Breach Response:

Saving face in the cyber-age

A comparative case-study on crisis communication efforts following data breaches

Master-thesis
Crisis and Security Management - Leiden University

Dennis van de Water
S1692984

Supervisor: Dr. E. De Busser

Word Count:
23.095 ex. ref. - 23.979 inc. ref.

Preface

This research is a submission in order to partially fulfil the requirements of the academic Master '*Crisis and Security Management'* at Leiden University. Tables, models, headers and illustrated comments within this research are excluded from the word-count. All research documents, such as coding-schemes, comment overviews and stock calculations can be made available on request.

Abstract

This comparative case study focusses on three distinct issues; determining what an appropriate corporate crisis-response would be in terms of crisis communication with regard to data breaches, evaluating three recent, high-profile data breach cases based on the adequateness of their response and attempting to validate the found results by determining the outcome of the three cases. In its attempts to do so it has proposed a new model for aiding in determining adequate response-strategies: the *preventability-model*. Furthermore, this research has brought to light numerous mistakes in the crisis response efforts of the evaluated cases and it has identified gaps of knowledge in the field of crisis communications caused by the complex nature of reputational damage.

Acknowledgements

By submitting this thesis I would like to thank a number of people without whom this research would never have reached its final form. Firstly I would like to thank my father, who, with his valuable discussions and proof-reads managed to keep me working on the research without losing too much attention. Additionally I would like to thank my dear friend David Rosdorff who, despite having better things to do, provided me with valuable advice throughout this project. Furthermore I would like to thank my girlfriend who often provided me with much needed mental support from the other side of the country. Most importantly I would like to thank Dr. De Busser as without her professional guidance this research would never have reached its current state.

Dedication

I would like to dedicate this research to the loving memory of my mother, without whom I would never have made it this far in life.

List of Abbreviations

While the full meaning of most abbreviations is given in the text upon their first appearance, this list of used abbreviations is included for the sake of overview.

Abbreviation	Full meaning
AES-128	Official technical term for the 128-bits Advanced Encryption Standard
CCSD	Comparative Case Study Design
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
CSO	Chief Security Officer
ECB	Official technical term for the Electronic Code Book method of data-encryption
GBP	British Pound Sterling (£)
ICO	Information Commissioner's Office of the United Kingdom
OAIC	Office of the Australian Information Commissioner of the Australian Government
SCCT	Situational Crisis Communication Theory
USD	United States Dollar ($)

Contents

I Introduction

As the process of global digitalisation progresses at a rapid pace, the world becomes ever more interconnected. While this creates many new opportunities and advantages it also carries inherent risks. One of those new risks is formed by cybercrime with cyber-attacks in particular. Despite new cybersecurity measures continuously being implemented by organisations, breaches of these security measures due to cyberattacks are steadily on the rise with the frequency of these breaches reportedly having increased by 11% from 2018 to 2019 and by 64% since 2014 (Bissell, LaSalle & Cin, 2019). These types of breaches amounted to the exposure of roughly 4.1 billion confidential records over the first half of 2019 alone (Cyber Risk Analytics, 08-2019). The exposure of such records may have far-stretching consequences for organisations and individuals alike as sensitive information such as account information, credit card details or internal business documents are being made available for misuse. Furthermore, despite the global average cost of a cybersecurity breach being estimated on 3.92 million USD (Ponemon, 23-07-2019), organisations and businesses continue to further digitalize their workspace rendering more organisational information vulnerable to these breaches (LogicMonitor, 13-12-2017).

While the instances of cybersecurity breaches are increasing and their impact can be disastrous, studies found that over 75% of businesses have no cybersecurity incident response plan in place (Ponemon Institute, 04-2019). While this might seem surprising regarding the interests at stake during cybersecurity breaches, it might form the indicator of the underlying problem that not much is known on how to tackle such breaches. While many previous studies are focussed on analysing more traditional crisis situations, research on cybersecurity issues and crises related to them mostly stick to identifying what happened and describing the technical details. The subject of tackling cybersecurity breaches, and the dimension of communication surrounding them, as a result largely remains uncharted territory.

It is therefore that this research project will focus on identifying what would theoretically be an adequate response to cybersecurity data breaches and to what extent these response-strategies differ from the ones already practiced by corporations suffering from such breaches. Therefore the main research question becomes the following:

> *''To what extent can corporate communication response to cybersecurity breaches be deemed adequate?''*

In order to answer this question, this research project will compare three recent, high-profile cases of cybersecurity breaches in order to comparatively analyse them on their crisis communication efforts and how these compare to crisis communication theory. Through this process, this research project aims to determine what communication efforts regarding cybersecurity breaches can be deemed adequate and should therefore be employed during future breaches. In order to further concretize the main research question, as it is essentially a rather broad one, it will be divided into four different sub-questions. These sub-questions are the following:

1. *How can the theoretically adequate crisis response regarding cybersecurity breaches be determined?*
2. *To what extent can the crisis communication efforts in the cases be deemed theoretically adequate?*[1]
3. *To what extent can the cases be compared in terms of the theoretical adequateness of their crisis communication efforts?*

[1] See the Theory and Methods chapters for a full explanation

4. *To what extent can the theoretically adequate response-strategies be validated by the outcome?*

As can be seen from these sub-questions, each sub-question describes a different aspect of the research, where the first question focusses on forming a theoretical model to determine which response-strategies can be deemed adequate, the second and third questions focus on analysing recent cases in order to assess and evaluate their crisis response. Finally, the fourth question focusses on attempting to assess the real-life practical implications of the selected response-strategies.

Answering the main research question carries significant academic importance as it allows for applying and testing established crisis communication theories on inherently modern and generally unexplored phenomena such as cybersecurity breaches. Furthermore, answering the research question grants the ability to categorize cybersecurity breaches into established crisis types such as those described by Coombs (2007). Additionally, in its attempt to assess the practical outcome of certain crisis response strategies, this research may be able to provide insight into gaps of knowledge regarding the field of crisis communication. Finally, this research project may form the first step towards the establishment of an academic framework that can be used to explain the impact of cybersecurity breaches in terms of sustained reputational damage.

Apart from the academic relevance the research project also carries a substantial amount of societal relevance as answering its research question may result in a better understanding of how to deal with cybersecurity breaches in terms of limiting reputational damage. These guidelines may in turn be used by organisations, both private and public, to establish or validate cybersecurity incident response plans. Since, as has been noted earlier, the majority of businesses still lack such a plan, the knowledge from this project may allow these businesses to finally have a sense on which to base the development of these plans. In a more general sense, the results of this research project may eventually contribute to a business-society that is better prepared to respond to cybersecurity breaches and mitigate their reputational threats.

II Theory and Literature

This theoretical chapter will focus on exploring theories relevant to this research and explaining how these will be applied or used. Additionally, the main concepts of this research will be conceptualized and previous research regarding similar topics will be briefly reviewed.

2.1 Theoretical Framework

In this paragraph, the main theories related to the research will be explored and their application to the research will be explained.

2.1.1. Attribution Theory and Situational Crisis Communication Theory[2]

Coombs' Situational Crisis Communication Theory (SCCT) provides clear and scientifically supported guidelines on what communication strategies to pursue following different types of crises. It therefore provides a suitable framework with which to determine the theoretical adequacy of the employed post-crisis response within different cases. As such this theory will be used to label and evaluate the employed post-crisis response in the different cases in terms of their crisis-communication. Additionally, applying Coombs' framework on a variety of cybersecurity cases allows for testing the framework against the reality regarding such modern cases. The theoretical notions underlying Coombs' SCCT (2007 & 2011) will therefore form the main theoretical pillar that guides the analysis and the subsequent answering of the research questions.

In his article '*Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory'* (2007) Timothy Coombs, for the first time forms his own theory on crisis communication that allows for organisations and crisis managers to have a framework through which to understand and anticipate reputational threats due to crises (Coombs, 2007: 163). This theory, which he calls the '*Situational Crisis Communication Theory'* (Coombs, 2007: 163), is based on empirical evidence and provides a set of crisis communication guidelines through which crisis managers can protect their organisational reputation (Coombs, 2007: 163).

Coombs bases his theory several assumptions, first he states that crises pose a threat to organisational reputation as this reputation consists of the way stakeholders think about the organisation and crises provide the stakeholders with reasons to think badly of the organisation (Coombs, 20017: 164). Furthermore, SSCT has its roots in the attribution theory which states that people will always search for a cause of events and are likely to attribute responsibility for the events to the organisations that played a role in it and can, to a certain extent, be deemed responsible (Weiner, 1985), therefore crises may result in anger and the attribution of blame towards the organisation(s) involved (McDonald & Hartel, 2000). On the other hand, when the crisis is outside of the responsibility of the organisation, meaning that it was the result of external factors such as technical failure or natural disasters etc., The stakeholder reaction may take the form of sympathy which can be beneficial to the organisation (Coombs, 2007: 166).

According to SCCT there exist three factors that shape the reputational threat of a crisis, these are the initial crisis responsibility, the organisational crisis history and the prior reputation of the organisation (Coombs, 2007: 166).

SCCT divides the types of crises into three categories regarding initial crisis responsibility, the first category, *''the victim cluster''* consists of crises which have a very low level of organisational responsibility for the crisis, such as crises resulting from natural disasters. In crises of this category the organisation is mostly seen as a victim of the crisis. The second category, ''*the accidental cluster''* consists of crises that can be considered accidents and are unintentional, such as technical errors, therefore knowing a minimal attribution of responsibility. Finally the last category, ''*the preventable cluster''* consists of crises caused by preventable actions such as human errors,

[2] Partial adaptation from one of my own previous research papers on Crisis Communication, for reference see: Van de Water, D. (2020)

organisational oversights or misdeeds or even intentional harm. Crises of this category often result in strong attributions of responsibility and therefore pose a severe threat to organisational reputations (Coombs, 2007: 167-168)

When it comes to organisational crisis history, SCCT states that if the organisation has experienced similar crises in the past, this might lead stakeholders to believe that the organisation has an ongoing problem that needs to be dealt with, therefore increasing the blame attribution and subsequently the reputational damage dealt by crises (Coombs, 2007: 169). The prior reputation on the other hand, may go two ways. If the organisation has previously been known to treat its stakeholders well, it might diminish the reputational damage of a crisis. However, if the organisation has a reputational history of treating its stakeholders poorly this might increase reputational damage done by crises (Coombs, 2007: 167).

After discussing this framework for anticipating the reputational impact of a crisis, Coombs goes on to discuss different crisis communication strategies (Coombs, 2007: 170) and link them to this previous theoretical framework by stating in which cases each communication strategy should be employed, based on empirical evidence (Coombs, 2007: 173). By doing so Coombs essentially creates a method through which it is possible to evaluate crisis communication efforts by reviewing the adequateness of the chosen crisis communication strategies in these efforts.

As these crisis communication strategies and the recommendations on when they should be deployed form an essential basis for the evaluation parts of the analyses within this study, it is important to mention them fully. In order to retain clarity with regard to these enumerations, both the crisis communication strategies and the recommendations following them will be reproduced fully in the following two separate tables accompanied by a short explanation relating to each table.

Crisis response strategies according to Coombs' SCCT

In his article Coombs mentions ten different types of crisis communication strategies that can be employed in order to protect organisational reputations from the effects of crises. He divides these response-strategies into two groups, being the *''primary crisis response strategies''* and the *''secondary crisis response strategies''* (Coombs, 2007: 170).

The primary response-strategies-group consists of strategies that are deemed to be the most effective in protecting reputational assets. This group is divided in three distinct categories being; *Deny*-strategies, which focus on framing the crisis in such a way that any connection between the organisation and the crisis is removed, *Diminish*-strategies, that aim to either lessen the organisation's role in the crisis or convince people to view the crisis less negatively and *Rebuild*-strategies which aim to improve and rebuild the organisation's reputation by offering an apology and material or symbolic aid (Coombs, 2007: 171-172).

The secondary response-strategies-group, which offers less opportunity to protect or develop reputational assets and can only be effective if a positive relationship with stakeholders already existed pre-crisis, consists of only one category: *Bolstering*-strategies. These strategies focus on reinforcing the organisational reputation by reminding the public of past organisational successes, praising the efforts of stakeholders during the crisis or trying to win sympathy by situating the organisation as a victim of the crisis (Coombs, 2007: 172). The full overview of all response-strategies incorporated into SCCT and their descriptions can be found in table 1.

Table 1: Crisis response strategies according to SCCT (Coombs, 2007: 170)

Primary crisis response strategies

Deny crisis response strategies

- *Attack the accuser:* Organisation confronts the person or group claiming something is wrong with the organisation or its response.
- *Denial:* Organisation asserts that there is no crisis or denies presumed aspects of the crisis.
- *Scapegoat:* Organisation blames some person or group outside of the organisation for the crisis.

Diminish crisis response strategies

- *Excuse:* Organisation minimizes organisational responsibility by denying intent to do harm and/or claiming inability to control the events that triggered the crisis.
- *Justification:* Organisation minimizes perceived damage caused by the crisis by justifying its actions.

Rebuild crisis response strategies

- *Compensation:* Organisation offers money or other gifts to victims.
- *Apology:* Organisation takes responsibility for the crisis by expressing its regret and/or asking stakeholders for forgiveness.

Secondary crisis response strategies

Bolstering crisis response strategies

- *Reminder:* Organisation emphasizes its qualities or reminds stakeholders about past good works of the organisation.
- *Ingratiation:* Organisation praises stakeholders for their efforts during the crisis.

(Partial adaptation of Coombs, 2007: 170)

Crisis response strategy recommendations according to Coomb's SCCT

In addition to specifying the different possible communication or response-strategies that can be deployed during a crisis, SCCT also provides guidelines regarding which strategies should be deployed in certain situations. SCCT argues that the best communication strategy is determined by the inherent factors constituting the crisis mentioned earlier, being the type of crisis (regarding the level of responsibility of the organisation), the crisis-history of the organisation and the organisational reputation prior to the crisis (Coombs, 2007: 167-168). In a later reformulation of his SCCT-theory Coombs refers to these last two factors (The presence of either an organisational history of crises or a negative reputation prior to the crisis) as *'intensifying factors'* as they intensify the threat that is posed by the crisis (Coombs & Holladay, 2011: 39). Based on this knowledge SCCT initially formulated eight distinct guidelines in order to determine which response- or communication strategy would be or would have been most suited to the situation (Coombs, 2007: 173), this set was later reformed and expanded to ten recommendations, of which two are deemed to be a *Base response* to the crisis that should always be employed (Coombs & Holladay, 2011: 42) These ten recommendations can be found in Table 2. In addition to these recommendations, Coombs does mention that certain boundaries might exist in determining which strategy would be best suited to the situation at hand as financial constraints or a predetermined media-frame might limit the possible actions (Coombs, 2007: 173).

