the purpose of recovery. Alonso-Almeida et al. (2015), provide evidence that in financial crises, proactive strategies undertaken by restaurants help create trust among customers and reinforce customer loyalty; subsequently these companies achieve a sustained competitive advantage by using a loyal customer base as a dynamic capability. In line with the aforementioned studies, dynamic capabilities renders itself a necessary component to data breach recovery, which involves both IS infrastructure and crisis management.

In order for firms to innovate, adapt, and create change that could be potentially favorable to customers and create threats for competitors, Teece (2007) proposes that corporate agility is crucial for firms to achieve a sustained competitive advantage and this could potentially be achieved by sensing threats early on, seizing opportunities, and continuously transforming themselves to achieve value. Teece's (2007) framework is further explained below:

(i) Sensing - This activity involves identification, development, co-development, and assessment of a technological opportunity that could potentially serve the needs of customers (Teece, 2014). Furthermore, sensing gives the organization an opportunity to also scan for potential threats that are likely to disrupt the functioning of the organization.

(ii) Seizing - When companies are involved in activities pertaining to seizing, they are trying to develop and select opportunities that fit with the organizations' goals. Moreover, this activity also helps organizations recognize valuable knowledge that they have to offer and make strategic decisions accordingly (Kump et al., 2018).

(iii) Reconfiguring - This activity involves enhancing, combining, protecting, and reconfiguring tangible and intangible assets within an organization keeping in line with technological and market changes.

From the perspective of firms that extensively rely on information technology (IT), Breznik et al. (2019) provide evidence and establish a framework for how six key firm capabilities can be sensed,

seized, and transformed, and what practices could potentially be adopted under each of these activities. They are presented in Table 1.

Table 1: Practices Supporting the Development of Firm Capabilities as Dynamic Capabilities

Dynamic Capability	Sensing	Seizing	Transforming
Managerial	• Environmental scanning • Keep open communication channels	• Promote networking • Develop relationships with various stakeholders	• Build adaptive business models • Skill building • Ensure team cooperation
Marketing	• Identify target markets, customers, and threat of competition	• Train employees to identify changing customer needs	• Ensure customer satisfaction and build loyal customer base
Technological	• Recognize evolving technological developments	• Seize opportunities with regards to technological developments	• Develop technological advanced new products and services
R&D	• Recognize potential R&D partners	• Recognize right opportunities to use R&D	• Adopt newly acquired knowledge to improve business performance
Innovation	• Recognize innovation capability of competitors	• Motivate creativity processes amongst employees	• Develop market oriented innovations • Reward employees
Human Resource	• Recognize need for employees with specific skillsets	• Run recruitment drives	• Facilitate knowledge transfer between newly hired employees and existing employees

Source: Breznik et al., 2019.

A brief description of each of the capabilities presented in Table 1 are as follows:

(i) Managerial capability – As part of developing this capability, from a sensing perspective, managers could potentially keep track of the environment and have open communication channels. Once the sensing activity is complete, managers could seize opportunities to develop strong relationships with customers and other stakeholders, as well as promote networking opportunities. Lastly, as part of the transformation process, managers could find ways to build adaptive business models, continuously develop skills at all levels of the organization, and ensure that a team-based environment exists.

(ii) Marketing capability – As part of developing the marketing capability, firms must initially sense who the target markets are and where the threat of competition lies. Next employees must be trained to identify changing customer needs and seize information from target markets. Lastly, firms must find ways to transform their marketing capability by ensuring continuous customer satisfaction and subsequently retaining loyal customers through building long-term partnerships.

(iii) Technological capability – In order to enhance their technological capabilities, employees must sense and seize evolving opportunities with regards to technological developments and trends and consequently develop new products and services as part of the reconfiguration process.

(iv) R&D capability – This capability involves seizing opportunities that could potentially develop R&D, recognize R&D developments of competitors, and accordingly adopt newly acquired knowledge to improve businesses processes within the organization.

(v) Innovation capability – With regards to furthering their innovation capabilities, organizations could potentially recognize innovation capabilities of their competitors and customers involved in the innovation process, motivate their employees to get creative and innovative, and subsequently, develop new ideas into market-oriented innovations as well as reward employees for their creativity.

(vi) Human resource capability – The organization could potentially identify that they are lacking employees with specific skill sets, run a recruitment drive to find qualified recruits, and facilitate knowledge transformation processes between new employees and existing employees.

In the context of data breaches, we refer to the aforementioned framework and provide a discussion of how organizations affected by these breaches could potentially utilize the six capabilities within the organization and accordingly deploy them to counteract the negative effects. Following the practices illustrated by Breznik et al., (2019) our case analyses in subsequent sections demonstrates how companies could redefine their practices to recover from these data breaches.

4. Research Method

We use a multiple case study approach from existing case studies to investigate how organizations recover from data breaches. Case studies allow for studying phenomena in real-life contexts, while also allowing researchers to extract insightful information about the role of information systems in changing organizational processes and structures (Benbasat et al., 1987). We choose three cases based on secondary data for this study: (1) the Target data breach of 2013, (2) the Anthem data breach of 2014, and (3) the Yahoo data breach of 2014. Firstly, both data breaches from Target and Anthem provides analytical capabilities to examine successful business recovery following the data breaches through the use of dynamic capabilities. Alternatively, the Yahoo data breach demonstrates how the lack of organizational reform following a data breach without the use of a dynamic capabilities framework can lead to failure.

