Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches

Zareef Mohammed
MISA, State University of New York College at Plattsburgh, Plattsburgh, New York, USA

Received 29 May 2021
Revised 30 September 2021
22 October 2021
Accepted 25 October 2021

Abstract

Purpose – Data breaches are an increasing phenomenon in today's digital society. Despite the preparations an organization must take to prevent a data breach, it is still necessary to develop strategies in the event of a data breach. This paper explores the key recovery areas necessary for data breach recovery.

Design/methodology/approach – Stakeholder theory and three recovery areas (customer, employee and process recovery) are proposed as necessary theoretical lens to study data breach recovery. Three data breach cases (Anthem, Equifax, and Citrix) were presented to provide merit to the argument of the proposed theoretical foundations of stakeholder theory and recovery areas for data breach recovery research.

Findings – Insights from these cases reveal four areas of recovery are necessary for data breach recovery – customer recovery, employee recovery, process recovery and regulatory recovery.

Originality/value – These areas are presented in the data recovery areas model and are necessary for: (1) organizations to focus on these areas when resolving data breaches and (2) future data breach recovery researchers in developing their research in the field.

Keywords Data breach recovery, Stakeholder theory, Service failure recovery, Information security, Information privacy

Paper type Conceptual paper

1. Introduction

Data breaches are a common phenomenon in today's digital age. The Identity Theft Resource Center (ITRC) reported approximately 1,108 data breaches in the year of 2020 (ITRC, 2020). Despite this number being a decrease by 19% from 2019, data breaches incur financial costs, along with additional negative outcomes such as the unfavorable reputation a company suffers from its clients and the public, post-breach. Financial costs associated with data breaches can incur, on average, $3.2 million in data breach costs, following reparation activities and lawsuits, while also suffering a 5% decline of stock prices after the data breach is disclosed (Ponemon Institute, 2017). Furthermore, organizations often face adversity with consumer relations, as many consumers may lose confidence in the organization's ability to protect information. An organization that suffers a data breach may compromise the organization's ability to operate in a competitive manner due to cases of regulatory compliance investigations, or compromise of other salient information assets necessary for an organization to operate optimally.

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 2 No. 1, 2022
pp. 41-59
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-05-2021-0014

A data breach is defined as an intentional or unintentional exposure of (electronically) collected data from an organization, which may include financial, personal or customer data (Goode *et al.*, 2017). Data breaches are commonly seen as an information privacy issue owing to the large impact it has on consumers if their personally identifiable information (PII) was compromised (Culnan and Williams, 2009). However, data breaches have also been used interchangeably as "security breaches" (Cavusoglu *et al.*, 2004) and "information breaches" (Malhotra and Malhotra, 2011). Essentially, a data breach at an organization may compromise both an organization's critical and non-critical information assets necessary for the organization's operations or information collected from stakeholders such as consumers and partners. Either way, any information that is deemed critical and is compromised can have negative impacts on an organization. It is often considered more severe if the compromised information belongs to consumers and other third-parties due to issues of service failure and breach of trust (Bansel and Zahedi, 2015; Choi *et al.*, 2016; Goode *et al.*, 2017).

Information systems (IS) research into data breaches often examine preemptive components to prevent data breaches (Culnan and Williams, 2009) or engage in customer recovery activities (Choi *et al.*, 2016; Goode *et al.*, 2017). However, preventative measures to data breaches, while important, and customer recovery tactics are not the only considerations for an organization following a data breach. Post-breach, an organization becomes chaotic as there are multiple areas of concern that require reparation for the organization's sustainability. Organizations need to account for the effect data breaches have on their functional areas and the effect data breaches have on the stakeholders of the organization.

Following a data breach, an organization needs to identify the affected stakeholders, as well as how these stakeholders themselves may affect the organization. Failure to assuage the concerns of the key stakeholders affected by data breaches can cause an organization to fail in its efforts toward data breach recovery. Hence, the aim of this paper is to explore the key recovery areas necessary for data breach recovery. The paper proposes the use of stakeholder theory in combination with the recovery areas identified from the service failure literature as a theoretical lens to study data breach recovery. Specifically, this paper is a conceptual study which is driven by the following questions: (1) Who are the stakeholders that are affected by, and affects, an organization after a data breach and (2) What are the recovery areas focal to successful data breach recovery? Three data breach cases are presented to provide merit to the argument of this paper, which contributes to the information security and privacy research disciplines by proposing a data breach recovery areas model. The next section of this paper discusses related literature to data breach recovery, followed by the theoretical foundations, illustrative cases, and finally, the discussion and conclusion.

2. Related literature

Research pertaining to data breach recovery in the IS discipline is relatively new. Prior research has often focused on preventative security and privacy measures to data breaches (Boss *et al.*, 2009; Culnan and Willaims, 2009; D'Arcy *et al.*, 2009; Mohammed *et al.*, 2017; Siponen and Vance, 2010). However, post-breach research often pertains to the impacts that the data breach has on the organization. Gaarg *et al.* (2003) established that a data breach can negatively affect an organization's share price. Similar findings were established using an event study approach to determine the effect of breach notifications on market value, market reactions and financial performance, resulting in negative relationships (Cavusoglu *et al.*, 2004; Ko and Durantes, 2006; Ko *et al.*, 2009; Goel and Shawky, 2009; Goldstein *et al.*, 2011; Telang and Wattal, 2007). These negative effects are also prevalent among investors (Andoo-Baidoo *et al.*, 2010). Yet, despite the effect of a data breach (or subsequently the breach notification that follows), research has also indicated that the type of data breach (for

example, the attacker type, how the data breach occurred, etc.) have varying, but still negative, impacts on the organization (Gordon *et al.*, 2011; Ko *et al.*, 2009; Morse *et al.*, 2011).

Despite the need for investigations pertaining to the preventative measures toward avoiding data breaches, it is evident that data breaches keep occurring. Organizations need to be prepared to handle the fallout of a data breach incident. Data breaches have often been likened, if not fully considered, to be a type of service failure (Bansel and Zahedi, 2015; Choi *et al.*, 2016; Goode *et al.*, 2017). A service failure is a disruption of the service processes of an organization, which often results in negative consumer attitudes toward an organization (Chen *et al.*, 2018; Goode *et al.*, 2017). There exists a plethora of research pertaining to service failure recovery often focusing on service failures such as flight cancellations and delays from airlines or similar contexts (Hazee *et al.*, 2017).

Service failure literature often studies customer outcomes such as negative word-of-mouth, loyalty, consumer trust repair, consumer re-patronage, consumer satisfaction, to name a few (Bozic, 2017; Casidy and Shin, 2015; Choi and Choi, 2014; Hazee *et al.*, 2017; Konuk, 2018; Noone, 2012). These studies often focus on understanding consumer reparation. Service failure literature renders itself applicable to data breach recovery because of the similarities between them. Researchers have adopted the service failure literature into data breach recovery, such as in the case of Bansal and Zahedi (2015) who studied trust repair after a data breach occurred, and Choi *et al.* (2016) who investigated the factors that would reduce customer likelihood to switching and negative word-of-mouth. Bansal and Zahedi (2015) established that the type of response an organization gives following a data breach (apology or denial) influences repaired trust but is moderated by whether the data breach was caused by an external hacking incident or the unauthorized sharing of PII. Choi *et al.* (2016) applied the justice framework of procedural, distributive and interactional justice, establishing that an organization's implementation of these justice approaches can influence a customer's psychological responses, and in turn affect the customer's word-of-mouth and likelihood of switching decisions. Goode *et al.* (2017) utilized expectation confirmation of compensation to determine the effects on three outcome variables: service quality, continuance intention and repurchase intention. Their study established that the levels of disconfirmation of compensation share a curvilinear relationship with these three outcome variables.