Base-response as a pre-requisite for proper crisis communication

While Coombs' own 2007 article initially only incorporated ten different response-strategies divided over 4 distinct categories, in his later article from 2011, a pre-requisite for the effectiveness of all response-strategies is added (Coombs & Holladay, 2011). This pre-requisite is called the *'Base-*

response' and is mentioned in the list of SCCT-recommendations (Coombs & Holladay, 2011; Table 2). This base-response is a type of response that should be applied in all instances of crisis communication efforts, regardless of the type of crisis (Coombs & Holladay, 2011; Table 2). The *Base-response* consists of two interdependent aspects, being the information-aspect and the care-aspect or 'care-response' (Coombs & Holladay, 2011: 42; Table 2). Since the *Base-response* is such a broad and universally applicable response-strategy, it is expected to often form the majority of content in crisis communication efforts. This is due to the fact that any form of information about the crisis and its consequences or any notice about resolving the crisis and preventing instances of the same sort in the future, are deemed to be a part of the *Base-response.*

Table 2: Crisis response strategy recommendations according to SCCT (Coombs & Holladay, 2011: 42)

1	All victims or potential victims should receive instructing information, including recall information. This is one-half of the base response to a crisis.
2	All victims should be provided an expression of sympathy, any information about corrective actions, and trauma counseling when needed. This can be called the "care response." This is the second-half of the base response to a crisis.
3	For crises with minimal attributions of crisis responsibility and no intensifying factors, instructing information and care response is sufficient.
4	For crises with minimal attributions of crisis responsibility and an intensifying factor, add excuse and/or justification strategies to the instructing information and care response.
5	For crises with low attributions of crisis responsibility, and no intensifying factors, add excuse and/or justification strategies to the instructing information and care response.
6	For crises with low attributions of crisis responsibility and an intensifying factor, add compensation and/or apology strategies to the instructing information and care response.
7	For crises with strong attributions of crisis responsibility, add compensation and/or apology strategies to the instructing information and care response.
8	The compensation strategy is used anytime victims suffer serious harm.
9	The reminder and ingratiation strategies can be used to supplement any response.
10	Denial and attack the accuser strategies are best used only for combating rumors and/or challenges to the morality of an organization's behaviors.

(Full adaptation of: Coombs & Holladay, 2011: 42)

2.1.2. Cluster category of Cybersecurity data-breaches

As Coombs discusses in his article, there exist different categories or types of crises with each their own optimal response-strategies. These categories, which he calls 'crisis-clusters' function as artificial labels for crises to distinguish them from one another both in terms of actual responsibility and expected blame attribution (Coombs, 2007). This last part is important as it denotes that even if a crisis cannot be fully deemed the fault of an organisation, if its stakeholders still consider it the organisations fault or responsibility it will often still be considered a case of high probable blame attribution in terms of crisis characteristics and recommended response-strategies (Coombs, 2007; Coombs & Holladay, 2011; Wang & Park, 2017).

In order for this research project to determine which employed crisis response-strategies can be deemed theoretically adequate it is important to first determine the crisis-category of the analysed cybersecurity incidents. Academic literature however, provides no clear guideline on how to characterize cybersecurity data breaches as authors in the field are generally divided on how to categorize such an incident.

On the one hand, there are authors such as Krishna & Vibber who base their categorization of

the crisis fully on the objective aspects of fault, thus ignoring the importance of actual public blame attribution (2017). In their article '*Victims or conspirators?'* they classify the 2014 hack of Sony Pictures as a victim-cluster crisis (Krishna & Vibber, 2017). They base this on the fact that the crisis resulted from foreign state-sponsored interference making the crisis a form of malevolence stemming from an external actor.

While such a consideration seems reasonable other authors reject this notion of cybersecurity breaches being victim-cluster crises. Authors such as Ramakrishna for instance state that data breaches are the result of human errors as they are often attributed to out of date systems, careless employees, lacking security policies or an altogether failure to secure the systems against hostile actions (Ramakrishna, 2012). Following the reasoning of Ramakrishna data breaches would fall under the preventable-cluster of crises. Such reasoning is supported by Jenkins, Anandarajan and D'Ovidio (2014) who state that in cases of cybersecurity-related data breaches, the best strategy for organisations is to adopt a rebuilding strategy in which taking responsibility, apologizing and corrective action take the central stage (Jenkings et al., 2014). By stating this Jenkins et al. agree with Ramakrishna that data breaches are preventable-cluster crises, as these response-strategies are inherent to this type of crisis (Coombs & Holladay, 2011). In contrast to Ramakrishna however, Jenkins et al. do not base their notion on the objective characteristics underlying data breach incidents, but rather on the probable blame attribution stemming from such crises. The authors argue that due to the impact of data breaches on stakeholders, in the form of their personal information being accessed and possibly used by a malignant party, the stakeholders are prone to carry negative feelings towards the organisations tasked with protecting this information (Jenkins et al., 2014). As a result those stakeholders are likely to attribute blame towards these organisations for failing to protect their data. Reputation loss is often unavoidable in such cases but Jenkins et al. argue that it is wise for the affected organisations to utilize the opportunity of addressing their stakeholders to take responsibility and apologize as if it were fully their fault in order to minimize the reputational damage (Jenkins et al., 2014).

Due to the lack of consensus concerning the cluster type of data breaches, it is necessary to adopt an original approach regarding this topic. In order to prevent adopting the wrong crisis type, possibly leading to insignificant results of this research project, an extra chapter is added to the case description part of this research (Chapter IV). After describing all cases, the found aspects of the cases will be used to assess the cases in terms of crisis-cluster. If the cluster-type the crises adhere to is assessed SCCT's recommendations can be used to determine the theoretical adequate response-strategies for each of the cases.

2.1.3 Failure of Foresight

As there is still uncertainty regarding the crisis-cluster under which data breaches should fall, it is important to devise a way to determine this cluster-type per case. The theory of '*Failure of Foresight'* is a theory that aims to explain how man-made crises come to happen and how they can develop. This theory can be utilized to assess whether or not the cybersecurity breaches in the cases might have been preventable. This in turn allows for scientifically determining the cluster type to which the crises adhere.

The theory, first formed by Barry Turner in his 1976 article ''*The Organizational and Interorganizational Development of Disasters''* (Turner, 1976) states that man-made crises are often the result of a so-called *failure of foresight*. This term entails the fact that crises are often the result of a number of common causal features that lead to a failure to predict or prevent a crisis. In order to understand Turner's theory it is important to realize that he claims that each crisis usually consists of six different stages of which the first two take place before the event of crisis and are thus of particular importance in explaining why crises happen (Turner, 1976). Since Turner argues that most crisis-studies focus on the stages during and after crises (stages III to VI) he focusses his theory on explaining the first two stages being stage I: *the stage of initial beliefs and norms*, and stage II: *the*

incubation period (Turner, 1976) In order to link these stages to the creation of man-made crises, Turner goes on to comparatively analyse three different crises with regard to the events of their first two stages. By doing so Turner managed to identify seven common causal features that were present in each of the cases and explained the emergence and development of the crises through the presence of a *failure of foresight*. These common causal features will each be briefly explained.

Rigidities in perception and belief in organisational settings

This first common causal feature found by Turner entails the possible collective blind-spot organisations and members of the organisation might have or develop with regard to important issues. This blind-spot is often the result of a pre-existing organisational culture or a predominant set of beliefs and practices within the organisation. In a sense this feature entails a form of tunnel-vision both in attitudes and perception of organisational members resulting from the organisational culture that leads to, in hindsight, important issues being ignored or missed completely. This in turn might lead to these ignored issues developing into an organisational crisis (Turner, 1976).

The decoy problem

The second common causal feature identified by Turner entails the accidental treating of the wrong problem. Turner states that organisations often tend to focus all their attention on problems or hazards that they are familiar with but that this practice of treating a well-known problem may in turn distract attention from other, lesser-known problems which might eventually go on to cause trouble or even a full-blown crisis. Since this feature deals with a problem of distraction, Turner calls this feature '*the decoy problem'* (Turner, 1976).

Organisational exclusivity: disregard of non-members

The third feature denotes situations in which outsiders, for example non-members of the organisation or third parties, have already foreseen the danger that eventually led to the crisis and even tried to alert the organisation of its presence but are simply ignored or met with a dismissive response (Turner, 1976). This feature is often the result of an inherent belief within the organisation that they are the experts on the matter and they know best, or at least better than outsiders, regarding the matters they are dealing with (Turner, 1976). Of course, neglect of these warnings has a relatively high chance to result in an escalation of the danger with a possible crisis as its consequence.

Information difficulties

The feature of information difficulties is rather self-explanatory as it essentially entails the failure of an organisation to thoroughly and exhaustively communicate a complex or vague situation, such as a danger of organisational hazard, to relevant individuals or parties. This communication failure is often the result of a pre-existing organisational problem with regard to the communication structure and practices. Such information difficulties might, in turn, contribute to the initial emergence or eventual mishandling of dangers and as such eventually contribute to the emergence of crises (Turner, 1976).

Involvement of strangers

Another common feature of *failure of foresight*, according to Turner, is the involvement of strangers (Turner, 1976). According to Turner, the presence of uninformed or untrained people in potentially hazardous situations might lead to either improper or downright unpredictable behaviour (Turner, 1976). The presence of strangers displaying such behaviour will often actively complicate safe-operation-practices and may escalate situations that are initially thought to be under control into crisis-situations.

Failure to comply with existing regulations

The sixth common causal feature of *failure of foresight* consists of organisations disregarding or simply failing to comply with existing regulations. This practice might either result from a lack of effort on behalf of the organisation or its members, but might similarly result from the regulations being outdated and thus being ignored on purposes or being difficult to apply due to technical, social

or cultural conditions that have changed over time (Turner, 1976). Regardless of the reasoning behind the practice, the failure to comply with regulations may lead to dangerous and unpredictable situations.

Minimizing emergent danger

The last common causal feature identified by Turner is the practice of minimizing or underestimating emergent danger. This happens when impending dangers are recognized but are underestimated or undervalued (Turner, 1976). This leaves the organisation with a vulnerability to the danger which might in turn lead to the organisation failing to adequately respond and deal with the danger thus leaving room for the danger to develop itself into a crisis.

2.2 Conceptualization of the main terms

2.2.1 Cybersecurity breach

The term ‘’security breach’’ encompasses an event in which security systems are in place but these systems are either circumvented or cracked (Symanovich, 15-09-2018). While the term ‘security breach’ is most often used in the context of cyberattacks and cybersecurity, the term itself is in essence very broad and is, in professional contexts, also used to denote more traditional forms of security circumvention (e.g. the circumvention of airport security by criminals etc.)(Dibazar, Yousefi, Park, George & Berger, 2011). For the sake of clarity and cohesiveness, this research project will therefore use the more novel term ‘*cybersecurity breach’* to denote events in which cybersecurity systems were cracked or circumvented. Additionally, it is important to realize that while many organisations and individuals use the terms ‘security breach’ and ‘data breach’ interchangeably, they encompass different events. It is important to realize that a security breach deals with ill-willing individuals getting past security systems, while a data breach often forms the next step; the perpetrators actually accessing and exploiting data that was protected by the security systems (Symanovich, 15-09-2018). Data breaches are therefore a select, but frequent, form of security breaches and not all security breaches lead to data breaches.

2.2.2 Crisis response

The term ‘crisis response’ is a broad and ambiguous concept that often denotes all assets and actions employed by an organisation or a group of organisations to deal with an ongoing or past crisis. Within the academic world however, the concept is often divided into two distinct categories;

Immediate crisis response

The first conceptualisation of crisis response encompasses the immediate (or near immediate) actions taken to resolve a crisis. In a sense, it denotes the collective of crisis management actions taken in order to alleviate of fully resolve a crisis, such as the lockdown of critical systems or the cooperation with regional authorities. Authors that use the concept in this way are, among others, Moynihan (2009), Pearson & Clair (1998) and Smits (2015).

Post-crisis response

The second conceptualisation of crisis response is the collective of crisis communication efforts employed by organisations in order to mitigate and deal with the public impact of a crisis, which can for the sake of overview be regarded as the *‘post-crisis response’*. This conceptualisation is a frequently used definition of crisis response and is used by authors such as Coombs (2007) Claeys & Cauberghe (2012) and Sisco, Collins & Zoch (2010). This conceptualisation of the term crisis response will be the central definition that will be used during this research project. therefore, during this research project, the term crisis-response will predominantly be used to indicate the post-crisis communication efforts.

2.2.3. Adequacy

The adequacy of chosen strategies will in this research mainly be determined on a theoretical basis. While SCCT provides clear and scientifically proven guidelines on how to deal with certain crisis types, it fails to properly provide a model through which the crisis-category or crisis cluster of modern crises such as data breaches might be assessed (Coombs & Holladay, 2011). Therefore, in order to assess the adequacy of certain response-strategies, the set of response-strategies that could theoretically be deemed adequate for each of the cases should first be deduced. In order to do this, this research proposes the *preventability-model* which uses the concept of '*failure of foresight'* in order to determine mistakes that contributed to the current state of the different studied crises therefore simultaneously assessing their preventability and thus their crisis-cluster type (See chapter IV). If the aspects of the crisis, such as the crisis cluster, are known, SCCT's recommendations can be followed in order to determine the theoretically adequate set of strategies for each of the cases (Coombs & Holladay, 2011).

2.2.4 Outcome

Within this research 'outcome' as a concept will be used to evaluate whether the proposed model and its evaluation of the cases can be validated and supported by the practical results of the cases. In a certain sense the outcome focusses on the 'effectiveness' of the employed response-strategies in mitigating reputational damage.

However, there are multiple factors that make such a validation hard if not impossible. Firstly outcome as effectiveness is, in an academic sense, considered to be an ambiguous concept that is not easily conceptualised. Most authors agree that effectiveness, and with it outcome, has its roots in input- and output-studies and is mostly used to indicate the process of generating the most or best output with a predetermined input (Scheerens & Creemers, 1989; Harrington, Gordon, Osgood-Roach, Jensen & Aengst, 2015). Within the field of crisis management, effective crisis management is often defined as an organisations ability to successfully resolve and recover from a crisis, thus leading to a 'good' outcome (Mitroff, Shrivastava & Udwadia, 1987).

Coombs, who focusses on post-crisis responses, denotes that the outcome of crises is dependent on the communication surrounding the crisis (Coombs, 2007). He claims that communication efforts lead to a desirable outcome if they manage to repair an organisations reputation and/or prevent reputational damage as this in turn allows the organisation to quickly recover from the crisis (Coombs, 2007). While SCCT's recommendations are based on scientific evidence evaluating the impact of response-strategies in a large number of cases, most research based on SCCT does not make efforts to properly revaluate SCCT's recommendations on a per-case basis. Research that does try to assess the outcome of certain response-strategies mostly limit themselves to a singular questionable aspect of the outcome such as a singular dip in market value (Wang & Park, 2017), the analysis of social-media comments (Krishna & Vibber, 2017) or reframe attempts by the media (Kim, Johnson & Park, 2017). However, none of these methods on its own is able to sufficiently determine the actual outcome in terms of reputational damage and thus response-effectiveness. The lack of an holistic method for determining outcome is understandable however, due to the highly ambiguous nature of reputational damage, a lack of academic consensus on the impact of crisis communication and the extensive and complicated nature of cases plaguing assessments of correlation with external factors (Coombs, Frandsen, Holladay & Johansen, 2010; Mattila, 2009).

This led many acclaimed researchers and even pioneers in the field of crisis communication to adopt a rather unscientific stance towards the determination of outcome in cases, being an assessment based on rationally linking certain post-crisis events in a case to the employed crisis-response-strategies without uncovering scientific evidence to support such a link (Coombs et al., 2010; Benoit; 1997).