All case studies were analyzed based on secondary sources. Specifically, the aforementioned data breaches were chosen for analysis since the magnitude of the breaches was severe in all three cases, compromising consumers' PII in the millions, as well as the fallout that ensued thereafter. Additionally, they all occurred within recent years, which allows for enough time to observe the change in practices of the organizations after the breach to ensure their survivability, in terms of technological changes, business processes, and organizational structures. We summarize Target's data breach from a case study by Dube (2016) in the following section, while Anthem's case study is compiled from several sources, including the website and news outlets. Yahoo's data breach was summarized from a case study by Trautman and Omerod (2017).

4.1. Target Data Breach of 2014

Target is one of the largest retailers in the United States (US), along with Walmart. As documented in the case study by Dube (2016), on December 19th 2013, Target had announced that a data breach involving the theft of over 40 million consumers' PII, including credit and debit cards used to make purchases in US stores, had occurred. Furthermore, in January 2014, Target disclosed that up to 70 million additional customers' PII were compromised, including names, telephone numbers, home addresses, and email addresses. The data breach affected around 10% of US-based debit and credit cards.

Hackers had managed to compromise Target's point-of-sale network between November 15th and 27th 2013, during the pre-Christmas and Black Friday shopping season, by installing the "BlackPOS"

malware, originating from Russia, on Target's terminals. BlackPOS is a memory-scraping malware designed to capture credit and debit card data on compromised point-of-sale terminals. The memory-scraper exploited the vulnerability of point-of-sale systems by copying the data stored on random access memory and subsequently dumping them onto one of Target's web servers, to which the attackers had gained unauthorized access.

Despite the security measures Target had taken, which included network segmentation, firewalls, and malware detection suites, among others, as well as being compliant with the Payment Card Industry Data Security Standard (PCI-DSS), the attack vector that compromised Target's systems came from one of their vendors – Fazio Mechanical Services. A simple phishing email was used to gain user code and password information from a Fazio Mechanical Services employee, which in turn allowed the attackers to connect remotely with Target's network.

In order to counteract suspicious activity due to unauthorized access, Target had invested $1.6 million in the FireEye system, which created virtual chambers that lured hackers, so they could be detected before they penetrate a system. Despite numerous escalating alerts, which were received starting on the 30th of November 2013, the local security team analyzed these alerts with the conclusion that no action was necessary. These alerts were ignored and could have potentially prevented the data breach. Furthermore, Target declined to activate one of the features of the system that detected and eradicated software that was flagged as "malicious" or "unauthorized", because they did not completely trust this new system. Additionally, one of Target's antivirus systems had also detected suspicious activity on the server, but that alert was also ignored. Target only learned of the breach when representatives of the US Department of Justice (DoJ) had informed them of a number of fraudulent debit and credit card transactions with a suspected link to transactions made at Target.

4.1.1. Fallout of Data Breach

The hackers had sold the stolen credit cards on an online black market. The fallout of this data breach led to numerous negative outcomes for Target, which included loss in reputation and market value. Target was eager to hide the data breach but had to publicly disclose the breach on December 19th, 2013. Not only was Target criticized for ignoring the alerts which could have prevented the breach, but also for their resistance in disclosing the breach to the public, as well as their handling of customers' concerns over the breach. Customer surveys of the company indicated that customers' perceptions of Target were negative, which was eventually reflected in their financial outcomes. Target's profits declined by 46%, with a drop of 5.3% in revenues, that managers associated with consumers' fears. Target reported a total cost of $252 million, with $90 million associated with cyber insurance, and the closure of 133 stores in Canada. Target was also required to pay up to $67 million to credit card issuers based on a settlement with Visa. Banks such as JP Morgan-Chase had to re-issue credit cards as well as place limits on transactions and withdrawals from credit and debit cards. These banks lobbied for Target to reimburse them for the costs associated with addressing this fallout.

On March 5th 2014, the Chief Information Officer (CIO) of Target resigned and two key positions were created for external recruitment: (i) Executive Vice President and Chief Information Security Officer (CISO), and (ii) an Executive Vice President and Chief Compliance Officer (CCO) roles. These new positions and the functions that developed were meant to centralize the management and governance of information security in the organization. Additionally, in May 2014 the Chief Executive Officer (CEO) of Target was fired, with rumors of other members of the Board-of-Directors also being evaluated for their role and contribution in the organization. From these organizational changes as evident in the case study, it can be inferred that the leadership of Target's organizational structure had changed as a consequence of the data breach, given that many of the new members of the hierarchy came into such positions after the event.

To address the issues with customers, and their security and privacy practices, Target embarked on a public relations campaign assuring customers that the technological components responsible for the breach had been found and destroyed. They explained that no customer would be liable for fraudulent transactions and offered a free subscription to a credit monitoring service. Additionally, Target prioritized their "chip-and-PIN" project to implement a chip card and personal identification number (PIN) payment system. This involved the replacement of all point-of-sale terminals to read the chip from credit and debit cards, as well as Target credit cards (REDcard), which is considered a more secure practice. Despite the massive fallout from this breach, however, today Target is still considered a major competitor to Walmart, with growing stock prices[2], and have yet, as of this writing, to suffer another massive data breach. In the next subsection, we discuss the data breach by Anthem, which we will use alongside this Target data breach to analyze using our theoretical framework.

4.2. Anthem's Data Breach in 2015

Anthem is one of the largest health insurance companies based in Indianapolis, Indiana, in the US. In February 2015, Anthem disclosed that they were subject to a data breach, wherein cyber attackers gained unauthorized access to one of their parent company's systems. This resulted in a compromise of consumers and Anthem Blue Cross and Blue Shield employees then covered or covered in the past by Anthem's health insurance policies. Stolen PII included social security numbers, medical IDs, birthdates, addresses, and detailed employment and income data of nearly 80 million Americans; however, it is believed that no financial or medical information was stolen. In a statement to address the breach, Anthem's CEO, Joseph Swedish stated:

> "Anthem's own associates' personal information – including my own – was accessed during the security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data."