While the service failure literature greatly aids the investigation of data breach recovery, it is important to distinguish the difference between a service failure and a data breach. Service failure literature encompasses a multitude of service failures, however, what is common among them is the direct relationship between the service (i.e. the process of the organization) that the organization performs and the customer. Specifically, for a service failure, it is presumed that the organization needs to apply reparative measures with their customers for a service that the customer directly subscribes to – such as in the case of transportation service, where the organization would attempt to repair relations with customers following delayed or cancelled flights. However, there are two significant factors that make data breaches unique from other forms of data breaches.

Firstly, data protection is not the primary service for a transaction between an organization and customer, unlike services such as a flight or hotel accommodations. Rather, customers expect their PII will be kept protected by an organization as a by-product of their transaction with the organization for some product or service. While this protection of PII is still a service that the organization performs, it is only required if the customer makes a transaction of goods or other services. Thus, a data breach may have dual considerations from customers' perspectives. Customers may be satisfied with the service they are applying for but dissatisfied and threatened by the harm caused by the data breach.

Secondly, data breaches may incur heavier impacts on customers and other stakeholders as opposed to other service failures. When an individual's PII is compromised, they may be harmed through identity theft or financial losses (Culnan and Williams, 2009). As opposed to

service failure in the context of transportation or the food industry, the impact of a data breach may have more severe consequences, which may offset the satisfaction the customer has with the service they actively transacted with the organization to attain. This difference does not invalidate the application of service failure recovery research to data breach recovery research, but rather, requires data breach researchers to consider multiple other components of the organization that may be affected by data breaches. The theoretical foundations are discussed next.

3. Theoretical foundations

This paper argues that the successful recovery from a data breach requires an organization to identify the stakeholders that are affected by the data breach and in turn can affect the organization due to the data breach, as well as developing strategies to regain these stakeholders' trust in the organization. Hence, this paper proposes the application of stakeholder theory, in combination with the identified recovery areas within the service failure literature for exploring the key recovery efforts needed for an organization to successfully recover from a data breach. This is discussed next by firstly discussing stakeholder theory, and then delving into the major recovery areas identified in the service failure literature.

3.1 Stakeholder theory

Stakeholder theory pertains to the identification of stakeholders that can affect or are affected by the actions of an organization and the managerial responses by the organization to address this dyadic effect of the organization and stakeholders' interactions (Chan and Pan, 2008). Stakeholder theory is often seen as a normative theory, yet as explained by Freeman *et al.* (2020), it can be used for normative, descriptive and instrumental purposes. Freeman *et al.* (2020) explain that the core elements of stakeholder theory as the inclusion of:

> Human actors and their interactions in the process of (particularly, but not limited to, economic) value creation and trade in a turbulent world including the alignment of values, norms, and ethics as mechanisms for efficient and effective flourishing within and among organizations. (p. 219)

Researchers utilizing stakeholder theory have focused on the stakeholder identification process and the stakeholder management process (Friedman and Miles, 2002; Jawahar and McLaughlin, 2001). Stakeholder identification is separated into primary stakeholders and secondary stakeholders, whereby primary stakeholders pertain to those stakeholders that are crucial to the organization's success (Chan and Pan, 2008; Clarkson, 1995). Jawahar and McLaughlin (2001) developed a descriptive stakeholder theory, where the identification of primary stakeholders was based on the integration of organizational life cycle theory, resource dependence theory, prospect theory and stakeholder management. The descriptive stakeholder theory explained that during the organization's life cycle stage, some stakeholders will be more crucial than other stakeholders, however, as the organization moves from one stage to another, the importance of a stakeholder may increase or decrease accordingly to satisfy the organization's needs.

Stakeholder management seeks to propose strategies that would deal with the effects of the stakeholders (Chan and Pan, 2008). After the stakeholder identification stage, the stakeholder management stage finds its roots in strategic management research which involves the development of effective policies and strategies (Freeman *et al.*, 2020). Several strategic management approaches have been studied, which involves proactive, accommodative, defensive and reactive strategies (Chan and Pan, 2008; Clarkson, 1995; Jawahar and McLaughlin, 2001; Wartick and Chochran, 1985). The former approaches are more attractive than the latter two approaches to stakeholders (Chan and Pan, 2008).

Stakeholder theory assumes an organization is a system, with several components interacting and affecting one another (Freeman *et al.*, 2020; Kast and Rosenzweig, 1972). Considering data breach recovery, stakeholder theory is a salient theory for the analysis of which stakeholders are affected by the data breaches, which stakeholders will in turn affect the organization following the data breach, as well as the strategies required for solving these issues. Essentially, falling short on satisfying or attending to the issues related to stakeholders can cause detrimental effects to an organization.

3.2 Service failure recovery areas

Like service failure research, data breach recovery efforts focus on components that an organization requires to sustain themselves financially. This often includes investigating customer reactions and developing reparative measures to retain customers. However, data breach recovery efforts cannot only focus on reparation activities to customers. Johnston and Michel (2008) explained that three recovery efforts exist for service failure recovery that an organization must concentrate on: customer recovery, employee recovery and process recovery. These areas are interactional in that customer recovery is affected and can affect employee and process recovery and vice versa (see Figure 1).

Customer recovery is heavily focused on in both the service failure literature and in the data breach recovery literature (Goode *et al.*, 2017; Johnston and Michel, 2008). Findings in the service failure literature reveal several strategies for customer recovery, such as compensation, among others (Johnston and Michel, 2008). Customer recovery efforts can influence the customer actions towards loyalty, likelihood of switching, satisfaction and customer re-patronage (Bozic, 2017; Casidy and Shin, 2015; Choi and Choi, 2014; Hazee *et al.*, 2017; Konuk, 2018; Noone, 2012). However, a service recovery paradox (SRP) has been identified in the service failure literature where customers are likely to think more highly of the organization after the organization has addressed a service failure as opposed to before it occurred (Krishna *et al.*, 2014). This may be attributed to another service recovery – process recovery. Essentially, the customer may view the organization as moralistic if the organization made great efforts to address the service failure. Data breach recovery literature heavily focuses on customer recovery (Bansal and Zahedi, 2015; Choi *et al.*, 2016; Goode *et al.*, 2017).