Because of this lack of a holistic method, this research will, in order to potentially answer the fourth sub-question, attempt to assess the outcome and its possible link with the employed response-strategies through the use of a combined approach. This combined approach will encompass popular

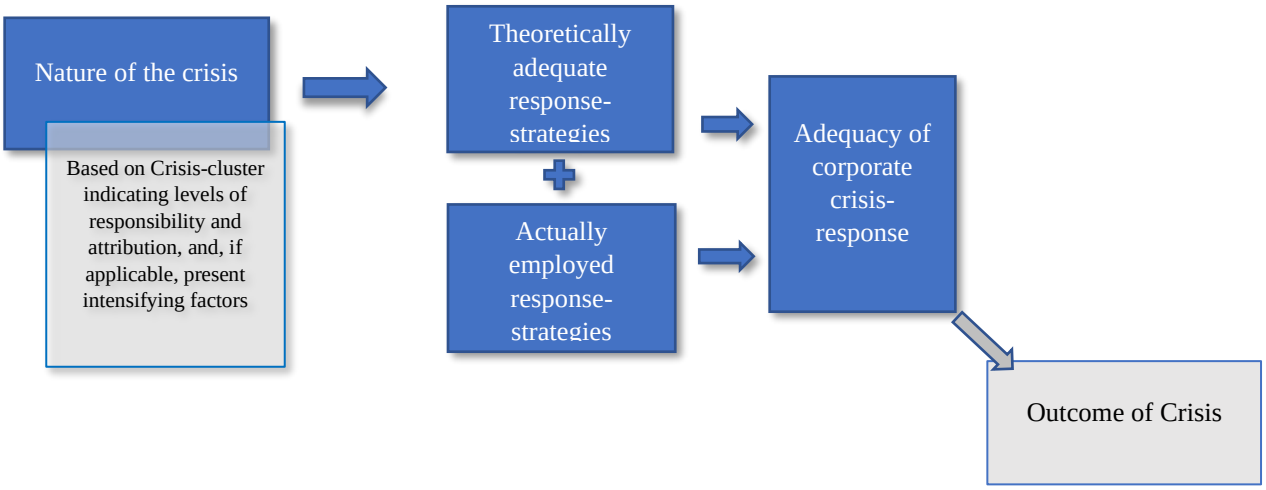
methods such as a comment-analysis and an interpretation of stock-value effects, but also a more qualitative approach in the form of analysing the nature of critique on the cases.

In the case that such an approach to outcome fails or does not provide enough scientific evidence to properly support its indications, the issues with this approach will be discussed in order to further the understanding of the complex nature of crisis communication research. In such a case the results of the combined approach method should be regarded as an indication of the outcome that approximates its results instead of scientifically proving them. In this case it is important to realise that determining the outcome in a fully scientific manner is not the main goal of this research. Instead, it is a way to potentially validate its findings concerning the adequacy of found response-strategies.

2.3 Conceptual relations

In this research project the adherence to adequate response-strategies forms the dependent variable. This dependent variable relies on two independent variables being; the theoretically adequate set of response-strategies and the actually employed set of response-strategies in the cases. If the independent variables are investigated more thoroughly however, it becomes clear that the independent variable of theoretically adequate response-strategies is in a sense also a dependent variable on its own. This is due to the fact that the theoretical adequacy of response-strategies depends on the nature of the crisis in terms of its cluster-category and potentially present *intensifying factors*. As such the conceptual relations model of this research becomes the following:

Model 1: Conceptual relations model



The type of crisis in this case forms the constant factor as this will remain the same between the cases: cybersecurity breaches.

III Methods

3.1 Research Design

In order to answer the posed research question and its sub-questions a qualitative, comparative case-study was performed that compared three prominent cases concerning cybersecurity breaches in terms of their crisis-response-strategies. The main method with which the information regarding the cases was analysed consisted of a content analysis. This allowed the cases to be analysed and coded in a structured way, to better facilitate a comparison between the cases.

3.1.1 Comparative case-study

A comparative case-study allows the researcher to qualitatively engage with different cases on a wide variety of levels in order to find similarities and differences between the cases that might indicate or explain a causal phenomenon (Bartlett & Vavrus, 2016). The cases are initially selected on the premise of similarity in aspects between the cases, this allows for an in-depth analysis of possible differences between the cases and conclusions on what may explain these differences (Bennett, 2004)

Within the context of this research project, employing a comparative case-study design (or CCSD) allows for the selection of a variety of cases in which similar organisations dealt with similar circumstances (cybersecurity breaches) and a comparison of the crisis response actions and strategies they employed as these may show inherent differences. Using a CCSD additionally allows for the thorough consideration of all actions taken within a case since its qualitative nature presupposes that the researcher actively explores all aspects and reasonings within a case to be able to properly compare them. The downside of this qualitative nature however is that supposedly found causal mechanisms are hard to prove since they may similarly be caused by intervening factors or just mere coincidence. Furthermore, employing a CCSD comes with the inherent problem of case selection and a risk of selection bias (Bennett, 2004). In order to mitigate these issues, it is important for a researcher to avoid selecting his cases on the dependent variable (Collier and Mahoney, 1996) and to select cases with as many similarities as possible in order to rule out the presence of alternative causal variables (Berg-Schlosser & Meur, 2009).

Since CCSD is only the design of the research project, it needs to be properly supplemented by a method of data-analysis, by the use of which the data found between the cases can be analysed.

3.1.2 Content Analysis

The main method of data-analysis in this research project consists of a structural content-analysis. The method of content analysis can be described as ‘’*any technique for making inferences by objectively and systematically identifying specified characteristics or messages’’* (Holsti, 1969 as mentioned by Woodrum 1984: 2). A content analysis is mainly performed through selecting relevant sources, mostly documents, selecting theories on which to base the analysis, establishing a codebook based on these theories and then structurally coding the different sources with the help of the codebook (Woodrum, 1984). By applying this method, the sources can be objectively interpreted and elements relating to the theories within these documents can be indicated, highlighted and compared with each other. This allows for a somewhat quantitative assessment of inherently qualitative documents without disregarding their characteristics, themes and meaning (Woordrum, 1984). Other advantages of employing content analysis as a research method are the fact that it is an inexpensive method, it is a safe method in the sense that errors or mistakes can easily be resolved by returning to the relevant text and it does not infringe on the research subjects as the text is only analysed and not edited (Woodrum, 1984).

Utilizing content analysis also comes with some risks and disadvantages. One of these is the possibility of coder bias; a situation in which the researcher bases his coding system on biased principles, which results in reliability and validity issues (Woodrum, 1984). Furthermore, the assumption of content analysis that texts are objective displays of the truth can become one of its pitfalls (Woodrum, 1984). In order to counter these issues the researcher must be cautious in his development of a codebook and his coding-efforts and ground these processes in his selected theories,

so as to ensure that minimal bias becomes part of the process. Additionally, the researcher must carefully select his sources to respect the objective nature of the content analysis.

Within this research project content analysis is used to analyse crisis response statements from the different cases in order to assess to what extent the crisis-communication efforts of the organisations adhere to the theoretically adequate framework. It is therefore that the codebook used in the content analysis consists of an operationalisation of the different aspects of Coombs SCCT (2007) as explored in the theory chapter. The Codebook is further elaborated upon in Chapter 3.2, and is also included in this research as an annex (See Annex 1).

By choosing a content analysis as the main research method the researcher agrees to carefully consider and elaborate upon a multitude of dimensions subject to the content analysis. The most important dimension to consider regarding a content analysis are the type of content analysis that is conducted and the unit of analysis that is employed, these dimensions are discussed in the following paragraph. The dimensions relating to the data-selection and -interpretation stage of the content analysis are discussed in paragraph 3.3.3.

Type of Content Analysis

One of the main choices guiding the usage of a content analysis as a research method is which type of content analysis to employ. There are two general types of content analysis, being the quantitative analysis and the qualitative analysis (Mayring, 2004).

A quantitative content analysis is a type of content analysis that, as the name would suggest, focusses on identifying quantities. This type of content analysis is often used in order to measure the importance of subjects through documenting the number of instances in which indicators of these subjects are mentioned within the content that is analysed (Oleinik, 2011; Evans, McIntosh, Lin, & Cates, 2007). The downside to this method is that the research question must be structured in such a way to allow answering through the measurement of quantities (Oleinik, 2011).

To allow identification of inherently qualitative subjects such as strategies or intentions, researchers may instead opt for a qualitative content analysis. A qualitative content analysis takes into account the context of the indicators found and allows for interpretation of statements in order to deduce the author's message. (Oleinik, 2011).

While both types of content analysis can be simultaneously employed, for example by using quantitative analysis in order to identify important paragraphs, after which qualitative analysis is used to code these paragraphs (Oleinik, 2011), this research will mainly employ a qualitative content analysis. This is due to two factors; the scope of the research question and expectations surrounding the analysis.

In order to answer the research question it is necessary to determine what crisis-response-strategies the organizations employed and whether these strategies are adequate based on SCCT's recommendations. In answering this question it is not relevant to examine how many times a certain strategy is used within a document.

Secondly, due to the fact that the *Base response*, according to expectations based on SCCT, is likely to be present within every crisis-communication statement analysed. Interpreting results in a fully quantitative manner would lead to non-results as the *Base response* would undoubtedly be the most emphasized strategy within every case, a result that is made redundant by the knowledge that every attempt to provide information regarding the crisis is a form of *Base response.*

A quantitative approach to the content analysis can however prove useful when the statements and the cases they adhere to are compared to each other. In such a comparison knowledge on how many statements include certain strategies that might facilitate generalisation efforts.

Unit of analysis[3]

Another important question is which unit of analysis to select. Briefly explained, the unit of analysis in a research project is the direct form of content that is being studied, analysed and labelled (Elo & Kyngäs, 2008). With a content analysis of statements the unit of analysis might for example be chapters, paragraphs, sentences or even words. Based on a review of the structure of the selected documents and the theory underlying the content analysis, a denotation of paragraphs as the unit of analysis throughout this study has been selected. This is mainly due to the fact that crisis communication statements are generally rather short statements but still deliberately thought out and with a certain 'flow' to them in terms of response-strategies following up on one another. Most statements are already divided into distinct paragraphs that are each based around a certain response-strategy. Utilising a smaller unit of analysis such as sentences or even word-groups, would lead to double coding as indicators that consist of multiple words or sentences get coded multiple times as an instance of the same strategies. The trade-off that comes with employing a relatively large unit of analysis is that it increases the chance of multiple different response-strategies being identified within one unit of analysis. While such a result might be unwanted in certain studies, the quantity of the employed response-strategies within a document is not relevant for this research, the focus lies on identifying what response-strategies are employed. Finding multiple response-strategies within the same unit of analysis would therefore not negatively affect the research as the different response-strategies are identified nonetheless.

Furthermore, it is important to mention that the selected data will be analysed as a whole. This means that every content-centric part of the text of a document will be part of an analysed unit of analysis.

3.2 Operationalisation

3.2.1 Operationalising crisis response-strategies

In order to scientifically determine which response-strategies and actions are deployed in the cases, a codebook has been created to guide and structure the content analysis (Forman & Damschroder, 2007). As the content analysis is meant to determine to what extent the different cases selected in this research conform to the theoretical framework created in the theory section, the codebook has been created on the basis of Coombs' SCCT (2007). As can be seen in chapter 2.1.2. SCCT provides a clear selection and overview of the different crisis-response-strategies that might be employed in a post-crisis situation. These listed response-strategies and their characteristics have been adapted into a cohesive codebook that exists of five possible codes, or response-strategy-categories, that encompass all ten possible crisis-response-strategies that can be employed during a crisis response (See Annex 1 & Table 1).

3.2.2. The 'Base-Response' as an additional category

It must be mentioned that based on SCCT one would expect only four categories of response-strategies to exist, however, when viewing SCCT's recommendations it becomes clear that an important category of strategies is often overlooked. This category is identified by Coombs as the '*Base response'* (Coombs & Holladay, 2011; See Table 2). The *base-response*, as described by SCCT, is not so much a strategy on itself as it is a line of response-strategy that is a necessary pre-requisite to a proper response (Coombs & Holladay, 2011). Because of this importance, and the possibility of a lacking *base-response* rendering an otherwise reasonable crisis communication effort invalid, the *base-response* has been included in the codebook as the fifth category of response-strategies. Additionally, the different facets of the Base response such as *Crisis information, Display of empathy* or promises of *Corrective action*, have been adopted as the indicators identifying the presence or lack thereof of a proper *base-response*.

[3] Edited and rewritten version based of an earlier paper by the author on the subject of content analysis with regard to crisis communication, for reference see Decuypere & Van de Water (2020)

3.2.3. Operationalising outcome

As mentioned in chapter 2.2.4. this research will, through answering its fourth sub-question, attempt to determine to which extent its results can be validated by the actual crisis-outcome of the cases. In order to do this, the outcome has been operationalised in three different components based on a combination of existing research and rational deduction.

The first component is *'market effects'*. This component is based on the theoretical notions that reputational damage resulting from crises should be visible through market effects such as stock value drops or overall business devaluation (Wang & Park, 2017; Way, Khan & Veitch, 2013). A fairly recent report by Bitglass noted that in the case of data breaches, stock prices on average fall as much as 7.5% (Bitglass, 2019). While a part of such stock effects can be attributed to expectations of crisis-related costs, existing research states that a substantial part of such losses expresses a reputational loss (Way et al. 2013). Because of this, stock value drops following the crisis responses in the three cases are evaluated in order to determine whether there is any notable difference between them that can be explained by the crisis response-strategies of the relevant companies.

The second component is one that is more traditionally related to the crisis communication field, namely *'public response'*. As reputational damage essentially boils down to a negative change in the perception of the stakeholders with regard to the relevant organisation, measuring the public response is one of the most commonly used ways to determine the extent of such damage. The most popular method to measure public response with regard to crisis communication is to analyse publicly accessible comment sections. This method is used by numerous scholars including Zhang, Kotkov Veijalainen & Semenov (2016), Krishna & Vibber (2017) and Libin & Xiaotong (2019). These comment sections can be taken from different sources such as social-media platforms, forum-threads or digital news articles (Zhang et al., 2016; Krishna & Vibber, 2017). Due to the popularity and scientific prevalence of comment analysis in the field of crisis communication, this research will try to determine the component of public response through a comment analysis. During the investigation into the three selected cases of this research, it became apparent that none of these cases led to extensive social media discussions nor to widespread public comment sections in media articles. Two news sources however do contain articles for all three cases on which public reactions are allowed, these are The New York Times and CNET. Due to the technology-oriented nature of the cases and the fact that mixing comments from multiple news-sources would lead to unreliable results, only the comments on CNET articles are selected for analysis. The actual analysis of these comments will be done through a thematic comment analysis which is a form of light content analysis. Like the main content analysis of this research, this comment analysis is based on its own codebook (See Annex 2).

The final component of reputational damage that is selected for this research is added on the basis of rational deduction. As, in order to explain differences in outcome, it is important to know how certain response-strategies affected the outcome, it is important to evaluate which aspects of a crisis response were criticized the most. Therefore the component of *'response critique'* will be added to the indication of the outcome. This component will be structured based on two different sources. Firstly, meta-articles were written on all three cases. These articles essentially consist of published reactions from industry experts on the relevant case, and can be found on security-related websites such as ITSecurityGuru.org and HelpNetSecurity.com. Secondly, the public comments that are analysed in the comment analysis often include a direct critique on the crisis response and may therefore also be a useful source. As such these sources will be analysed with a light thematic discourse analysis, meaning that reactions in these sources that fit the thematic condition of '*critique on response*' are selected for analysis. Based on this thematic selection, the most prevalent critiques will be discussed in order to provide an indication of which strategies or aspects of a response created the most negative responses. While this evaluation of critique will not be enough to determine the outcome of a case on itself, it provides a practical addition to the other two components as it allows an insight into the reasoning behind the reputational damage.