Anthem claimed the attack was "sophisticated", however further details on the attack revealed that it was most likely uncomplicated. The breach was discovered when a database administrator had noticed his credentials were used to run a database query masked to look like a legitimate query from the administrators, but upon further inspection, it was revealed as suspicious and a possible intrusion (Ragan, 2015). Anthem used TeraData for its data warehousing infrastructure, which came with a number of security controls, including user-level security controls, role-based access controls, encryption mechanisms, along with auditing and monitoring features. It is reported that Anthem did not encrypt a number of their files, however, since the database administrator's account was compromised, with escalated privileges, it was irrelevant if Anthem used encryption or not. Further analysis of the breach revealed that five of their employees' credentials were compromised.

Analysis of the cyberattack pointed to the work of a state-sponsored Chinese cyber espionage group named, primarily, "Deep Panda". It is suspected that the attack was carried out via phishing, as a domain was registered in April 2014 with the domain name, 'we11point.com', to masquerade as one of Anthem's websites. A debate exists as to whether it was a phishing attack or if malware was used to hijack a session and capture login credentials. According to Mandiant, a security firm hired to investigate the breach, Anthem did not take reasonable steps to protect their data, such as using "two-factor authentication, failure to change passwords frequently, as well as insufficient controls to monitor data usage and exfiltration".

4.2.1. Fallout of Anthem's Data Breach

While the breach at Anthem was not deemed severe as personal, health, and financial information was not compromised, due to SSNs and PIIs being compromised the breach was considered significant with serious ramifications that could harm Anthem's employees and customers. Anthem faced several civil-class lawsuits, which resulted in an agreement to pay $115 million in damages, in addition to the plaintiffs' attorneys demands that Anthem guarantees a "certain level of funding for information security and to implement or maintain numerous specific changes to its data security systems, including encryption of certain information and archiving sensitive data with strict access controls" (Pierson, 2017). While Anthem denied any wrongdoings in the breach, a federal judge ruled that their security audits from before and after the breach should be made public. Anthem pledged:

> "As part of the settlement, Anthem has agreed to continue the significant information security practice changes that we undertook in the wake of the cyber attack, and we have agreed to implement additional protections over the next three years."

Anthem indicated that some of the security practices they had changed as a result of the attack involved the following: (i) resetting all passwords for associates and contractors, (ii) re-issuing new IDs and passwords for users with escalated privileges, (iii) implementing a three-tier authentication model along with one-time, limited-duration passwords for elevated privileges of user access and (iv) expanding security logging and monitoring capabilities. Additionally, Anthem explained that their commitment to security also involved "encryption of certain information". The company also offered services, including free credit reporting and identity protection services, to those affected by the breach, as overseen by a third-party settlement administrator.

4.3. Yahoo Data Breach

Yahoo is one of the major web services providers that competes against Google and Microsoft's Bing. They provide a search engine platform for Internet browsing in addition to offering many Internet-based services in the realm of emails, finance, shopping, advertising, groups and social media, to name a few. Due to severe financial losses, Yahoo sought to sell the company. In March 2016, they engaged in half-day presentations to seven interested parties seeking to buy off Yahoo. A Strategic Review Committee (SRC) that was engaged in advising Yahoo on the matter suggested engaging in negotiations with Verizon for the following reasons: Verizon's bid was the highest, they were in compliance with the transaction terms proposed by the SRC, were also sufficiently funded to complete the transaction, and completed their due diligence reviews in a timely and effective manner.

In July 2016, the proposal for Yahoo's acquisition by Verizon was approved. However, on September 2016, Yahoo announced that they had experienced data breaches around 2013 and 2014, with over a billion accounts compromised in 2013. This was the largest data breach at the time and involved the compromise of user information such as names, email addresses, telephone numbers, dates of birth, encrypted passwords, and security questions in some cases. Apart from the compromise of users' PII, Yahoo was met with distrust and suspicion given that they reported that they were unaware of any data breaches to a Securities and Exchange Commissions (SEC) filing in 2016. The breach in 2014 was attributed to forged web cookies which allowed for falsified login credentials. It was later revealed that in total, three billion user accounts were actually compromised which tripled the number from what was originally projected (Perlroth, 2017).

4.3.1. Fallout of Yahoo's Data Breach

The breaches occurred in 2013 and 2014. However, the revelation of the data breach to the public was disclosed in September 2016 which was after Yahoo had received and approved a proposal for buy-out by Verizon. It is assumed that the CEO, Marissa Mayer, became aware of the data breach in July 2016, however, Yahoo's information security team was aware of a data breach compromising a large portion of user data at the end of December 2014. Essentially, Yahoo's security team, and their management, failed to pursue investigation of the data breach, leading to an elongated period of time between the data breach event and public notification. Furthermore, upon learning of the data breach, Yahoo spent approximately two months to disclose the data breach to users and shareholders, as well as, Verizon, with whom they were in the midst of an acquisition transaction.

