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

Kuipers, S.L.; Schonheit, M.

File Correction Details

Correction is made. No of Corrections: 5

Online Correction Link: https://eproofing.springer.com/ePj/journals/b0NQ-d8UbNAk23VJFNWMHS_GvpYtr43zIP22ilPxnMJ1vkbaNH6EKFlejyMfYo1qB5JbfbOe3WiAGEdnmbNctzexfbOyFs2J_rHll8Lf_hbmK349Wb45WVJJ5rLxMnmn

Image Annotation Details

No Details Found

Attached File Details

No Details Found

Query Details

1. **Please confirm the affiliations**
   confirmed
2. **Please confirm the corresponding author**
   confirmed
3. **Please provide author biographies**
   Sanneke Kuipers, PhD, is associate professor of crisis governance at Leiden University's Institute of Security and Global Affairs. Michael Schonheit, Msc, works as consultant Cyber Risk Advisory at Deloitte, The Netherlands.
4. **AUTHOR: Reference Gustafsson et al. 2020 has not been included in the Reference List, please supply full publication details.**
   Gustafsson, Stefanie, Nicole Gillespie, Rosalind Searle, Veronica Hope Hailey and Graham Dietz (2020) Preserving Organizational Trust During Disruption, in: Organization Studies, online early view, DOI 10.1177/0170840620912705
5. **AUTHOR: Reference George and Bennett (2005), Hinterleitner (2020) has not been included in the Reference List, please supply full publication details.**
   George, Alexander and Andrew Bennett (2005) The Methods of Structured Focused Comparison, chapter 3 (pp. 67-72) in Case Studies and Theory Development in the Social Sciences, Cambridge MA: MIT Press.
   Hinterleitner, Markus (2020) Policy Controversies and Political Blame Games, Cambridge: Cambridge University Press.
6. **Please provide the closed quote in the sentence 'They coined the term...'**
   "Breach Fatigue"
7. **Please provide the closed quotes in the sentence 'The WSJ reported how the MSCI index in...'**
   Equifax "was ill prepared to face the increasing frequency and sophistication of data breaches" [E5: 1].
8. **Please confirm the section level headings**
   add heading for 'Findings and Discussion'
9. **In case of major corrections/changes please inform the editors crr@rsm.nl**
   no major corrections to report
10. **Reference Nicole and Dietz (2009) is given in list but not cited in text. Please cite in text or delete from list.**
    should be Gillespie, N. and Dietz, G. (2009), already cited in text in the section 'Reputation Threats and Crisis Communication'

Original Article

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

Sanneke Kuipers Email : s.l.kuipers@fgga.leidenuniv.nl
Michael Schonheit

Leiden University's Institute of Security and Global Affairs, The Hague, The Netherlands

Deloitte, Amsterdam, The Netherlands

Abstract

Online data breaches are recurrent and damaging cyber incidents fors 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. Base responses such as comprehensive and exhaustive guidelines, and detailed explanations about the incident to consumers helped to reduce the damage. Corporations responding to data breaches by hacking benefit from admission of responsibility in spite of the initial characterization of such crises as victim crisis types. 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 **AQ1** reporting. Social media communication did not play an important role in the response of the organizations involved. **AQ2** The consistent and timely adoption of compensation, apology, and rectification strategies, combined with reinforcing strategies such as ingratiation and bolstering, positively influenced reputational **AQ3** recovery from the crisis.

Keywords

Crisis communication
Data breach
Cybersecurity

SECTION1

Introduction

Online data breaches represent one of the most recurrent and damaging cyber incidents for organizations worldwide. 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). 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, p. 1), for instance through phishing emails, DDoS attacks, and Trojan horses.

Data breaches increasingly impose on organizations worldwide unparalleled monetary costs (MERGroup 2020; Arghire 2020). Direct costs affecting organizations suffering a data breach include: business disruption and recovery, forensic investigations, legal proceedings, regulatory fines, and credit monitoring for customers. These costs constitute just the tip of iceberg. Indirect costs include reputational damages and loss of consumer trust, which can turn the cyber incident into a corporate reputational crisis that affects business in the long run (Kim et al. 2017; Wang and Park 2017).

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

Data breaches are an increasing risk (both in terms of probability and damage) to nearly all private and public organizations storing sensitive client data. Data breaches provide us with highly comparable cross-industry cases of reputation threats and damage. Data breaches are what Bentley et al. (2018, p. 138) call "ambiguous crisis situations," because it is not always obvious who is to blame for causing the data breach, whether the organization at hand is actually a victim or a culprit and, thus, what the appropriate crisis communication strategy entails. In addition, because breached organizations are more likely to advise stakeholders on what actions they could or should take after a breach to protect their private information (Bentley 2018), data breaches are ideal cases for studying the effect of base responses in crisis communication, which have received little attention so far (Park 2017). Also, the comparative study of two sets of data breach cases over time, can tell us more about the use of social media in crisis communication and about differences in perception of responsibility attribution regarding cyber incidents over time. Therefore, this paper offers a comparative case study on how organizations can mitigate reputational damages in the aftermath of data breaches through crisis communication strategies. The selected cases of corporate data breaches vary in financial and reputational recovery from the crisis to assess the influence of communication strategies.

This study also adds to the domain of cybersecurity research. While the vast majority of studies on data breaches focus on the legal and technological aspects of the phenomenon, the intersection with crisis communication strategies remains under-researched and undertheorized. With the cyber domain being dominated by security scholars focusing on prevention, vulnerabilities, and threats, cyber crisis management, focusing on consequences and responses to cyber incidents, remains vastly overlooked (Hawkins 2017; Kim et al. 2017). 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. A study on a cybersecurity incident response, such as data breaches by hacking, would contribute to our knowledge in the cyber domain which faces such incidents increasingly.