3.3 Case study and selection of cases

3.3.1 Case-selection

In order for a comparison between cases to work it is necessary to select cases that can be compared. A selection has been made based on extensive research into important cyberattacks and data breaches.

The first selected case is the Yahoo cybersecurity breach that was discovered in 2016 but had been going on since 2014 and resulted in a data-breach compromising over half a billion accounts initially and over 3 billion accounts in total, breaking the record for largest data-breach of all time (NBC, 22-09-2016; Trautman & Ormerod, 2016). Among the stolen information were names, e-mail addresses, phone numbers, birth dates, passwords and security questions (Trautman & Ormerod, 2016). Controversy surrounded Yahoo's behaviour as it was found that Yahoo had claimed to not be aware of any security breaches in a 2016 SEC-filing, despite some of its employees having been aware of the breach since 2014, and the CEO being aware since July 2016 (Trautman & Ormerod, 2016). The breaches likely resulted from shortcomings in Yahoo's security systems, with the organisation faring a full year without a chief information security officer (CISO), denying resources to its CISO and resisting implementation of encryption systems (Trautman & Ormerod, 2016). While Yahoo claims that the cybersecurity breach was orchestrated by a foreign state-sponsored actor, the organisation was largely held accountable for the breach and would eventually have to pay 117.5 Million USD in settlements of class-action lawsuits (Picchi, 15-10-2019). Furthermore, the reputational damage sustained by the cybersecurity breach-crisis led to Yahoo selling its internet business to Verizon for 4.48 Billion USD instead of the originally agreed-upon 4.83 Billion USD (Stempel, 09-04-2019). Three months after the initial announcement Yahoo announced another breach stemming from 2013 which it initially claimed was unrelated, but was later proven to be part of the 2014 breach (Perlroth, 03-10-2017). The findings from this 2013 breach raised the total of breached accounts to 3 billion (Perlroth, 03-10-2017). In this paper the 2014 and 2013 breaches will be regarded as one incident due to the fact that they are linked, Yahoo employed response strategies by denying this link and Yahoo published only one extra statement regarding the 2013 breach thus indicating that crisis communication efforts were internally linked as well.

The second selected case is Adobe Cybersecurity breach of 2013. Shortly after the cybersecurity breach, Adobe announced that its systems had been infiltrated and the perpetrators had gained access to personal data, including credit card information, of around 2.9 million of the company's customers (Kocieniewski, 03-10-2013). The perpetrators reportedly used earlier leaked source-code of certain Adobe programs to gain entrance to Adobe's systems and stole even more source-code during the breach, thus increasing the risk of new breaches (Kocieniewski, 03-10-2013; KrebsonSecurity, 03-10-2013). Within a few weeks after the breach however, a database of the stolen account information turned up online with reportedly over 150 million breached records in it, suggesting that a far larger amount of data had been stolen (Welch, 07-11-2013). Adobe itself did not respond on these figures and stated that only 38 million accounts had been breached and that all impacted users had already been notified of the breach (Welch, 07-11-2013). Eventually, Adobe was held accountable for the breach as there had been multiple signs that its security practices were in a poor state previous to the breach (OAIC, 01-06-2015). Following this revelation, the organisation was repeatedly sued by different actors leading to Adobe eventually paying 1.18 Million USD in legal expenses and another 1 million USD in settlements (Huffman, 11-11-2016; Pauli, 17-08-2015).

The third and last selected case is the Marriott cybersecurity data-breach of 2018. On 08-09-2018 the international hotel-chain Marriott detected a cybersecurity breach following the identification of suspicious attempts to access internal reservation systems of Marriott's Starwood brands by a security tool (Fruhlinger, 12-02-2020). Through an internal investigation it was found that the security systems of the Starwood reservation systems had been compromised in 2014 leading to the perpetrators gaining access to the personal information of anyone who made a reservation following the breach at the affected hotels (Gressin, 04-12-2018; Fruhlinger, 12-02-2020). Various forms of personal information were reportedly stolen including credit card numbers, passport

numbers, travel information and personal details such as correspondence addresses and birthdates (Nohe, 22-03-2019; Fruhlinger, 12-02-2020). Decryption efforts and further investigations led to the revelation that an estimated 500 million guest records had been compromised and had their data collected (Fruhlinger, 12-02-2020; O'Flaherty, 11-03-2019). Marriott was largely held accountable for the stolen data due to multiple security issues (Nohe, 22-03-2019; Fruhlinger, 12-02-2020). Following the cybersecurity data breach Marriott was hit with multiple class-action lawsuits, was fined 120 Million USD under the GDPR and led to a further reported cost of 28 Million USD. (Fox, 01-03-2019; Nohe, 22-03-2019).

A more in-depth case description focussed on blame attribution and the crisis response efforts can be found in chapter IV.

3.3.2 Reasoning behind the case selection

As it is important to keep similar factors between cases in mind in order to isolate effects between variables, cases that show many similarities in their context have been selected. For instance, all these cybersecurity breaches relate to each other in the sense that they all happened within five years from each other, during the 2010's, therefore guaranteeing a more or less constant digital climate. Furthermore, all cases consist of major organisations with a global presence being targeted and suffering a data breach. Due to their global presence the cases involved vast amounts of stakeholders and subsequently vast amounts of compromised data. Finally, another set of important criteria in selecting these cases is that all the aspects of all cases are heavily documented both by primary and secondary authors due to their prominent nature.

3.3.3 Data selection

The data selection within this study is dependent on the scope with which the data is to be used. As this study focusses on the post-crisis response with crisis communication efforts as its main element, data is selected to fit this scope.

Universe of the data

The main goal in analysing the post-crisis response is determining which crisis-response-strategies were employed. This leads to a data-universe that includes all organisational crisis communication statements that followed cybersecurity crises. These statements on a universe-level can be found in a variety of forms. For example, Statements exist that are written and published on official media-outlets such as the websites or press channels of an organisation thus guaranteeing authorship of the organisation. But non-written statements are also part of the universe, these include verbal statements made in speeches or during press conferences by organisational representatives and even answers given to questions of the press. Finally, a modern form of statement, being the social media-statement, can also be deemed a part of the data-universe as this form of statement is often used to give timely and quick updates on ongoing situations (Graham, Avery & Park, 2015). Due to the broad nature of the data relevant to the universe of the topic of this research, the data needs to be narrowed down in order to provide a representative selection of data that guarantees the feasibility of analysis.

Data collection criteria and characteristics of the data

The first step in narrowing down the available data is to limit the data to statements made regarding the selected cases. This brings the available data down to statements following only the selected three instances of cybersecurity data-breaches. Secondly, in order for the crisis-response-strategies to be determined, only statements aimed at stakeholders such as customers, clients and shareholders are relevant since organisations do not need to employ communication-strategies in internal communications as attempts to re-frame the crisis within the organisation will not impact the external effects of the crisis. It is therefore that only external communication statements remain in the pool of selected data. Finally, in order to guarantee objectivity and continuity in analysis between the cases, only statements published on official organisational outlets and written by organisational

representatives are included in the content analysis. This excludes any verbal statements or statements published through secondary sources such as news articles. Statements published through social media channels by official organisational social media accounts would, in theory, be included in the analysis. However, investigation and indexation of the available statements have shown that in none of the cases social media outlets played a role in the crisis communication efforts, therefore they will be largely absent from the content analysis.

This narrowing of the data leads to a selection of ten official, written crisis statements authored by the relevant organisation or its representatives. These ten statements are unevenly spread over the cases with three statements adhering to the Yahoo case, three statements adhering to the Adobe case and four statements adhering to the Marriott case. Of these ten statements three statements take on the form of a 'FAQ-style' statement; consisting of questions and answers both formulated by the organisation that created the statement. The other seven statements are of a more conventional nature, by taking on the role of informational statements or development updates regarding their respective cybersecurity-crises.

By utilising only primary sources that are authored by the relevant organisations themselves, the process of an accurate identification of response-strategies is facilitated since any response-strategies found originate directly from the actor central in the analysis. This negates the risk of misrepresentation that might result from utilising secondary sources in order to identify crisis response strategies.

For the other parts of this research, such as the case description and the indication of the outcome, secondary sources will mainly be used. This is due to the fact that primary sources on these topics mainly do not exist. The case description and the case assessment following it will depend on a combination of news articles and academic papers that detail on the aspects of the different cases. For the indication of the outcome on the other hand, market statistics from Yahoo-finance, comment sections from CNET-articles and meta-articles from various specialist sites will be used.

IV. Case Descriptions & Assessment of case-types

4.1 Case descriptions

Yahoo

Aspects of the crisis

On 22-09-2016 Yahoo publicly disclosed on its own platform *Tumblr* that it had detected a data breach in its systems stemming from a 2014 attack by a 'state-sponsored actor' which it claimed affected around 500 million accounts (Trautman & Ormerod, 2016; Yahoo, 22-09-2016[a]). In this first announcement Yahoo provided information on the breach and instructions for users to protect themselves (Yahoo, 22-09-2016[a]). Later on the same day Yahoo posted a second, more elaborate statement in a FAQ-format which provided information through a question-answer format (Yahoo, 22-09-2016[b]). On December 14 2016 Yahoo published a final statement in FAQ-format that detailed on the 2013 data-breach. In this statement Yahoo takes effort to provide information on the data breach, provide users with instructions and keep the two breaches separate (Yahoo, 14-12-2016).

The data that was stolen from user accounts during the breach included names, email addresses, birth dates, encrypted passwords, security questions and telephone numbers (Trautman & Ormerod, 2016). According to Yahoo's Chief Information Security Officer at the time, Bob Lord, the vast majority of accessed passwords and security questions was encrypted with *'bcrypt'*, which is generally deemed a complex and safe encryption (Goodin, 22-09-2016).

Despite the relative security of the majority of the data however, there was still a portion of the stolen data that used the older, less secure MD5 encryption method which could be easily decrypted by the aggressors (Menn, Finkle & Volz, 18-12-2016). This dichotomy in encryption methods of the accessed data stemmed from the fact that Yahoo had been changing its encryption method only just before the data breach in 2014 (Menn et al., 18-12-2016). While this might have seemed like a case of unfortunate timing, Yahoo's conversion from MD5 to bcrypt was relatively late as software experts, including the Software Engineering Institute of Carnegie Mellon University issued a public warning against the use of MD5 years prior in 2008. MD5 was thus declared unfit for usage by security professionals long before Yahoo decided to abandon it (Menn, Finkle & Volz, 18-12-2016; Carnegie Mellon University, 31-12-2008). Adding to these vulnerabilities generated by the encryption protocols, requests for security updates and upgrades by Yahoo's cybersecurity team prior to 2014 were often denied both to save costs and because of the fear that added security inconveniences would turn away customers (Trautman & Ormerod, 2016; Menn et al., 18-12-2016). This behaviour continued into early 2014 as Yahoo hired a new CISO who left the company again in 2015 as his attempts and requests to implement security measures such as end-to-end encryption and intrusion-detection-mechanisms were repeatedly denied on the basis of hindering the indexation of data (Trautman & Ormerod, 2016; Perlroth & Goel, 29-09-2016). Furthermore, the company's then CEO Marissa Mayer rejected suggestions of implementing automatic resets for all users' passwords as she expected this would lead to a further shrink in the userbase (Trautman & Ormerod, 2016).

In terms of immediate handling of the breach when it became known, Yahoo appears to have been lacking as well. When an internal investigation report detailed on the nature of the 2014 breach it noted that the senior executives did not properly comprehend or investigate the information given to them by the security team (Trautman & Ormerod, 2016). Furthermore, Yahoo decided to not immediately publicly disclose the breach upon learning of the nature of the breach. While there had been found evidence of the breach by the security team in December 2014 and all aspects of the breach were internally known since July 2016, the company decided to wait with disclosing the breach until September of that year (Trautman & Ormerod, 2016). Only three months after the public announcement of the breach, when the company was already acquired by parent company Verizon, Yahoo disclosed the data breach stemming from 2013 and stated that it had compromised all its 3 billion accounts (Stempel & Finkle, 03-10-2017). Yahoo denied allegations that this 2013 data breach was related or even part of the earlier announced 2014 data breach (Perlroth, 03-10-2017). Despite

Yahoo's claim that the breaches were unrelated, investigators into the breaches found that the attackers behind both breaches were Russian and possibly linked to the Russian government, thus establishing a link between the two breaches (Perlroth, 03-10-2017).

Timeline of crisis response

Table 3: Timeline of Yahoo's crisis response

Date	2013	2014	December 2014	July 2016	22-09-2016	22-09-2016	14-12-2016
Event	Perpetrators gain access to Yahoo data for the first time	Perpetrators gain access to Yahoo data for the second time	Aspects of a data breach are known by some of the employees	Management is aware of all the aspects of the 2014 data breach	Statement I concerning the 2014 breach gets published	Statement II concerning the 2014 breach gets published	Statement III gets published, 2013 data breach is publicly disclosed

Adobe

Aspects of the crisis

On October 3 2013 the Chief Security Officer of Adobe, Brad Arkin, published an announcement on behalf of Adobe on the company's official website (Adobe, 03-10-2013). In this announcement Adobe mentioned it was investigating illegal access to the source code of multiple of its products (Adobe, 03-10-2013). Adobe stated that it got aware of this access due to combined efforts of outsiders and that it was currently not aware of any exploits threatening the products or its data (Adobe, 03-10-2013[a]). Later that day Brad Arkin, acting on behalf of Adobe, posted a second announcement in which the company stated that its investigation thus far found that data of 2.9 million customers was breached following the illegal access to their systems (Adobe, 03-10-2013[b]). This compromised data included names, encrypted credit and debit card numbers, expiration dates and further information related to orders made by customers (Adobe, 03-10-2013[b]). Sometime[4] after the incident Adobe released its final statement regarding the data breach. This statement took on the form of a FAQ-style report that addressed central questions regarding the incident (Adobe, 15-10-2018). In this final statement Adobe increased the number of affected customers to 3.1 million (Adobe, 15-10-2018).

In contrast to the claims of affected customers reported by Adobe, investigation into the data breach revealed that the actual number of breached accounts was closer to 38 million, thus being tenfold the size of the initially reported number (Whitney, 29-10-2013; Finkle, 29-10-2013). In various media statements Adobe announced that it acknowledged this new number of affected accounts, but never made an official written statement on the higher number of affected accounts or included it in edits of their original statements (Whitney, 29-10-2013; Adobe, 15-10-2018). The database of breached records eventually ended up online and reportedly included over 150 million breached records amounting to an uncompressed file size of around 10 GB (Welch, 07-11-2013; Ducklin, 04-11-2013). Adobe did not issue any statement regarding this newly reported number, either implicating that the 150 million number of records adhered to the already reported 38 million active accounts, that the unreported number of breached records included inactive or invalid accounts or that Adobe tried to avoid these allegations by not responding to them.