The failure to respond to the data breach incident led to a reduced price in the acquisition by Verizon. Initially, Yahoo's core business was to be sold for $4.8 billion. However, after the notification of the data breach, Verizon reduced the buy-out price by $350 million – Yahoo was essentially sold for $4.48 billion instead. Furthermore, Verizon not only acquired Yahoo's core business, but also its business assets in the Alibaba Group Holdings and Yahoo Japan. Yahoo was then subjected to rename themselves Altaba Inc. CEO Marissa Mayer and co-founder David Filo were required to step down from the board of directors, among other members. Yahoo was also fined $50 million in legal settlements[3]. The liability for cybersecurity and the legal settlements was accepted by Verizon, however, Yahoo lost its identity as a result.

5. Analysis

Analysis of the cases selected for study is performed using a hermeneutics approach. Hermeneutics is concerned with the meaning of text or text analogue, deriving patterns from these texts (Myers, 2004). We apply the *firm capability framework* developed by Breznik et al. (2019) which is based on Teece's (2007) arguments that firms gain competitive advantages through the *sensing*, *seizing*, and *reconfiguring* of capabilities.

5.1. Analysis of Target Data Breach

Target's data breach resulted in disastrous consequences which included heavy financial penalties of $252 million, reduced customer confidence, and a drop in stock prices. However, despite these outcomes, the company still survived the data breach, and is still currently a major competitor in the retail industry. A number of their practices adopted after the data breach can be attributed to their survival. Table 2 displays the analysis of how Target sensed, seized, and transformed their existing firm capabilities as dynamic capabilities to survive the data breach.

Table 2: Analyses of Target Case

Firm Capabilities	Sensing	Seizing	Reconfiguring
Managerial	• Risk identification of networked systems • Need for stronger integration of information security management and governance • Need for cybersecurity sharing initiatives • Need for improved organization structure	• Managing vendor account on stricter policies • Development of CISO and CCO roles • Developed partnerships with ISAC and the Retail Cyber Intelligence Sharing Center	• Re-envisioning PII's asset value as sensitive data on similar level to organization's own data • Re-engineering organization's management structure for information security and privacy governance
Marketing	• Need for customer recovery campaigns	• Engaged in public relations campaign to assure customers • Removal of liability to customers for fraudulent transactions • Offered free credit-monitoring service subscription	• Service provision to customers in the form of credit-monitoring
Technological	• Need for more secure POS terminals • Need for stronger networking standards	• Implemented two-factor Authentication • Pin-and-Chip implementation • Enhanced logging and monitoring system • Whitelisting on POS terminals • Network segmentation	• Reconfiguring Information Technology structure to reflect a more secure model
R&D	• Constant research requirements	• Enhanced logging and monitoring • Continued research into emerging threats from partnerships with threat-sharing initiatives	• Reconfiguring Information Technology structure to reflect a more secure model
Innovation	*N/A*	*N/A*	*N/A*
HR	• Need for corporate responsibility • Need for necessary security workforce	• Change in CEO and CIO positions • Hiring of CISO and CCO roles	• Integration of business and technology needs, security requirements and compliance measures

From the **managerial capabilities** perspective, Target recognized (or in other words *sensed*) the growing risk of unsecured systems through third-party entities. The data breach was attributed to the compromise of a user's credentials from Fazio Mechanical Services, which then led to the escalation of the attack by logging into Target's systems with the authorized credentials of the compromised user. Target *sensed* and *seized* the opportunity to address this risk by disabling multiple vendor accounts and reducing the privileges of specific accounts. Furthermore, Target's executives *sensed* and recognized the need for a different organizational structure; hence they seized the opportunity to develop both Chief

Information Security Officer (CISO) and Chief Compliance Officer (CCO) positions following the resignation of the CIO. This allowed for Target to ensure that expertise was developed in both security and privacy realms. Furthermore, creating these roles also ensured that necessary compliance measures were followed for handling PII and the companies' information assets. Target also became a member of two different threat-sharing initiatives, namely, Financial Services Information Sharing Analysis Center (ISAC) and the Retail Cyber Intelligence Sharing Center. Being a member of these threat-sharing initiatives would give them the opportunity to get alerts quickly as new threats were constantly analyzed in real-time. Lastly, as part of the *reconfiguration process*, managers needed to be equipped with the capability to recognize and re-envision PII on the same level as other sensitive organizational data; additionally, the management structure had to be re-organized to ensure that Target complied with security and privacy policies.

With regards to the **marketing capabilities** perspective necessary for data breach recovery, Target *sensed* and recognized the need for customer recovery and did so by developing public relations campaigns which would assure customers that technological components responsible for the data breach were destroyed and that new, more secure systems were being deployed. Furthermore, customers were not held liable to fraudulent transactions. As both a *seizing* and *reconfiguring* opportunity, Target also assured customers through offering free credit-monitoring services. This was not a one-time action, but an ongoing service to regain customer trust.

From the **technology capabilities** perspective, Target was required to change the security posture of the organization. *Sensing* and recognizing numerous vulnerabilities in the system, Target *seized* the opportunity to implement two-factor authentication, and prioritized their "chip-and-PIN" project to implement a chip card and personal identification number (PIN) payment system. This involved the replacement of all point-of-sale terminals to read the chip from credit and debit cards, as well as Target credit cards (REDcard), which is considered a more secure practice. Furthermore, the new POS systems utilized whitelisting of approved applications to avoid unwanted malware from being executed and compromising customer data. Additionally, Target moved away from a flat network structure to network segmentation (*wherein attackers would find it challenging to compromise critical information systems as such systems would exist on different subnets and behind firewalls with reduced open paths for network connectivity*).

Target recognized the need for stronger monitoring of network traffic which led to the implementation of enhanced logging and monitoring processes, necessary for detecting and preventing malicious activity. This is based on both the **technological capabilities** needed for stronger networking standards, as well as the **R&D capabilities** need for continued research of network traffic for malicious activity. In addition, cooperating with the threat-sharing initiatives allowed for the continued research to protect Target from future data breaches. For both the **technological** and **R&D capabilities**, Target was required to reconfigure their Information Technology (IT) structure to reflect a more secure role.