This article, thus, looks at the crisis response and asks why some organizations maintain their reputation with consumers in the aftermath of a cyber data breach, while others fail to do so. It finds that while the effects of crisis communication response strategies are much in line with previous studies using Situational Crisis Communication Theory (SCCT), corporations responding to data breaches enjoy clear added value from base responses, self-disclosure, and admission of responsibility in spite of the initial characterization of such crises as victim crisis types. In addition, the cases studied later in time seem to experience what we call "breach fatigue" among their audience and invoke less public arousal than earlier cases. The next section will introduce the main insights from on crisis communication to theoretically explain variation in reputation damage in eight data breach cases.

SECTION1

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 et al. 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. The source of the threat, its scope, and its consequences are often (partly) invisible and ill-understood, which increases uncertainty and delays urgency in the response phase.

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 et al. 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 (Huq 2015).

Full prevention is nearly impossible as cybercriminals typically find themselves ahead of the security curve. A purely preventive approach, thus, needs to be complemented with mitigation measures when prevention is unattainable or too costly (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 et al. 2018). By nature, the attention for mitigation and recovery within the cybersecurity domain mainly goes out to the technical and legal aspects of cybersecurity breaches and not to crisis communication as part of the incident response. As the current study shows, crisis communication can make a substantial difference with regard to the extent of the damage and the speed of recovery.

SECTION1

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, p. 38). The SCCT framework allows to generalize and predict outcomes, anticipating patterns of dependency and establishing systematic inferences among the variables at play. In line with Coombs (2007a, b), Avery and Park (2016) emphasize the need to study the effect of crisis communication strategies involving the audience as primary target, instead of the organization itself. As such, the SCCT is very much outward oriented and does not focus much on actual repair of perceived deficiencies in the organization that made it crisis prone in the first place, in contrast with studies on trust preservation and repair in corporate organizations (Gillespie and Dietz 2014; Gillespie et al. 2014; Gustafsson et al. 2020 **AQ4**).

Coombs (2010) stresses a link between the inherent features of a crisis and the most commensurate response to the event. The SCCT framework discerns between crisis types and intensifying factors to assess the degree of crisis responsibility that stakeholders will attribute to the organization after an incident. First, the typology of crises is based on initial organizational responsibility: victim crisis, accidental crisis, and preventable crisis. Each crisis type links to a predetermined communication response strategy cluster. These strategy clusters (Deny, Diminish, Rebuilding, Reinforcing), can be effective as standalone methods or in conjunction with others (Amaresan 2019; Coombs 2010). Crisis types correspond to the framing of the event rather than the nature of the crisis itself.

Crises are typically social constructs and subject to framing and exploitation (Boin et al. 2009). Also in SCCT, the crisis type does not constitute a preliminary fixed category (Coombs 2007a, b). Framing relates crises to different degrees or attributed responsibility and corresponds to minimal crisis responsibility (victim crisis), low-moderate crisis responsibility (accidental crisis), and high crisis responsibility (preventable crisis). The more an organization is perceived to be accountable for a crisis, the more its reputation will suffer as it will no longer be trusted to adequately prevent crises or respond to crises.

Victim crises include situations believed to be entirely outside of the organization's control, such as natural disasters, employee misbehavior, and product tampering by external parties. The victim crisis implies only a mild reputational threat. Accidental crises are linked to the organization's course of actions, but they lack any intentionality or control over the event (Coombs 2004). Accidental crises pose moderate reputational threats. Preventable or intentional crises represent situations where high crisis responsibility is attributed to the organization, generating severe reputational threats (Coombs 2010). The organization is held directly accountable for the crisis development because it intentionally caused the crisis or could have avoided its occurrence yet failed to do so. Human errors are generally believed to preventable, a relevant distinction for the purpose of this study (Morris et al. 1999).

Studies on accountability and blaming in both public and private organizational settings instruct us that direct crisis responsibility is not the only factor that can influence the reputation threat posed by a crisis (Brändström and Kuipers 2003; Hinterleitner 2020). For businesses, Coombs (2010) introduced two intensifying factors: crisis severity and performance history. Crisis severity refers to the impactful proportions of a crisis regardless of the responsibility of the organization, in terms of environmental, financial, or human damage (see also Hearit 2006). Performance history is the result of similar incidents that implicated the same organization in the past and the structural quality of the relationship between that same organization and its public, stakeholders, or consumers, prior to the incident. When a crisis comes to light, the media and public base their attribution of responsibility on these variables, or "causal antecedents" (Coombs 2004). Causal antecedents give an organization a disadvantageous position since the public is likely to attribute it with a higher level of responsibility for yet "another" crisis (Coombs 2010; cf Boin et al. 2009).

SECTION1

Crisis Communication Response Strategies

Crisis response efforts should always begin with "base responses": *instructing* and *adjusting* information aimed directly at shaping the public perception of the event (Coombs and Holladay 2002). *Instructing* information serves to shield stakeholders from physical damage or additional harm triggered by the crisis. A *djusting* information communicates what the company is doing to prevent the crisis from reoccurring, by giving the audience information on reparation efforts, or conveying messages of concern or sympathy towards the affected parties (Coombs 2010). Both adjusting and instructing information signal that "the company prioritizes public safety and expresses concern for the victims" (Park 2017, p. 192).

Subsequently, organizations move onto selecting among response strategy clusters based on the reputation threat they face. While *reinforcing* strategies function as supplemental and supporting measures, *deny, diminish,* and *rebuild* are clusters of primary standalone responses. An organization can respond to increasing levels of attributed responsibility for a negative event with strategies that range from denial to rebuild. In the absence of intensifying factors (crisis severity, performance history), victim crises could be handled with deny measures, such as denial or scapegoating. Accidental crises require communication to upgrade towards diminish strategies, such as justification (downplay the impact) or deny volition (claiming lack of control over the event). Finally, responses to preventable crises should include rebuild strategies, ranging from apologies to rectification (demonstrating full commitment to future prevention) (Coombs 2010; Liu 2010). If intensifying factors apply, organizations should further upgrade their response to the commensurate increased threat level.