[4] The exact time of publication is unknown as the platform on which the statement was published only shows the moment the statement was updated for the last time. Though references to this statement dating from October 7th 2013 indicate that the final statement was published shortly after the initial statements. For this reference see: https://myemail.constantcontact.com/-Important-Adobe-Customer-Security-Alert.html?soid=1102584055726&aid=86bSUBKbKH0

Following the data breach incident, multiple reports surfaced detailing on Adobe's responsibility for the intensity and possible consequences of the breach. These reports claimed that Adobe made several mistakes in its security efforts that allowed for the data breach to carry severe consequences. These mistakes amounted to three main issues. Firstly, Adobe only encrypted its data, in contrast to the more commonly used 'hashing' method (Ducklin, 04-11-2013). The encryption used by Adobe led to all data being encrypted with a singular key, meaning that anyone who was able to get hold of the key or decrypt it got access to all encrypted data (Ducklin, 04-11-2013). Furthermore, the encryption method used was the ECB-mode, which is commonly regarded as an unsafe method as it leads to equal passwords, in terms of the symbols used, winding up looking similar in their encrypted forms (Ducklin, 04-11-2013; Cygilant, 25-11-2013; Goodin, 01-11-2013). These similarities between passwords make it easier for those accessing the database to rationally deduce the most common passwords such as 123456 or abc123, thus making it easier to crack the encryption key. The final critique against Adobe's security provisions noted that, while the passwords in the stolen dataset were encrypted, Adobe had not encrypted the password-hints adhering to these passwords (Ducklin, 04-11-2013; Cygilant, 25-11-2013). This once again made cracking the encryption key and passwords encoded with them fairly easy. In fact, the ease with which these passwords could be decrypted was demonstrated by Sophos security blogger Paul Ducklin who, over the course of an article, describes how to crack the encryption (Ducklin, 04-11-2013). The existence of these security flaws and the subsequent allegation of Adobe failing in its efforts to provide security for its users, were later investigated and acknowledged by the Office of the Australian Information Commissioner[5] (OAIC, 1-06-2015). Following these critiques Adobe did take the recommendations adhering to these critiques into account and made efforts to improve its security systems (OAIC, 1-06-2015). Nevertheless, due to the oversights of Adobe putting the personal data of millions of users at risk, the company was eventually fined 1 Million USD in a multistate lawsuit (Keane, 16-11-2016; KrebsonSecurity, 17-11-2016)

Timeline of crisis response

Table 4: Timeline of Adobe's crisis response

Date	**03-10-2013**	**03-10-2013**	**Somewhere between 03-10-2013 & 07-10-2013[6]**	**29-10-2013**	**04-11-2013**
Event	Adobe publishes statement I, discloses that it is aware of illegal access to its source code	Adobe publishes statement II, Discloses data breach	Adobe publishes statement III.	External investigation puts estimation of affected accounts on 38 Million, Adobe informally acknowledges this number.	External claims surface that the stolen dataset included information on 150 Million accounts, Adobe does not respond to these claims

Marriott

Aspects of the crisis

On November 30th 2018 The international hotel chain Marriott posted an announcement on its official website stating that the organisation had taken measures to investigate and address a security incident involving the database of its Starwood-line of hotels (Marriott, 30-11-2018[a]). In the announcement Marriott stated that it had been alerted on September 8th by an internal security tool that there had been an attempt to access the Starwood reservation database (Marriott, 30-11-2018[a]). On the basis of this information, the company stated that it started an investigation into the issue which concluded on

[5] From here on abbreviated as OAIC, the official abbreviation for the institution
[6] Exact time of publication unknown, see footnote 4

November 19th that there had been unauthorized access to the database from 2014 onward during which access was gained to guest information relating to guests of the Starwood-hotels (Marriott, 30-11-2018[a]). While Marriott stated in its first announcement that it was still busy indexing the accessed information, the company stated that it estimated that the accessed dataset contained information on approximately 500 million guests with an estimated 327 million guests having extensive personal information stolen (Marriott, 30-11-2018[a]). This extensive information may have included, according to Marriott, names, date of birth, gender, email-addresses, account information, arrival and departure information, reservation dates communication preferences and for some people even payment card numbers and expiration dates (Marriott, 30-11-2018). Marriott did claim that the data relating to payment cards had been encrypted with the AES-128 method, but that the company was unsure whether the components needed to decrypt the data were also taken (Marriott, 30-11-2018[a]).

On the same day, shortly after the first statement, Marriott published a second statement on its official news website. This second statement mainly consisted of the same content as the first statement, but added information regarding organised support for affected guests including a dedicated website and call-centre[7] for questions, and a year of free identity-monitoring services for affected guests of selected countries (Marriott, 30-11-2018[b]).

On January 4th 2019 Marriott published its third update regarding the breach (Marriott, 04-01-2019). This statement was a mixed statement, with the beginning being a status update and the information following it being stated in FAQ-format (Marriott, 04-01-2020). This third statement provided numerous updates on several aspects of the crisis, the statement sought to diminish several previously stated numbers. Firstly it claimed that the actual number of accessed guest records was now estimated at 383 Million instead of the previous estimation of 500 Million. Furthermore, Marriott stated that passport- and payment card numbers were only involved in only a relatively small fraction of the accessed records (Marriott, 04-01-2020). On the other hand, Marriott did mention some new issues as they acknowledged that they had found around 5.25 million passport numbers and around 2000 credit card numbers that had been unencrypted at the time of the breach, thus allowing the perpetrators direct access to them (Marriott, 04-01-2020). Finally, Marriott closed the statement by stating that it had discontinued the Starwood Reservations Database, instead merging it into the global Marriott database. On July 9th 2019 Marriott published its last update on the data breach. In this update Marriott only focussed on its dealings with the UK Information Commissioner's Office (ICO) which had at the time decided to issue a fine of 99.200.396 GBP against Marriott (Marriott, 09-07-2019). Marriott stated that it regretted this decision and that it would contest this decision. (Marriott, 09-07-2019). Marriott closed the statement by stating that it regretted the incident (Marriott, 09-07-2019).

The first thing that should be mentioned is the grave error of having unencrypted passport- and payment card numbers stored in a database. In a case like Marriott's where this data is accessed it has the potential to carry disastrous results for affected customers, such as identity theft or attempts to make unauthorized transactions. Furthermore, security professionals noted that Marriott made another mistake in its efforts to secure data as it stored the information needed to decrypt the encrypted information in the same system, allowing it to get stolen at the same time as the encrypted data (Ashford, 30-11-2018). Additionally, as the breach reportedly originated in 2014, it predated Marriott's acquisition of the Starwood branch, this means that Marriott failed to detect the breach during its due diligence process and indicates a lack in the company's detection capabilities (Ashford, 30-11-2018; ICO, 09-07-2019). Apart from the technical details, multiple issues with Marriott's and Starwood's security structures surfaced after the breach. Ex-employees of Starwood for instance told news outlets that they had been aware that the Starwood database was a security hazard as they reportedly found it increasingly hard to secure said database. (McMillan, 02-12-2018; Fruhlinger, 12-02-2020). It also surfaced that prior to its acquisition, Starwood had suffered another data breach, namely in 2015 (McMillan, 02-12-2018; Fruhlinger, 12-02-2020). As the breach that surfaced in 2018

[7] No longer accessible at the time of writing

was already present during the 2015 breach, investigations into the 2015 breach by both Marriott and Starwood should, at the time, have uncovered the second breach stemming from 2014, which would have saved Marriott the consequences of the 2018 discovery of the breach (McMillan, 02-12-2018).

Timeline of crisis response

Table 5: Timeline of Marriott's crisis response

Date	2014	2015	2016	08-09-2018	19-11-2018	30-11-2018	30-11-2018	04-01-2019	09-07-2019
Event	Perpetrators gain access to Starwood database for the first time	Other perpetrators gain access to Starwood systems, 2014 breach remains undetected	Marriott acquires Starwood	Marriott gets alerted of signs of 2014 data breach, investigation is launched	Marriott finds evidence regarding 2014 data breach	Statement I is published, disclosing 2014 data breach	Statement II is published	Statement III is published	Statement IV is published

4.2 Assessment of the cases

In order to determine which crisis-response-strategies would have been theoretically adequate in the different cases based on SCCT, it is important to first determine under which crisis cluster the cases can be categorized. In order to determine this, the cases need to be assessed in terms of their aspects. As the theoretical background and the previous literature review have demonstrated, there is no clear consensus as to within which crisis cluster cybersecurity data breaches fall. Therefore, as has been explained earlier, Turner's theory on failure of foresight (1976) will be used to assess the cases in order to determine whether failure of foresight was present in any of the cases and thus determine the preventability and blame attribution expectations of each crisis. If the preventability and subsequently the expected blame attribution within each case are known, the crisis cluster under which the cases fall can be determined which in turn allows for an identification of the theoretically most adequate response-strategies in each of the cases based on SCCT's recommendations (See Table 2). Based on the knowledge of what would have theoretically been the most adequate response-strategies, expectations can be formulated regarding the choice of response-strategies in each of the cases and the expected effectivity of the chosen response-strategies.

4.2.1 Cluster assessment

Yahoo

From its case description it has become apparent that there were multiple mistakes made by Yahoo that have contributed to the scale and the severity of its data breach. The first error that Yahoo made was to only begin to change its encryption method five years after public announcements had surfaced that the used encryption method was unsafe to use. This disregard of a public announcement made by experts in the field demonstrates the presence of a clear failure of foresight, namely an instance of *Organisational exclusivity* in which an organisation ignores, or fails to adequately act upon, alerts raised by non-members of the organisation (Turner, 1976).

The second error Yahoo made, leading up to the crisis was ignoring the advice and requests of its cybersecurity team in order to focus on saving costs and retaining its customer base through guaranteeing simplicity. This error indicates a failure of foresight, in fact, it may to some extent be considered as an indication of two separate failures of foresight. The fact that Yahoo was so focussed on saving costs that it ignored its cybersecurity and created a blind spot for this area clearly indicates the presence of *Rigidities in perception and belief in organisational setting*. This is due to the fact that the predominant set of beliefs present in Yahoo's decision-making process, a belief that cost-saving should take precedent over security, made the company ignore cybersecurity (Turner, 1976). Additionally, this error by Yahoo indicates the presence of *The decoy problem* as Yahoo saw its already dwindling userbase as the main problem it was facing, thus neglecting its present security flaws which in turn enabled the data breach (Turner, 1976).

Finally, the fact that Yahoo's senior executives did not fully comprehend, and thus inadequately investigated, the information provided to them by the security team indicates the presence of *Information difficulties*. This can be concluded by the fact that the security team understood the implications of the presence of signs of a data breach but failed to adequately communicate the danger stemming from these signs to the senior executives. This led to the senior executives being late to investigate the signs and in turn allowed the data breach to remain unnoticed for several years.

Since the aspects of the Yahoo case indicate the presence of four separate instances of failure of foresight, one might conclude that the crisis could have been prevented if these failures of foresight would not have been present. While it is hard to argue that nothing would have happened, had all these errors not been present, any instance of a data breach would certainly not have been as extensive and the data breach would most likely have been noticed in a far earlier stage. Since these errors enabled the current form of the crisis, Yahoo carries a substantial amount of responsibility for the current form of the crisis. Since these errors are publicly disclosed they are likely to have attributed to a higher amount of blame attribution towards Yahoo regarding the breach.

Due to all these factors, it becomes clear that the Yahoo data breach falls within the preventable-cluster of crises as it arguably carries substantial to high blame attribution and the crisis in its actual state could have been prevented.

Adobe

In the Adobe case less, but equally substantial, failures of foresight are present. Firstly the encryption issues should be mentioned. While Adobe did take efforts to encrypt its data, it used relatively unsafe encrypting methods that used the same encryption key for all data. This oversight indicates the presence of *Rigidities in perception and belief in organisational settings* as Adobe did go through the effort to encrypt its user data but had a blind-spot regarding the weaknesses in its encryption, instead believing that the data was protected well enough. This is demonstrated by the fact that Adobe claimed in its crisis statement that it did not believe the perpetrators accessed decrypted data (Adobe, 03-10-2013[b]).

Adobe's initial underestimation of the extent of the data breach and subsequent underestimation of the number of affected accounts indicate the presence of another failure of foresight. These underestimations are instances of *Minimizing emergent danger* as Adobe initially believed and stated that the access to its source code did not directly affect its users and when the company found out users were affected it severely underestimated the number of affected accounts.

Finally, by using weak encryption methods and not encrypting security questions adhering to the weakly encrypted passwords, Adobe breached existing rules and regulations governing data protection in the countries in which the company is active such as the Australian *'Privacy Act 1988'* (AOIC, 01-06-2015). The fact that Adobe's security systems failed to comply with these regulations despite the guidelines inherent to these regulations being openly accessible and applicable to Adobe, can be regarded as a *Failure to comply with existing regulations* and thus indicates another failure of foresight.

Through this assessment it becomes clear that three different forms of failure of foresight can be identified in the Adobe case. Whilst some of these failures of foresight such as the *failure to comply with existing regulations* and *Rigidities in perception and organisational beliefs* directly contributed to the severity of the data breach, the instance of *Minimizing emergent danger* impacted the crisis communication efforts of the organisation as the incorrectness of the statements likely affected the trustworthiness and reliability of the company's communication efforts. Because of the presence of these three failures of foresight it is reasonable to state that the crisis, as it stands in its current form, could have been prevented as the severity of the data breach could have been limited and the trustworthiness of the organisation's communication efforts could have been upheld had Adobe not underestimated the situation. This in turn leads to Adobe being substantially responsible

for the current state of the crisis and thus most likely being attributed a high amount of blame for the breach, making this breach an instance of a preventable-cluster crisis.

Marriott

In the Marriott case, the most important instance of failure of foresight is found in the fact that Marriott kept highly sensitive personal information on its customers in an unencrypted state and the company kept its encryption key on the same server as encrypted data. Not only can these be considered risky moves by Marriott, but they also go against regulations set by the GDPR under which Marriott falls, thus explaining ICO's decision to fine the company (ICO, 09-07-2019). The fact that the rules concerning data protection are regulated by the GDPR and Marriott nevertheless failed to comply with these rules indicates the presence of a failure of foresight in the form of a *Failure to comply with existing regulations*.

Additionally, the fact that the data breach discovered in 2018 had been present since 2014 and managed to go unnoticed despite investigations into another security breach and a due diligence process executed by Marriott indicates the presence of *Rigidities in perception and belief in organisational setting*. This is due to the fact that the actions of both Starwood and later Marriott were apparently conducted in such a way that it allowed the 2014-2018 breach to become a blind-spot and remain unnoticed.

Finally, the fact that it had been known by Starwood employees that the reservation database was hard to keep secure, but this information was only made known after the employees had left the organisation indicates the existence of *Information difficulties*, allowing the database to remain a security hazard.

The failures of foresight present in the Marriott case allowed the data breach to; include unprotected data, the protected data to be easily decryptable due to an unprotected decryption key, and the data breach to go unnoticed since 2014 allowing the perpetrators sustained access to the database. Therefore the failures of foresight directly contributed to the severity and extensiveness of the data breach which in turn impacts the amount of blame attributed to Marriott. As the data breach in its current form could have been prevented if failures of foresight would not have been present, it must be concluded that the Marriott data breach, like the Yahoo and Adobe breaches before it, falls under the preventable-cluster of crises.

