



Universiteit
Leiden
The Netherlands

Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises

Kuipers, S.L.; Schonheit, M.

Citation

Kuipers, S. L., & Schonheit, M. (2021). Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. *Corporate Reputation Review*.
doi:10.1057/s41299-021-00121-9

Version: Not Applicable (or Unknown)

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/3249895>

Note: To cite this publication please use the final published version (if applicable).

Corporate Reputation Review

Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises

--Manuscript Draft--

Manuscript Number:	
Full Title:	Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises
Article Type:	Original Article
Funding Information:	
Abstract:	Online data breaches are recurrent and damaging cyber incidents for organizations worldwide. This study examines how organizations can effectively mitigate reputational damages in the aftermath of data breaches by hacking through situational crisis communication strategies. Comparable data breach crises do not have an equally negative impact on organizational reputation. Providing comprehensive and exhaustive guidelines, and detailed explanations about the incident to consumers helped to reduce the damage. Organizations that primarily relied on one single strategy, performed better than those that inconsistently blended strategies. Particularly denial was ultimately detrimental to organizational reputation. Self-disclosure allowed companies to positively influence media reporting. Social media communication did not play an important role in the response of the organizations involved. The consistent and timely adoption of compensation, apology and rectification strategies, combined with reinforcing strategies such as ingratiation and bolstering, positively influenced reputational recovery from the crisis.
Corresponding Author:	Sanneke Kuipers, Ph.D. Leiden University: Universiteit Leiden NETHERLANDS
Corresponding Author Secondary Information:	
Corresponding Author's Institution:	Leiden University: Universiteit Leiden
Corresponding Author's Secondary Institution:	
First Author:	Michael Schonheit, Msc
First Author Secondary Information:	
Order of Authors:	Michael Schonheit, Msc Sanneke Kuipers, Ph.D.
Order of Authors Secondary Information:	
Author Comments:	Dear editor(s) Please accept the submission of our manuscript 'Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises' which we think would be a good fit for your esteemed journal. Thank you so much for your time and consideration. We look forward to hearing from you. Sincerely, Sanneke Kuipers and Michael Schonheit

Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises

Michael Schonheit¹

Sanneke Kuipers, Leiden University, ORCID 0000-0002-0934-5406^{2 3}

ABSTRACT

Online data breaches are recurrent and damaging cyber incidents for organizations worldwide. This study examines how organizations can effectively mitigate reputational damages in the aftermath of data breaches by hacking through situational crisis communication strategies. Comparable data breach crises do not have an equally negative impact on organizational reputation. Providing comprehensive and exhaustive guidelines, and detailed explanations about the incident to consumers helped to reduce the damage. Organizations that primarily relied on one single strategy, performed better than those that inconsistently blended strategies. Particularly denial was ultimately detrimental to organizational reputation. Self-disclosure allowed companies to positively influence media reporting. Social media communication did not play an important role in the response of the organizations involved. The consistent and timely adoption of compensation, apology and rectification strategies, combined with reinforcing strategies such as ingratiation and bolstering, positively influenced reputational recovery from the crisis.

KEYWORDS: crisis communication, data breach, cyber security

le 1.4 Integrating Recovery Trends and Response Strategies

¹ Michael Schonheit works as consultant for Deloitte, the Netherlands.

² Sanneke Kuipers is associate professor Crisis Governance at Leiden University's Institute of Security and Global Affairs. Contact author at: s.l.kuipers@fgga.leidenuniv.nl

³ On behalf of all authors, the corresponding author states that there is no conflict of interest.

Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises

ABSTRACT

Online data breaches are recurrent and damaging cyber incidents for organizations worldwide. This study examines how organizations can effectively mitigate reputational damages in the aftermath of data breaches by hacking through situational crisis communication strategies. Comparable data breach crises do not have an equally negative impact on organizational reputation. Providing comprehensive and exhaustive guidelines, and detailed explanations about the incident to consumers helped to reduce the damage. Organizations that primarily relied on one single strategy, performed better than those that inconsistently blended strategies. Particularly denial was ultimately detrimental to organizational reputation. Self-disclosure allowed companies to positively influence media reporting. Social media communication did not play an important role in the response of the organizations involved. The consistent and timely adoption of compensation, apology and rectification strategies, combined with reinforcing strategies such as ingratiation and bolstering, positively influenced reputational recovery from the crisis.

KEYWORDS: crisis communication, data breach, cyber security

Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises

Introduction

With the emergence of the digital economy, cybersecurity has rapidly become a critical condition for organizations to thrive and maintain their core business activities. As business information and communication systems are increasingly reliant on digital technology and data, the paramount objective of cybersecurity revolves around preserving the availability, integrity and confidentiality of online data (MERGroup 2020). Online data breaches represent one of the most recurrent and damaging cyber incidents for organizations worldwide. The Risk Based Security's 2020 year-end report estimates that in 2019 alone 15.1 billion confidential records have been exposed to unauthorized use. This statistic represents an increase by 284% compared to 2018, and confirms a constant trend throughout the decade (Sobers 2020; Winder 2020).

Online data breaches are conditional on factors endogenous to organizations, including inconsistent data retention and handling policies, internal misuse, system vulnerabilities and human errors. Nevertheless, for exposed records to be leveraged into identity theft or fraudulent abuse of confidential information, data breaches also depend on external actors criminally exploiting unauthorized access to data. Therefore, we define as data breach: "unauthorized entry point into a corporation's database that allows cyber hackers to access customer information"(Martin 2019, 1), for instance through phishing emails, DDoS attacks, and Trojan horses.

Data breaches impose on organizations worldwide unparalleled monetary costs (MERGroup 2020; Arghire 2020). While total cyber security expenditures worldwide have rose from approximately \$113 billion in 2015 to \$173 billion in 2020, in the same timeframe the costs of data breaches and cybercrime at large have doubled, reaching an astonishing total of

1 \$6 trillion (Columbus 2020). Direct costs affecting organizations suffering a data breach
2 include: business disruption and recovery, forensic investigations, legal proceedings, regulatory
3 fines, credit monitoring for customers, crisis management advisory. These costs constitute just
4 the tip of iceberg. Indirect costs include reputational damages and loss of consumer trust, which
5 can turn the cyber incident into a corporate reputational crisis that affects business in the long
6 run (Kim, Johnson, and Park 2017; Wang and Park 2017)
7

8 Indirect organizational damages are particularly relevant for defining the options left to
9 organizations to effectively reduce the impact of a data breach. While cyber incidents cannot
10 be entirely prevented by cybersecurity measures, reputational damages depend on the public
11 perception of an organization in crisis, to be mitigated in the incident response phase with
12 effective crisis communication strategies (Kim, Johnson, and Park 2017; Wang and Park 2017)
13

14 Therefore we study crisis communication strategies that organizations can employ to
15 effectively reduce reputational damages and loss of consumer trust. This study aims to examine
16 how organizations can mitigate reputational damages in the aftermath of data breaches through
17 crisis communication strategies. The selected cases of corporate data breaches vary on the
18 degree of financial and reputational recovery from the crisis to assess the influence of
19 communication strategies.
20

21 While the vast majority of studies on data breaches focus on the legal and technological
22 aspects of the phenomenon, the intersection with crisis communication strategies remains
23 under-researched and undertheorized. With the cyber domain being dominated by security
24 scholars focusing on prevention, vulnerabilities and threats, cyber crisis management, focusing
25 on consequences and responses to cyber incidents, remains vastly overlooked (Hawkins 2017;
26 Kim, Johnson, and Park 2017). This article thus asks why some organizations maintain their
27 reputation with consumers in the aftermath of a cyber data breach, while others fail to do so.
28

The next section will introduce the main insights from on crisis communication to explain variation in reputation damage in eight data breach cases.

Cyber crises and data breaches

Cyber crises are exceptionally difficult to manage, as their nature complicates the key characteristics of off-line crises: threat, uncertainty and urgency (Rosenthal, Charles, and 't Hart 1989). First of all, threats in cyberspace are not straightforward: they may manifest themselves in a variety of ways, affect multiple unrelated parties, and involve stakeholders and authorities from widely dispersed geographical and different functional domains. To responsible actors, the source of the threat, its scope and its consequences are often (partly) invisible and ill-understood, which increases uncertainty in the response phase. Invisibility and ignorance may also influence awareness and sense of urgency, which are further influenced by the fact that the threat and even the escalation path of the crisis, may go undetected for a while and morphs over time. The consequences manifest themselves in seemingly unconnected ways, or the symptoms may have been repaired while the root cause lives on.

Data breaches only become crises, when they are both exposed and impactful. They are exceptionally difficult to detect, resulting in a time lag between the actual breach and its exposure (Chickowski 2013; Lopes, Guarda, and Oliveira 2019). Data breaches become impactful when they compromise the confidentiality, integrity, and availability of company data (Rouse 2020). That same suspicious email containing a malicious payload or that software being in fact a drive-by malware unintentionally downloaded on the system, can suddenly turn everyday events into cybersecurity incidents (Hikmet et al. 2015).

Full prevention is nearly impossible as cybercriminals typically find themselves ahead of the security curve. No matter how consistently organizations commit to their avoidance, data breaches are likely to occur. A purely preventive approach thus needs to be complemented with

mitigation measures. When prevention is unattainable or too costly, the imperative is to accept the risks and mitigate the consequences (Comfort, Boin, and Demchak 2010; Wisner, Gaillard, and Kelman 2012; Sen and Borle 2015) Data breaches, where both the probability and impact of adverse events are high, therefore require prevention, detection, as well as recovery measures. This mixed approach, embodied in the National Institute of Standards and Technology (NIST) framework, is the fundamental pillar of cyber risk management (Krumay, Bernroider, and Walser 2018).

However, legal and technical studies in the realm of cyber security largely prioritize a preventive approach. Investigating the attack sequence of a data breach by hacking aims at exposing eventual vulnerabilities and improving organizational resilience against future events. Similarly, the system of liabilities imposed in a given legal system has the underlying intent of deterring offenders and simultaneously encourage organizations to invest in their information security system to prevent unintended disclosures of information. However, Kim et al. (2017) argue there is a substantial lack of scholarly research that deals with data breaches from a crisis response perspective, particularly in terms of crisis communication.