Process recovery is more related to the operations management area of research, as it pertains to the improvement of business processes following a service failure. Process recovery is linked to customer recovery, as many customers seek improvements in business processes, both for the benefit of themselves and other customers (Johnston and Michel, 2008). Specifically, process recovery is argued to have an interactional effect with customer recovery, as the improvement of processes within an organization can allow for recovering current customers affected by a service failure, as well as, future customers, if these recovery efforts are communicated to customers (Vaerenbergh *et al.*, 2012). Within the context of data breaches, an organization will require improved business processes. The chance of a data

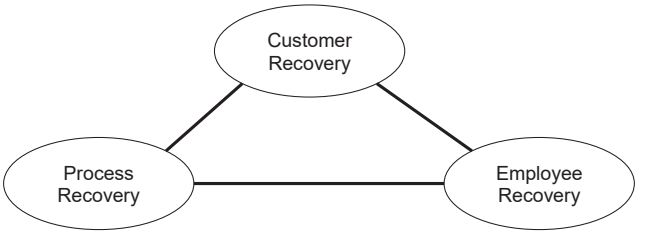

Figure 1.
Service failure recovery areas

breach occurring may be due to human elements, such as employees falling for phishing attacks, but the impact of the data breach may be attributed to the information security and privacy programs instituted within the organization. Following a data breach, these programs need to be revised to support the overall business goals, while ensuring risk is minimized and the likelihood of a data breach is reduced.

Employee recovery pertains to addressing the issues employees will face following a data breach. Specifically, employees are often faced with complaints from emotional customers, and employees themselves may experience a high degree of stress in attempting to resolve these issues (Johnston and Michel, 2008). Employees need to be trained on how to resolve service failures (Boshoff and Leong, 1998), while at the same time, an organization needs to help employees deal with the problems they face following a service failure (Johnston and Clark, 2005). With regards to data breaches, employees are not only faced with handling customer issues, but are also faced with security and privacy awareness requirements to ensure similar incidents do not occur in the future. In addition, data breaches may often involve employees' PII being compromised as well. For example, a data breach may involve the compromise of customer PII, but an employee may also be a customer of the organization as well. In such a situation, the employee has double the stress, as they are required to help resolve the business processes recovery and customer recovery efforts, while at the same time worry about the harm caused from the compromise of their own PII. Alternatively, the employee may not hold the dual role of being both internal and external to the organization, but instead, the impact of the data breach could be immense enough to the extent that both customer PII and internal employee records are also compromised. Either way, it is upon the organization to develop strategies to resolve these issues as it may have an impact on other areas of the data breach recovery process.

3.3 Stakeholders and service failure areas

This paper proposes stakeholder theory in combination with the areas of service failure recovery identified in service failure literature as necessary considerations for data breach research, as seen in the conceptual framework (see Table 1). As mentioned in Section 3.2, the service failure literature identifies customer, employee and process recovery as important facets of service failure recovery – and so too these areas should be considered as salient within the data breach recovery literature. However, limiting data breach studies to simply these three areas may not be fully sufficient given the uniqueness of a data breach in comparison to other service failures. Hence, stakeholder theory can help in better identifying these recovery areas for data breaches.

Concept	Description
Stakeholder theory	
Identify stakeholders • Internal stakeholders • External stakeholders	The identification of the (internal) members of an organization, as well as the (external) entities that may have an effect on an organization or may be affected by an organization. This would include employees and customers, and their interactions with the organization following a data breach
Recovery areas	
Customer recovery	The strategies enacted by an organization to alleviate the concerns and harms associated to customers following a data breach
Employee recovery	The strategies enacted by an organization to address the issues employees may face following a data breach
Process recovery	The improvement of business processes following a data breach to enhance the information security and privacy practices of an organization

Table 1.
Conceptual framework

The customer and employee recovery areas involve the apparent and major internal and external stakeholders of an organization, while the process recovery pertains to the strategies that can affect these stakeholders. Taken as a baseline, these three areas should be focused on in data breaches. However, other stakeholders may play a role in the data recovery process. Specifically, effective data breach recovery should begin with the identification of stakeholders which enables the identification of recovery areas (and their relation to the stakeholders), which in turn allows for a company to engage in data breach recovery actions (see Figure 2). In the next section, illustrative cases are presented to provide merit to the proposed conceptual model of this paper.

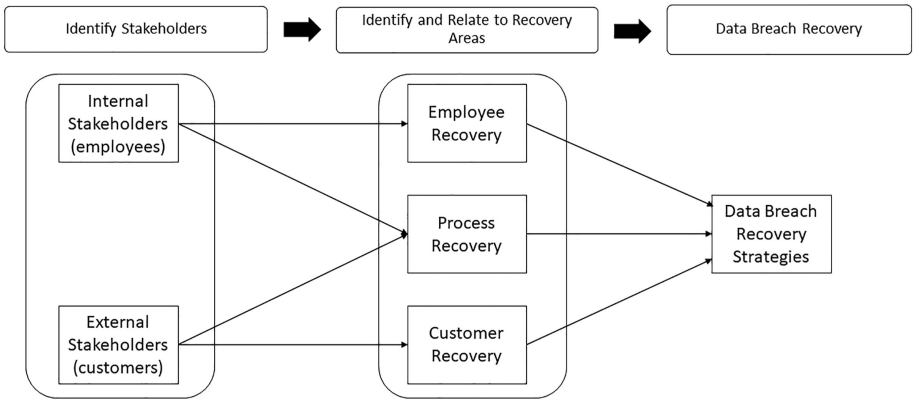

Figure 2.
Data breach recovery

4. Illustrative cases – drawing insights from major data breaches

Three data breach cases are used in this paper to elucidate the saliency of stakeholder theory and recovery areas as a theoretical foundation for conducting data breach research. Specifically, these data breach cases are the Anthem data breach of 2015, the Equifax data breach of 2017 and the Citrix data breach of 2019. The details of each case were derived from multiple secondary data sources such as news articles or case studies. IS research has used similar approaches where cases of major events helped to establish theory or explore research areas (Culnan and Williams, 2009; Wall *et al.*, 2015).

These cases were chosen for several reasons. Firstly, the data breaches were recent (i.e. occurred in the past 10 years). Data breaches often take years to resolve as it often involves process changes and lawsuits. Hence, to draw insights from a data breach incident, the data breach cases should have a few years to account for as many changes that occurred to the organizations because of the data breaches. Secondly, each data breach occurred roughly two years apart (i.e. 2015, 2017 and 2019), so that some evidence from these data breaches could be attained in some systematic manner. Finally, each data breach affected a vast majority of customers and/or employees. Furthermore, the data breach cases chosen were all well-established companies. These cases are discussed in the following subsections.

4.1 Anthem's data breach

Anthem is one of the largest medical healthcare insurance companies in the United States, based in Indianapolis, Indiana. They provide numerous healthcare services such as dental and medical insurances. In February of 2015, Anthem suffered a data breach affecting nearly eighty million Americans (Osbourne, 2015). Anthem disclosed this data breach stating that attackers had gained unauthorized access to one of their parent company's systems.