Innovation capabilities is a necessary firm capability for establishing competitive advantage (Breznik et al., 2019). However, for surviving data breaches and implementing stronger security and privacy practices, it may not be a necessary capability. Specifically, a company may not be required to produce a new product or service that has a unique and innovative nature to better protect their systems. Rather, benchmarking proactive security and privacy practices – both managerial and technical – can lead to better data protection and data breach prevention. In the case of Target, their technological implementations were not innovative, as they were already established practices in other organizations. Additionally, the development of different executive positions for better management and governance of information security and privacy had been implemented in previous organizations. In particular, one organization, ChoicePoint, which suffered a massive data breach in 2006, created a Chief Credentialing, Compliance and Privacy Officer (CCCPO) role (Litan, 2006). Hence, redefining the organizational

structure itself was not new. While **innovative capabilities** may further enhance the security and privacy posture of an organization in recovering from a data breach, it may not be a necessary component, as evident in the case of Target.

Finally, for **HR capabilities**, Target *sensed* and recognized the need for engaging in corporate responsibility due to the lack of attention given to preventing the data breach. Consequently, Target *seized* the opportunity to retire both the existing CEO and CIO, as well as conduct a review of the executive board of directors. Hiring the right people to provide leadership was necessary. At the same time, releasing those that were in a position to prevent the data breach but were not responsible enough to do so, could potentially have signaled to customers that change would occur and that their PIIs would be protected. Additionally, hiring both the new CISO and CCO would establish a stronger workforce with emphasis on protecting customers' PII. To build this workforce and subsequently *reconfigure*, Target required the establishment of these roles based on the convergence of business and technology needs, security requirements, and compliance measures.

In summary, Target was required to re-envision the role of PII in the organization. Organizations usually see PII as a resource that can be used for mining data, which would help them in developing specific promotional strategies catered to specific customers. However, the issue of privacy of PII is a major factor that can severely harm organizations due to consumers' fears. This requires organizations to restructure consumers' PII from a resource for data mining, into an asset that requires similar levels of protection as the company's very own data. Specifically, just as a company would segregate their network and provide encryption to secure information pertaining to their finances, intellectual property, and other critical information, they need to avoid decoupling consumers' PII from their own data, and provide the same or greater levels of protection, as suggested by Culnan and Williams (2009).

5.2. Anthem Data Breach

Anthem suffered a massive data breach in 2015 resulting in costs of $115 million in damages, and were found to be in violation of HIPAA before the data breach took place (US Department of Health and Human Services, 2017). While Anthem continues today as a successful healthcare provider, they did suffer another data breach in 2017. The impact of the follow-up data breach was much less severe, affecting only 18, 500 customers. Furthermore, the follow-up data breach was attributed to its consulting firm, Launchpoint Ventures. Nevertheless, when analyzing Anthem's data breach, one key **firm capability** that was ignored was **HR capabilities**. Anthem denied fault in the data breach of 2015, yet, Mandiant indicated that they did not take proper steps to ensure the customer data was well protected. Anthem was required to provide a stronger information security and privacy protection program, however, data did not reveal whether they considered restructuring the reporting structure of the CISO or CIO, nor is there mention of enhanced security education, awareness and training programs following the data breach. In comparison, following the data breach of ChoicePoint in 2006, employees were required to perform regular security training programs to prevent further data breaches (Litan, 2006). This was not the case for Anthem, whereby the follow-up data breach was attributed to an employee who was compromised via identity theft (Coombs, 2017). The analysis of the Anthem case is present in Table 3.

Table 3: Analyses of Anthem Case

Firm Capabilities	Sensing	Seizing	Reconfiguring
Managerial	• Cyber security strategy	• HIPAA Compliance • Collaboration with law enforcement and Mandiant for forensic analysis on data breach • Third-party settlement administrator for customer data protection	• Three-year protection plan
Marketing	• Required customer recovery program	• 24-month free credit reporting • Identity repair and protection	• Service provision to customers' data protection needs
Technological	• Enact stronger technological security standards	• Resetting passwords • Two-factor authentication • Data encryption • Expanded security logging and monitoring capabilities	• Reconfiguring Information Technology structure to reflect a more secure model
R&D	• Continued research requirements	• Expanded security logging and monitoring capabilities	• Reconfiguring Information Technology structure to reflect a more secure model
Innovation	*N/A*	*N/A*	*N/A*
HR	*N/A*	*N/A*	*N/A*

From the **managerial capabilities** perspective, Anthem *sensed* that they required an updated cybersecurity strategy, and *seized* the opportunity to ensure that they were HIPAA compliant with the Health Insurance Portability and Accountability Act (HIPAA). Additionally, *sensing* and recognizing that they needed to regain customer trust, they cooperated with a third-party settlement administrator to ensure that customers' data was adequately protected. Eventually, Anthem *reconfigured* their routines and processes to establish a three-year protection plan as part of their cyber security strategy, in order to recover from the data breach.

Similar to the Target case, Anthem *sensed* that customer recovery was key and *seized* the opportunity to establish customer reparation activities through compensation in the form of free two-year credit reporting, as well as offering identity repair and protection services. This was their strategy to enhance their **marketing capabilities**. Moreover, the plan was not a one-time initiative of assurance, but rather a customer reparation project involving long-term service to recover from the consequences of the data breach, as a means of *reconfiguring* their marketing capabilities.