As Table 1 shows, *reinforcing* strategies supplement primary crisis communication responses. For instance, *bolstering* means drawing on past merits and achievements, while *ingratiation* commends stakeholders for their support and loyalty (Coombs 2007a; Liu 2010).

Table 1 SCCT response strategy clusters

Deny	Diminish	Rebuild	Reinforcing
Ignore	Justification	Apology	Ingratiation
Scapegoat	Deny volition[a]	Rectification[a]	Bolstering
Suffering		Compensation	
Source Coombs (2007a) and Coombs and Holladay (2010)			
[a]Addition extrapolated from Liu (2010)			

Studies on the effect of crisis communication strategies on corporate reputation damages tell us that surprisingly, the most often employed strategies (denial, bolstering) are also the least effective, particularly when used for a crisis type that asks for admitting more responsibility or for a more consistent response (Kim et al. 2017; Coombs 2007a, b; Robertson 2012; Park 2017). Only few studies have addressed how to communicate effectively during a cybersecurity incident or data breach. We, therefore, 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.

SECTION1

Effective Crisis Communication and Data Breaches

Data breaches are not a self-evident crisis category in terms of communication strategy. Organizations undergoing a data breach crisis tend to adopt defensive strategies, normally undertaken in cases of minimal attributed responsibility (Kim et al. 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 policies, and poor implementation of procedures (Ramakrishna 2012). Jenkins et al. (2014) even argue that the standard response to a data breach should involve apology and regret strategies.

The high degree of attributed responsibility recognized by Ramakrishna (2012) and Jenkins et al (2014) could moderately decline when breaches are caused by hacking due to

the involvement of third-party offenders. Data breach by hacking is, therefore, a selection criterion for our comparative case study. Data breaches (by hacking) find themselves halfway between the victim crisis type and the preventable crisis one, in the accidental crisis cluster, which presumes low direct controllability and no intentionality. A corporate response posture to data breaches (by hacking) would then first resort to base responses (adjusting and instructing) coupled with either diminish or rebuild strategies. Park (2017) finds that the effect of base responses as part of the communication strategy has in fact been understudied so far, even though they are required for all crises. Bentley et al. argue (2018) that corporations suffering data breaches use relatively often base responses in their communication strategy, which emphasizes the need to study the effects thereof in our cases.

In a comparison of communication strategies used, between data breaches and other corporate crises (product recalls, employee misconduct, offensive content), Bentley et al. (2018) find that in case of data breaches, corporations are (1) less likely to admit responsibility; (2) less likely to express empathy to the affected customers; and (3) more likely to instruct stakeholders on what to do (base responses). Bentley et al. do not look into the effect of these responses in their comparative study. This study aims to compare the effects of the above response recipes chosen by each organization in dealing with data breaches. We expect to find that indeed base responses (instructing and adjusting) are appreciated by stakeholders, and as such are helpful strategies to mitigate the consequences of the crisis in terms of damage to reputation. We also expect to find that the ambiguity of the crisis type (victim or accidental crisis) is better faced with a strategy admitting responsibility and attempts to rebuild in line with the accidental crisis than with denial strategies that only befit victim crises.

SECTION1

Research Method

To answer the question why some organizational reputations after data breaches recover and others do not, we need to compare cases in-depth on their crisis communication strategies. Following a Most Similar System Design, the data breach cases share contextual similarities and a similar expected level of attributed responsibility. The comparative case study is a suitable method for structured focused comparison of two sets of data breach cases with varying outcomes in reputation damage and crisis recovery (George and Bennett 2005). The two sets of cases are selected from different time periods, to also study the effect of the emergence of data breaches as a relatively new phenomenon, and look into the effects of the **AQ5** use of social media in crisis communication. Below we will outline how we compared and analyzed the reputation damage in terms of economic impact and negative media coverage.

SECTION2

The Outcome Variable: Economic and Reputational Repercussions

The selected cases vary in terms of successful and unsuccessful recovery from their data breaches as shown by a combined analysis of both economic and reputational damage. The analysis of the economic impact of a PR data breach is based on the fluctuation of the stock market value of the organization in question, in relation to the overall market trend (Metrica 2011; Robertson 2012; Reed 2015; Bischoff 2019). This method remains the most widely adopted to measure the economic consequences of adverse events. The stock values and change in revenue will be observed at different points in time preceding and following the event in order to depict and control the trend in their price fluctuation (MacKinlay 1997; Campbell et al. 2003; Hovav and D'Arcy 2004; Goel et al. 2007).

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 et al. 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 et al. 2003; Weverbergh and Vermoesen 2020). News media articles will be coded positive or negative based on the analysis and quantification of statements that increase (negative) or reduce (positive) the level of attributed responsibility, crisis severity, and performance history associated to the organization navigating the crisis (see Appendix 3x). "Neutral" coverage corresponds to articles on the particular case, that do not convey information on the role played by the organization within the crisis or do not qualitatively portray its involvement in terms of attributed responsibility (Eisenegger 2008; Formentin 2010; Ki and Nekmat 2014). For each case, the score is computed by applying the following formula, including the neutral coverage within the denominator:

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

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. The media search has been carried out by setting the following query: "Data breach" OR Hack OR Hacking AND [company name]. The case studies include every article that appeared on the case in the selected three month time period. This selection is in conformity with most applied studies reviewed and updated rankings (Coombs 2010; Robertson 2012; Kim et al. 2017). In addition, the search results have been complemented by searching each news media outlet online archive for the relative period and organization name, and therefore, the case studies include a few articles from alternative media sources such as Forbes and The Financial Times. Both the news media and press release coding schemes have been processed via ATLAS.ti. See Appendix 4 for the coding scheme.