The attack on Anthem was identified when a database administrator for Anthem observed that a query using his credentials was initiated, when he did not initiate it himself (Ragan, 2015). It was also revealed that five other technical employees had their credentials compromised (Ragan, 2015). The database contained several pieces of sensitive PII such as medical IDs, email addresses, physical addresses, client names, date of births and social security numbers (SSN). Other sensitive medical records were not compromised, such as test results or financial information (Osborne, 2015). The compromised records involved both Anthem's customers and employees, as stated by the Chief Executive Officer (CEO) of Anthem at the time, Joseph Swedish:

> 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. (Barbash and Phillip, 2015)

Anthem used TerraData for their data warehousing infrastructure, which included several security controls, including user-level security controls, role-based access controls, encryption and auditing and monitoring features (Ragan, 2015). However, the attackers had used a spear-phishing attack to attain administrator credentials, which meant that these security controls could be bypassed by spoofing authenticated user activity. The attack was attributed to a state-sponsored Chinese cyber espionage group, and two Chinese nationals were indicted for the attack (O'Donnell, 2019). According to the Assistant Attorney General Brian Benczkowski:

> The allegations in the indictment unsealed today outline the activities of a brazen China-based computer hacking group that committed one of the worst data breaches in history. These defendants allegedly attacked U.S. businesses operating in four distinct industry sectors and violated the privacy of over 78 million people stealing their PII. The Department of Justice and our law enforcement partners are committed to protecting PII and will aggressively prosecute perpetrators of hacking schemes like this, wherever they occur. (O'Donnell, 2019)

In sum, Anthem's data breach was based on a purposeful attack as they were targeted for sensitive information and being among the top health insurance companies in the United States. The attack was initiated through a spear-phishing attack that led to the compromise of several technical member's access credentials, including administrator access. In total, around 80 million records were compromised.

Anthem was charged with several civil-class lawsuits. Pierson (2017) reported that Anthem had agreed to pay $115 million in damages. Among these lawsuits were those for violation of the Health Insurance Portability and Accountability Act (HIPAA) (US Department of Health and Human Services, 2018). An Office of Civil Rights (OCR) investigation revealed that Anthem lacked an enterprise-wide risk analysis, had insufficient procedures to review IS activity on a regular basis, insufficient identification and response to suspected or known security incidents, as well as did not implement the adequate minimum access controls to prevent cyber attackers from accessing sensitive PII (Armerding, 2019). In addition to these fines, Anthem was required to guarantee that they would allocate funding for a more proactive information security program involving changes to their security systems, which includes encryption of certain information and archiving sensitive data with strict access controls, to which they pledged to do over a three-year period.

Anthem provided customers who were affected by the data breach with two years of free credit monitoring, while any customer who was already enrolled in credit monitoring were given the option to receive up to $50 in cash (Pierson, 2017). In addition to compensatory measures to customers, Anthem has taken several steps to enhance their security operations. These include implementing two-factor authentication on all remote tools, resetting all passwords for associates and contractors, re-issuing new IDs and passwords for users with

escalated privileges, and expanding their security logging and monitoring capabilities (McGee, 2017; O'Neill, 2017).

4.1.1 Insights from Anthem's data breach. 4.1.1.1 Stakeholders. Anthem's data breach affected both customers and employees. Specifically, employees of the organization were also customers whose data were compromised (Barbash and Phillip, 2015). While these employees may have had a dual role, their concerns and frustrations would be different from that of regular customers since they were directly linked to the organization and its practices. A third external stakeholder emerged – regulatory bodies. Anthem was charged with several civil-class lawsuits including violations to HIPAA.

4.1.1.2 Customer recovery. Following the data breach, customers were identified as one of the key stakeholders that were affected. In turn, they could affect Anthem by engaging in several practices such as exiting business with the organization or spreading negative word-of-mouth. Anthem engaged in customer recovery processes such as providing two free years of credit monitoring or the option of $50 in cash if the customer was already enrolled in such services (Pierson, 2017). Specifically, Anthem offered a form of compensation to the customers that were affected by the data breach, while admitting to some fault in the occurrence of the data breach.

4.1.1.3 Employee recovery. Employees were also among those who were affected by the data breach, as some of them were also customers. Apart from this, employees may have gained additional stress from the data breach – to which employee recovery focuses on. Employee recovery may also involve additional processes such as restructuring, training and changing of culture, with regards to newer cybersecurity approaches needed by the organization. More intricate details about the issues employees would have faced following the data breach are not found in the Anthem case, given the extensive attention on the outcomes related to the customers, however, it does provide support that employee recovery is a needed area of research following a data breach.

4.1.1.4 Process recovery. Following the data breach, Anthem engaged in several steps to enhance their security operations, which involved implementing two-factor authentication, resetting passwords, re-issuing new IDs and expanding their security logging and monitoring capabilities. Process recovery is directly related to the other stakeholders of the organization – the customers, employees and regulatory bodies. Specifically, process recovery provides assurance to these stakeholders that the organization will improve their cybersecurity practices, while directly affecting employees themselves (such as in the case of additional security training or operational practices). Essentially, this recovery area is driven by the stakeholders of the organization, as can be seen in the case of Anthem.

4.1.1.5 Regulatory recovery. While not initially considered a part of the three recovery areas in the service failure literature, regulatory recovery emerges as a key recovery area for data breaches. Organizations are bounded by regulations pertaining to the collection and use of customers' PII. Data breaches often involve violations of these regulations, such as in the case of Anthem, where HIPAA compliance was lacking. This added to the costs Anthem had to pay following the data breach, while also requiring them to institute additional cybersecurity practices.

4.2 Equifax data breach

In 2017, Equifax experienced a major data breach that affected 145 million Americans (Srinivasan *et al.*, 2019). Equifax is one of three major US credit reporting companies alongside TransUnion and Experian. These credit reporting companies are responsible for collecting and providing credit information to both clients and organizations. Equifax business is centered around credit reports and scores used by customers and organizations for bill payment history, debt, loans and other financial information services. The case for

Equifax's data breach was adapted from Srinivasan *et al.*'s (2019) case study, where only the key points of the data breach are highlighted.

Even before the data breach, Equifax's information security processes were lacking, where they were compromised each year since 2013 (Srinivasan *et al.*, 2019). Specifically, credit reports, customer information and employee data were all exposed within these years prior to the data breach in 2017. They were warned about future problems and weak security infrastructure from a researcher, as well as from Mandiant – an organization that provides cybersecurity services to other organizations, among other cyber risk analysis firms (Srinivasan *et al.*, 2019). Equifax ignored these warnings which led to the data breach that occurred. Equifax's data breach was caused by a vulnerability within the Apache Struts open-source software used for building web applications. The Apache Foundation was notified of this vulnerability by a researcher and a software patch was issued on March 6th to address this vulnerability. Warnings of this vulnerability were issued by Cisco Systems and the US Department of Homeland Security's Computer Emergency Readiness Team (CERT) on March 8th (Srinivasan *et al.*, 2019).

Equifax ignored the Apache Struts vulnerability leading to the data breach. The attackers exfiltrated PII which included customers names, home addresses, phone numbers, date of birth, SSN, driver's license numbers and credit card numbers (Electronic Privacy Information Center, 2021). Equifax discovered the data breach in July, which was followed by notifying members of the board of the data breach in August (Srinivasan *et al.*, 2019). In early August, the Chief Financial Officer (CFO), president of the US information solutions, and the president of the workforce solutions sold approximately $1.8 million worth of stocks. Equifax did not release information about the data breach until September 7th, 2017. The public announcement of the data breach led to a decline of Equifax's stock price by about 35%.