Reputation threats and crisis communication

The Situational Crisis Communication Theory (SCCT), holds that ‘attributions of crisis responsibility have a significant effect on how people perceive the reputation of an organization in crisis and their affective and behavioral responses to that organization following a crisis’ (Coombs 2010, 38). In contrast to Image Restoration Theory, which guided the study by Gwebu et al. (2018) that similarly deals with communication response to data breaches, the SCCT, by providing a comprehensive framework to reconcile response strategies with situational elements of a crisis, allows to generalize and predict outcomes, anticipating patterns of dependency and establishing systematic inferences among the variables at play. Coombs (2010) stresses a link

1 between the inherent features of a crisis and the most commensurate response to such an event.
2 SCCT offers a comprehensive framework to reconcile response strategies with situational
3 elements of a crisis. The framework discerns between crisis types and intensifying factors to
4 assess the degree of crisis responsibility that stakeholders will attribute to the organization after
5 an incident.
6
7
8
9
10

11 First, SCCT postulates a typology of crises based on initial organizational responsibility:
12 victim crisis, accidental crisis and preventable crisis. Each crisis type links to a predetermined
13 communication response strategy cluster. These strategy clusters (Deny, Diminish, Rebuilding,
14 Reinforcing), can be effective as standalone methods or in conjunction with others (Amaresan
15 2019; Coombs 2010). Crisis types correspond to the framing of the event rather than the nature
16 of the crisis itself.
17
18
19
20
21
22
23
24
25

26 A crisis type is a construct resulting from the narrative of the events as reported by media
27 and communication channels and does not constitute a preliminary fixed category (Coombs
28 2007b; 2007a). Exploiting the so-called framing-effect communicators can influence public
29 perception. Crisis types relate to different degrees or attributed responsibility and correspond
30 to minimal crisis responsibility (victim crisis), low-moderate crisis responsibility (accidental
31 crisis), high crisis responsibility (preventable crisis). The more an organization is perceived to
32 be accountable for a crisis, the more its reputation will suffer.
33
34
35
36
37
38
39
40
41
42

43 Victim crises include situations believed to be entirely outside of the organization's
44 control, such as natural disasters, employee misbehavior, and product tampering by external
45 parties. The victim crisis exempts the organization from having a causal role, implying a mild
46 reputational threat. In Accidental crises, the organization's course of actions lacked any
47 intentionality and it had limited control over the event (Coombs 2004). Accidental crises imply
48 a low attribution of crisis responsibility to the organization, and they pose moderate reputational
49 threats. Preventable or intentional crises represent situations where high crisis responsibility is
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 attributed to the organization, generating severe reputational threats (Coombs 2010). The
2 organization is held directly accountable for the crisis development because it intentionally
3 caused the crisis or could have avoided its occurrence yet failed to do so. This typology ranges
4 between crises involving competency-based trust violations (accidents) in the form of human
5 errors, to integrity-based trust violations (scandals) such as organizational misdeeds (Coombs
6 2007a). Human errors are generally believed to preventable, a distinction which is particularly
7 relevant for the purpose of this study (Morris, Moore, and Sim 1999).
8
9

10 Direct crisis responsibility is not the only factor that can influence the reputation threat
11 posed by a crisis. Coombs (2010) introduced two intensifying factors: crisis severity and
12 performance history. Crisis severity refers to the impactful proportions of a crisis regardless of
13 the responsibility of the organization, in terms of environmental, financial or human damage.
14 Performance history is the sum of two intertwined but independent variables: crisis history and
15 relationship history. Crisis history refers to similar incidents that implicated the same
16 organization in the past. Relationship history relates to the structural quality of the relationship
17 between that same organization and its public, stakeholders or consumers, prior to the incident.
18 When a crisis comes to light, the media and public base their attribution of cause on the crisis
19 history and relationship history of the organization, which take the form of “causal antecedents”
20 (Coombs 2004). Such causal antecedents give an organization a disadvantageous position since
21 the public is likely to attribute it with a higher level of responsibility for yet ‘another’ crisis
22 (Coombs 2010).
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50

51 **Crisis communication response strategies**

52
53

54 Crisis response efforts should always begin with ‘base responses’: *instructing* and *adjusting*
55 information tasks aimed directly at shaping the public perception of the event (Coombs and
56 Holladay 2002). Instructing information serves to secure or shield stakeholders from physical
57
58
59
60
61
62
63
64
65

1 damages, or additional harm triggered by the crisis. Additionally, *adjusting* information
2 influences the narrative of the events, by feeding the audience with information over the
3 evolution or reparation of the crisis, or conveying messages of concern or sympathy towards
4 the affected parties (Coombs 2010).
5
6
7
8

9 Subsequently, organizations move onto selecting among response strategy clusters
10 based on the reputation threat they face. These clusters, *denial*, *diminish*, *rebuild*, and
11 *reinforcing* strategies, include strategies with similar core functionality and applicability. While
12 *reinforcing* strategies function as supplemental and supporting measures, *deny*, *diminish* and
13 *rebuild* are clusters of primary standalone responses. An organization can choose to respond to
14 increasing levels of attributed responsibility for a negative event between strategies that range
15 from denial to rebuild. In absence of intensifying factors (crisis severity, performance history),
16 these response options correspond to the identified crisis typologies: victim, accidental and
17 preventable crises (see Table 1.1). Victim crises could be handled with deny measures, such as
18 scapegoating or denial. Accidental crises need diminish strategies, such as excuses (refute
19 intentions) or deny volition (claiming lack of control over the event). Finally, responses to
20 preventable crises should include rebuild strategies, ranging from apologies to transcendence
21 (positive statements detaching the company from the crisis) (Coombs 2010). If intensifying
22 factors apply, organizations should upgrade their response to the commensurate increased threat
23 level.
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44

45 *Reinforcing* strategies are not standalone response strategies but they supplement
46 primary crisis communication responses. For instance, *bolstering* means drawing on past merits
47 and achievements, while *ingratiation* commends stakeholders for their support and loyalty, and
48 *endorsement* publicly makes reference to a third party supporting or validating the work done
49 by the organization. Also, organizations can resort to *victimage* to reaffirm to the audience that
50 the organization is itself a victim of the crisis (Coombs 2007a; Liu 2010).
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

[Table 1.1 SCCT response strategy clusters HERE]

Only few studies have tested the effect of crisis communication strategies on corporate reputational damages (Avery and Park 2016; Coombs 2007b; 2007a; Robertson 2012; Park 2017) An even more limited number of studies have addressed how to communicate effectively during a cyber security incident or data breach. Robertson (2012) suggests that best practices from the general field of crisis communication and cyber-specific crisis communication are aligned. We therefor proceed towards gathering first-hand observations from reputational crises ignited by data breaches to assess what strategies are to be considered most effective in those cases.

Effective Crisis Communication and Data breaches

Selecting the appropriate response depends on the level of attributed responsibility, which makes an accurate assessment of the reputation threat imperative for crisis communication managers. Data breaches are not a self-evident crisis category in terms of communication strategy. Most studies address data breaches as a source of risk and not as crises, either in operational or reputational terms (Khan et al. 2019). This tendency is rooted in the academic and practical prioritization of a preventive approach over a mitigating one, overshadowing the relevancy of crisis management and communication theories for cyber incidents.

This ambiguity in crisis classification affects the way existing studies currently assess the level of attributed responsibility for data breach crises. Organizations undergoing a data breach crisis tend to adopt defensive strategies, normally undertaken in cases of minimal attributed responsibility (Kim, Johnson, and Park 2017). Yet, as man-made incidents, data breaches may require more accommodative responses in light of a higher attributed responsibility for the organization's obsolete security systems, lack of training and security

1 policies, poor implementation of procedures (Ramakrishna 2012). Jenkins et al. (2014) even
2 argues that the standard response to a data breach should involve apology and regret strategies.
3

4 The high degree of attributed responsibility recognized by Ramakrishna (2012) and
5 Jenkins et al (2014) could moderately decline in cases of breaches by hacking due to the
6 involvement of third-party offenders. Data breach by hacking is therefore a selection criterion
7 for our comparative case study. Data breaches (by hacking) find themselves halfway between
8 the victim crisis type and the preventable crisis one, in the accidental crisis cluster, which
9 presumes the involvement of the organization with low direct controllability and no
10 intentionality. A corporate response posture to data breaches (by hacking) would then first
11 resort to base responses (adjusting and instructing) coupled with either diminish or rebuild
12 strategies. This study aims to compare the effects of the response recipes chosen by each
13 organization in dealing with data breaches.
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

31 **The outcome variable: economic and reputational repercussions**

32 To answer the question why some organizational reputations after data breaches recover and
33 others do not, we need to compare cases in-depth on their crisis communication strategies.
34 Following a Most Similar System Design, the data breach cases share contextual similarities
35 and a similar expected level of attributed responsibility. Meanwhile, they vary in terms of
36 successful and unsuccessful recovery from their data breaches. A combined analysis of both
37 economic and reputational damage serves to assess the recovery of companies in this study.
38
39
40
41
42
43
44
45
46
47

48 First, we assess the economic impact of a PR data breach is based on the fluctuation of
49 the stock market value of the organization in question, in relation to the overall market trend
50 (Metrica 2011; Robertson 2012; Reed 2015; Bischoff 2019). This method remains the most
51 widely adopted to measure the consequences of adverse events in economic terms. The stock
52 values will be observed at different points in time preceding and following the event in order
53
54
55
56
57
58
59
60
61
62
63
64
65

to depict and control the trend in their price fluctuation (MacKinlay 1997; Campbell et al. 2003; Hovav and D'Arcy 2004; Goel, Brown, and Shawky 2007).

To control for concurrent effects of overall market performance during that same period, the specific company stock prices on the New York Stock Exchange (NYSE) will be compared with the NYSE Composite Index (NYA). In addition, the companies' year-on-year percentage change in revenue will be calculated for the fiscal quarter preceding the breach announcement and the two following it. The direct costs imposed by legal proceedings and compensations, or by contractions in sales all together might affect the volume of earnings.

Second, assessment of reputation damage requires media news tracking. Research on corporate reputation often studies media coverage for an assessment of reputational damage (Wartick 1992; Carroll and McCombs 2003; Kim, Johnson, and Park 2017). A Reputation Index attributes to companies a score ranging between -100 and 100, with the first indicating only negative coverage and the latter only positive media coverage (Eisenegger 2004; Cravens, Oliver, and Ramamoorti 2003; Weverbergh and Vermoesen 2020). The score is attributed by applying the following formula:

$$\frac{\text{Good Press} - \text{Bad Press}}{\text{All Press}} \times 100$$

This assessment of the relevant press will use the ProQuest automated online search platform, monitoring the media coverage during the three months following each crisis. The main media outlets of reference are the main US newspapers in terms of distribution and influence: The Washington Post, New York Times, Wall Street Journal, and USA Today. This selection is in conformity with most applied studies reviewed and updated rankings (Coombs 2010; Robertson 2012; Kim, Johnson, and Park 2017).

Combined, the indicators per case on stock devaluation and negative media coverage that followed the data breach, will reveal the variation in effectiveness of the recovery strategy deployed. The selected observation period of 3 months presumes, in line with Bishoff (2019), that the reputation damage mainly occurs in the period immediately following the event (Kim, Johnson, and Park 2017; Robertson 2012). As a result, this study will select the 2 most and least effective cases per each of two observed periods, resulting in a total of 8 cases.

Case selection

For a valid comparison of the effects on recovery from a reputational crisis, the selected cases need to have a similar initial attribution of responsibility. The data breach incidents must therefore be comparable in volume and sensitivity of records disclosed and the method of breaching. First, a comparable volume of data breached implies the illicit disclosure of a significant amount of consumers' records. An appropriate benchmark for the impact of the data breach is that the volume of compromised information pertains to at least 1 million records (Bischoff 2019). Such incidents are most likely to provide similar *crisis severity* as an intensifying factor to the reputational threat. In contrast to Gwebu et al. (2018), by focusing on stabilizing the degree of crisis severity rather than crisis history, we effectively allow for more quantifiable and inclusive criteria to build the dataset.