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 et al. 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.

SECTION3

Case Selection

For a valid comparison of recovery from a reputational crisis, the selected cases need a similar initial attribution of responsibility. The data breach incidents must, therefore, be comparable in volume and sensitivity of records disclosed and method of breaching. First, a comparable volume of data breached implies illicit disclosure of a significant amount of consumers' records. An appropriate benchmark for the impact of a data breach is that 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.

Table 2 List of data breaches from Period I (2007–2013)

	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 Syster	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 Securitie	04-01-2009	1,2	Poor Security	New York Stock Exchange	NF
11	Nationwide Mutual Insura	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 Healt	07-10-2011	1,6	Lost/Stolen Media	N/A	NF
15	NYSEG & Rochester (Avang	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 C	**	2,6	Paper Data Loss	New York Stock Exchange	NF
21	Educational Credit Manag	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 Supermar	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 3 List of data breaches from Period II (2014–2019)

	Company	Date Of Public Announcemen	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	Premera 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 dl	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 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

A second selection criterion is the sensitivity of the data disclosed 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 et al. 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 information including card and account numbers; and third, Protected Health Information (PHI), related to any medical information linked to a subject. Compromising these data seriously affects people's lives and leaves little room for instant reparatory fixes (Bischoff 2019).

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

A focus on breaches by hacking, rules out alternative factors influencing public perception of data breaches achieved in a *physical locus* (paper data loss, unauthorized entry), committed *unintentionally* (data leakages) or caused by negligence, malicious insiders or inappropriate security measures. This will increase comparability of the level of attributed responsibility (Khan et al. 2019). Finally, all cases selected have incurred legal proceedings which increases comparability of the direct and indirect costs imposed by the data breach.

Experts identify the role of social media as pivotal for achieving effective crisis communication (Reed 2015; Preen 2020). For assessing the crisis communication response, organizations' own press releases, their reactions reported in articles from the selected newspapers, and posts published on the organizations' Facebook and Twitter accounts will be tracked and analyzed. To control for the role of progressive digitalization of media communication and the evolution of social media, we will analyze four events that occurred between 2007 and 2013 (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 these 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 et al. 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 **AQ6** 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.

The selected cases have the same organizational context, as they are all listed on the New York Stock Exchange (NYSE) (Cf. Bischoff 2019; Szmigiera 2020). 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 from 2014 to 2019. Next, the three remaining selection criteria—hacking as data breach cause, the stock exchange of the organization, and the certainty of legal costs—further reduces the population to select from based on variation in the dependent variable, and representation of different sectors (see Tables 2 and 3).

The final dataset is composed of 8 corporate data breaches, distributed equally across the periods (see Tables 2 and 3). Each period features specialized retailer companies (Target, The Home Depot, or TJX), credit reporting and payment services companies (Global Payments and Equifax), and insurance and financial service providers (Anthem and Capital One). At last, electronics manufacturer SONY completes the list of cases in this comparative analysis.

SECTION2

Stock and Revenue Analysis

The assessment of the stock price movement of the selected organizations over a period of three months after the event follows standard event study guidelines (Hovav and D'Arcy 2004; Goel et al. 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 impacted 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 these observations.

Between 2014 and 2019, organizations suffering a data breach perform in an opposite direction. Anthem and The Home Depot have in fact increased their stock value during the timeframe observed. The other organizations took a serious fall before stabilizing at a loss. Meanwhile, the NYA Index shows moderate growth in the same period. The year-on-year periodic revenue data confirm the results of the stock performance analysis.

SECTION2

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.

SECTION3

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 sets the timeline straight, revealing that the breach started at least 18 months before and that TJX simply had "no idea what was going on" [TJX7: 1]. By this point, media widely discussed TJX cybersecurity failures, repeatedly quoting sources inside the company to ridicule their security posture: "It was as easy as breaking into a house through a side window that was wide open" [TJX5: 2]. The apology at the end of the 3 months window, indicated that TJX was slow at assuming responsibility. While one article assumed a particularly soft stance in treating TJX's role in the crisis, and two neutral, 4 articles painted a significantly worse picture. The TJX Reputation Index score, thus, is equal to − 43, a result obtained by applying the following formula: (1–4) × 100/7.

SECTION3

The SONY Data Breach

The data breach that struck SONY compromised 77 million records and a Play Station network outage of over 20 days. Users, therefore, directly experienced the consequences of the hack long before the company made a first public statement about it. Only one of the ten news stories retrieved for this case did not directly accuse the company of wrongdoings but provided the audience with guidelines on how to protect themselves [S1].

The main narrative centered on SONY's shortcomings in its crisis response. Various critics blamed the company for initially dismissing the event as a routine incident, for the failed attempt at scapegoating the hacktivist group Anonymous, and ultimately for their "lack of transparency and their seeming inability to issue clear, unambiguous instructions to their (former) customers" [S10: 1]. SONY had "failed the internet" and without a transformation "it will be a fallen giant indeed" [S5: 2, S8: 3]. While the Japanese conglomerate was firmly denying that credit cards information was compromised, card fraud linked to the breach began to feature in the press, together with several class action lawsuits against SONY for encryption security failures and consumer law violations [S6, S9]. For instance, the Financial Times claimed that SONY "failed to encrypt data and establish adequate firewalls to handle a server intrusion contingency, failed to provide prompt and adequate warnings of security breaches, and unreasonably delayed in bringing the PSN service back on line" [S4: 1]. In addition, the media began to report on ongoing FBI investigations [S2, S3, S6, S8, S10].

In sum, 9 out of 10 sources analyzed strongly attributed responsibility to Sony, which following the Reputation Index formula (0–9) × 100/10, results in a score of -90.