Both the **technological** and **R&D capabilities** overlapped into each other from the perspective of data breach recovery, similar to the case of Target. Anthem *sensed* threats and vulnerabilities to their security infrastructure after the data breach and *seized* the opportunity to improve the same by encrypting critical data, as well as improving upon their access control and password policies. Anthem also engaged in expanding their security logging and monitoring capabilities. These activities stemmed from the need to implement stronger technological security standards, as well as the need for continued research of network traffic and user behavior on critical information systems, in hopes of *transforming* their technological and R&D capabilities.

As stated in the case of Target, **innovation capabilities** are less important in data breach recovery so long as the recovering organization implements security and privacy measures that can adequately protect against attacks. However, **HR capabilities** are a key component to data breach recovery as well as generally good security and privacy practices. Specifically, employee security education, training and awareness programs are necessary to ensure policy compliance and reduce IS misuse (D'Arcy & Hovav, 2009). While the information security function of an organization is responsible for the development of these programs, it is the task of HR to ensure that they are conducted and employees are held accountable to it. It is essentially a collaborative effort of both the security and privacy function of the organization and HR. In the case of Anthem, these capabilities were not seen, which can lead to the inference that the second data breach in 2017 was a result of the inability of Anthem to capitalize upon this capability.

5.3. Analysis of Yahoo Data Breach

At the time of the data breach, Yahoo was seeking to sell their business to another corporation. They were successful at achieving a $4.8 billion proposal by Verizon; however, this was before the organization revealed they suffered data breaches (Trautman & Ormerod, 2017). Yahoo was not necessarily seeking to recover from the data breach as they were already in the midst of selling the company, however, the consequence of the data breach led to a reduced price in the buy-out, as well as penalties to the organization's executive structure. Furthermore, Yahoo was required to rebrand themselves as Altaba Inc. However, several key insights can be gleaned from the Yahoo case in their inability to address the data breach, even within the short span of time in which senior management learned of the data breach and the announcement of the release.

Firstly, according to Trautman and Ormerod (2017), it can be observed that while Yahoo was not aware of all the details surrounding the data breach in 2014, they were aware of a data breach. The organization failed to pursue investigations, which was a result of poor **management capabilities**. The case study of Trautman and Ormerod (2017) also revealed that during the years in which the data breach occurred, Yahoo's management was complacent with the organization's technological infrastructure, and often ignored necessary security and privacy protections, such as encryption. Management saw security as a cost, and withheld investments in the security technological infrastructure necessary for securing users' PII. In addition, Yahoo was not proactive in their **marketing capabilities** to any stakeholder – users or Verizon, as they delayed the public disclosure of the data breach, rather than addressing it at an early stage.

The state of Yahoo in seeking to sell their business when they disclosed the data breach to the public indicates that they may have had little incentive to recover from the data breach. Afterall, from Yahoo's perspective, if the acquisition was successful, all liabilities would go to the buying company – Verizon. However, Yahoo did risk Verizon exiting the transaction. In addition, they lost $350 million from the buyout, members of senior management, acquisition of all business assets, and the identity they once had. Had there been a proper recovery strategy, wherein Yahoo could have utilized their existing firm capabilities to sense threats, seize opportunities, and reconfigure their resource base, the outcome could have been fruitful, as in the case of Target and Anthem.; however, that was not the case.

6. Discussion and Conclusion

This study examined the necessary organizational change – which also includes security and privacy practices – required for surviving the impacts of data breaches. A multiple case study analysis approach was used for this study whereby the data breach cases of Target, Anthem, and Yahoo were all examined using the **dynamic capabilities** framework. Observations from these three cases revealed that Target was the most successful following their data breach, whereas both Anthem and Yahoo were less

successful. Anthem, while successful in the data breach recovery process, did fall victim to another data breach in 2017. Alternatively, Yahoo suffered severely in being forced to rebrand the company as well as accept the lowered buy-out cost from the Verizon acquisition.

When observing the practices of these three cases, it can be seen that the **dynamic capabilities** of *sensing*, *seizing*, and *reconfiguring* were all necessary capabilities that acted upon the **firm capabilities**. Among the **firm capabilities**, however, only *innovation capabilities* can be considered as less important when it comes to data breach recovery. This is due to the nature of data breaches, where an organization may not necessarily need to innovate organizational, security, or privacy practices, but instead follow best practices. In all three cases, the organizations were lacking in their organizational, privacy, and security practices before the data breach occurred. However, *managerial*, *marketing*, *technological*, *R&D*, and *HR capabilities* were all necessary for successful data breach recovery. Specifically, Target engaged in all five above-mentioned **firm capabilities**, whereas, Anthem ignored the *HR Capability*, and Yahoo did not engage in any, based on the analysis. Supporting the observation of the saliency of these five capabilities is the follow-up data breach from Anthem which was caused by identity theft of an employee. This can be attributed to the lack of *HR capabilities* as ensuring proper security and privacy training is a partially shared responsibility by HR and IT functions in an organization. Furthermore, as revealed in the case study, Yahoo failed to engage in restructuring their organization on the basis of any of the above-mentioned **firm capabilities**. There was, however, some bleeding of **dynamic capabilities** between the firm **capabilities**. In particular, *technological* and *R&D capabilities* are often intertwined and involve the similar **dynamic capabilities**. This is not surprising, however, as Breznik et al. (2019) explained the close link these two capabilities share. Similar effects could also be observed, albeit to a lesser extent, between *managerial* and *HR capabilities*.