A second selection criterion is the sensitivity of the data disclosed during the breach and the degree of difficulty faced by the organization in applying corrective measures. We include three types of compromised data, together forming the category "*Highly Sensitive Information*" (McCallister, Grance, and Scarfone 2010). First of all, Personally Identifiable Information (PII), that can be directly leveraged into identification crimes without the need to be associated to a second identifier, such as passport numbers, national identification numbers, driver's licenses or equivalent. Second, Payment Card Industry data (PCI), which include any protected financial

1 information including card and account numbers. Third, Protected Health Information (PHI),
2 related to any medical information linked to a subject. The compromising of these data seriously
3 affects people's lives, and leaves little room for instant reparatory fixes (Bischoff 2019).
4
5

6
7 Selecting data breaches that disclosed at least 1 million records of highly sensitive
8 information, allows us to compare data breaches in multinationals across different sectors and
9 industries. By focusing on these data breach characteristics, we can expand the relevance and
10 external validity of this research for cyber crisis communication response practices across
11 corporate organizations, sectors and countries.
12
13

14
15 The selected cases have the same organizational context, as they are all listed on the
16 New York Stock Exchange (NYSE), which represents most of the established major-league
17 businesses, whose stocks are perceived as more stable (Bischoff 2019; Szmigiera 2020). We
18 will focus only on cases of breaches by hacking, in an attempt to rule out alternative factors
19 influencing public perception of data breaches achieved in a *physical locus* (paper data loss,
20 unauthorized entry), committed *unintentionally* (data leakages) or explicitly caused by
21 negligence, malicious insiders or inappropriate security measures. This will increase
22 comparability of the level of attributed responsibility (Khan et al. 2019). Finally, all cases
23 selected have incurred legal proceedings which increases comparability of the direct and
24 indirect costs imposed by the data breach.
25
26

27
28 For assessing the crisis communication response, organizations' own press releases,
29 their reactions reported in articles from the selected newspapers, and posts published on the
30 organizations' Facebook and Twitter accounts will be tracked and analyzed. Experts identify
31 the role of social media as pivotal for achieving effective crisis communication (Reed 2015;
32 Preen 2020).
33
34

35
36 To control for the role of progressive digitalization of media communication and the
37 evolution of social media, we will analyze four events that occurred between 2007 and 2013
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

(the first period), and four data breaches that occurred between 2014 and 2019 (the second period). The first period represents the launch phase of all the most important social media platforms. The second period represents the most prolific phase in their use. Both periods allow us to select among the highest number of data breaches compared to any other decade in history and generate insights with high relevance for today's corporate and media landscape (Kim, Johnson, and Park 2017; Zhou 2020).

Bishoff (2019) and Klebnikov (2019) claim that newer data breach cases meet less harsh market and media reactions than older cases. They coined the term “*Breach Fatigue*: the market and the public at large are becoming accustomed to instances of data breaches, and do not react as strongly as they used to. Also, organizations may have been learning from past crises and becoming more aware and prepared at managing data breach reputational crises. To control for this possibility, in addition to comparing data breach cases varying on the degree of recovery within each of the two distinct periods selected, the two periods are compared.

Case information from Bishoff's study (2019), the Privacy Rights Clearinghouse's database (2020), and the Identity Theft Resource Center's (ITRC) annual reports (n.d.) from 2007 to 2019 generated a comprehensive inventory of 64 corporate data breaches. All 64 cases pertained both to more than 1 million records and included highly sensitive information, 28 of which occurred between 2007 and 2013 and 36 in the 2014-2019 timeframe. Next, the three remaining selection criteria—hacking as data breach cause, the stock exchange of the organization, and the certainty of legal costs—suggest 13 cases to further select from based on variation in the dependent variable, and representation of different sectors (see Tables 1.2 and 1.3).

The final dataset is composed of 8 corporate data breaches, distributed equally across the periods (see Table 1.2 and 1.3). Each period features specialized retailer companies, such as Target, The Home Depot, or TJX, credit reporting and payment services companies such as

Global Payments and Equifax, and insurance and financial service providers such as Anthem and Capital One. Lastly, technology and electronics manufacturer giant SONY completes the list of cases constituting this comparative analysis.

[Table 1.2: List of Data Breaches from Period I (2007-2013) HERE]

[Table 1.3: List of Data Breaches from Period II (2014-2019) HERE]

Stock and Revenue analysis

The assessment of the stock price movement of the selected organizations over a period of 3 months after the event follows standard event study guidelines as explained in the operationalization of this study (Hovav and D'Arcy 2004; Goel, Brown, and Shawky 2007; Campbell et al. 2003; MacKinlay 1997). Between 2007 and 2013 none of the selected organizations came unscathed out of a data breach event.

The disclosure of the breach impacts the stock values the very next day. After the initial shock, none of the organizations was able to recover their stock price loss in the three following months. Target and TJX followed a similar pattern of stock value changes: both companies contained the adverse effects of the crisis at first, but saw an enormous downfall halfway the period observed and only partially recovered their losses towards the end. By contrast, SONY and Global Payments' stock price followed a far more linear path. Global Payments reports an astonishing value loss of -17.7% and SONY -19%, over three times more than Target and TJX. The overall NYSE market capitalization remained quite stable during the Target and SONY data breaches, while being subject to more significant oscillations during the TJX (attenuating the disruptive impact) and Global Payments periods (potentially aggravating the impact). The year-on-year revenue changes confirm the tendency observed from the stock analysis.

Between 2014 and 2019, organizations suffering a data breach perform in an opposite direction. Two of the breached organizations, Anthem and The Home Depot, have in fact

increased their stock value during the timeframe observed. The other organizations both took a serious fall and then stabilized at a loss. Meanwhile, the NYA Index has maintained a stable gain and even shows moderate growth in the same period. The year-on-year periodic revenue data confirm the results of the stock performance analysis.

5.3 News Media tracking and Reputation Index scores

To assess the reputational effect on the breach organizations as depicted by media, coding the narrative adopted in media articles will inform the calculation of the Reputational Index Coefficient (Eisenegger 2004). Given the specific nature of the crises addressed in the articles, the value scale is naturally tipped towards a negative tone, rendering eventual positive statements detaching the company from the crisis (transcendence) or praising its past and present behavior (bolstering) as particularly significant factors from a weighting perspective.

THE TJX DATA BREACH: The TJX case broke the record for the amount of data disclosed and was treated as an unprecedented phenomenon by every actor involved [7]. Three New York Times reports published immediately after the event, refrained from pointing fingers to TJX directly, but addressed the event as a symptom of an emerging, wider, problem [TJX2, TJX3, TJX4]. Due to inadequate enforcement of regulatory requirements, the TJX case was part of “a collective problem with collective responsibility” [TJX1: 1]. Along with reporting concerns expressed by TJX management, another article reduced the size of the disclosed records to “substantially less than millions” [TJX2: 1]. Later, the Wall Street Journal and the Washington Post pointed at the larger size of the data breach and at serious concerns arising from the banking sector, along with declarations from victims reporting fraudulent activities on their accounts.

Initially TJX dismissed the inflammatory claims: “We're not commenting about what others are saying about the situation” [TJX6: 1]. Then the Washington Post set the timeline

1 straight, revealing that the breach started at least 18 months before and that TJX simply had “no
2 idea what was going on” [TJX7: 1]. By this point, media widely discussed TJX cybersecurity
3 failures, repeatedly quoting sources inside the company to ridicule their security posture: “It
4 was as easy as breaking into a house through a side window that was wide open” [TJX5: 2].
5 The apology at the end of the 3 months window, indicated that TJX was slow at assuming
6 responsibility. While one article assumed a particularly soft stance in treating TJX’s role in the
7 crisis, and two neutral, 4 articles painted a significantly worse picture. The TJX Reputation
8 Index score thus equals -43, a result obtained by applying the following formula: $(1-4) \times 100/7$.
9
10
11
12
13
14
15
16
17
18
19
20

21 **THE SONY DATA BREACH:** The data breach that struck SONY compromised 77 million
22 records and a Play Station network outage of over 20 days. Users therefore directly experienced
23 the consequences of the hack long before the company made a first public statement about it.
24 Only one of the ten news stories retrieved for this case did not directly accuse the company of
25 wrongdoings but provided the audience with guidelines on how to protect themselves [S1]
26
27
28
29
30
31
32
33

34 The main narrative centered around SONY’s shortcomings in its crisis response.
35 Various critics blamed the company for initially dismissing the event as a routine incident, for
36 the failed attempt at scapegoating the hacktivist group Anonymous, and ultimately for their
37 “lack of transparency and their seeming inability to issue clear, unambiguous instructions to
38 their (former) customers” [S10: 1]. SONY had “failed the internet” and without a
39 transformation “it will be a fallen giant indeed” [S5: 2, S8: 3]. While the Japanese conglomerate
40 was firmly denying that credit cards information was compromised, card fraud linked to the
41 breach began to feature in the press, together with several class action lawsuits against SONY
42 for encryption security failures and consumer law violations [S6, S9]. For instance, the
43 Financial Times claimed that SONY “failed to encrypt data and establish adequate firewalls to
44 handle a server intrusion contingency, failed to provide prompt and adequate warnings of
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 security breaches, and unreasonably delayed in bringing the PSN service back on line” [S4: 1].