SECTION3

The Target Data Breach

In December 2013, hackers exfiltrated 110 million records, penetrating Target's server environments by leveraging third-party vendor credentials into poorly segmented POS systems. The incident was first reported by KrebsonSecurity, which immediately put Target on the defensive [17]. In total, 24 news stories surfaced throughout the crisis indicating the gravity of the reputation risk Target faced. The articles referred to Target's refusal to comment on the details of the breach and anticipated the risk of fines and profit losses during a critical time of year (Christmas) for the retail corporation. These media reports further disputed Target's excuse that the attack was highly sophisticated [TG1, TG15, TG16].

Instead, news sources focused on the insufficient cybersecurity preparedness of Target demonstrated before and during the event [TG11, TG13, TG17, TG19]. Two articles somewhat downplayed Target's role in the data breach, claiming that such instances are common across sectors and that states should have enhanced roles in preserving data security [TG2, TG18]. Five news articles critically reported on the size of the breach and the economic and legal repercussions suffered by the company including a 46% drop on quarter sales. Target's cybersecurity systems had been "astonishingly open" and Target "foolishly resisted" the introduction of more secure but expensive chip-based cards [TG13: 1; TG11: 2]. Meanwhile, Target's response was seen as evasive and superficial, as its executives initially refused to disclose information, declaring to be in compliance with regulations and limiting their comments to effusive apologies [TG2, TG3, TG4].

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

Nearly three months after the breach, the pendulum swung back. Five articles strongly reinforced attributions of responsibility when new facts came to light, portraying internal divisions among executives, overwhelmed call centers, CEO communication struggles, costs over 1 billion dollars, and insufficient compensation efforts leading to contractions in Target's consumers base [TG6, TG10, TG14, TG20, TG24]. Overall, with 6 positive, 6 neutral, and 12 negative news stories, the cumulative score attributed to Target through the Reputation Index formula is equal to − 25 [(6–12) × 100/24].

SECTION3

The Global Payments Data Breach

Global Payments attracted far less media coverage and only in the first week of the crisis. The hack, initially brought up by Krebsonsecurity, caused alleged compromise of 10 million payment card accounts. The WP and the WSJ introduced the news by downplaying the proportions of the breach compared to other cases, with dismissive statements referring to Global Payments as a "little known company" [GP4: 1, GP1]. Also, these articles emphasized structural vulnerabilities affecting payment service merchants at large. Forbes even further detached Global Payments from the responsibility for the event, by asserting that the company "merely passes on transaction details to card networks like Visa and MasterCard" and that it had already taken the necessary measures to contain the leakage [GP5].

Other news redirected the responsibility again towards Global Payments. Three articles zoomed in on Visa's removal of Global Payments from its list of "compliant service providers" [GP3, GP4: 1, GP6). Reporters underlined the history of cybersecurity incidents involving the organization and the damages suffered by consumers: "Even if they (consumers) are not actually liable for any fraudulent charges, their lives can be disrupted significantly at any moment—and nobody gets reimbursed for that" [GP6: 1]. With 2 accounts treating the event neutrally, 1 positive news story and 3 that instead directly tainted its image, the calculated Reputation index amounts to – 33.3 [(1–3) × 100/6].

SECTION3

The Home Depot Data Breach

The Home Depot corporate crisis generated six media stories during the first 3 months, including only one negative NYT article published on the day after the breach announcement. The NYT revealed statements of The Home Depot's employees that organization executives were well aware of existing vulnerabilities and that they dismissed the concerns voiced by internal IT teams. The Home Depot was, "despite alarms as far back as 2008, […] slow to raise its defenses" [HD2: 1]. Three articles even distanced the company from highly sophisticated attack executed through "custom-built malware," possibly involving Russian criminals [HD1, HD2, HD6].

External attackers and unprecedented techniques shifted the focus away from The Home Depot's vulnerabilities, together with various experts voicing reassurance over the strong security posture of the organization. The articles consistently reported company updates on the investigation results and its detailed expressions of apology, which dominated the news from the start. For instance, a WP article asserted the day after the breach that the malware had been "eliminated from the company's systems" instead of questioning how it was dropped in the first place [HD1: 1]. In addition, all media sources extensively addressed the company's compensation scheme, consisting of free credit monitoring and gift cards from the beginning.

Media often quoted from The Home Depot's corporate updates directly. While two articles blamed The Home Depot, they still reported the organizations' admission of guilt and contextualized it in the larger scheme of cyber incidents in the retail sector: "Thefts like the one that hit The Home Depot […] are the 'new normal', according to security experts" [HD5: 1]. To summarize, the Reputation Index formula leads to a coefficient of + 33.3 [(3–1) × 100/6].

SECTION3

The Anthem Data Breach

Private health insurer Anthem disclosed its data breach itself on February 4th 2015. The breach included 80 million leaks of personal identification information containing social security numbers. The self-disclosure arguably placed the organization in an advantageous position. The majority of the media articles praised Anthems timely and proactive notification of the breach. Cybersecurity experts and FBI officials endorsed Anthem's response compared to the usual modus operandi: "organizations don't

typically provide notification this early on" [A5: 1, A1, A2]. In addition, media described the attack as highly sophisticated and blamed Chinese criminal groups, meanwhile informing the audience about Anthem's consistent investments prior to the breach and its commitment to cybersecurity through upgrading encryption standards on its database [A1, A4, A6].

Media emphasised that attackers had not exfiltrated medical records and reduced the gravity of the fact, lifting Anthem from additional responsibilities [A6]. Articles extensively reported on Anthem's collaborative efforts with authorities, and on Anthem's investigation updates, its apology statements and operational information. Only one negative article addressed the lawsuits and FBI investigations launched against Anthem for failed protection of its database, which allegedly hosted all patient details in one location [A8]. The final reputational score added up to + 62.5, derived from the formula: (6–1) × 100/8.