To address the situation, Equifax engaged in providing several services to customers that were affected by the data breach. Specifically, free credit file monitoring services, credit lock and reports, identity theft insurance and SSN scanning on the dark web for one year were offered (Srinivasan *et al.*, 2019). However, despite the actions Equifax took post-breach to assuage the concerns of affected customers, they did face several challenges that further hurt the company's public image. Equifax had set up a website for customers to obtain information concerning the data breach but shared a fake website link on their twitter account that was setup by a researcher to demonstrate the security flaws of the website's domain. Furthermore, the services offered by Equifax faced criticism where customers needed to call TrustedID (the identity theft protection service owned by Equifax) after a year of free service to cancel their subscription or they would be charged monthly.

Several C-level executives resigned from Equifax, including the CEO, Chief Security Officer (CSO) and Chief Information Officer (CIO). Numerous lawsuits were filed against Equifax (Srinivasan *et al.*, 2019). The three executives who sold stock in August were charged with insider trading, along with investigations from the New York State Attorney General, San Francisco City Attorney and the Federal trade Commission (FTC). The FTC claimed that Equifax did not adhere to the "FTC Act Section 5: Unfair or Deceptive Acts or Practices", as well as the Gramm–Leach–Bliley (GLBL) Act's Safeguards Rule (FTC, 2019). Specifically, hackers accessed administrators' credentials from a file that was unencrypted leading to the data breach that followed – whereas the organization was supposed to implement technological and managerial cybersecurity measures to prevent this from happening.

Equifax was required to implement several changes following the data breach. Firstly, the Change-to-Win (CtW) sent six proposals to Equifax, focused mainly on the governance structure and accountability within the organization (Srinivasan *et al.*, 2019). Equifax was also required to designate an employee to oversee the cybersecurity program, conduct annual information security risk assessments of internal and external information management, apply the appropriate controls to prevent cyberattacks to their information assets, as well as

testing and monitoring their security safeguards (FTC, 2019). Additionally, Equifax would also be required to obtain annual certifications and third-party assessments attesting to the effectiveness of their information security programs, as well as ensuring their service providers engaged in similar cybersecurity procedures, if they accessed PII stored by Equifax (FTC, 2019).

4.2.1 Insights form Equifax data breach. 4.2.1.1 Stakeholders. Like Anthem, the stakeholders directly involved in the Equifax data breach were customers, employees and regulatory bodies. The data breach involved exposure of credit reports and customer information. Furthermore, investigations of the data breach found Equifax were in violation of the "FTC Act Section 5: Unfair or Deceptive Acts or Practices".

4.2.1.2 Customer recovery. Equifax offered free credit monitoring services, credit lock and reports, identity theft insurance, and SSN scanning on the dark web. Despite the offers made to regain customers' favor, Equifax did, however, face difficulties in their attempts. Overall, the data breach incident indicated the salience of customer recovery efforts following a massive data breach.

4.2.1.3 Employee recovery. Unlike the case of Anthem – it is unknown whether employees were also affected by the data breach (like customers), even though the likelihood is high. However, several organizational changes did occur. Before the data breach was made public, Equifax's top management engaged in suspicious actions, such as selling of stock. Eventually, this led to the resignation of the CEO, CSO and CIO. Newer management were hired for the organizational needs, as well as for improving the cybersecurity program. It stands to reason that these changes may cause internal conflicts within an organization and among employees.

4.2.1.4 Process recovery. Following the data breach, Equifax was required to improve their cybersecurity procedures. Specifically, they were required to designate an employee to oversee the cybersecurity program, conduct annual information security risk assessments, apply controls to prevent cyberattacks, improve upon their testing and monitoring safeguards and obtain third-party testaments of an improved cybersecurity program. While the case does not indicate whether Equifax carried through on these processes – the requirement of them following the data breach indicates process recovery is a key recovery area that Equifax needed to focus on.

4.2.1.5 Regulatory recovery. In the case of the Equifax data breach, the FTC claimed that Equifax did not adhere to the "FTC Act Section 5: Unfair or Deceptive Acts or Practices", as well as the GLBL Act's Safeguard Rule. The extent of how these regulations affected Equifax were not detailed in the case, but it is probable that they fed into the settlements that Equifax would have to pay, as well as other recovery activities. Nevertheless, the case provides merit that regulatory recovery is an important area of consideration due to the involvement of regulations pertaining to the privacy of PII collected from customers.

4.3 Citrix data breach

Citrix is a software development company located in Fort Lauderdale, Florida, and has been established since 1989, offering many cloud-based services (Gainsight, 2019). In 2019, the company suffered a data breach involving the exfiltration of six terabytes (6 TB) of data from an Iranian hacker group (Khandelwal, 2019). The data stolen affected approximately 24,314 individuals who were employees, contractors, interns, job candidates, beneficiaries and dependents of the company (Weston, 2021). Investigations suggested that the attackers used a "password spraying" attack – a type of attack that uses the same password for many different accounts to avoid account lockouts, and after gaining some access to the system, they would work on escalating privileges to more sensitive information (Khandelwal, 2019). Data stolen from the data breach included emails, blueprints, sensitive internal files and

business documents (Khandelwal, 2019; Weston, 2021). Citrix did notify affected individuals about the data breach based on several data breach notification regulations within the United States (Krebs, 2020).

A former employee of Citrix, Lindsey Howard, had filed a class action lawsuit against Citrix due to the data breach (Weston, 2021). The lawsuit stated:

> The data breach was the inevitable result of Citrix's inadequate approach to data security and the protection of its employees' personal information that it collected during the course of its business.

Based on the lawsuit, a settlement agreement of $2.28 million was made for Citrix to pay the former and current employees that were affected by the data breach (Weston, 2021). In addition, Citrix promised reimbursement for out-of-pocket losses, reimbursement for time spent addressing the breach issues, monitoring services and alternative cash payments (Citrixdatabreach, 2021). Additionally, Citrix also made commitments to improve the information security program for a three-year period.

4.3.1 Insights from Citrix data breach. 4.3.1.1 Stakeholders. In the case of Citrix, the main stakeholders were employees, as opposed to the Anthem and Equifax data breaches where customers were the main stakeholders. Specifically, the company's data breach involved the leaking of emails, blueprints, sensitive internal files and business documents. While Citrix released a data breach notification in an expedited manner – this was based on varying data breach notification laws in several states.

4.3.1.2 Customer recovery. In the case of the Citrix data breach, there is little evidence to support customer recovery as part of the data breach recovery areas, unlike in the case of Anthem and Equifax. However, this is due to the data breach focused on employee data and not customer data. A data breach constitutes the exposure of electronically collected data – whether that data is based on the company's proprietary or personnel data, or data collected on external entities. Hence, a data breach may not always be associated with customers. This does not devalue the role of customer recovery in data breach recovery, but rather shows that data breach recovery is a complex phenomenon which may involve several aspects of an organization – and in some cases, affect different stakeholders.

4.3.1.3 Employee recovery. The main stakeholders affected in the Citrix data breach were that of employees. Recovery efforts were undertaken to assuage the concerns of the employees, such as a monetary compensation to the (former and current) employees of the organization, reimbursement for the time spent addressing the data breach issues, monitoring services and alternative cash payments. This data breach case emphasizes the issues employees face, showcasing that employee recovery is a salient aspect of data breach recovery research – including how employees feel about their personal information is being collected while working at the organization and the protections placed on that personal information.