2 In addition, the media began to report on ongoing FBI investigations [S2, S3, S6, S8, S10].

3
4 In sum, 9 out of 10 sources analyzed strongly attributed responsibility to Sony, which
5 following the Reputation Index formula $(0-9) \times 100/10$, results in a score of -90.
6
7

8
9
10
11 **THE TARGET DATA BREACH:** In December 2013, hackers exfiltrated 110 million records,
12 penetrating Target’s server environments by leveraging third-party vendor credentials into
13 poorly segmented POS systems. The incident was first reported by KrebsOnSecurity, which
14 immediately put Target on the defensive [17]. In total 24 news stories surfaced throughout the
15 crisis indicating the gravity of the reputation risk Target faced. The articles referred to Target’s
16 refusal to comment on the details of the breach, and anticipated the risk of fines and profit losses
17 during a critical time of year (Christmas) for the retail corporation. These media reports further
18 disputed Target’s excuse that the attack was highly sophisticated [TG1, TG15, TG16]
19
20
21
22
23
24
25
26
27
28
29
30

31 Instead, news sources focused on the insufficient cybersecurity preparedness of Target
32 demonstrated before and during the event [TG11, TG13, TG17, TG19]. Two articles somewhat
33 downplayed Target’s role in the data breach, claiming that such instances are common across
34 sectors and that states should have enhanced roles in preserving data security [TG2, TG18].
35 Five news articles critically reported on the size of the breach and the economic and legal
36 repercussions suffered by the company including a 46% drop on quarter sales. Target’s
37 cybersecurity systems had been “astonishingly open” and Target “foolishly resisted” the
38 introduction of more secure but expensive chip-based cards [TG13: 1; TG11: 2]. Meanwhile,
39 Target’s response was seen as evasive and superficial, as its executives initially refused to
40 disclose information, declaring to be in compliance with regulations and limiting their
41 comments to effusive apologies [TG2, TG3, TG4].
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 However, as news that the hackers penetrated the systems through third-party vendors
2 emerged, the Washington Post and Wall Street Journal started to include praise for Target's
3 compensation commitments and for Target's CEO Gregg Steinhafel using various
4 communication channels for instructing information, apologies and compensation plans. These
5 articles claimed the company was retaining customers and shareholders by adopting
6 communication strategies by the "playbook" [TG7: 1]. The more positive frames and the source
7 of the cyber vulnerability, de facto shifted the blame to smaller companies that paved the way
8 to hackers for breaching major corporations [TG4, TG5, TG6, TG8, TG23]. Other news stories
9 were neutrally balancing attributions of responsibility with vague comments such as "it happens
10 every day, everywhere" [TG10, TG12, TG15, TG22].
11
12
13
14
15
16
17
18
19
20
21
22
23

24 Nearly three months after the breach, the pendulum swung back. Five articles strongly
25 reinforced attributions of responsibility when new facts came to light, portraying internal
26 divisions among executives, overwhelmed call centers, CEO communication struggles, costs
27 over 1 billion dollars and insufficient compensation efforts leading to contractions in Target's
28 consumers base [TG6, TG10, TG14, TG20, TG24]. Overall, with 6 positive, 6 neutral and 12
29 negative news stories, the cumulative score attributed to Target through the Reputation Index
30 formula equals -25 $[(6-12) \times 100 / 24]$.
31
32
33
34
35
36
37
38
39
40
41
42

43 **THE GLOBAL PAYMENTS DATA BREACH:** Global Payments attracted far less media coverage
44 and only in the first week of the crisis. The hack, initially brought up by Krebs on security, caused
45 alleged compromise of 10 million payment card accounts. The WP and the WSJ introduced the
46 news by downplaying the proportions of the breach compared to other cases, with dismissive
47 statements referring to Global Payments as a "little known company" [GP4: 1, GP1]. Also,
48 these articles emphasized structural vulnerabilities affecting payment service merchants at
49 large. Forbes even further detached Global Payments from the responsibility for the event, by
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 asserting that the company “merely passes on transaction details to card networks like Visa and
2 MasterCard” and that it had already taken the necessary measures to contain the leakage [GP5].
3

4 Other news redirected the responsibility again towards Global Payments. Three articles
5 zoomed in on Visa’s removal of Global Payments from its list of “compliant service providers”
6 [GP3, GP4: 1, GP6]. Reporters underlined the history of cyber security incidents involving the
7 organization and the damages suffered by consumers: “Even if they (consumers) are not
8 actually liable for any fraudulent charges, their lives can be disrupted significantly at any
9 moment—and nobody gets reimbursed for that” [GP6: 1]. With 2 accounts treating the event
10 neutrally, 1 positive news story and 3 that instead directly tainted its image, the calculated
11 Reputation index amounts to -33,3 $[(1-3) \times 100 / 6]$.
12
13
14
15
16
17
18
19
20
21
22
23
24
25

26 **THE HOME DEPOT DATA BREACH:** The Home Depot corporate crisis generated six media
27 stories during the first 3 months, including only one negative NYT article published on the day
28 after the breach announcement. The NYT revealed statements of The Home Depot’s employees
29 that organization executives were well aware of existing vulnerabilities and that they dismissed
30 the concerns voiced by internal IT teams. The Home Depot was, “despite alarms as far back as
31 2008, [...] slow to raise its defenses” [HD2: 1]. Three articles even distanced the company from
32 highly sophisticated attack executed through “custom-built malware”, possibly involving
33 Russian criminals [HD1, HD2, HD6].
34
35
36
37
38
39
40
41
42
43
44

45 External attackers, and unprecedented techniques shifted the focus away from The
46 Home Depot’s vulnerabilities, together with various experts voicing reassurance over the strong
47 security posture of the organization. The articles consistently reported company updates on the
48 investigation results and its detailed expressions of apology, which dominated the news from
49 the start. For instance, a WP article asserted the day after the breach that the malware had been
50 “eliminated from the company’s systems” instead of questioning how it was dropped in the first
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 place [HD1: 1]. In addition, all media sources extensively addressed the company's
2 compensation scheme, consisting of free credit monitoring and gift cards from the beginning.
3

4 Media often quoted from The Home Depot's corporate updates directly. While two
5 articles blamed The Home Depot, they still reported the organizations' admission of guilt, and
6 contextualized it in the larger scheme of cyber incidents in the retail sector: "Thefts like the one
7 that hit The Home Depot [...] are the 'new normal', according to security experts" [HD5: 1].
8 To summarize, the Reputation Index formula leads to a coefficient of +33,3 $[(3-1) \times 100 / 6]$.
9
10
11
12
13
14
15
16
17
18

19 **THE ANTHEM DATA BREACH:** Private health insurer Anthem disclosed its data breach itself on
20 February 4th 2015. The breach included 80 million leaks of personal identification information
21 containing social security numbers. The self-disclosure arguably placed the organization in an
22 advantageous position. The majority of the media articles praised Anthems timely and proactive
23 notification of the breach. Cybersecurity experts and FBI officials endorsed Anthem's response
24 compared to the usual modus operandi: "organizations don't typically provide notification this
25 early on" [A5: 1, A1, A2]. In addition, media described the attack as highly sophisticated and
26 blamed Chinese criminal groups, meanwhile informing the audience about Anthem's consistent
27 investments prior to the breach and its commitment to cybersecurity through upgrading
28 encryption standards on its database [A1, A4, A6].
29
30
31
32
33
34
35
36
37
38
39
40
41
42

43 Media emphasized that attackers had not exfiltrated medical records and reduced the
44 gravity of the fact, lifting Anthem from additional responsibilities [A6]. Articles extensively
45 reported on Anthem's collaborative efforts with authorities, and on Anthem's investigation
46 updates, its apology statements and operational information. Only one negative article
47 addressed the lawsuits and FBI investigations launched against Anthem for failed protection of
48 its database, which allegedly hosted all patient details in one location [A8]. The final
49 reputational score added up to +62.5, derived from the formula: $(6-1) \times 100 / 8$.
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1
2 **THE EQUIFAX DATA BREACH :** The 2017 Equifax data breach, exfiltrating around 143 million
3
4 consumers PII data from the credit reporting agency's systems, is the largest considered here.
5
6 Its self-disclosure did not spare the organization from negative coverage. The media articles
7
8 represent an inventory of Equifax's mistakes, starting with allegations of inside trading by three
9
10 company executives who sold Equifax stocks worth 2 million before announcing the breach
11
12 with significant delay.
13
14
15

16
17 The evasive comments by the organizations' executives on the details of the breach and
18
19 the stock sale scandal added insult to injury [E1, E2, E3, E5, E6, E8, E9, E10]. Multiple sources
20
21 reported consumer outrage in relation to malfunctioning websites, non-responsive twitter
22
23 accounts and unreachable call centers. Equifax's failure to respond soon became a crisis in
24
25 itself, as its "struggle to deal with the fallout from a massive security breach is growing as
26
27 lawmakers are asking questions about what happened and more consumers are lawyering up"
28
29 [E10: 1]. Later news pointed at the company's flawed software and failure to patch well-known
30
31 vulnerabilities for over a year, although according to Equifax own annual report they had been
32
33 a "regular target" for years [E3: 1]. The WSJ reported how the MSCI index in 2016 had booted
34
35 Equifax from its listing, as Equifax "was ill- prepared to face the "increasing frequency and
36
37 sophistication of data breaches" [E5: 1].
38
39
40
41
42

43
44 As if the situation was not serious enough, media reports revealed that Equifax
45
46 customers had been redirected to a new company webpage where hackers had also installed
47
48 malware, which Equifax spokespersons reportedly again denied and then attributed to third
49
50 party contractors [E4]. Negative media attention resulted in a Reputation score of -100, the
51
52 lowest possible coefficient [(0-10)x100/10].
53
54
55
56
57
58
59
60
61
62
63
64
65

THE CAPITAL ONE FINANCIAL CORP. DATA BREACH: Fintech bank Capital One retrieved evidence of a hack by performing a routine scanning of its systems, and soon caught the hacker. News reports took a somewhat indulgent stance towards the organization. With the identified hacker as a clear responsible party, none of the reports explicitly attributed responsibility for the crisis to Capital One [C2, C5, C6, C7]. Second, Capital One's fame as one of the most technologically advanced enterprises in the market, softened the tone of media coverage [C3]. Articles outlined how the organization "immediately fixed" the gap and that there was no evidence of data being sold or distributed [C7: 2]. In addition, news stories underlined the company's statements of regret and apology.

With the hacker as perfect scapegoat, the company communicated empathically to the public [C2, C6]. Capital One was meanwhile depicted at the heart of fintech innovation programmes under fire, with competitors struggling to catch up [C2, C3, C5]. The score, based on 4 neutral and 3 positive media reports, therefore equals +42.85 $[(3-0) \times 100 / 7]$.

6.1 Assessing Organizational Responses

All cases from the first period have suffered substantial reputation damage. While SCCT research suggests to select strategies from only one primary cluster and complement them with the reinforcing pack, not one organization abides by this rule. Global Payments first adopted a justification approach, claiming that only a segment of its processing system had been compromised, and that the incident did "not involve our merchants or their relationships with their customers" [PR10: 1, PR11]. The company opened its press release with a bolstering reminder that Global Payments is: "a leader in payment processing services" [PR10]. Then Global Payments radically changed its approach by timidly apologizing and offering free credit monitoring and insurance protection, that were subsequently never implemented [PR12].

1 TJX's press releases also included the entire range of the three SCCT response clusters.
2 First, the company chose a Deny posture regarding the timing and proportions of the incident
3 [TJX7]. Then, TJX employed deny volition responses (minimizing the number of records
4 disclosed to "significantly less than millions") and justified the tardiness of their response by
5 claiming to have little control over the event [PR22: 1, PR23, TJX2]. The organization
6 eventually apologized, but simultaneously claimed that compensations were unnecessary. TJX
7 instead shifted responsibility to consumers, who should "carefully review their account
8 statements and immediately notify their credit or debit card company or bank if they suspect
9 fraudulent use" [PR23].
10
11
12
13
14
15
16
17
18
19
20

21 SONY's recovery struggle is immediately evident from their response communication,
22 starting with brief and insufficient updates on its PlayStation Blog, two weeks after its users
23 noticed the network outage. Then they awkwardly played the victim role: "In the last few
24 months, SONY has faced a terrible earthquake and tsunami in Japan. But now we are facing a
25 very man-made event – a criminal attack on us" [PR24, PR25]. Simultaneously, SONY used
26 ingratiation as a reinforcing strategy thanking its customers for their "patience, understanding
27 and goodwill". They emphasized that no credit card data were being accessed (justification)
28 [PR25: 1, PR27]. Finally, the organization promised a "welcome back" package with an identity
29 theft insurance policy (compensation), without further information regarding its delivery.
30
31
32
33
34
35
36
37
38
39
40
41
42

43 Target responded with apology and compensation right from the start, combined with
44 an inconsistent variety of other approaches. In no less than 8 press releases, Target first
45 lamented "It was a crime against Target, our team members, and most importantly, our guests"
46 (victim), while simultaneously questioning the impact of the breach in light of "very few reports
47 of actual fraud" (justification) [PR13, PR14, PR15, PR16]. The company continuously denied
48 control over development of the incident (deny volition), and subsequently evaded
49 responsibility for potential theft of PCI information by denying they had the key to begin with
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

[PR18, PR19]. Target assumed a progressively more accommodative strategy towards the end, including compensation efforts and apologies [PR18, PR19].