4.2.2. Assessment of theoretically adequate response strategies

As all three cases fall within the preventable-cluster of crises, it means that all three cases are instances in which there is a high amount of organisational responsibility for the crisis and subsequently a high amount of expected blame attribution (Coombs, 2007). In the cases of Yahoo and Marriott, the expected blame attribution is heightened even more as both cases have a prior history of similar incidents. In the Marriott case this is demonstrated in the fact that the compromised database had previously dealt with a security breach in 2015, in the Yahoo case this is apparent from the fact that after the disclosure of the 2014 data breach, another related data breach stemming from 2013 was discovered. However, since all cases were already considered to be falling within the preventable-cluster of crises these expectations of additional blame attribution do not change the selection of strategies that theoretically should have been used. Additionally, due to their status as corporate giants in their respective fields, all three companies can be deemed to have had had a prior reputation of being trustworthy. When the assessment of organisational responsibility concerning the three cases is applied to SCCT's recommendations, as shown in Table 2 of chapter II it becomes clear which response strategies would theoretically have been adequate in the three cases. According to these expectations the organisations in all three the cases should have opted for a *Base response* in combination with *Rebuild-strategies* in the form of *Apologies* and *Compensation*, which they could optionally supplement with *Bolstering*-strategies to bolster their reputation and the *Denial* or *Attack the accuser*-strategies in order to combat potential false rumours (See Table 2; Coombs & Holladay, 2011). This is because of the fact that all three cases deal a high amount of organisational

responsibility due to the present failure of foresight which warrants application of SCCT recommendations 1,2,7 & 10 (See Table 2; Coombs & Holladay, 2011). For the sake of overview the following table will summarize the theoretically adequate response strategies:

Table 6: Theoretically adequate response strategies following SCCT's recommendations

Case	Organisational responsibility	Intensifying factors present	Adequate response strategies following SCCT (See Table 2)
Yahoo	High, due to failures of foresight	Prior similar crisis	Necessary - Base response - Rebuild strategies (Apology & Compensation) Optional - Bolstering (in order to bolster reputation) - Deny and Attack the accuser strategies (Only in order to combat false rumours)
Adobe	High, due to failures of foresight	-	Necessary - Base response - Rebuild strategies (Apology & Compensation) Optional - Bolstering (in order to bolster reputation) - Deny and Attack the accuser strategies (Only in order to combat false rumours)
Marriott	High, due to failures of foresight	Prior similar crisis	Necessary - Base response - Rebuild strategies (Apology & Compensation) Optional - Bolstering (in order to bolster reputation) - Deny and Attack the accuser strategies (Only in order to combat false rumours)

V. Analysis

5.1 Results of Strategy-analysis

Yahoo

Following the 2013-2014 data breach Yahoo published three statements that contained different response-strategies. The response-strategies found in each of these statements will be discussed in the following paragraphs.

Statement 1

Yahoo's first statement regarding the data breach was published on 22-09-2016 and written by Chief Information Officer Bob Lord, on behalf of Yahoo (Yahoo, 22-09-2016[a]). The Statement, officially titled *'An important message about Yahoo user security''* started by providing information disclosing the 2014 data breach (Yahoo, 22-09-2016[a]). While Yahoo begins the statement by providing *Crisis information* and thus employing a *Base response*, the company is quick to target a third party as responsible for the crisis, thus engaging a *Scapegoat*-strategy.

Without providing any evidence, Yahoo stated it believes that information was stolen by a state-sponsored actor:

''A recent investigation by Yahoo has confirmed that a copy of certain user account information was stolen from the company's network in late 2014 by what it believes is a state-sponsored actor'' (Yahoo, 22-09-2016[a]).

As Yahoo provides no evidence supporting this statement or clear indication of why the company believes a state-sponsored actor is behind the breach, this statement has to be deemed an instance of the *Scapegoat*-strategy. Through targeting a specific form of actor, namely a state-sponsored one, Yahoo tries to deny blame. By claiming the actor was state-sponsored Yahoo most probably aimed to win a certain amount of sympathy as one might not reasonably a corporation to successfully hold of targeted attacks with the resources of a nation behind them.

After indicating a state-sponsored actor as likely perpetrator, Yahoo goes on to describe the characteristics of the data in an instance of *Crisis information:*

'' The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers.'' (Yahoo, 22-09-2016[a])

The statement then goes on to state that Yahoo is engaging *Corrective Action* by working with law enforcement and taking protective action for users:

Yahoo is working closely with law enforcement on this matter. We are taking action to protect our users:

• We are notifying potentially affected users. The content of the email Yahoo is sending to those users will be available at https://yahoo.com/security-notice-content beginning at 11:30 am (PDT). [..]

• We invalidated unencrypted security questions and answers so they cannot be used to access an account. [..]

While the rest of the statement mainly consists of further *Crisis information* in the form of recommendations for users and general information regarding the crisis, there are a number of interesting statements with which Yahoo concludes its message.

Firstly Yahoo tries to engage an *Excuse*-strategy by claiming that crises such as this data breach are commonplace and the result of constant targeting by adversaries:

''An increasingly connected world has come with increasingly sophisticated threats. Industry, government and users are constantly in the crosshairs of adversaries.'' (Yahoo, 22-09-2016[a])

After this Yahoo makes a promise of continued *Corrective action*:

''Through strategic proactive detection initiatives and active response to unauthorized access of accounts, Yahoo will continue to strive to stay ahead of these ever-evolving online threats [..]'' (Yahoo, 22-09-2016[a])

Finally. the statement is concluded on a disclaimer specifying the uncertainty of the information, thus once again providing *Crisis information*:

''The final conclusions of the investigation may differ from the findings to date due to various factors including, but not limited to, the discovery of new or additional information and other developments that may arise during the course of the investigation.'' (Yahoo, 22-09-2016 [a]).

In total, four strategies, falling within three different categories, can be found in this first statement. These strategies are *Crisis information* and *Corrective Action* falling under the *Base response*, *Scapegoat* falling under *Deny-strategies* and *Excuse* falling under *Diminish-Strategies*.

Statement 2

Yahoo's second statement, which was published the same day, was officially called ''*Yahoo Security Notice September 22, 2016''* and took on a FAQ-form repeating much of the same information (Yahoo, 22-09-2016[b]). This second statement only marginally differs from the first statement as it directly copied most of its statements regarding *Crisis information* and *Corrective action* only adding some minor recommendations for users and information regarding these recommendations and the encryption of the stolen data (Yahoo, 22-09-2016[b]).

The real differences between Yahoo's first and second statements lie in the fact that Yahoo increases its emphasis on blaming a state-sponsored actor, as this actor gets indicated three times in total, all without any evidence supplementing these claims, and in the fact that Yahoo drops its initial *Excuse*-strategy by not including the *Excuse*-statement from its first response-statement and employs an instance of *Denial* (Yahoo, 22-09-2016[b]).

This instance of *Denial* is found in the fact that Yahoo denies that any accounts of its Tumblr platform were affected by the data breach:

''The systems from which the data was stolen contained no Tumblr user data at the time of the theft.'' (Yahoo, 22-09-2016[b])

While this *Denial* does not aim to deny the existence of a crisis altogether, it does aim to limit the extent of the crisis by excluding a large userbase from the pool of affected accounts.

The total of employed strategies in this document amount to four different strategies divided over two categories, being: *Crisis information* and *Corrective action* adhering to the *Base response*-category and *Scapegoat* and *Denial* adhering to the *Deny*-category.

Statement 3

The third response-statement that Yahoo published was published on 14-12-2016 and was different from the other two statements in the sense that it announced the existence of the 2013 breach (Yahoo, 14-12-2016). The statement, officially called ''*Yahoo Security Notice December 14, 2016''* again primarily engaged a *Base response* in the form of *Crisis information* and *Corrective action* (Yahoo, 14-12-2016).

In terms of *Crisis information* the statement largely detailed about the detection, extensiveness and nature of the data breach (Yahoo, 14-12-2016). Yahoo stated that outside forensic experts had found Yahoo user data, leading Yahoo to believe over a billion user accounts were compromised:

''Based on further analysis of this data by the forensic experts, we believe an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts [..]'' (Yahoo, 14-12-2016)

Furthermore, Yahoo stated for the first time that they found that the intruders had managed to forge cookies, possibly allowing them to access accounts without needing to enter their passwords:

''[..] our outside forensic experts have been investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password.'' (Yahoo, 14-12-2016)

Other than this announcement of the existence of the 2013 breach and the information regarding the forging of cookies, *Crisis information* provided by Yahoo mainly repeated information and recommendations already stated in earlier communications (Yahoo, 14-12-2016).

The *Corrective action* that is described by Yahoo in this last statement only adds that users affected by the cookie forging are being notified by the external experts and the forged cookies were invalidated:

''The company is notifying the affected account holders, and has invalidated the forged cookies.'' (Yahoo, 14-12-2016)

Apart from this addition, the *Corrective action* described in this last response-statement is copied fully from the earlier statements and only indicates that the newly indicated affected users will be subject to the same corrective action that was employed on affected users found in an earlier stage, meaning their security questions will be invalidated and they will be required to change their passwords.

Similar to the last two statements, Yahoo continues its *Scapegoat*-strategy in this third statement by claiming that it has linked the same state-sponsored actor indicated in earlier responses to this breach as well:

''We have connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft we disclosed on September 22, 2016.'' (Yahoo, 14-12-2016).

While Yahoo claims it has managed to connect the activity to the state-sponsored actor, the company once again does not provide any proof or indication supporting this statement.

What is interesting is that Yahoo, whilst claiming that it found the same perpetrator behind both the 2013 and 2014 breaches, does make effort to deny rumours that both breaches are part of the same, larger breach, thus engaging in a new instance of *Denial*:

''We believe that the August 2013 incident is likely distinct from the incident we disclosed on September 22, 2016.'' (Yahoo, 14-12-2016).

In addition to this Yahoo repeats its claim that Tumblr-accounts remain unaffected:

''The systems from which the data was stolen in August 2013 contained no Tumblr user data at the time of the theft. Additionally, Yahoo has no indication that the forged cookies were used to access Tumblr accounts.'' (Yahoo, 14-12-2016).

Yahoo's last statement included a total of four strategies spread over two categories being; *Crisis information* and *Corrective action* Adhering to the *Base-response*-category and *Denial* and *Scapegoat* adhering to the *Deny*-category.

Overall use of strategies

Through all three its statements Yahoo has employed five distinct strategies, two of which, *Crisis information* and *Corrective action* count as a *Base response*. The other three consisted of two *Deny*-category strategies, namely *Denial* and *Scapegoat* and one *Diminish*-category strategy being *Excuse*.

In order to provide an overview, the following table presents all used strategies in each statement and the amount of statements containing the strategy:

Table 7: Presence of crisis response-strategies in Yahoo-case

Strategies by Category / Statement	1	2	3	***Overall***
Base response				
Crisis Information	✓	✓	✓	***✓(3/3)***
Display of Empathy (care response)	×	×	×	***×***
Corrective Action (care response)	✓	✓	✓	***✓(3/3)***
Deny				
Attack the Accuser	×	×	×	
Denial	×	✓	✓	***✓(2/3)***
Scapegoat	✓	✓	✓	***✓(3/3)***
Diminish				
Excuse	✓	×	×	***✓(1/3)***
Justification	×	×	×	***×***
Rebuild				
Compensation	×	×	×	***×***
Apology	×	×	×	***×***
Bolstering				
Reminder	×	×	×	***×***
Ingratiation	×	×	×	***×***
Victimage	×	×	×	***×***

Adobe

As Adobe decided to publish its crisis communication soon after the initial discovery of cybersecurity breaches in its systems, its statements gradually evolved to contain more information and aspects of the crisis. In total Adobe published three official crisis response-statements with each of them containing a number of different strategies. The strategies that were found during the content analysis will be discussed in the following paragraphs.

Statement 1

In its first statement, published by CSO Brad Arkin on behalf of the company on 10-03-2013, Adobe began its statement with *Crisis information* by announcing that it was investigating an instance of illegal access to the source code of some of its programs:

''Adobe is investigating the illegal access of source code for Adobe Acrobat, ColdFusion, ColdFusion Builder and other Adobe products by an unauthorized third party.'' (Adobe, 10-03-2013[a]).

It continued the *Crisis information* by recommending that users, in order to guarantee their security in relation to the source code access, only use updated versions of its software and by providing them links to web pages detailing about the security systems of its products:

'' [..] we recommend customers run only supported versions of the software, apply all available security updates, and follow the advice in the Acrobat Enterprise Toolkit and the ColdFusion Lockdown Guide. These steps are intended to help mitigate attacks [..]'' (Adobe, 10-03-2013[a]).

Despite these recommendations, Adobe *Denied* being aware of the existence of a crisis or any specific increase of risk targeting its customers:

''Based on our findings to date, we are not aware of any specific increased risk to customers as a result of this incident.''

''We are not aware of any zero-day exploits targeting any Adobe products.''

(Adobe, 03-10-2013[a])

Additionally, Adobe went out of its way to thank the efforts of certain stakeholders in handling the incident, thus engaging in a light form of *Ingratiation*:

Adobe thanks Brian Krebs, of KrebsOnSecurity.com, and Alex Holden, chief information security officer, Hold Security LLC. holdsecurity.com for their help in our response to this incident. (Adobe, 03-10-2013[a])

In total, indicators of three strategies falling under three different categories can be found in this first statement. These are: *Crisis information* being a part of the *Base response*, *Denial* falling under the *Deny*-category and *Ingratiation* falling under the *Bolstering*-category.

Statement 2

Adobe's second statement, also published by Brad Arkin, was published on the same day. In this statement Adobe acknowledged that there had been attacks on their system following the illegal access to the source code which led to a data-breach (Adobe, 03-10-2013[b]).

Adobe starts of the statement by applying an *Excuse*-strategy:

''Cyber attacks are one of the unfortunate realities of doing business today. Given the profile and widespread use of many of our products, Adobe has attracted increasing attention from cyber attackers.'' (Adobe, 10-03-2013[b]).

With this statement, Adobe clearly ties to diminish its blame attribution by stating that cyber-attacks are normal to the current age and that the targeting of Adobe was in a certain way unpreventable due to the widespread use of its products.

In terms of *Base response* adobe uses this second response-statement to provide a lot of *Crisis information* regarding the aspects of the crisis and the number of accounts affected:

''[..] the attackers accessed Adobe customer IDs and encrypted passwords on our systems. We also believe the attackers removed from our systems certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders.'' (Adobe, 10-03-2013[b])

In addition to this *Crisis information* Adobe detailed about *Corrective action* including:

''*[…] resetting relevant customer passwords […]''* and *''[…] notifying customers whose credit or debit card information we believe to be involved in the incident.''* (Adobe, 10-03-2013[b]).

Despite acknowledging the large number of affected accounts, Adobe maintained its *Denial* of the existence of a specific increase in risk to customers as a result of access to the source code:

''Based on our findings to date, we are not aware of any specific increased risk to customers as a result of this incident.'' (Adobe, 10-03-2013[b]).

Furthermore, Adobe again employed *Denial* in stating that:

''[…] We [Adobe] do not believe the attackers removed decrypted credit or debit card numbers from our systems.'' (Adobe, 10-03-2013[b]).

Adobe also decided to employ both *Rebuild*-strategies in this second statement as the company showed regret: *''We deeply regret that this incident occurred.''* and offered some form of compensation in order for certain customers to better deal with the consequences of the crisis: ''*Adobe is also offering customers, whose credit or debit card information was involved, the option of*

enrolling in a one-year complimentary credit monitoring membership where available.'' (Adobe, 10-03-2013[b])

Finally, in addition to the primary strategies that Adobe employed in the statement, the company also tried to employ *Bolstering*-strategies where possible. It did this in the form of *Reminders* by emphasizing its positive qualities and by positively emphasizing the extent of its efforts:

''We value the trust of our customers.'' And *''We're working **diligently** internally [..]''* (Adobe, 10-03-2013).