4.3.1.4 Process recovery. Process recovery is seen as a salient area of data breach recovery in the Citrix data breach as well. Citrix promised to enhance their cybersecurity program over a three-year period. While the case does not detail what these cybersecurity approaches are, it is evident that the commitment is a result of the data breach, in hopes that other data breaches do not occur, and as a means of assuring stakeholders that the company has accepted responsibility over the data breach.

4.3.1.5 Regulatory recovery. The case does indicate that Citrix's actions of notifying individuals of the data breach was based on data breach notification laws in several states of the United States. However, there is no direct evidence in the case that indicates Citrix was in violation of any regulations that they needed to repair following the data breach. This may be due to the recency of the data breach case, or it may indicate that Citrix were already in compliance to regulations, yet those regulations were ineffective against the attack that caused the data breach. Cybersecurity regulations and standards exist to help improve

cybersecurity programs but may not necessarily prevent data breaches in general. Research has found that many privacy laws are often reactive and outdated (DeGeorge, 2006), hence, it is possible for a company to adhere to all mandatory regulations but still experience a data breach. In this case, regulatory recovery may not be an especially focused area, but it is still salient for many organizations that experience data breaches in general. Essentially, data breach events may vary in who they affect with significant costs to the organization. The next section presents the discussion and conclusion.

5. Discussion

This paper explores the key recovery areas necessary for data breach recovery and proposes the use of stakeholder theory to better identify the recovery areas necessary for effective data breach recovery. While prior research considers data breaches as a form of service failure (Goode *et al.*, 2017), it is important to distinguish the difference between data breaches and other service failures. Data breaches do not impact the main service for which customers are transacting with an organization for, while also possibly carrying a much heavier impact to both customers and the organization. Ultimately, data breaches may be likened to service failures from the perspective of the impact on the customer, but it can also involve breaches which do not impact customers, but rather the critical information assets of an organization alone. While the latter is more of a security concern, and the former involves issues of security and privacy, they are still important considerations for studying data breach recovery.

Taking a systems view of an organization (Kast and Rosenzweig, 1972), a data breach may affect multiple components of an organization, directly and indirectly. The components of an organization, i.e. its functional areas and operations, impact one another as a working system would, which in turn influences the internal and external stakeholders of the organization (Freeman *et al.*, 2020; Phillips *et al.*, 2003). As such, it is necessary to identify the stakeholders affected by and in turn affects an organization in the event of a data breach. This paper proposed the implementation of stakeholder theory in combination with the service failure recovery areas (customer recovery, employee recovery and process recovery) as a theoretical lens to identify the necessary recovery areas needed for an organization to sustain itself following a data breach.

Three illustrative cases were presented to provide merit to the proposed conceptual model – Anthem's 2015, Equifax's 2017 and Citrix's 2019 data breaches. Insights drawn from these cases revealed that data breach recovery entails four main areas: customer, employee, process and regulatory recovery influenced by the stakeholders affected by the data breach. In addition, these stakeholders, except for regulatory bodies, conform to the recovery areas identified in the service failure recovery research – customer and employee recovery. Moreover, apart from activities toward stakeholders, multiple security and privacy activities (i.e. processes) are redesigned to better recover from the data breach. Table 2 summarizes these insights based on the conceptual framework.

The insights provided by the three cases indicate that data breaches are a complicated phenomenon that may not always involve the same stakeholders. Hence, identifying the stakeholders that are affected or affect the organization is a key element to data breach recovery. This allows for identifying the recovery areas that need to be focused on for successful data breach recovery. As can be seen in Table 2, both Anthem and Equifax involved the same stakeholders, while Citrix focused on the employees. For Citrix, customer recovery was not an area of focus, as it was in the case of Anthem and Equifax. This does not detract from the salience of any of the four identified recovery areas for data breach recovery (i.e. customer, employee, process and regulatory recovery). Rather, insights from the three cases indicates that each of these recovery areas plays a key role in data breach recovery, in general, though the specific area of focus pertains to the stakeholders involved in each data

Concept	Anthem	Equifax	Citrix
Stakeholders	• Customers • Employees • Regulatory Bodies	• Customers • Employees • Regulatory Bodies	• Employees
Recovery areas			
Customer recovery	Free credit monitoring or cash	• Free credit monitoring • Credit lock and reports • Identity theft insurance • SSN scanning on dark web	None that are apparent: Customers were not affected on the data breach
Employee recovery	Details on specific employee recovery activities were not found in the case, however, employees were also affected by the data breach as many employees' data were compromised, including the CEO at the time	Changes in organizational structure and management were caused by the data breach	• Reimbursement for time spent addressing data breach • Monitoring services • Alternative cash payments
Process recovery	• Implementation of two-factor authentication • Resetting passwords • Re-issuing ID's • Expanding security logging and monitoring capabilities	• Designate employee to oversee cybersecurity procedures • Conduct annual risk assessments • Apply appropriate cybersecurity controls • Improve testing and monitoring systems • Evaluated by third parties on cybersecurity effectiveness	• Commitment to enhance cybersecurity practices
Regulatory recovery	Additional costs due to HIPAA violations and improved cybersecurity practices required for HIPAA compliance	Violations of FTC Act Section 5: Unfair or Deceptive Acts or practices, as well as GLBL Act's safeguard Rule	None that are apparent: Notification actions were influenced by notification laws, but otherwise, there is little support for any recovery actions pertaining to regulations

Table 2.
Summary of insights

breach. Figure 3 presents the recovery areas pertaining to data breach recovery as derived from the stakeholders linked to an organization following a data breach.

5.1 Contributions

Data breach recovery fits within the realms of information security and information privacy research areas. This paper is exploratory and conceptual but contributes to these areas of information security and information privacy by providing a data breach recovery areas model. By identifying these recovery areas, this study lists the main areas of research necessary for data breach recovery literature. Specifically, data breach recovery literature is often limited to the customer recovery efforts of an organization (Bansal and Zahedi, 2015, Choi *et al.*, 2016; Goode *et al.*, 2017). These studies have provided excellent insights into customer recovery processes following a data breach but does not account for whether an

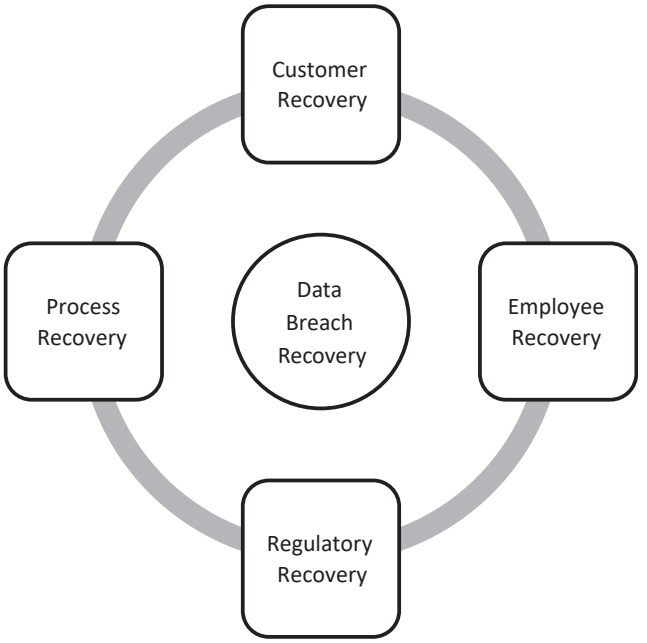

Figure 3.
Data breach recovery areas

organization will be able to sustain itself following a data breach. Data breach researchers need to also investigate employee issues, process issues, and regulatory issues following data breaches, which is a similar call to research in the service failure recovery field (Johnston and Michel, 2008). This may be done through micro-models of investigating one of the above identified recovery areas, like that of past IS research on customer recovery efforts (Bansal and Zahedi, 2015; Choi *et al.*, 2016; Goode *et al.*, 2017), or through a macro-model examining the effect these recovery areas have, on the whole, toward an organization's sustainability following a data breach.