In the second period observed, organizations overall seemed to have had better recoveries. With the exception of Equifax, which fared worst of all corporations studied, the companies suffered minimal financial backlashes or even recovered from the breach (The Home Depot and Anthem). In line with SCCT expectations, these companies relied more consistently on response strategies belonging to one cluster, combined with Reinforcing strategies. Two organizations, namely Equifax (“We pride ourselves on being a leader in managing and protecting data” – [PR7: 1]) and The Home Depot mixed their consistent adoption of Bolstering strategies with Diminish ones. Equifax introduced a thorough technical analysis of the breach and reiterated multiple times how no evidence was found indicating the compromise of core data (justification) [PR6]. The Home Depot used a deny volition approach stating that the hack had been particularly sophisticated [PR8].

Equifax, The Home Depot and Capital One used the entire set of Bolstering strategies. In contrast to Equifax, both other companies promptly informed the audience of breach discovery. They paired this straightforward approach with extensive technical explanations concerning attack methodologies and cybersecurity improvement plans [PR9, PR4]. Capital One conveyed a detailed and transparent narrative to the public and also proactively admitted and contextualized system vulnerabilities [PR5]. While Anthem primarily apologized and updated customers on the case, its main focus was on instructing the public on the procedure required for accessing a compensation package [PR1, PR2]. The Home Depot was similarly consumer-attentive, offering free compensatory measures to anyone who “used a payment card at a The Home Depot store in 2014” [PR8: 1].

The Home Depot stated that an advanced encryption project had been completed, eventually leading to a better security posture in the future (bolstering and rectification). It

strengthened its apology by thanking its consumers for their patience (ingratiation). Capital One's CEO released a profuse apology, refusing to simply scapegoat a third-party actor for their own responsibility: "While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened, I sincerely apologize for the understandable worry this incident must be causing those affected and I am committed to making it right" [PR4, PR5].

Table 1.4 shows the recovery trends and crisis communication response strategies of the organizations. [Table 1.4 Integrating Recovery Trends and Response Strategies HERE]

6.2 Between periods

With the exception of Equifax, all cases analyzed between 2014 and 2019 performed considerably better than those within the first period, both in terms of financial (stock and revenues performances) and media reputation recovery. So, data breach crises do not have an equally negative impact on organizational reputation but seem influenced by the communication strategies of the organization. In the second period, base response strategies (adjusting and instructing) had improved qualitatively with more comprehensive and exhaustive guidelines, and detailed explanations about the incident to consumers. Moreover, these organizations resorted to Rebuild strategies in unison with Reinforcing measures to contain the crisis. While data breaches as accidental crises could imply the use of Diminish strategies, the strong degree of perceived crisis severity suggests exclusively Rebuild strategies as the best recipe for the crisis response.

Organizations that primarily relied on one single strategy cluster, performed better than those that inconsistently blended strategies from different clusters. Particularly the inclusion of Deny strategies was ultimately detrimental to organizational reputation. Surprisingly, the *performance history* (crisis history and relationship history), did not really seem to influence

1 the outcome. While a number of organizations (SONY, TJX, Global Payments, Anthem and
2 Capital One), had experienced similar incidences in the past, media coverage rarely featured
3 these cases. In fact, the media even praised Capital One for its previous successful technological
4 advancements, despite having been involved in cyber security issues before.
5
6
7
8

9 The ability of the organizations to control the narrative of the events also differed
10 between the first and second time period. The fact that certain organizations, such as Anthem,
11 The Home Depot and Capital One proactively disclosed the breach themselves, positively
12 influenced media reporting. Self-disclosure allowed these companies to influence the news
13 coverage in defining the hacking attack as “highly sophisticated” or “unprecedented”, as
14 opposed to an exposure of vulnerabilities inherent to the organizations’ security system.
15
16
17
18
19
20
21
22
23

24 Organizations that waited to disclose the incident, or to implement apology or
25 compensation strategies (Equifax, TJX, SONY, Global Payments), met harsh criticism from
26 media and consumers. Others overcompensated the initial delay by flooding the press with crisis
27 updates, generating increased coverage that hampered their image in the long run (Target). Yet
28 organizations that came forward transparently, completely and proactively about the data
29 breach, were either praised in the news for their approach (Anthem), or managed to limit the
30 media attention to the first days of the crisis (Capital One, The Home Depot).
31
32
33
34
35
36
37
38
39
40

41 Social media communication did not play an important role in the crisis communication
42 strategies. Only two companies have used their Twitter accounts to provide crisis updates:
43 Equifax and Capital One, but given their opposite outcomes the influence of this factor on
44 organizational recovery remains unclear. Surprisingly the remaining companies did not even
45 have a social media account at the time of the breach.
46
47
48
49
50
51
52
53
54
55

56 7. Conclusions

57
58
59
60
61
62
63
64
65

1 This research asked why some organizations maintain their good reputation in the aftermath of
2 a data breach, and others fail to do so. The selection of comparable cases with similar attributed
3 responsibility implies that reputation damage is influenced by crisis communication in the
4 cases. The consistent and timely adoption of compensation, apology and rectification strategies,
5 positively influenced reputational recovery from data breach crises.
6
7
8
9
10

11 A number of conditions form interesting cues for future research. Maintaining a correct
12 cyber security posture comprehensive of monitoring capacity and incident handling, providing
13 detailed and exhaustive technical information about the incident, pro-actively owning the
14 narrative of the events with transparency, and attentive customer-focused behavior, are all
15 crucial for reducing reputation damage after data breaches. More recent corporate data breach
16 cases suffer less reputation damage—perhaps as a result of breach fatigue, which implies
17 reduced issue salience in the media and less harsh public reactions. Organizations also overall
18 performed better in more recent communication responses, applying the appropriate strategies
19 consistently. At the same time, their legal and corporate environment has been rapidly changing,
20 requiring companies to comply to more stringent requirements. The progressive
21 institutionalization of the cyber domain, might also have influenced data breach response
22 practices, together with previous failures and lessons learned. What is certain, is that data
23 breaches are becoming the new normal, and organizations should better be prepared to respond
24 effectively.
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47

48 **References**

- 49 Amaresan, S. 2019. “Situational Crisis Communication Theory and How It Helps a
50 Business.” *Hubspot*, 2019. [https://blog.hubspot.com/service/situational-crisis-](https://blog.hubspot.com/service/situational-crisis-communication-theory)
51 [communication-theory](https://blog.hubspot.com/service/situational-crisis-communication-theory).
52
53
54
55 Arghire, J. 2020. “Over 15.1 Billion Records Exposed in Data Breaches in 2019.” *Security*
56 *Week*, 2020. [https://www.securityweek.com/over-151-billion-records-exposed-data-](https://www.securityweek.com/over-151-billion-records-exposed-data-breaches-2019)
57 [breaches-2019](https://www.securityweek.com/over-151-billion-records-exposed-data-breaches-2019).
58
59
60
61
62
63
64
65

- Avery, Elizabeth, and Sejin Park. 2016. "Effects of Crisis Efficacy on Intentions to Follow Directives during Crisis." *Journal of Public Relations Research*.
<https://doi.org/10.1080/1062726X.2016.1165681>.
- Bischoff, P. 2019. "How Data Breaches Affect Stock Market Share Prices." Comparitech. 2019. <https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/>.
- Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." *Journal of Computer Security*.
<https://doi.org/10.3233/JCS-2003-11308>.
- Carroll, Craig E., and Maxwell McCombs. 2003. "Agenda-Setting Effects of Business News on the Public's Images and Opinions about Major Corporations." *Corporate Reputation Review*. <https://doi.org/10.1057/palgrave.crr.1540188>.
- Chickowski, Ericka. 2013. "Why Are We So Slow To Detect Data Breaches?" Dark Reading. 2013. <https://www.darkreading.com/attacks-breaches/why-are-we-so-slow-to-detect-data-breaches/d/d-id/1139970>.
- Columbus, Louis. 2020. "Roundup Of Cybersecurity Forecasts And Market Estimates." *Forbes*, 2020. <https://www.forbes.com/sites/louiscolumbus/2020/04/05/>.
- Comfort, Louise, Arjen Boin, and Chris Demchak. 2010. *Designing Resilience*. Pittsburgh: Pittsburgh University Press.
- Coombs, W. Timothy. 2004. "Impact of Past Crises on Current Crisis Communication: Insights from Situational Crisis Communication Theory." *Journal of Business Communication*. <https://doi.org/10.1177/0021943604265607>.
- . 2007a. "Attribution Theory as a Guide for Post-Crisis Communication Research." *Public Relations Review*. <https://doi.org/10.1016/j.pubrev.2006.11.016>.
- . 2007b. "Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory." *Corporate Reputation Review*. <https://doi.org/10.1057/palgrave.crr.1550049>.
- . 2010. "Parameters for Crisis Communication." In *The Handbook of Crisis Communication*. <https://doi.org/10.1002/9781444314885.ch1>.
- Coombs, W. Timothy, and Sherry J. Holladay. 2002. "Helping Crisis Managers Protect Reputational Assets: Initial Tests of the Situational Crisis Communication Theory." *Management Communication Quarterly*. <https://doi.org/10.1177/089331802237233>.
- Cravens, Karen S., Elizabeth Goad Oliver, and Sridhar Ramamoorti. 2003. "The Reputation