The observations made from this multiple case study analysis leads to proposing a **data breach recovery framework** rooted in the **firm** and **dynamic capabilities** approach developed by Breznik et al. (2019). Our proposed **data breach recovery framework** suggests that research in data breach recovery at the organizational level is reliant upon the *sensing*, *seizing*, and *reconfiguring* capabilities of a firm's *managerial, marketing, technological, R&D,* and *HR capabilities.* It should be noted that while *innovative capabilities* could possibly enhance the data breach recovery process, it is not a necessary component that could cause data breach recovery to fail if not acted upon by the organization.

This study consists of two main contributions. Firstly, we explain the necessary changes organizations are required to undergo to recover from data breaches. Specifically, organizations are required to act upon the dynamic needs of sensing environmental needs, seizing (or implementing) practices to address these needs, and reconfiguring processes to enact these needs, on five salient organizational functional needs – management, marketing, technology, R&D, and HR. Secondly, we proposed a model: the **data breach recovery framework**, which is rooted in Breznik et al.'s (2019) model, but analyzed in the context of data breaches which could be used by future researchers to better understand the data breach recovery process at an organizational level. Moreover, by identifying the necessary components of data breach recovery at an organizational level, research could advance into investigations of how organizations can further develop and capitalize upon the opportunities presented by data breach recovery. Essentially, this study opens a dialogue on organizational research on data breaches, their internal and external factors, as well as the outcomes following data breaches. In the next subsection, we discuss some managerial implications of this study.

6.1. Managerial Implications

With regards to managerial implications we believe that first and foremost, as part of enhancing and building managerial capabilities, employees must receive training on a regular basis to ensure that they build the required skillsets to sense and handle early signs of a data breach. Secondly, organizations

must redefine their strategy with regards to how they handle personally identifiable information (PII) of customers. As companies repeatedly use PII in creating targeted mobile and online marketing promotions aimed at specific groups of customers, it is imperative that companies set policies that explicitly create awareness for the customers about how their PII is utilized and what measures are taken to protect their data. By being more transparent with customers about how the data is handled, organizations could potentially enhance their marketing capabilities by building trust with their customers and establishing a loyal customer base. Additionally, organizations could also offer new products and services to the customer, with regards to identity theft protection and monitoring threats to the customer data, by continuously improving their innovation capabilities and benchmarking against competitors. However, with regards to keeping their infrastructure safe and secure, organizations should continuously invest in R&D in order to build and enhance their R&D and technological capabilities. Lastly, with regards to improving upon HR capabilities, organizations should strive to recruit employees who will not only be an asset, but will be involved in knowledge sharing initiatives, thereby ensuring that teamwork exists at all levels within the organization.

6.2. Limitations and Future Research

While our study uses secondary data for analyses similar to prior studies (Culnan & Williams, 2009; Dhillion & Moores, 2001), it is not without limitations. Firstly, as data was collected from secondary sources, it meant that unknown facts about each case could have existed that were not analyzed. Our second limitation was the number of case studies used. We used three case studies, each with differing outcomes to examine the dynamic capabilities framework proposed by Breznik et al. (2019) in the context of data breaches. More case studies could have been used, however, our choice of these three specific data breach case studies was reliant upon the impact of these three data breaches. Furthermore, the choice of these three data breaches allowed for studying the patterns among these cases found when the outcomes were different.

We propose a few directions for future research which can enhance or expound upon the phenomena studied in this paper. Firstly, we suggest that primary case studies could be used to test the framework presented in this study. In addition, quantitative approaches may be used, such as the use of an event-study approach. An event-study can assess the impact of the changes within an organization and the market value before and after the event.

In the event of a data breach, in addition to customer loyalty being in jeopardy, organizations are likely to lose the trust of the customers and this may result in customers switching to other competing brands in addition to them terminating their relationship with the organizations. In order to regain the trust of the customer as well as prevent them from brand switching, organizations should immediately draw up a compensation and recovery plan to ensure that customers do not feel isolated. Additionally, organizations should further step up their relationship building efforts with the customers, by being more transparent about how the data breaches occurred in the first place and what steps are being taken to ensure this does not happen again. Further research could potentially investigate which specific CRM practices are being adopted by organizations to regain trust and retain loyal customers.

References

Alonso-Almeida, M. D. M., Bremser, K., & Llach, J. 2015. Proactive and reactive strategies deployed by restaurants in times of crisis: Effects on capabilities, organization and competitive advantage. *International Journal of Contemporary Hospitality Management*, *27*(7), 1641–1661.

Bansal, G., & Zahedi, F. M. 2015. Trust violation and repair: The information privacy perspective. *Decision Support Systems*, *71*, 62–77.

Battisti, M., & Deakins, D. 2017. The relationship between dynamic capabilities, the firm's resource base and performance in a post-disaster environment. *International Small Business Journal*, *35*(1), 78–98.

Bélanger, F., & Crossler, R. E. 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, *35*(4), 1017–1042.

Benbasat, I., Goldstein, D. K., & Mead, M. 1987. The case research strategy in studies of information systems. *MIS Quarterly*, *11*(3), 369–386.

Breznik, L., Lahovnik, M., & Dimovski, V. 2019. Exploiting Firm Capabilities by Sensing, Seizing and Reconfiguring Capabilities: An Empirical Investigation. *Economic and Business Review for Central and South-Eastern Europe*, *21*(1), 5–135.

Cavusoglu, H., Mishra, B., & Raghunathan, S. 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104.

Choi, B. C., Kim, S. S., & Jiang, Z. 2016. Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, *33*(3), 904–933.