SECTION3

The Equifax Data Breach

The 2017 Equifax data breach, exfiltrating around 143 million consumers PII data from the credit reporting agency's systems, is the largest considered here. Its self-disclosure did not spare the organization from negative coverage. The media articles represent an inventory of Equifax's mistakes, starting with allegations of inside trading by three company executives who sold Equifax stocks worth 2 million before announcing the breach with significant delay.

The evasive comments by the organizations' executives on the details of the breach and the stock sale scandal added insult to injury [E1, E2, E3, E5, E6, E8, E9, E10]. Multiple sources reported consumer outrage in relation to malfunctioning websites, non-responsive twitter accounts and unreachable call centers. Equifax's failure to respond soon became a crisis in itself, as its "struggle to deal with the fallout from a massive security breach is growing as lawmakers are asking questions about what happened and more consumers are lawyering up" [E10: 1]. Later news pointed at the company's flawed software and failure to patch well-known vulnerabilities for over a year, although according to Equifax own annual report they had been a "regular target" for years [E3: 1]. The AQ7 WSJ reported how the MSCI index in 2016 had booted Equifax from its listing, as Equifax "was ill prepared to face the "increasing frequency and sophistication of data breaches" [E5: 1].

As if the situation was not serious enough, media reports revealed that Equifax customers had been redirected to a new company webpage where hackers had also installed malware, which Equifax spokespersons reportedly again denied and then attributed to third-party contractors [E4]. Negative media attention resulted in a Reputation score of -100, the lowest possible coefficient [(0–10) × 100/10].

SECTION3

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 programs under fire, with competitors struggling to catch up [C2, C3, C5]. The score, based on 4 neutral and 3 positive media reports, therefore, is equal to + 42.85 [(3–0) × 100/7].

SECTION2

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, which were subsequently never implemented [PR12].

TJX's press releases also included the entire range of the three SCCT response clusters. First, the company chose a Deny posture regarding the timing and proportions of the incident [TJX7]. Drawing from the Diminish cluster TJX employed a justification approach (minimizing the number of records disclosed to "significantly less than millions") and employed a deny volition strategy to justify the tardiness of their response by claiming to have little control over the event [PR22: 1, PR23, TJX2]. The organization eventually apologized but simultaneously claimed that compensations were unnecessary. TJX instead shifted responsibility to consumers, who should "carefully review their account statements and immediately notify their credit or debit card company or bank if they suspect fraudulent use" [PR23].

SONY's recovery struggle is immediately evident from their response communication, starting with brief and insufficient updates on its PlayStation Blog, two weeks after its users noticed the network outage. Then, SONY primarily drew from the Deny cluster, both by claiming that "Hackers, after all, do their best to cover their tracks," and by playing the victim role AQ8 going absurdly off-topic: "In the last few months, SONY has faced a terrible earthquake and tsunami in Japan. But now we are facing a very man-made event—a criminal attack on us" [PR24, PR25]. Simultaneously, SONY used ingratiation as a reinforcing strategy thanking its customers for their "patience, understanding and goodwill." They emphasized that no credit-card data were being accessed (justification) [PR25: 1, PR27]. Finally, the organization promised a "welcome back" package with an identity theft insurance policy (compensation), without further information regarding its delivery.

Target responded with apology and compensation right from the start, combined with an inconsistent variety of other approaches. In no less than 8 press releases, Target first lamented "It was a crime against Target, our team members, and most importantly, our guests" (suffering), while simultaneously questioning the impact of the breach in light of "very few reports of actual fraud" (justification) [PR13, PR14, PR15, PR16]. AQ9 The company continuously denied control over development of the incident (deny volition) and subsequently evaded responsibility for potential theft of PCI information by denying they had the key to begin with [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 4 shows the recovery trends and crisis communication response strategies of the organizations.

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. This not only can partly be a consequence of declining data breach interest or arousal over time but also seems influenced by the communication strategies of the organization.

Findings and Discussion this should be a heading at the same level as 'Conclusions'

Base response strategies (instructing and adjusting) form an important part of the crisis communication arsenal of corporations facing data breaches (Bentley 2018). This study addresses a gap in the literature by looking into the effects of those base response strategies on reputation damage (cf. Park 2017). We find that particularly in the second period, base response strategies had improved qualitatively with more comprehensive and exhaustive guidelines, and detailed explanations about the incident to consumers. This seemed to address an important stakeholder need and seemed to have a positive effect on mitigating the reputation damage caused by the data breach.

We expected that the ambiguity of the crisis type characteristic of data breaches to influence the crisis response strategies chosen and their effects. In line with Bentley et al. (2018), corporations in the first period—2009–2013—were not inclined to admit responsibility. They did not so much play the victim card ("suffering" communication strategies), but they used other deny and diminish strategies that would be more appropriate for organizations facing victim crises. Only slowly did they opt for strategies from the "rebuild" cluster, something Christopher Hood called the "staged retreat"—being forced from denial to admission of responsibility—approach to blaming in the public sector (Hood 2014). Our research shows that admitting responsibility, offering apology, and compensation as one would in response to a blameworthy incident (the accident or intentional crisis type) has a more positive effect on reputation recovery after data breaches, than the denial and diminish strategies. Perhaps corporate learning took place, as many organizations in the period between 2014 and 2019 resorted successfully 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 perceived crisis severity suggests exclusively Rebuild strategies as the best recipe for the crisis response.

In line with SCCT predictions, 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 the outcome. Similar incidents in the past rarely featured in media coverage. In fact, the media even praised Capital One for previous successful technological advancements, despite having been involved in cybersecurity issues before.

Self-disclosure positively influenced media reporting. Self-disclosure allowed companies to control the narrative in the news coverage defining the hacking attack as "highly sophisticated" or "unprecedented," as opposed to an exposure of vulnerabilities inherent to the organizations' security system. Organizations that waited to disclose the incident, or to implement apology or compensation strategies (Equifax, TJX, SONY, Global Payments), met harsh criticism from media and consumers. Yet organizations that came forward transparently, completely and proactively about the data breach, were either praised for their approach (Anthem), or managed to limit the media attention (Capital One, The Home Depot).