- Index: Measuring and Managing Corporate Reputation.” *European Management Journal*. [https://doi.org/10.1016/S0263-2373\(03\)00015-X](https://doi.org/10.1016/S0263-2373(03)00015-X).
- Eisenegger, Mark. 2004. “Reputationskonstitution in Der Mediengesellschaft.” In *Mediengesellschaft*. https://doi.org/10.1007/978-3-322-95686-6_14.
- Goel, Sanjay, Christopher Brown, and Hany Shawky. 2007. “Measuring the Impact of Security Breaches on Stock Valuations of Firms.” *6th Annual Security Conference*.
- Gwebu, Kholekile L., Jing Wang, and Li Wang. 2018. “The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management.” *Journal of Management Information Systems*. <https://doi.org/10.1080/07421222.2018.1451962>.
- Hawkins, Nick. 2017. “Why Communication Is Vital during a Cyber-Attack.” *Network Security*. [https://doi.org/10.1016/S1353-4858\(17\)30028-4](https://doi.org/10.1016/S1353-4858(17)30028-4).
- Hikmet, Neset, Anol Bhattacharjee, Nir Menachemi, Varol O Kayhan, Robert G Brooks, Rod Ward, Christine Stevens, et al. 2015. “Follow the Data : Dissecting Data Breaches and Debunking Myths.” *Journal of Professional Nursing*.
- Hovav, Anat, and John D’Arcy. 2004. “The Impact of Virus Attack Announcements on the Market Value of Firms.” *Information Systems Security*. <https://doi.org/10.1201/1086/44530.13.3.20040701/83067.5>.
- ITRC. n.d. “Breach Reports [on 2007-2018].” Identity Theft Research Center (ITRC). Accessed December 8, 2020. <https://www.idtheftcenter.org/images/breach/>.
- Jenkins, Alexander, Murugan Anandarajan, and Rob D’Ovidio. 2014. “‘All That Glitters Is Not Gold’: The Role of Impression Management in Data Breach Notification.” *Western Journal of Communication*. <https://doi.org/10.1080/10570314.2013.866686>.
- Khan, Freeha, Jung Hwan Kim, Robin Moore, and Lars Mathiassen. 2019. “Data Breach Risks and Resolutions: A Literature Synthesis.” In *25th Americas Conference on Information Systems, AMCIS 2019*.
- Kim, Bokyung, Kristine Johnson, and Sun Young Park. 2017. “Lessons from the Five Data Breaches: Analyzing Framed Crisis Response Strategies and Crisis Severity.” *Cogent Business and Management*. <https://doi.org/10.1080/23311975.2017.1354525>.
- Klebnikov, Sergei. 2019. “Companies With Security Fails Don’t See Their Stocks Drop As Much, According To Report.” *Forbes*, 2019. <https://www.forbes.com/sites/sergeiklebnikov/2019/11/06/companies-with-security-fails-dont-see-their-stocks-drop-as-much-according-to-report/?sh=1eefc56162e0>.
- Krumay, Barbara, Edward W.N. Bernroider, and Roman Walser. 2018. “Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature

- Review Considering the NIST Cybersecurity Framework.” In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-030-03638-6_23.
- Liu, Brooke Fischer. 2010. “Effective Public Relations in Racially Charged Crises: Not Black or White.” In *The Handbook of Crisis Communication*, edited by Sherri Coombs, W. Timothy; Holladay, 335–58. Blackwell.
- Lopes, Isabel Maria, Teresa Guarda, and Pedro Oliveira. 2019. “Implementation of ISO 27001 Standards as GDPR Compliance Facilitator.” *Journal of Information Systems Engineering & Management*. <https://doi.org/10.29333/jisem/5888>.
- MacKinlay, A. Craig. 1997. “Event Studies in Economics and Finance.” *Journal of Economic Literature*.
- Martin, Nicole. 2019. “What Is A Data Breach?” *Forbes*, 2019. <https://www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/?sh=59582b2014bb>.
- McCallister, E, T. Grance, and K Scarfone. 2010. “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122 NIST.” Washington DC.
- MERGroup. 2020. “The Dark Side of Digitalization.” Cybersecurity. 2020. <https://mer-group.com/the-dark-side-of-digitalization/>.
- Metrica. 2011. “Reputation Review 2011.” Oxford Metrica. 2011. [http://www.oxfordmetrica.com/public/CMS/Files/825/Aon_Oxford Metrica Reputation Review_2011.pdf](http://www.oxfordmetrica.com/public/CMS/Files/825/Aon_Oxford%20Metrica%20Reputation%20Review_2011.pdf).
- Morris, Michael W., Paul C. Moore, and Damien L.H. Sim. 1999. “Choosing Remedies after Accidents: Counterfactual Thoughts and the Focus on Fixing ‘Human Error.’” *Psychonomic Bulletin and Review*. <https://doi.org/10.3758/BF03212966>.
- Park, Hanna. 2017. “Exploring Effective Crisis Response Strategies.” *Public Relations Review*. <https://doi.org/10.1016/j.pubrev.2016.12.001>.
- Preen, J. 2020. “The Case Against Situational Crisis Communication Theory.” BC Training. 2020. <https://www.b-c-training.com/bulletin/the-case-against-situational-crisis-communication-theory>.
- Privacy Rights Clearinghouse. 2020. “Databreaches Chronology Database.” <https://privacyrights.org/data-breaches>.
- Ramakrishna, A. 2012. “An Exploratory Analysis of Data Breaches from 2005-2011: Trends and Insights.” *Journal of Information Privacy and Security* 8 (2): 33–56.

- Reed, Rick T. 2015. "Recovering Corporate Consumer Trust: A Study of Crisis Response Strategies and Repairing Damaged Trust." *Dissertation Abstracts International: Section B: The Sciences and Engineering*.
- Robertson, Jo. 2012. "Tell It All?: Challenging Crisis Communications' Rules." *Public Relations Journal*.
- Rosenthal, Uri, Michael Charles, and Paul 't Hart. 1989. *Coping with Crisis*. Springfield: Charles C. Thomas.
- Rouse, M. 2020. "Security Information and Event Management (SIEM)." SearchSecurity. 2020. <https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM>.
- Sen, Ravi, and Sharad Borle. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach." *Journal of Management Information Systems*. <https://doi.org/10.1080/07421222.2015.1063315>.
- Sobers, R. 2020. "107 Must-Know Data Breach Statistics for 2020." Varonis Data Security. 2020. <https://www.varonis.com/blog/data-breach-statistics/>.
- Szmigiera, M. 2020. "Largest Stock Exchange Operators Worldwide as of Mar 2020." Statista. 2020. <https://www.statista.com/statistics/270126/largest-stock-exchange-operators-by-market-capitalization-of-listed-companies/>.
- Wang, P., and S. Park. 2017. "Communication in Cyber Security." *Issues in Information Systems* 18 (2): 136–47.
- Wartick, Steven L. 1992. "The Relationship between Intense Media Exposure and Change in Corporate Reputation." *Business & Society*. <https://doi.org/10.1177/000765039203100104>.
- Weverbergh, R, and K Vermoesen. 2020. "Measuring PR: The (Media) Reputation Index." FINN. 2020. <https://www.finn.agency/nl/blogs/measuring-pr-media-reputation-index>.
- Winder, Davey. 2020. "Hacker Gives Away 386 Million Stolen Records On Dark Web." *Forbes*, 2020. <https://www.forbes.com/sites/daveywinder/2020/07/29/>.
- Wisner, Ben, J. C. Gaillard, and Ilan Kelman. 2012. "Framing Disaster: Theories and Stories Seeking to Understand Hazards, Vulnerability and Risk." In *Handbook of Hazards and Disaster Risk Reduction*.
- Zhou, Yucheng. 2020. "Analyzing Historical Data Breaches to Improve Public Cloud Security Postures." *ProQuest Dissertations and Theses*.

Appendix 1. Press Releases

Number	Reference	Date (d/m/y)
PR1	Anthem, 2015a	05/02/2015
PR2	Anthem, 2015b	06/02/2015
PR3	Anthem, 2015c	13/02/2015
PR4	Capital One, 2019a	29/07/2019
PR5	Capital One, 2019b	23/09/2019
PR6	Equifax, 2017a	07/09/2017
PR7	Equifax, 2017b	02/10/2017
PR8	The Home Depot, 2014a	18/09/2014
PR9	The Home Depot, 2014b	06/11/2014
PR10	Global Payments, 2012a	30/03/2012
PR11	Global Payments, 2012b	01/04/2012
PR12	Global Payments, 2012c	12/06/2012
PR13	Target, 2013a	19/12/2013
PR14	Target, 2013b	20/12/2013
PR15	Target, 2013c	20/12/2013
PR16	Target, 2013d	21/12/2013
PR17	Target, 2013e	23/12/2013
PR18	Target, 2013f	24/12/2013
PR19	Target, 2013g	27/12/2013
PR20	Target, 2013h	10/01/2014
PR21	Target, 2013i	03/02/2014
PR22	TJX, 2007a	17/01/2007
PR23	TJX, 2007b	21/02/2007
PR24	SONY, 2011a	26/04/2011
PR25	SONY, 2011b	03/05/2011
PR26	SONY, 2011c	04/05/2011
PR27	SONY, 2011d	05/05/2011

Appendix 2 Media Sources by Case

Target				
Washington Post	TG1	Timberg et al	Target says 40 million credit, debit cards may have been compromised in security breach	2013/12/19
	TG2	Tsukayama	Target data breach: what you should know	2013/12/19
	TG3	Yang et al	Target says up to 70 million more customers were hit by December data breach	2014/01/10

	TG4	Jayakumar	Target breach: What you need to know	2014/01/10
	TG5	Tsukayama	Target says customers signing up for free credit monitoring after data breach	2014/01/13
	TG6	Jayakumar	Target tries to reassure customers after data breach revelations	2014/01/13
	TG7	McGregor	Target CEO opens up about data breach	2014/01/13
	TG8	Douglas	Target breach could represent leading edge of wave of serious cybercrime	2014/02/09
	TG9	Jayakumar	Data breach hits Target's profits, but that's only the tip of the iceberg	2014/02/26
New York Times	TG10	Harris	A Sneaky Path Into Target Customers' Wallets	2014/01/17
	TG11	Editorial	Preventing the Next Data Breach	2014/01/25
	TG12	Perlroth	Heat System Called Door to Target for Hackers	2014/02/05
	TG13	Harris et al	Target Missed Signs of a Data Breach	2014/03/13
	TG14	Harris	Target Had Chance to Stop Breach, Senators Say	2014/03/26
Usa Today	TG15	Eversley	Target confirms massive credit-card data breach	2013/12/18
	TG16	Snider	Target data breach spurs lawsuits, investigations	2013/12/22
	TG17	Malcolm	Target: Data stolen from up to 70 million customers	2014/01/10
	TG18	Prah	Target's data breach highlights state role in privacy	2014/01/16
	TG19	Kratsas	Reports: Target warned before data breach	2014/02/14
	TG20	Malcolm	Target sees drop in customer visits after breach	2014/03/11
Wall Street Journal	TG21	Sidel	Target Hit by Credit-Card Breach	2013/12/19
	TG22	Ziobro	Target Breach Began With Contractor's Electronic Billing Link	2014/02/06
	TG23	Langley	Inside Target, CEO Gregg Steinhafel Struggles to Contain Giant Cybertheft	2014/02/18
	TG24	Ziobro	Target Earnings Slide 46% After Data Breach	2014/02/26
	SONY			
Washington Post	S1	Tsukayama	SONY got hacked; what should I do?	2011/04/27
	S2	Tsukayama	FBI looks into SONY's PlayStation security breach	2011/04/29
	S3	Tsukayama	Cyber attack was large-scale, SONY says	2011/05/04
Financial Times	S4	Palmer	SONY faces lawsuit over PlayStation hack	2011/04/28
	S5	Brown	SONY scrambles to limit hacking scandal	2011/05/03
	S6	Menn et al	SONY faces fury over data delay	2011/04/27
	S7	Bradshaw	SONY chief in PlayStation hack apology	2011/05/06
New York Times	S8	Schiesel	PlayStation Security Breach a Test of Consumers' Trust	2011/04/27
	S9	Bilton et al	SONY Says PlayStation Hacker Got Personal Data	2011/04/26
Forbes	S10	Noer	SONY Response to PlayStation Security Breach Abysmal	2011/05/04