5.2 Practical implications

As this paper is mainly conceptual in nature, there are limited practical implications that can be derived from observing the illustrative cases that were presented. Firstly, while preemptive approaches to prevent data breaches are must for all organizations, acknowledging that a data breach can and most probably will occur is a necessity for C-level executives in an organization. Organizations are often attacked based on their presence, as well as, by chance due to optimism from attackers (Ransbotham and Mitra, 2009). Any organization can suffer a data breach, and it is important for top management to enforce a strategy for handling the event of these incidents. This requires primarily identifying the main stakeholders who can greatly influence the organization following a data breach. Insights from the data breach cases identifies customers, employees, and regulatory bodies as the main stakeholders, however, there may be other stakeholders that can affect an organization in a primary capacity towards the organization's success or failure following a data breach. Managers need to consider who can affect the organization during a data breach and how to address the issues raised by them.

Secondly, senior executives should prepare for recovery events by dividing workgroups or task forces to the four identified areas of customer recovery, employee recovery, regulatory

recovery and process recovery. Both customer and employee recovery efforts should be swift and impactful to offset the harm caused by the data breach. Essentially, showing that organization is a moral agent (Culnan and Williams, 2009; Mohammed *et al.*, 2017) can provide a level of assurance to these stakeholders. Process recovery and regulatory recovery should involve task forces to engage in analyzing the processes that failed to prevent the data breach, and components of required regulations that were short of achieving the "bare minimum". While the process and regulatory recovery efforts can be expedited by engaging in proper security and privacy practices beforehand, it is important for an organization to be prepared to defend their security and privacy operations to regulatory bodies, while improving upon any socio-technical vulnerabilities that were exploited in the attack. In the next section, the conclusion is presented.

6. Conclusion

In conclusion, this paper explores the key recovery areas affected by essential stakeholders to an organization to effectively recover from a data breach. Insights from three data breach cases reveals that customer, employee, process and regulatory recovery areas are important areas of research for effective data breach recovery. The study contains few limitations. Firstly, three illustrative cases derived from secondary sources were used to provide merit to the conceptual framework consisting of stakeholder theory and recovery areas derived from the service failure literature. While this is acceptable for drawing insights and support to a conceptual model, future research papers should attain data from primary sources. Secondly, the use of stakeholder theory has been debated against as a theoretical lens where opponents have argued that the theory contains "tensions" and it is a "perspective" rather than a theory (Phillips *et al.*, 2003). Freeman *et al.* (2020), however, countered this argument by claiming that a theory does not need to be falsified, and that stakeholder theory provides insights into human actors and their interaction in the value creation process within organizations. Given this argument, for the purposes of this paper, stakeholder theory was sufficient in exploring the recovery areas necessary for data breach recovery. Future studies should build upon this conceptual model.

References

Andoh-Baidoo, F.K., Amoako-Gyampah, K. and Osei-Bryson, K.M. (2010), "How internet security breaches harm market value", *IEEE Security and Privacy*, Vol. 8 No. 1, pp. 36-42..

Armerding, T. (2019), "Advances in healthcare security since the Anthem data breach", available at: https://www.synopsys.com/blogs/software-security/anthem-healthcare-data-breach/.

Bansal, G. and Zahedi, F.M. (2015), "Trust violation and repair: the information privacy perspective", *Decision Support Systems*, Vol. 71, pp. 62-77.

Barbash, F. and Phillip, A. (2015), "Massive data hack of health insurer Anthem potentially exposes millions", available at: https://www.washingtonpost.com/news/morning-mix/wp/2015/02/05/massive-data-hack-of-health-insurer-anthem-exposes-millions/.

Boshoff, C.R. and Leong, J. (1998), "Empowerment, attribution and apologizing as dimensions of service recovery: an experimental study", *International Journal of Service Industry Management*, Vol. 9 No. 1, pp. 24-47.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", *European Journal of Information Systems*, Vol. 18, pp. 151-164.

Bozic, B. (2017), "Consumer trust repair: a critical literature review", *European Management Journal*, Vol. 35, pp. 538-547.

Casidy, R. and Shin, H. (2015), "The effects of harm directions and service recovery strategies on customer forgiveness and negative word-of-mouth intentions", *Journal of Retailing and Consumer Services*, Vol. 27, pp. 103-112.

Cavusoglu, H., Mishra, B. and 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*, Vol. 9 No. 1, pp. 69-104.

Chan, C.M.L. and Pan, S.L. (2008), "User engagement in e-government systems implementation: a comparative case study of two Singaporean e-government initiatives", *Journal of Strategic Information Systems*, Vol. 17, pp. 124-139.

Chen, T., Ma, K., Bian, X., Zheng, C. and Devlin, J. (2018), "Is high recovery more effective than expected recovery in addressing service failure? – a moral judgement perspective", *Journal of Business Research*, Vol. 33 No. 3, pp. 904-933.

Choi, B. and Choi, B. (2014), "The effects of perceived service recovery justice on customer affection, loyalty, and word-of-mouth", *European Journal of Marketing*, Vol. 48 No. 1, pp. 108-131.

Choi, B.C.F., Kim, S.S. and Jiang, Z. (2016), "Influence of firm's recovery endeavors upon privacy breach on online customer behavior", *Journal of Management Information Systems*, Vol. 33 No. 3, pp. 904-933.

Citrixdatabreach (2021), "In re: citrix data breach litigation", available at: https://www.citrixdatabreachsettlement.com/.

Clarkson, M.B.E. (1995), *A Risk Based Model of Stakeholder Theory*, University of Toronto, Toronto.

Culnan, M.J. and Williams, C.C. (2009), "How ethics can enhance organizational privacy: lessons from the ChoicePoint and TJX data breaches", *MIS Quarterly*, Vol. 33 No. 4, pp. 673-687.

DeGeorge, R.T. (2006), *The Ethics of Information Technology and Business*, Wiley Blackwell.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.

Electronic Information Privacy Center (2021), "Equifax data breach", available at: https://epic.org/privacy/data-breach/equifax/.

Federal Trade Commission (2019), "Equifax to pay $575 million as part of settlement with FTC, CFPB, and States related to 2017 data breach", available at: https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

Freeman, R.E., Phillips, R. and Sisodia, R. (2020), "Tensions in stakeholder theory", *Business and Society*, Vol. 59 No. 2, pp. 213-231.

Friedman, A.D. and Miles, S. (2002), "Developing stakeholder theory", *Journal of Management Studies*, Vol. 39 No. 1, pp. 1-21.