Social media communication did not play an important role in the crisis communication strategies. Only two companies have used Twitter to provide crisis updates: Equifax and Capital One, but their opposite outcomes leaves the influence of this factor on organizational reputation unclear. Surprisingly the remaining companies did not even have a social media account at the time of the breach.

SECTION1

Conclusion

This research asked why some organizations maintain their good reputation in the aftermath of a data breach, and others fail to do so. The analysis of comparable cases with similar attributed responsibility suggests that crisis communication influences reputation damage. Maintaining a correct cybersecurity posture comprehensive of monitoring capacity and incident handling, providing detailed and exhaustive technical information about the incident, proactively owning the narrative of the events with transparency, and attentive customer-focused behavior, are all crucial for reducing reputation damage after data breaches. The base responses are clearly important in crisis communication strategies after data breaches. In addition, in spite of feeling victimized by hacking, corporations should instead treat data breaches as accidents for which they bear responsibility: consistent and timely adoption of compensation, apology, and rectification strategies, positively influenced reputational recovery from data breach crises.

Of course, this study has its limitations, with only eight cases to draw from. The high comparability of data breaches across sectors and the fact that data breaches are such a wide spread high probability, high-impact threat, make our tentative findings highly relevant. Future studies should include a high number of data breach cases to see if our findings hold statistically and if regression analysis can help to discern between the effects of base responses, self-disclosure, or consistency and clusters of strategies chosen. A number of conditions form interesting cues for future research.

. More recent corporate data breach please remove '.' before sentence cases suffer less reputation damage—perhaps as a result of breach fatigue, which implies reduced issue salience and less harsh public reactions. This possible trend invites future research, also to look for a tipping point where "one crisis too many" ignites a firestorm of criticism.

In addition, further research could look into other reasons for the improved performance in more recent communication responses after data breaches, applying the appropriate strategies consistently. All organizations in the more recent period of observation opted for self-disclosure of the incident but this may also relate to the rapid changes in their legal and corporate environment, requiring companies to comply with more stringent requirements. The progressive institutionalization of the cyber domain might also have influenced data breach response practices, together with previous failures and lessons learned. What is certain, is that data breaches are becoming the new normal, and organizations should better be prepared to respond effectively.

Publisher's Note

Funding

No funding

Declarations

Conflict of interest

The authors have no conflicts of interest to report.

SECTION1

Appendix 1: Press Releases

Number	References	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

SECTION1

Appendix 2: Media Sources by Case

Please adjust Appendix 2.

>>Not only 'Target' should be in white font on a dark background, but so should all case headings be (SONY, TJX, Global Payments, The Home Depot, Anthem, Equifax and Capital One) to give them equal emphasis.

>>there should be no white pace between line S8 and S9 in the table, and no white space between C4 and C5.

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

SECTION1

Appendix 3: Codebook Organization's Crisis Response Strategies

The operational definitions adopted to create to codebook have been extracted from the works of Coombs and Holladay (2010), Liu (2010) and Coombs (2007a).

Code	Code Name	Operational Definition	Example
DENY	Ignore	To implicitly deny a crisis by refraining to respond	Initially TJX dismissed the inflammatory claims: "We're not commenting about what others are saying about the situation" [TJX6: 1]
	Suffering	Proactively assume the role of the victim in regard to the events of the crisis	"In the last few months, SONY has faced a terrible earthquake and tsunami in Japan. But now we are facing a very man-made event – a criminal attack on us" [PR25]
	Scapegoat	To shift the responsibility for the events towards an external party	"Sony has been the victim of a very carefully planned, very professional, highly sophisticated criminal cyber attack." We discovered that the intruders had planted a file on one of our Sony Online Entertainment servers named "Anonymous" with the words "We are Legion." [PR27] "Hackers, after all, do their best to cover their tracks" [PR25]
DIMINISH	Justification	To minimize the impact or the proportions of the crisis event	"The data breach did not involve our merchants or their relationships with their customers" [PR11] "There have been very few reports of actual breach" [PR13]
	Deny Volition	To minimize responsibility for the event or its derivates by asserting lack of control over its occurrence	"Given the nature of the breach, the size and international scope of our operations, and the complexity of the way credit-card transactions are processed, [The response] is, by necessity, taking time" [PR22]
REBUILD	Apology	To make amends for the misconduct that enabled the outbreak of the crisis	"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" [C2]
	Compensation	To offer an indemnification to the victims in order to repair damages inflicted	Identity Theft Repair Assistance: Should a member experience fraud, an investigator will do the work to recover financial losses, restore the member's credit, and ensure the member's identity is returned to its proper condition. This assistance will cover any fraud that has occurred since the incident first began. [PR3]
	Rectification	To demonstrating full commitment to preventing future recurrences of the crisis	"Safeguarding our customers' information is essential to our mission as a financial institution. We have invested heavily in cybersecurity and will continue to do so. We will incorporate the learnings from this incident to further strengthen our cyber defenses" [PR4]
RECTIFY	Ingratiation	To commend stakeholders and customers on their support and loyalty towards the organization	"We greatly appreciate your patience, understanding and goodwill as we do whatever it takes to resolve these issues as quickly and efficiently as practicable" [PR25]
	Bolstering	To draw on past merits and achievements obtained by the organization to offset the negative consequences of the crisis	"We pride ourselves on being a leader in managing and protecting data" [PR7]

SECTION1

Appendix 4: Codebook Media Coverage

Based on Eisenegger (2004), cf. Cravens et al. (2003), Eisenegger and Imhof (2008), Formentin (2010), Ki and Nekmat (2014), and Weverbergh and Vermoesen 2020.