	TJX			
Washington Post	TJX1	Nakashima	Customer Data Breach began in May 2005, TJX says	2007/02/22
New York Times	TJX2	Dash,	Data Breach Could Affect Millions of TJX Shoppers	2007/01/19
	TJX3	Dash,	Retail security breach may be biggest in U.S. - Business - International Herald Tribune	2007/01/19
	TJX4	Stone et al	TJX Says Customer Data Was Stolen	2007/01/18
Wall Street Journal	TJX5	Sidel	TJX Data breach poses woe for bank	2007/01/19
	TJX6	Pereira	Wide Credit-Card Fraud Surfaces in TJX Hacking	2007/02/25
	TJX7	Pereira	How Credit Card Data Went out wireless door	2007/05/04
	Global Payments			
Washington Post	GP1	Tsukayama	FAQ: The Global Payments hack	2012/04/02
New York Times	GP2	Silver-Greenberg et al	MasterCard and Visa Investigate Data Breach	2012/04/01
	GP3	Silver-Greenberg	After a Data Breach, Visa Removes a Service Provider	2012/04/01
Wall Street Journal	GP4	Sidel et al	Data Breach Sparks Worry Hack Attack at Card Processor Compromises Potentially Thousands of Accounts	2012/03/29
Forbes	GP5	Trefis Team	Global Payments Data Breach Exposes Card Payments Vulnerability	2012/04/03
	GP6	Kosner	Massive Credit Card Breach of Estimated 10 Million Accounts	2012/03/31
	The Home Depot			
Washington Post	HD1	Peterson	The Home Depot breach put 56 million payment cards at risk	2014/09/18
New York Times	HD2	Creswell et al	Ex-Employees Say The Home Depot Left Data Vulnerable	2014/09/19
Forbes	HD3	Vinton	With 56 Million Cards Compromised, The Home Depot's Breach Is Bigger Than Target's	2014/09/18
Wall Street Journal	HD4	Sidel	The Home Depot's 56 Million Card Breach Bigger Than Target's	2014/09/18
	HD5	Banjo	The Home Depot Hackers Exposed 53 Million Email Addresses	2014/11/06
Usa Today	HD6	Winter	The Home Depot hackers used vendor log-on	2014/11/06
	Anthem			
New York Times	A1	Abelson et al	Millions of Anthem Customers Targeted in Cyberattack	2015/02/05
	A2	Abelson et al	Anthem Hacking Points to Security Vulnerability of Health Care Industry	2015/02/06
	A3	Abelson et al	Data Breach at Anthem May Forecast a Trend	2015/02/06

	A4	Bernard	Protecting Yourself From the Consequences of Anthem's Data Breach	2015/02/05
Wall Street Journal	A5	Mathews et al	Health Insurer Anthem Hit by Hackers Breach Gets Away With Names, Social Security Numbers of Customers, Employees	2015/02/04
Usa Today	A6	Weise	Millions of Anthem customers alerted to hack	2015/02/05
	A7	News source	Anthem/Blue Cross-Blue Shield hit with cyber-attack	2015/02/05
	A8	Weise	First lawsuits launched in Anthem hack	2015/02/07
Equifax				
Washington Post	E1	Merle	Outrage builds after Equifax executives banked \$2 million in stock sales following data breach	2017/09/08
New York Times	E2	Bernard et al	Equifax Says Cyberattack May Have Affected 143 Million in the U.S.	2017/09/07
Wall Street Journal	E3	Andriotis et al	We've Been Breached: Inside the Equifax Hack.	2017/09/18
	E4	Rapoport et al	States Push Equifax to Explain Why It Took 6 Weeks to Disclose Hack.	2017/10/28
	E5	Loder	A Warning Shot on Equifax	2017/10/06
Usa Today	E6	Weise	Equifax web snafu another reminder to protect your credit info	2017/09/08
	E7	Guynn	Equifax says it was not breached again, but vendor on site served 'malicious content'	2017/12/12
	E8	Mccoy et al	Equifax CEO retires amid cyberbreach fallout	2017/09/26
	E9	Dastagir	Equifax data breach: How to freeze your credit	2017/09/09
	E10	Weise et al	Equifax's struggle after massive security breach	2017/09/11
Capital One				
New York Times	C1	NYT	Capital One Data Breach Compromises Data of Over 100 Million	2019/07/29
Wall Street Journal	C2	Hong	Capital One Reports Data Breach Affecting 100 Million Customers	2019/07/30
	C3	Rudegeair et al	Capital One Hack Hits the Reputation of a Tech-Savvy Bank	2019/07/30
Usa Today	C4	Tyko	Capital One suspect indicted by federal grand jury on wire fraud and data theft charges	2019/08/28
	C5	Baig et al	Capital One data breach: What's the cost of data hacks for customers and businesses?	2019/07/30
	C6	Telford et al	Here's how to make sure you're safe after the Capital One hack	2019/07/30
	C7	Siegel	Capital One looked to the cloud for security. But its own firewall couldn't stop a hacker	2019/07/30

Tables and Figures

Table 1.1 SCCT response strategy clusters

Deny	Diminish	Rebuild	Reinforcing
<i>Attack the accuser</i>	<i>Excuse</i>	<i>Compensation</i>	<i>Bolstering</i>
<i>Denial</i>	<i>Justification</i>	<i>Apology</i>	<i>Ingratiation</i>
<i>Scapegoat</i>	<i>Deny volition*</i>	<i>Rectification*</i>	<i>Victimage</i>
<i>Ignore**</i>	<i>Separation**</i>	<i>Transcendence**</i>	<i>Endorsement**</i>

Source: Coombs (2002,2004,2007a) and Coombs & Holladay (2010)

*= addition extrapolated from: Liu (2010)

**= addition extrapolated from: Holladay (2010)

Table 1.2: List of Data Breaches from Period I (2007-2013)

1	Company	Date Of Public Announcement	Number of Records	Method of Breach	Listing Index	Legal Proceedings
2	Global Payments	29-03-2012	7	Hacked	New York Stock Exchange	Yes
3	TJX	17-01-2007	46	Hacked	New York Stock Exchange	Yes
4	Sony	26-04-2011	77	Hacked	New York Stock Exchange	Yes
5	Target	18-12-2013	110	Hacked	New York Stock Exchange	Yes
6	Heartland Payment System	20-01-2009	130	Hacked	New York Stock Exchange	Yes
7	Compass Bank	01-01-2008	1	Malicious Insiders	Madrid Stock Exchange	No
8	Royal Bank Of Scotland	23-12-2008	1,1	Hacked	London Stock exchange*	NF
9	Staples	19-12-2013	1,2	Hacked	New York Stock Exchange	NF
10	Lincoln Financial Securities	04-01-2009	1,2	Poor Security	New York Stock Exchange	NF
11	Nationwide Mutual Insurance	16-11-2012	1,2	Hacked	N/A	Yes
12	AvMed Inc	03-06-2009	1,22	Lost/Stolen Media	N/A	Yes
13	Health Net	19-11-2009	1,5	Lost/Stolen Media	New York Stock Exchange	Yes
14	Nemours Children's Health	07-10-2011	1,6	Lost/Stolen Media	N/A	NF
15	NYSEG & Rochester (Avangrid)	24-01-2012	1,8	Poor Security	New York Stock Exchange	NF
16	Health Net	15-03-2011	1,9	Lost/Stolen Media	New York Stock Exchange	Yes
17	Countrywide	02-08-2008	2	Malicious Insiders	London Stock exchange*	Yes
18	Betfair	30-09-2010	2,3	Hacked	London Stock exchange*	Yes
19	Schnucks	30-03-2013	2,4	Hacked	N/A	Yes
20	JP Morgan Chase- Circuit City	**	2,6	Paper Data Loss	New York Stock Exchange	NF
21	Educational Credit Management	20-03-2010	3,3	Lost/Stolen Media	N/A	NF
22	Advocate Medical Group	24-08-2013	4	Lost/Stolen Media	N/A	Yes
23	Hannaford Bros Supermarkets	17-03-2008	4,2	Hacked	Euronext	Yes
24	CheckFree Corporation	02-12-2009	5	Hacked	NASDAQ	NF
25	GS Caltex	05-09-2008	11,1	Malicious Insiders	N/A	No
26	Ney York Mellon	22-05-2008	12,5	Lost/Stolen Media	New York Stock Exchange	Yes
27	Auction.co.kr	12-02-2008	18	Hacked	KOSDAQ	NF
28	Steam (Valve Corp.)	11-11-2011	35	Hacked	N/A	NF
29	Adobe	03-10-2013	38	Hacked	NASDAQ	Yes

Table 1.3: List of Data Breaches from Period II (2014-2019)

Company	Date Of Public Announcement	Number of Records	Method of Breach	Listing Index	Legal Proceedings
Equifax	07-09-2017	143	Hacked	New York Stock Exchange	Yes
Capital One	30-07-2019	100	Hacked	New York Stock Exchange	Yes
Anthem	04-02-2015	80	Hacked	New York Stock Exchange	Yes
Home Depot	18-09-2014	56	Hacked	New York Stock Exchange	Yes
Uber	21-09-2017	57	Hacked	New York Stock Exchange	Yes
Experian - T-Mobile US	01-10-2015	15	Hacked	New York Stock Exchange	Yes
Sony	24-11-2014	10	Hacked	New York Stock Exchange	Yes
Neiman Marcus	10/01/2014*	1,2	Hacked	New York Stock Exchange	Yes
First American	24-05-2019	885	Poor Security	New York Stock Exchange	Yes
Marriott	30-11-2018	500	Hacked	NASDAQ	Yes
JP Morgan Chase (No pr	28/08-25*/09/2014	83	Hacked	New York Stock Exchange	No
Wawa	19-12-2019	30	Hacked	N/A	Yes
Lifelabs	17-12-2019	15	Hacked	N/A	Yes
Government Payment Se	14-09-2018	14	Poor Security	N/A	NF
Quest Diagnostics	03-06-2019	12	Poor Security	New York Stock Exchange	Yes
Premiera Blue	17-03-2015	11	Hacked	N/A	Yes
Excellus BlueCross Blue	09-09-2015	11	Hacked	N/A	Yes
Cathay Pacific Airways	24-10-2018	9,4	Hacked	Hong Kong Stock Exchange	Yes
Hudson Bay Company d	01-04-2018	5	Hacked	Toronto Stock Exchange	Yes
DoorDash	26-09-2019	4,9	Hacked	N/A	Yes
Scottrade	02-10-2015	4,6	Hacked	N/A	Yes
UCLA Health	17-07-2015	4,5	Hacked	N/A	Yes
Community Health Syste	18-08-2014	4,5	Hacked	New York Stock Exchange	No
Desjardins	20-06-2019	4,2	Malicious Insiders	N/A	Yes
Firebase (Google)	20-06-2018	4,1	Poor Security	NASDAQ	Yes
Medical Informatics Eng	10-06-2015	3,9	Hacked	N/A	Yes
Banner Health	03-08-2016	3,7	Hacked	N/A	Yes
Jason's Deli	12-01-2018	3,5	Hacked	N/A	Yes
AccuDoc Solutions, Inc.	27/11//2018	2,7	Hacked	N/A	NF
Michaels Stores	17-04-2014	2,6	Hacked	NASDAQ	Yes
21st Century Oncology	04-03-2016	2,2	Hacked	N/A	Yes
Eddie Bauer, LLC	18-08-2016	2,2	Hacked	OTC	Yes
T-Mobile	20-08-2018	2	Hacked	New York Stock Exchange	NF
SunTrust Banks, Inc.	20-04-2018	1,5	Malicious Insiders	New York Stock Exchange	Yes
Systema Software	15-20/09/2015	1,5	Poor Security	N/A	NF
UnityPoint Health	31-07-2018	1,4	Hacked	N/A	Yes