In total, over the course of this second statement, Adobe employed seven response-strategies falling within all five categories. These strategies are *Crisis information* and *Corrective action* forming the *Base response*, *Denial* falling under the *Deny*-category, *Excuse* falling within the *Diminish*-category, *Compensation* and *Apology* falling within the *Rebuild*-category and finally *Reminder* falling within the *Bolstering*-category.

Statement 3

As in the Yahoo case, Adobe's third statement predominantly consisted of earlier published statements in a more comprehensive FAQ-style format (Adobe, 15-10-2018).

In terms of *Crisis information*, while Adobe mainly repeated earlier statements regarding information on the situation, they did add some new information and recommendations such as increasing number of affected customers to 3.1 Million, providing instructions on changing passwords and providing information on the notification process:

'' We also believe the attackers removed from our systems certain information relating to 3.1 million Adobe customers'' (Adobe, 15-10-2018).

In terms of *Corrective action* Adobe again mostly repeated prior instances of *Corrective action* and added that it took the liberty to automatically reset the passwords of users it found to be affected and the company eliminated invalid records of accounts no longer in use:

''In the process of verifying and notifying customers whose Adobe IDs and passwords we believed to be involved, we eliminated invalid records.''

''If your Adobe ID and current password were in the database that was taken, we have already reset your password.''

(Adobe, 15-10-2018)

Adobe also decided to continue its *Excuse*- and *Denial*- strategies by repeating the exact same claims and sentences from the second response-statement in this third and last response-statement. Adobe did add a disclaimer *Denying* that they had reported a specific number of affected accounts in an earlier stage:

''We did not reference a specific number of impacted Adobe ID accounts. We communicated the information we could validate at the time of the announcement.'' (Adobe, 15-10-2018).

Furthermore, Adobe continued its *Bolstering* in this last statement, adding and repeating subtle instances of the *Reminder*-strategy:

***''We value the trust of our customers.** We are working **aggressively** to prevent these types of events from occurring in the future. We are working **diligently** internally, as well as with external partners and law enforcement, to address the incident.''* (Adobe, 15-10-2018).

Finally, Adobe did add a new response-strategy of the *Deny*-category to its last statement. As Adobe noticed that multiple websites appeared claiming to have access to the stolen Adobe-data and offering users to validate whether their data was accessed or not, the company decided to engage an *Attack the accuser*-strategy in order to discredit these sites:

''These sites are not reliable sources of information on whether a particular user ID is at risk. [..] Adobe's authentication system of record, which cryptographically hashes and salts customer passwords, is not the source of the database these sites are using.'' (Adobe, 15-10-2018).

In total Adobe continued most of its earlier strategies in this statement including *Crisis information, Corrective action, Denial* and *Reminder* but decided to leave out *Compensation* and *Apology*, adding an *Attack the accuser* strategy in their place in order to combat false information and rumours.

Overall

Overall Adobe employed nine distinct response-strategies falling within all five categories.

Adobe met the *Base response* requirements by providing *Crisis information* and employing *Corrective action.* It utilised *Denial* and *Attack the accuser* from the *Deny*-category in order to deny certain aspects of the crisis and limit the framed extent of the crisis. It employed the *Diminish*-category in order to *Excuse* the existence of the crisis. It engaged *Apology*- and *Compensation*-strategies from the *Rebuild*-category to satisfy its stakeholders and rebuild its reputation. And finally, Adobe engaged in *Bolstering* in the form of a light *Ingratiation* and *Reminders* to emphasize their positive qualities and efforts.

For the sake of overview the employed strategies per statement are displayed in the following table:

Table 8: Presence of crisis response-strategies in Adobe-case

Strategies by Category / Statement	1	2	3	***Overall***
Base response				
Crisis Information	✓	✓	✓	***✓(3/3)***
Display of Empathy (care response)	×	×	×	***×***
Corrective Action (care response)	×	✓	✓	***✓(3/3)***
Deny				
Attack the Accuser	×	×	✓	***✓(1/3)***
Denial	✓	✓	✓	***✓(3/3)***
Scapegoat	×	×	×	***×***
Diminish				
Excuse	×	✓	✓	***✓(2/3)***
Justification	×	×	×	***×***
Rebuild				
Compensation	×	✓	×	***✓(1/3)***
Apology	×	✓	×	***✓(1/3)***
Bolstering				
Reminder	×	✓	✓	***✓(2/3)***
Ingratiation	✓	×	×	***✓(1/3)***
Victimage	×	×	×	***×***

Marriott

Statement 1

Marriott published its first announcement regarding the data-breach on 30-11-2018 (Marriott, 30-11-2018[a]). With this announcement, Marriott primarily aimed to inform its customers about the data breach and to let them know that Marriott is taking *Corrective action*.

The statement begins with an immediate instance of *Bolstering* in the form of a *Reminder* as Marriott reminds its customers that:

''Marriott values our guests and understands the importance of protecting personal information.'' (Marriott, 30-11-2018[a]).

After this initial instance of *Bolstering* Marriott repeatedly tries to subtly employ the same strategy by describing all its actions with positive adjectives in order to emphasize the qualities of their efforts:

*''From the start, we moved **quickly** to contain the incident and conduct a **thorough** investigation with the assistance of **leading** security experts.''* (Marriott, 30-11-2018[a]).

In this first statement Marriott also makes an effort to issue an *Apology* in the form of expressing regret:

''Marriott deeply regrets this incident happened.'' (Marriott, 30-11-2018[a]).

The rest of the statement mainly consists of *Base response* as Marriott provides *Crisis information* regarding aspects of the crisis such as the number of affected accounts and compromised data and announces instances of *Corrective action* it has taken:

''For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, [etc.]''

''We are supporting the efforts of law enforcement and working with leading security experts to improve. Marriott is also devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network.''

(Marriott, 30-11-2018[a]).

In conclusion, this first, short, statement by Marriott following the data breach included four strategies, two of which; *Corrective action* and *Crisis information* formed the *Base response*. The other employed strategies were *Apology,* falling under the *Rebuild*-category and *Reminder,* falling under the *Bolstering*-category

Statement 2

On the same day as the first announcement of the data breach, Marriott published its second official response-statement. This statement was based on the first statement and incorporated most of the content from the first announcement directly. The new content that could be found in this second statement mostly expanded upon response-strategies and claims from the first announcement (Marriott, 30-11-2018[b]).

In terms of *Crisis information* Marriott added some new information to the statement whilst repeating old information. This new information consisted of information about data-surveillance recommendations and specific details of a newly established dedicated call-centre for affected customers (Marriott, 30-11-2018[b]). This immediately ties in with *Corrective action* as Marriott, in addition to repeating its earlier statements on *Corrective* action, announced that it has established a dedicated call-centre and a website to support affected customers and that it was working to decouple the Starwood reservation systems in order to better secure its network:

"We have established a dedicated website (info.starwoodhotels.com) and call center to answer questions you may have about this incident. "

''Finally, we are devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network''

(Marriott, 30-11-2018[b]).

In terms of their *Apology*- and *Bolstering*-strategies Marriott continued and further supplemented its initial statement. The company quoted an *Apology* by its President and Chief Executive Officer in the statement:

''"We deeply regret this incident happened," said Arne Sorenson, Marriott's President and Chief Executive Officer. "We fell short of what our guests deserve and what we expect of ourselves.[…]'' (Marriott, 30-11-2018[b]).

Furthermore, the company added a *Reminder* of its commitment to security and safety to its *bolstering* efforts:

"Today, Marriott is reaffirming our commitment to our guests around the world.'' (Marriott, 30-11-2018[b]).

Marriott even lightly engaged in *Ingratiation* as the company expressed its gratitude for the patience of the affected guests:

[…] we appreciate your patience. (Marriott, 30-11-2018[b]).

Finally, Marriott added *Compensation* to its response as it offered its guests a free year of web-monitoring service *'WebWatcher'* with US-guests even receiving more services for free:

''Marriott is providing guests the opportunity to enroll in WebWatcher free of charge for one year. […] Guests from the United States who activate WebWatcher will also be provided fraud consultation services and reimbursement coverage for free. '' (Marriott, 30-11-2018[b]).

In Marriott's second statement indicators of six different strategies could be found. As in most of the cases, two of these strategies, *Crisis information* and *Corrective action* formed the Base response. The other found strategies were *Compensation* and *Apology* falling under the *Rebuild*-category and *Reminder* and *Ingratiation* adhering to the *Bolstering*-category.

Statement 3

Following the Yahoo- and Adobe-cases Marriott's next response-statement took on a FAQ-format. The main purpose of this statement was providing an update on the current state of the crisis, therefore earlier information that was still valid since the last statement remained the same and was essentially copied and pasted in this new statement, while areas of the crisis that did change received some updated information (Marriott, 04-01-2019). The newly added information mainly fell within the *Base response*-category as it consisted either of *Crisis information* or *Corrective action*.

The *Crisis information* in this third statement consisted of Marriott lowering its estimation of affected guest records, the company providing extra information regarding the encryption of the stolen data, and also the disclosure that some of the stolen data was kept in an unencrypted state:

''Marriott now believes that approximately 5.25 million unencrypted passport numbers were included in the information accessed by an unauthorized third party.''

''Marriott believes that there may be a small number (fewer than 2,000) of 15-digit and 16-digit numbers in other fields in the data involved that might be unencrypted payment card numbers.''

(Marriott, 04-01-2019)

The new instances of *Corrective action* mentioned by Marriott consisted of the company providing its call-centre with additional resources, the company announcing that it had successfully phased out the *Starwood*-database and the company announcing that it was further investigating the unencrypted data and would provide a fitting solution based on the results of this investigation:

''The company is continuing to analyze these numbers to better understand if they are payment card numbers and, if they are payment card numbers, the process it will put in place to assist guests.''

(Marriott, 04-01-2019)

While Marriott did not repeat or add an *Apology*, the company did repeat its earlier *Compensation*-offer in the form of a free WebWatcher membership.

Finally, Marriott decided to add a new instance of *Bolstering* in the form of a *Reminder* to the statement as the company claimed to: *''[…]work hard to address our customers' concerns and meet* ***the standard of excellence our customers deserve and expect from Marriott."*** By making this claim Marriott sought to *Remind* its guests of its prior 'excellent' standards and reputation.

In this third statement, Marriott mainly repeated its strategies of *Crisis information, Corrective action, Compensation* and *Bolstering* in the form of a *Reminder* whilst making some minor additions to each of these strategies. This leads to a *Base response* being present as well as strategies from the *Rebuild*- and *Bolstering*- categories.

Statement 4

Marriott's fourth and last statement was published on 09-07-2019 and was not much more than a last update on the data breach crisis and its results. The statement began with *Crisis information* regarding the consequences of the crisis for Marriott as the company announced that the ICO intended to fine in relation to the data breach (Marriott, 09-07-2019). Marriott informed its stakeholders that it intended to fight this intention:

''The company intends to respond and vigorously defend its position.'' (Marriott, 09-07-2019).

The statement then went on to employ a *Victimage*-strategy as Marriott quoted its president stating that he was disappointed with the notice of the ICO and considered it an unrightful decision of which the company became a victim as he stated that Marriott had always cooperated with the ICO:

''We are disappointed with this notice of intent from the ICO, which we will contest. Marriott has been cooperating with the ICO throughout its investigation into the incident […]'' (Arne Sorenson as quoted by Marriott, 09-07-2019).

The statement then went on to restate its *Apology*- and *Reminder*- strategies in a quote that combined sentences, indicating both strategies, from earlier statements:

"We deeply regret this incident happened. We take the privacy and security of guest information very seriously and continue to work hard to meet the standard of excellence that our guests expect from Marriott." (Arne Sorenson as quoted by Marriott, 09-07-2019).

This quote begins with an *Apology* in which Marriott expresses regret and takes responsibility for the data breach and then goes on to emphasize Marriot's qualities and 'standard of excellence' thus making it a combined instance of both *Apology* and *Bolstering* in the form of a *Reminder*.

Finally, Marriott concludes its last statement by repeating an instance of *Corrective Action* in the form of the company decoupling the target of the data breach; its Starwood guest reservation database.

In this last statement, Marriott met the *Base response* through new *Crisis information* and repeated *Corrective action* and complimented this *Base response* by repeating its earlier *Apology*- and

Reminder-strategies. The only new strategy found in this last statement is *Victimage* being an instance of *Bolstering*.

Overall

Over all its response-statements Marriott employed seven different strategies of which two, *Crisis information* and *Corrective action* formed the *Base response*. The other strategies employed by Marriott, being *Compensation, Apology, Reminder, Ingratiation* and *Victimage* were aimed at *Rebuilding* the organisation's reputation after the crisis and *Bolstering* what was left of its current reputation from before and during the crisis.

These strategies and the statements in which they were found are displayed in the following table:

Table 9: Presence of crisis response-strategies in Marriott-case

Strategies by Category / Statement	1	2	3	4	***Overall***
Base response					
Crisis Information	✓	✓	✓	✓	***✓(4/4)***
Display of Empathy (care response)	×	×	×	×	***×***
Corrective Action (care response)	✓	✓	✓	✓	***✓(4/4)***
Deny					
Attack the Accuser	×	×	×	×	***×***
Denial	×	×	×	×	***×***
Scapegoat	×	×	×	×	***×***
Diminish					
Excuse	×	×	×	×	***×***
Justification	×	×	×	×	***×***
Rebuild					
Compensation	×	✓	✓	×	***✓(2/4)***
Apology	✓	✓	×	✓	***✓(3/4)***
Bolstering					
Reminder	✓	✓	✓	✓	***✓(4/4)***
Ingratiation	×	✓	×	×	***✓(1/4)***
Victimage	×	×	×	✓	***✓(1/4)***

5.2 Cross-case comparison on theoretical adequacy

This chapter focuses on comparing the response-strategies found in the cases to the theoretically adequate response-strategies following SCCT as explored in Chapter 4.2.2. It will do this by evaluating whether the response-strategies that were employed in the different cases were adequate, and if not, what the organisations in the cases should have done in order for the response to be adequate. As some of the response-strategies both recommended by Coombs and employed in the three cases are conditional, meaning they can be adequate in certain instances, these response-strategies will be explored in order to determine whether the case warranted the use of the strategy.

Yahoo

In the Yahoo-case the theoretically adequate response should have consisted of a *Base response* supplemented by a *Rebuild*-response in the form of *Compensation* and *Apology* with an optional addition of *Bolstering* and if necessary a *Deny*-strategy in order to combat false rumours or information.

Throughout all its statements Yahoo repeatedly met the requirements of the *Base response* as it provided *Crisis information* which is the first half of the *Base response* and it detailed on *Corrective action* forming the second half of the *Base response;* the *care response*.

The company however failed to engage *Rebuild*-strategies as it, throughout its statements, never provided an *Apology* or offered any form of *Compensation* for its affected customers.