Code	Positive	Negative	Neutral
Description	Positive statements within a publication distance the organization from the causal chain of events, reduce the degree of *attributed responsibility* and *crisis severity*, or portray appreciation for its *performance history,* e.g., statements that portray the organization as victim, statements that praise the organization performance before, during and after the crisis, statements that minimize the impact of the crisis	Negative statements within a publication portray the organization as directly responsible for the events, increase the degree of *attributed responsibility* and *crisis severity*, or portray disapproval for its *performance history,* e.g., statements that address the organization as responsible for the crisis, statements that criticize the organization performance before, during and after the crisis, statements that emphasize the impact of the crisis	Neutral statements within a publication describe the organization navigating the crisis or the crisis itself, but do not convey information on the role played by the organization within the crisis or do not qualitatively portray its involvement in terms of attributed responsibility. This also includes informative statements about the event that do not address the organization's role in the crisis
Example	"Its decision to reveal the attack days after its discovery, even as the investigation is getting under way, may signal a changing attitude among corporate executives about rapid disclosures in the wake of breaches of companies". (A5)	"Equifax's struggle to deal with the fallout from a massive security breach is growing as lawmakers are asking questions about what happened and more consumers are lawyering up". (E6)	"Federal law requires health-care companies to inform consumers and regulators when they suffer a data breach involving personally identifiable information, but they have as many as 60 days after the discovery of an attack to report it." (A5)

References

Amaresan, S. 2019. Situational Crisis Communication Theory and How It Helps a Business. *Hubspot*, 2019. https://blog.hubspot.com/service/situational-crisis-communication-theory.

Arghire, J. 2020. Over 15.1 Billion Records Exposed in Data Breaches in 2019. *Security Week*, 2020. https://www.securityweek.com/over-151-billion-records-exposed-data-breaches-2019.

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.

Bentley, J.M., K.R. Oostman, and S.F.A. Shah. 2018. We're Sorry But It's Not Our Fault: Organizational Apologies in Ambiguous Crisis Situations. *Journal of Contingencies and Crisis Management* 26: 138–149.

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/.

Boin, A., P. 't Hart, and A. McConnell. 2009. Crisis exploitation: political and policy impacts of framing contests. *Journal of European Public Policy* 16 (1): 81–106.

Brändström, A., and S. Kuipers. 2003. From 'Normal Incidents' to Political Crises: Understanding the Selective Politicization of Policy Failures1. *Government and Opposition* 38 (3): 279–305.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2003. The Economic Cost of Publicly Announced Information Security Breaches. *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.

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.

Coombs, W. Timothy. 2007a. Attribution Theory as a Guide for Post-Crisis Communication Research. *Public Relations Review*. https://doi.org/10.1016/j.pubrev.2006.11.016.

Coombs, W. Timothy. 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.

Coombs, W. Timothy, and Sherry J. Holladay (eds.). 2010. *The Handbook of Crisis Communication, Blackwell*. 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.

Eisenegger, Mark. 2004. Reputationskonstitution in Der Mediengesellschaft. *Mediengesellschaft*. https://doi.org/10.1007/978-3-322-95686-6_14.

Eisenegger, Mark and Kurt Imhof. 2008. The True, the Good and the Beautiful: Reputation Management in the Media Society. In *Public Relations Research: European and International Perspectives and Innovation*, ed. A. Zerfass, B. van Ruler, K. Sriramesh, 125–146. Wiesbaden: University of Zurich. https://doi.org/10.1007/978-3-531-90918-9_8.

Formentin, Melanie J. 2010. *Extending Situational Crisis Communication Theory: Attitude and Reputation Following the 2004–05 NHL Lockout*. Scholar Commons: University of South Florida.

Nicole, Gillespie, and Graham Dietz. 2009. Trust AQ10 Repair After an Organization Level Failure. *Academy of Management Review* 34 (1): 127.

Gillespie, Nicole, Graham Dietz, and Steve Lockey. 2014. Organizational Reintegration and Trust Repair After an Integrity Violation: A Case Study. *Business Ethics Quarterly* 24 (3): 371–410. https://doi.org/10.5840/beq2014437.

Goel, Sanjay, Christopher Brown, and Hany Shawky. 2007. Measuring the Impact of Security Breaches on Stock Valuations of Firms. In *6th Annual Security Conference*.

Hawkins, Nick. 2017. Why Communication Is Vital During a Cyber-Attack. *Network Security*. https://doi.org/10.1016/S1353-4858(17)30028-4.

Hearit, Keith M. 2006. *Crisis Management by Apology: Corporate Response to Allegations of Wrongdoing*. London: Routledge.

Hood, Christopher. 2014. Accountability and Blame-Avoidance. In *The Oxford Handbook of Public Accountability*, ed. M.A.P. Bovens, R.E. Goodin, and T. Schillemans, 603–616. Oxford: Oxford University Press.

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.

Huq, N. 2015. Follow the Data : Dissecting Data Breaches and Debunking Myths. *TrendMicro Research Paper,* September 2015.

ITRC. n.d. Breach Reports [on 2007–2018]. Identity Theft Research Center (ITRC). https://www.idtheftcenter.org/images/breach/. Accessed 8 Dec 2020.

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*.

Ki, E., and E. Nekmat. 2014. Situational Crisis Communication and Interactivity: Usage and Effectiveness of Facebook for Crisis Management by Fortune 500 Companies. *Computers in Human Behavior* 35: 140–147.

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. *Lecture Notes in Computer Science*. 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*, ed. Sherry Holladay and W. Timothy Coombs, 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_OxfordMetricaReputationReview_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 Trading. 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): 136–147.

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/.

Zhou, Yucheng. 2020. Analyzing Historical Data Breaches to Improve Public Cloud Security Postures. *ProQuest Dissertations and Theses*.