Table 1.4 Integrating Recovery Trends and Response Strategies

Period I: 2007-2013							
Company	Stock Perfor.	Reputation Index	Deny	Diminish	Rebuild	Reinforcing	Social Media
TJX	-5.1%	-42.9	Ignore	Deny volition	Apology (late)		NO
SONY	-19.1%	-90	Ignore, Suffering, Scapegoat	Justification, Deny Volition	Compensation (late)	Ingratiation	NO
GLOBAL PAYMENTS	-16.6%	-33.3		Justification	Compensation, Apology (late)	Bolstering	NO
TARGET	-7%	-25	Suffering	Deny Volition	Rectification Compensation Apology		NO
Period II: 2014-2019							
Company	Stock Perfor.	Reputation Index	Deny	Diminish	Rebuild	Reinforcing	Social Media
HOME DEPOT	+13.1%	+33.3		Deny Volition	Compensation, Rectification, apology	Bolstering, Ingratiation	NO
ANTHEM	+13.4%	+62.5			Compensation Apology		NO
EQUIFAX	-16.4%	-100		Justification	Apology, Compensation, Rectification	Bolstering	YES
CAPITAL ONE	-2.9%	+42.85			Apology, rectification, Compensation	Bolstering	YES

Tables

Table 1.1 SCCT response strategy clusters

Deny	Diminish	Rebuild	Reinforcing
<i>Attack the accuser</i>	<i>Excuse</i>	<i>Compensation</i>	<i>Bolstering</i>
<i>Denial</i>	<i>Justification</i>	<i>Apology</i>	<i>Ingratiation</i>
<i>Scapegoat</i>	<i>Deny volition*</i>	<i>Rectification*</i>	<i>Victimage</i>
<i>Ignore**</i>	<i>Separation**</i>	<i>Transcendence**</i>	<i>Endorsement**</i>

Source: Coombs (2002,2004,2007a) and Coombs & Holladay (2010)

*= addition extrapolated from: Liu (2010)

**= addition extrapolated from: Holladay (2010)

Table 1.2: List of Data Breaches from Period I (2007-2013)

1	Company	Date Of Public Announcement	Number of Records	Method of Breach	Listing Index	Legal Proceedings
2	Global Payments	29-03-2012	7	Hacked	New York Stock Exchange	Yes
3	TJX	17-01-2007	46	Hacked	New York Stock Exchange	Yes
4	Sony	26-04-2011	77	Hacked	New York Stock Exchange	Yes
5	Target	18-12-2013	110	Hacked	New York Stock Exchange	Yes
6	Heartland Payment System	20-01-2009	130	Hacked	New York Stock Exchange	Yes
7	Compass Bank	01-01-2008	1	Malicious Insiders	Madrid Stock Exchange	No
8	Royal Bank Of Scotland	23-12-2008	1,1	Hacked	London Stock exchange*	NF
9	Staples	19-12-2013	1,2	Hacked	New York Stock Exchange	NF
10	Lincoln Financial Securities	04-01-2009	1,2	Poor Security	New York Stock Exchange	NF
11	Nationwide Mutual Insurance	16-11-2012	1,2	Hacked	N/A	Yes
12	AvMed Inc	03-06-2009	1,22	Lost/Stolen Media	N/A	Yes
13	Health Net	19-11-2009	1,5	Lost/Stolen Media	New York Stock Exchange	Yes
14	Nemours Children's Health	07-10-2011	1,6	Lost/Stolen Media	N/A	NF
15	NYSEG & Rochester (Avangard)	24-01-2012	1,8	Poor Security	New York Stock Exchange	NF
16	Health Net	15-03-2011	1,9	Lost/Stolen Media	New York Stock Exchange	Yes
17	Countrywide	02-08-2008	2	Malicious Insiders	London Stock exchange*	Yes
18	Betfair	30-09-2010	2,3	Hacked	London Stock exchange*	Yes
19	Schnucks	30-03-2013	2,4	Hacked	N/A	Yes
20	JP Morgan Chase- Circuit City	**	2,6	Paper Data Loss	New York Stock Exchange	NF
21	Educational Credit Management	20-03-2010	3,3	Lost/Stolen Media	N/A	NF
22	Advocate Medical Group	24-08-2013	4	Lost/Stolen Media	N/A	Yes
23	Hannaford Bros Supermarkets	17-03-2008	4,2	Hacked	Euronext	Yes
24	CheckFree Corporation	02-12-2009	5	Hacked	NASDAQ	NF
25	GS Caltex	05-09-2008	11,1	Malicious Insiders	N/A	No
26	Ney York Mellon	22-05-2008	12,5	Lost/Stolen Media	New York Stock Exchange	Yes
27	Auction.co.kr	12-02-2008	18	Hacked	KOSDAQ	NF
28	Steam (Valve Corp.)	11-11-2011	35	Hacked	N/A	NF
29	Adobe	03-10-2013	38	Hacked	NASDAQ	Yes

Table 1.3: List of Data Breaches from Period II (2014-2019)

1	Company	Date Of Public Announcement	Number of Records	Method of Breach	Listing Index	Legal Proceedings
2	Equifax	07-09-2017	143	Hacked	New York Stock Exchange	Yes
3	Capital One	30-07-2019	100	Hacked	New York Stock Exchange	Yes
4	Anthem	04-02-2015	80	Hacked	New York Stock Exchange	Yes
5	Home Depot	18-09-2014	56	Hacked	New York Stock Exchange	Yes
6	Uber	21-09-2017	57	Hacked	New York Stock Exchange	Yes
7	Experian - T-Mobile US	01-10-2015	15	Hacked	New York Stock Exchange	Yes
8	Sony	24-11-2014	10	Hacked	New York Stock Exchange	Yes
9	Neiman Marcus	10/01/2014*	1,2	Hacked	New York Stock Exchange	Yes
10	First American	24-05-2019	885	Poor Security	New York Stock Exchange	Yes
11	Marriott	30-11-2018	500	Hacked	NASDAQ	Yes
12	JP Morgan Chase (No pr	28/08-25*/09/2014	83	Hacked	New York Stock Exchange	No
13	Wawa	19-12-2019	30	Hacked	N/A	Yes
14	Lifelabs	17-12-2019	15	Hacked	N/A	Yes
15	Government Payment Se	14-09-2018	14	Poor Security	N/A	NF
16	Quest Diagnostics	03-06-2019	12	Poor Security	New York Stock Exchange	Yes
17	Premiera Blue	17-03-2015	11	Hacked	N/A	Yes
18	Excellus BlueCross Blue	09-09-2015	11	Hacked	N/A	Yes
19	Cathay Pacific Airways	24-10-2018	9,4	Hacked	Hong Kong Stock Exchange	Yes
20	Hudson Bay Company d	01-04-2018	5	Hacked	Toronto Stock Exchange	Yes
21	DoorDash	26-09-2019	4,9	Hacked	N/A	Yes
22	Scottrade	02-10-2015	4,6	Hacked	N/A	Yes
23	UCLA Health	17-07-2015	4,5	Hacked	N/A	Yes
24	Community Health Syste	18-08-2014	4,5	Hacked	New York Stock Exchange	No
25	Desjardins	20-06-2019	4,2	Malicious Insiders	N/A	Yes
26	Firebase (Google)	20-06-2018	4,1	Poor Security	NASDAQ	Yes
27	Medical Informatics Eng	10-06-2015	3,9	Hacked	N/A	Yes
28	Banner Health	03-08-2016	3,7	Hacked	N/A	Yes
29	Jason's Deli	12-01-2018	3,5	Hacked	N/A	Yes
30	AccuDoc Solutions, Inc.	27/11//2018	2,7	Hacked	N/A	NF
31	Michaels Stores	17-04-2014	2,6	Hacked	NASDAQ	Yes
32	21st Century Oncology	04-03-2016	2,2	Hacked	N/A	Yes
33	Eddie Bauer, LLC	18-08-2016	2,2	Hacked	OTC	Yes
34	T-Mobile	20-08-2018	2	Hacked	New York Stock Exchange	NF
35	SunTrust Banks, Inc.	20-04-2018	1,5	Malicious Insiders	New York Stock Exchange	Yes
36	Systema Software	15-20/09/2015	1,5	Poor Security	N/A	NF
37	UnityPoint Health	31-07-2018	1,4	Hacked	N/A	Yes

Table 1.4 Integrating Recovery Trends and Response Strategies

Period I: 2007-2013							
Company	Stock Perfor.	Reputation Index	Deny	Diminish	Rebuild	Reinforcing	Social Media
TJX	-5.1%	-42.9	Ignore	Deny volition	Apology (late)		NO
SONY	-19.1%	-90	Ignore, Suffering, Scapegoat	Justification, Deny Volition	Compensation (late)	Ingratiation	NO
GLOBAL PAYMENTS	-16.6%	-33.3		Justification	Compensation, Apology (late)	Bolstering	NO
TARGET	-7%	-25	Suffering	Deny Volition	Rectification Compensation Apology		NO
Period II: 2014-2019							
Company	Stock Perfor.	Reputation Index	Deny	Diminish	Rebuild	Reinforcing	Social Media
HOME DEPOT	+13.1%	+33.3		Deny Volition	Compensation, Rectification, apology	Bolstering, Ingratiation	NO
ANTHEM	+13.4%	+62.5			Compensation Apology		NO
EQUIFAX	-16.4%	-100		Justification	Apology, Compensation, Rectification	Bolstering	YES
CAPITAL ONE	-2.9%	+42.85			Apology, rectification, Compensation	Bolstering	YES