Gaarg, A., Curtis, J. and Halper, H. (2003), "Quantifying the financial impact of IT security breaches", *Information Management and Computer Security*, Vol. 11 No. 2, pp. 74-83.

Gainsight (2019), "Citrix upgrades to Gainsight NXT to enable its new customer lifecycle engagement methodology and drive higher retention", available at: https://www.gainsight.com/customer/citrix-2/.

Goel, S. and Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on firm values", *Information and Management*, Vol. 46 No. 7, pp. 404-410.

Goldstein, J., Chernobai, A. and Benaroch, M. (2011), "An event study analysis of the economic impact of IT operational risk and its subcategories", *Journal of the Association for Information Systems*, Vol. 12 No. 9, pp. 606-631.

Goode, S., Hoehle, H., Venkatesh, V. and Brown, S.A. (2017), "User compensation as a data breach recovery action: an investigation of the Sony PlayStation network breach", *MIS Quarterly*, Vol. 41 No. 3, pp. 703-727.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2011), "The impact of information security breaches: has there been a downward shift in costs?", *Journal of Computer Security*, Vol. 19 No. 1, pp. 33-56.

Hazee, S., Vaerenbergh, Y.V. and Armirotto, V. (2017), "Co-creating service recovery after service failure: the role of brand equity", *Journal of Business Research*, Vol. 74, pp. 101-109.

Identity Theft Resource Center (2020), "2020 data breach report", available at: https://notified.idtheftcenter.org/s/.

Jawahar, I.M. and McLaughlin, G.L. (2001), "Toward a descriptive stakeholder theory: an organizational life cycle approach", *Academy of Management Review*, Vol. 26 No. 3, pp. 397-414.

Johnston, R. and Clark, G. (2005), *Service Operations Management*, 2nd ed., Prentice-Hall, Harlow.

Johnston, R. and Michel, S. (2008), "Three outcomes of service recovery: customer recovery, process recovery and employee recovery", *International Journal of Operations and Production Management*, Vol. 28 No. 1, pp. 79-99.

Kast, F.E. and Rosenzweig, J.E. (1972), "General systems theory: applications for organization and management", *Academy of Management Journal*, Vol. 15, pp. 447-465.

Khandalwal, S. (2019), "Citrix data breach – Iranian hackers stole 6TB of sensitive data", available at: https://thehackernews.com/2019/03/citrix-data-breach.html.

Ko, M. and Dorantes, C. (2006), "The impact of information security breaches on financial performance of the breached firms: an empirical investigation", *Journal of Information Technology Management*, Vol. 17 No. 2, pp. 13-22.

Ko, M., Osei-Bryson, K.M. and Dorantes, C. (2009), "Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms", *Information Resources Management Journal*, Vol. 22 No. 2, pp. 1-21.

Konuk, F.A. (2018), "Price fairness, satisfaction, and trust as antecedents of purchase intentions towards organic food", *Journal of Consumer Behavior*, Vol. 17 No. 2, pp. 141-148.

Krebs, B. (2020), "Hackers were inside Citrix for five months", available at: https://krebsonsecurity.com/2020/02/hackers-were-inside-citrix-for-five-months/.

Krishna, A., Dangayach, G. and Sharma, S. (2014), "Service recovery paradox: the success parameters", *Global Business Review*, Vol. 15 No. 2, pp. 263-277.

Malhotra, A. and Malhotra, C. (2011), "Evaluating customer information breaches as service failures: an event study approach", *Journal of Service Research*, Vol. 14 No. 1, pp. 44-59.

McGee, M.K. (2017), "A new in-depth analysis of Anthem Breach: insurance commissioners conclude nation-state involved, reach settlement with insurer", available at: https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627.

Mohammed, Z.A., Tejay, G.P. and Squillace, J. (2017), "Utilizing normative theories to develop ethical actions for better privacy practices", *Journal of Information Privacy and Security*, Vol. 13 No. 4, pp. 296-315.

Morse, E.A., Raval, V. and Wingender, J.R. Jr (2011), "Market price effects of data security breaches", *Information Security Journal*, Vol. 20 No. 6, pp. 263-273.

Noone, B.M. (2012), "Overcompensating for severe service failure: perceived fairness and effort on negative word-of-mouth intent", *Journal of Services Management*, Vol. 26 No. 5, pp. 342-351.

Osborne, C. (2015), "Health insurer Anthem hit by hackers, up to 80 million records exposed", available at: https://www.zdnet.com/article/health-insurer-anthem-hit-by-hackers-up-to-80-million-records-exposed/.

O'Donnell, L. (2019), "Chinese hackers behind 2015 Anthem data breach indicted", available at: https://threatpost.com/chinese-hackers-anthem-data-breach-indicted/144572/.

O'Neill, P.H. (2017), "Anthem will pay $115 million in largest data breach settlement in history", available at: https://www.cyberscoop.com/anthem-data-breach-settlement/.

Phillips, R., Freeman, R.E. and Wicks, A.C. (2003), "What stakeholder theory is not", *Business Ethics Quarterly*, Vol. 13 No. 4, pp. 479-502.

Pierson, B. (2017), "Anthem to pay record $115 million to settle US lawsuits over data breach", available at: https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML.

Ponemon Institute (2017), "2017 Cost of data breach study – global overview", available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.

Ragan, S. (2015), "How does a data breach like this happen?", available at: https://www.csoonline.com/article/2881532/anthem-how-does-a-breach-like-this-happen.html.

Ransbotham, S. and Mitra, S. (2009), "Choice and chance: a conceptual model of paths to information security compromise", *Information Systems Research*, Vol. 20 No. 1, pp. 121-139.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Srinivasan, S., Pitcher, P. and Goldberg, J.S. (2019), *Data Breach at Equifax*, HBS No. 9-119-031, Harvard Business School Publishing, Boston, MA.

Telang, R. and Wattal, S. (2007), "An empirical analysis of the impact of software vulnerability announcements on firm stock price", *IEEE Transactions on Software Engineering*, Vol. 33 No. 8, pp. 544-557.

US Department of Health and Human Services (2018), "Anthem pays OCR $16 million in record HIPAA settlement following largest US health data breach in history", available at: https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html.

Vaerenbergh, Y.V., Lariviere, B. and Vermeir, I. (2012), "The impact of process recovery communication on customer satisfaction repurchase intentions, and word-of-mouth intentions", *Journal of Service Research*, Vol. 15 No. 3, pp. 262-279.

Wall, J.D., Lowrey, P.B. and Barlow, J. (2015), "Organizational violations of externally governed privacy and security rules: explaining and predicting selective violations under conditions of strain and excess", *Journal of the Association of Information Systems*, Vol. 17 No. 1, pp. 39-76.

Wartick, S.L. and Cochran, P.L. (1985), "The evolution of corporate social performance model", *Academy of Management Review*, Vol. 10 No. 4, pp. 758-769.

Weston, S. (2021), "Citrix employees win $2.3m settlement over 2019 data breach", available at: https://www.itpro.com/security/data-breaches/358454/citrix-to-settle-2019-data-breach-for-23-million.

Corresponding author
Zareef Mohammed can be contacted at: zmoha003@plattsburgh.edu