Culnan, M. J., & Armstrong, P. K. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Culnan, M. J., & Williams, C. C. 2009. How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly*, *33*(4), 673–687.

Coombs, B. 2017. New Anthem data breach by contractor affects more than 18,000 enrollees. Retrieved from : https://www.cnbc.com/2017/07/31/new-anthem-data-breach-by-contractor-affects-more-than-18000-enrollees.html

D'Arcy, J., & Hovav, A. 2009. Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, *89*(1), 59.

Desai, D., Sahu, S., & Sinha, P. K. 2007. Role of dynamic capability and information technology in customer relationship management: A study of Indian companies. *Vikalpa*, *32*(4), 45–62.

Dhillon, G., & Moores, S. 2001. Computer crimes: Theorizing about the enemy within. *Computers & Security*, *20*(8), 715–723.

Dube. L. 2016. Autopsy of a Data Breach : The Target Case. Retrieved from : https://www.hbsp.harvard.edu/product/HEC130-PDF-ENG?Ntt=&itemFindingMethod=Recommendation&recommendedBy=HEC187-PDF-ENG

Eisenhardt, K. M., & Martin, J. A. 2000. Dynamic capabilities: what are they?. *Strategic Management Journal*, *21*(10-11), 1105–1121.

Gatzlaff, K. M., & McCullough, K. A. 2010. The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61–83.

Goel, S., & Shawky, H. A. 2009. Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. 2017. User compensation as a data breach recovery action: An investigation of the Sony PlayStation Network breach. *MIS Quarterly*, *41*(3).

Gwebu, K. L., Wang, J., & Wang, L. 2018. The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683–714.

Hu, Q., Hart, P., & Cooke, D. 2007. The role of external and internal influences on information systems security–A neo-institutional perspective. *The Journal of Strategic Information Systems, 16*(2): 153–172.

Huang, L. C., Chu, H. C., Lien, C. Y., Hsiao, C. H., & Kao, T. 2009. Privacy preservation and information security protection for patients' portable electronic health records. *Computers in Biology and Medicine, 39*(9), 743–750.

Kump, B., Engelmann, A., Kessler, A., & Schweiger, C. 2018. Toward a dynamic capabilities scale: measuring organizational sensing, seizing, and transforming capacities. *Industrial and Corporate Change*.

Litan, A. 2006. Case Study: ChoicePoint Incident Leads to Improved Security, Others Must Follow. Retrieved from: https://www.gartner.com/en/documents/496516/case-study-choicepoint-incident-leads-to-improved-securit

Malhotra, A., & Kubowicz Malhotra, C. 2011. Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research, 14*(1), 44–59.

Martin, K. D., Borah, A., & Palmatier, R. W. 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58.

Myers, M. D. 2004. Hermeneutics in information systems research. *Social Theory and Philosophy for Information Systems*, 103–128.

Pavlou, P. A., & El Sawy, O. A. 2006. From IT leveraging competence to competitive advantage in turbulent environments: The case of new product development. *Information Systems Research, 17*(3), 198–227.

Peretti, K. K. 2008. Data breaches: What the underground world of carding reveals. *Santa Clara Computer & High Tech, 25*(2): 375–413.

Perlroth, N . 2017. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. Retrieved from : https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Peslak, A. R. 2006. Internet privacy policies of the largest international companies. *Journal of Electronic Commerce in Organizations, 4*(3): 46–63.

Pierson, B. 2017. Anthem to pay record $115 million to settle U.S. lawsuits over data breach. Retrieved from: https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML

Rasoulian, S., Grégoire, Y., Legoux, R., & Sénécal, S. 2017. Service crisis recovery and firm performance: Insights from information breach announcements. *Journal of the Academy of Marketing Science, 45*(6), 789–806.

Rotvold, G. 2008. How to create a security culture in your organization: a recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs. *Information Management Journal, 42*(6), 32–38.

Schwaig, K. S., Kane, G. C., & Storey, V. C. 2006. Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information and Management, 43*(7): 805–820.

Sher, P. J., & Lee, V. C. 2004. Information technology as a facilitator for enhancing dynamic capabilities through knowledge management. *Information & management, 41*(8), 933–945.

Teece, D. J., Pisano, G., & Shuen, A. 1997. Dynamic capabilities and strategic management. *Strategic Management Journal*, 18 (7): 509–533.

Teece, D., & Pisano, G. 1994. The dynamic capabilities of firms: An introduction. *Industrial and Corporate Change, 3*(3): 537–556.

Teece, D. J. 2014. The foundations of enterprise performance: Dynamic and ordinary capabilities in an (economic) theory of firms. *Academy of Management Perspectives, 28*(4), 328–352.

Trautman, L. J., & Ormerod, P. 2017. Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *American University Law Review, 66*, 1231–1291.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268.

Van Vaerenbergh, Y., Varga, D., De Keyser, A., & Orsingher, C. 2019. The service recovery journey: Conceptualization, integration, and directions for future research. *Journal of Service Research, 22*(2), 103–119.

Wade, M., & Hulland, J. 2004. The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly*, *28*(1), 107–142.

Witcher, B. J., & Chau, V. S. 2012. Varieties of capitalism and strategic management: Managing performance in multinationals after the global financial crisis. *British Journal of Management, 23*, S58–S73.

Endnotes

[1] Ponemon Institute. (2017). 2017 Cost of data breach study - Global overview. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.

[2] NASDAQ (2018). Target Corporation Common Stock (TGT) Quote & Summary Data. Retrieved from https://www.nasdaq.com/symbol/tgt.

[3] https://www.cbsnews.com/news/yahoo-data-breach-117-5-million-settlement-reached/