In terms of the *Deny*-strategies it employed, their adequateness should be considered mixed at best and inadequate at worst. Since Yahoo did not provide any evidence or proof of state-sponsored involvement in the breach, its *Scapegoat*-strategy is to be considered inadequate as it is unlikely to have convinced people of the victim-frame Yahoo tried to create for itself by blaming an unknown state-sponsored actor. Furthermore the *Scapegoat*-strategy also most likely backfired as Yahoo, in its announcement of the 2013 breach, once again stated that it believed that the same state-sponsored actor was responsible but counteracted this claim by *Denying* a link between the 2013 and 2014 breaches. This discrepancy between the claims made them implausible as they were unlikely to be both true at the same time, thus making the claims ineffective at creating a plausible crisis frame. Furthermore, Yahoo's *Denial* of Tumblr accounts being affected by the data breach is on itself a reasonable strategy to limit the extensiveness of the crisis if true. However, since users at the time were pushed to use Tumblr with their Yahoo integrated services and virtually all Yahoo accounts were breached, this *Denial* might carry little weight. So, while Yahoo made the right decision by only trying to *Deny* aspects of the crisis instead of the existence of the crisis as a whole, the way the company employed these *Deny*-strategies damaged the trustworthiness of their claims.

Additionally, Yahoo's usage of the *Excuse*-strategy has to be considered inadequate as due to the preventable nature of the crisis, as displayed by the failures of foresight present in the Yahoo-case, the company should have taken responsibility for the crisis and the users it affected instead of seeking to avoid responsibility.

Finally, Yahoo did not engage in the optional *Bolstering* and made no *Display of Empathy*, which can be considered to be missed chances as they might have increased sympathy for the organisation and reminded stakeholders of the company's good qualities, thus possibly lowering blame attribution.

Adobe

While Adobe did manage to employ all required response-strategies, the company instead included too many different response-strategies in its statements.

As is the case in all three the cases Adobe's response should have theoretically consisted of a *Base response*, supplemented by *Apology*- and *Compensation*-strategies and optionally some *Bolstering*- or *Deny*-strategies in order to bolster its image and combat false rumours.

By providing *Crisis information* and *Corrective action* Adobe met the *Base response*, while a *Display of Empathy* was lacking the fact that *Corrective action* was present did manage to fulfil the minimum requirements for the *care-response* part of the *Base response*.

Furthermore, in contrast to Yahoo, Adobe did employ *Rebuild*-strategies in the form of stating an *Apology* and offering its affected customers some form of *Compensation*. By doing so Adobe fulfilled the necessary response-strategies in terms of theoretical adequacy, however, these *Rebuild*-strategies were only employed in the second statement, thus possibly decreasing their effectiveness. While Adobe had at this stage fulfilled the necessary strategies in terms of theoretical adequacy, the company decided to employ even more response-strategies.

While *Deny*-strategies could have been adequate if they were employed in a rightful way, Adobe's use of these strategies was mixed. Adobe's initial *Denial* of the existence of a specific threat to its customers or products should be considered irresponsible as Adobe at that time knew that its source code was accessed and that such access was likely to increase cyber-attacks. Even more questionable is the fact that Adobe kept including this *Denial* in later statements that followed the initial announcement of a data breach that compromised numerous Adobe accounts. Further diminishing the effectiveness of these *Denial*-strategies is the fact that Adobe, in later statements, denied the truthfulness of the number of affected accounts it had stated in earlier statements. Adobe's use of the *Attack the accuser*-strategy can however be considered adequate as Adobe employed this strategy in order to stop the spread of false information by third parties and possibly protect its customers and its own reputation from the actions of unreliable third parties. By employing this strategy to fight false information that might have affected the crisis-frame as it would suggest that Adobe's compromised data was easily accessible, Adobe met the requirements set by SCCT for the usage of an *Attack the accuser* strategy. What is interesting is that, despite Adobe's widespread use of *Deny*-strategies, the company did not make an effort to *Deny* rumours stating that the compromised dataset included as much as 150 Million accounts. Denying or even responding to such a rumour by stating that this set included many invalid accounts could have worked in Adobe's benefit as the extensiveness of the crisis would have been limited.

Adobe's *Excuse*-strategy however, detracted from the adequacy of the response as it worked directly against Adobe's *Rebuild*-strategies. By *Apologizing* and providing affected customers with a *Compensation* Adobe suggested that it took responsibility for the crisis, as it should have. However, the *Excuse*-strategy sought to diminish Adobe's responsibility for the crisis by claiming that a breach in the case of Adobe would have been nearly unavoidable. This *Excuse*-strategy therefore directly contradicted Adobe's earlier *Rebuild*-strategies, leading to both sets of strategies being diminished in effectiveness.

Finally, Adobe's inclusion of *Bolstering* strategies was adequate, but subtle. As Adobe only used the *Reminder*-strategy to emphasize certain efforts and used *Ingratiation* to thank only two of its stakeholders, the *Bolstering*-strategies would likely not have had a substantial impact on the overall crisis response either in a positive or negative sense.

Marriott

As all cases fall under the same crisis-cluster, the theoretically adequate response-strategies in the Marriott case also consisted of a *Base response*, supplemented by *Rebuild*-strategies possibly reinforced by *Bolstering*-strategies and, if necessary, *Deny*-strategies to combat false information or rumours.

Like the two previous cases, Marriott met the *Base response* by providing *Crisis information* and *Corrective action*. And like the two previous cases, Marriott did not include a *Display of Empathy* in this *Base response*.

What distinguishes Marriott from the other two cases however, is that Marriott fully adhered to the theoretically adequate response-strategies by employing all required response-strategies without contradicting these strategies with the usage of non-required strategies.

In terms of its *Rebuild*-strategies Marriott adequately took responsibility by adding one or

multiple *Apologies* in three of its four statements and by offering a form of *Compensation* for affected users in two of its four statements.

Furthermore, Marriott adequately employed *Bolstering*-strategies as it incorporated some strong *Reminders* concerning the qualities and existing reputation of the company whilst also including subtle instances of *Bolstering* in the form of a light attempt at *Ingratiation* and *Reminders* in the form of positive adjectives describing the company's efforts.

Ranking the cases in terms of response-adequacy

When the theoretical adequateness of the employed response-strategies in the three cases is compared it becomes clear that the cases differ in the adequateness of their response.

Yahoo has diverged the most from the recommended response-strategies by refusing to employ any *Rebuild*-strategies such as the *Apology*-strategy or the *Compensation*-strategy. Furthermore, the response-strategies that Yahoo did employ, such as its *Denial*-, *Scapegoat*- and *Excuse*-strategies were either poorly executed, misplaced or counteracted by one of its other employed response-strategies. Finally, Yahoo neglected *Bolstering*-strategies altogether, thus missing its chance to reinforce what was left of its reputation during and after the crisis.

While Adobe did meet the minimum requirements for a theoretically adequate crisis response, it went overboard with its selection of response-strategies. Because of its broad employment of different response-strategies, Adobe impaired the effectiveness and believability of its initially required response-strategies as the extra strategies contradicted these initial strategies. The most evident instance of this can be found in the fact that Adobe initially seemed to claim responsibility for the crisis by offering an *Apology* and *Compensation* but then employed an *Excuse*-strategy to avoid responsibility. Furthermore, the *Deny*-strategies employed by Adobe were mixed in their adequacy and the company's *Bolstering* attempts were so subtle that they are not likely to carry a substantial effect on the company's reputation.

Marriott on the other hand fully followed SCCT's recommendations by only employing the necessary *Base response* and *Rebuild*-strategies coupled with both strong and subtle *Bolstering* attempts. By not employing unwarranted *Diminish*- or *Deny*- strategies Marriott appeared to take its responsibility for the crisis and seemed the most genuine in its crisis-response. Because of this Marriott's response should be considered the most adequate of the three.

5.3 Indication of the outcome

In this chapter, the results of the research methods focussing on the outcome and their implications will be discussed (See 3.2.3).

5.3.1 Market effects

The *market effect* component of reputational damage consists of any effects a company's market value or share-value suffered following the announcement of the crisis and the publishing of its crisis responses. While such a component is supported by both crisis communication researchers and stock-market research, attempts to assess these market effects in this research show that it is in no way a reliable 'one size fits all' solution for determining reputational damage (Wang & Park, 2017; Way, Khan & Veitch, 2013).

In assessing the market effects present in the different cases, a myriad of problems hindering this approach were encountered. Firstly, since Yahoo had been bought by Verizon in 2016, the company's historic stock- and market-value have become inaccessible as the company is removed from any stock market platforms. This makes any researcher trying to assess market effects in the Yahoo case dependent on secondary reports, which is far from ideal. Secondly, Adobe was generally not found to be affected in terms of market-value by the crisis, thus contradicting any previous research on the subject. This can possibly be explained by the fact that Adobe has a market share in the graphic design sector of over 90% in its home country The United States and was thus not likely to lose any substantial amount of customers regardless of its handling of the crisis. This may have resulted in stock owners retaining trust in the company (Datanyze, 2020). Furthermore, preceding the

time of the data breach, Adobe's stock value was increasing due to new product developments (La Monica, 12-11-2013; Yahoo Finance, n.d.[a]). This continuous growth might have absorbed any market effect resulting from the data breach and its crisis communication (La Monica, 12-30-2013).

Finally, even if market effects were visible, the surrounding market- and stock-mutations were volatile enough to make attributing any decrease in stock- or market-value to the reputational damage short-sighted at best and unreasonable at worst. Despite claims from researchers in both crisis communication and market studies on the ability of market effects being able to indicate reputational damage, all these factors lead to the adequateness of employing market effects as an indicator of reputational damage being highly questionable.

Despite the unsuitability of using market effects to prove reputational damage, the found market effects as based on secondary sources and historic market data, will nevertheless be briefly described for the sake of overview:

Table 10: Market effects present in the three cases

	Effect
Yahoo	• Share-value fell reportedly 3.6% after first announcement of the 2014 data breach consisting of the first two statements (Nolter, 23-12-2013). • After announcement of 2013 data breach, share-value reportedly fell an additional 4.8% (Reuters, 15-12-2016). • Following the crisis Yahoo's market value fell with 7.24% as the price for which it was acquired by Verizon dropped with 350 Million USD following the breaches (Stempel. 09-04-2019).
Adobe	• No directly noticeable effect after announcement or statements. Stock value kept rising (Yahoo Finance, n.d.[a]). • Total increase of 1% on day of announcement, in line with earlier growth of stock value (Yahoo Finance, n.d[a].; La Monica, 12-11-2013).
Marriott	• Initial stock value drop of 5.6% after statements on first day (Yahoo Finance, n.d.[b] ; Kilgore, 30-11-2018). • Later statements did not lead to a drop in stock value, some even reported a slight increase (Yahoo Finance, n.d.[b]). • Stock value in case of Marriott generally volatile, effects of data breach not visible in broader perspective (Yahoo Finance, n.d.[b])

As can be seen from this table Yahoo seems to have suffered the most negative market effects, which could be regarded as an indication of the practical validity of the theoretically adequate response-strategies. However, due to the general volatile nature of the stock market in terms of fluctuations and the fact that Adobe did not report any negative market effects, most likely due to external factors, using these market effects as an indication of the reputational damage would be unreliable.

5.3.2. Public response

As was mentioned in chapter 3 the *public response* component is determined through a thematic comment analysis of comments posted on CNET-articles. In total 249 user comments posted on ten different CNET articles have been analysed in order to determine their stance towards the relevant

companies. These 249 comments amount to almost all comments posted on all articles detailing on the crises central to this research. The only comments that were not analysed were those that were either double-posted or that contained the same content as an earlier comment from the same user. Like the main content analysis that sought to determine the utilised strategies in the cases, this thematic comment analysis was done on the basis of a dedicated codebook (See Annex 2).

Yahoo

In the case of Yahoo, a total of 100 comments was analysed. the majority of the comments posted on the articles detailing the crisis were negative towards the company. This amounted to a total percentage of 60% of comments. 34% of the comments were neutral in the sense that they either did not state a clearly positive or negative opinion on the company or that they did not discuss the company or its actions altogether. The final 6% of comments were found to have a positive sentiment towards the company, either defending it against blame attribution or praising its actions and handling of the crisis.

Adobe

The articles related to the Adobe case had the most comments posted and included the fiercest discussions of all the three cases. A total of 135 comments was analysed and coded. Of these 135 comments, a little more than half, 53.3% to be precise, expressed negative feelings towards the company or its actions. Around a third of the reactions, 36.3%, expressed neutral or no feelings towards the company or its actions. The remaining reactions, 10.4%, were positive in the sense that they praised the company for its efforts to resolve the crisis, defended the company against negative blame attribution or were just generally appreciative of Adobe.

Marriott

The Marriott-case is exceptional in terms of public response when compared to the other two cases. This is due to the fact that, while all of the Marriott-statements received their own CNET-articles, only three of these articles contained any public comments. Furthermore, the articles that did have comments, had only small numbers of them. In total, when all the Marriott articles are taken into account, only 14 comments were available to be analysed which is far fewer than in the other cases. In order to resolve generalisability issues that would stem from using such a small amount of comments, The New York Times, the only other source that had articles on all three cases with public comments enabled was considered to replace CNET as a source for comments. However, while going through the New York Times-articles it became apparent that the roles on this medium were reversed. While the New York Times-articles included over 200 comments on the Marriott case, the Adobe and Yahoo cases each only received around 10 to 20 comments, thus making them unusable with regard to the generalisability-aspect. As the two news outlets have vastly different userbases, with the more tech-oriented users utilising CNET and The New York Times having more of an unspecialised userbase, it would have been scientifically irresponsible to arbitrarily select comments from both news outlets. Because of this it was decided to continue with the CNET-focussed comment analysis and accept the limitation that Marriott results may not fully reflect reality and thus lack generalisability.

Of the comments analysed, only 28.6% contained a negative disposition towards Marriott. The majority of the comments, 57.1%, contained a neutral stance with regard to Marriott and its actions. Finally, a minority of the comments, 14.3%, had a positive disposition towards Marriott or defended the company against blame attribution.

Conclusion on public response

The results of the comment analysis would suggest that this research's results concerning the theoretically adequate response-strategies and their employment are correct since the company that deviated the most from the theoretically adequate set, Yahoo, had the largest share of negative comments and the smallest share of positive ones. Adobe, which did meet the requirements for an adequate response but negated its response by employing too many different strategies, had a less

negative public response and substantially more positive reactions than Yahoo (See Table 10). Finally, the Marriott data, although with its flaws, suggests that Marriott had the least negative public response as less than a third of the comments were negative and the rest positive or neutral (See Table 10). This would indicate validity of the results on adequacy as Marriott was the only company of the three who employed a fully adequate response without compromising it by employing unwarranted extra response-strategies.

While the differences in public response between the Adobe and the Yahoo cases might be considered usable in terms of generalisation, the results of this analysis cannot be fully taken as validation for the practical effectiveness of theoretically adequate response-strategies as the results of the Marriott case are simply based on a number too small to allow effective generalisation. This makes the results of the comment analysis an interesting indication of possible effects, but unfortunately not viable enough to actually serve as proof.

Table 11: Results of Thematic Comment Analysis, disposition of comments

	Positive	Neutral	Negative
Yahoo	6%	34%	60%
Adobe	10.4%	36.3%	53.3%
Marriott	14.3%	57.1%	28.6%

5.3.3 Response critique

In determining the response critique comments posted on all available CNET-articles and industry professional reactions from industry-overview articles were analysed.[8] Critiques on the companies' responses were selected and reviewed, in the case of multiple critiques on the same topic, those most explicit were incorporated into this chapter.

Yahoo

In the Yahoo-case critique was outed on multiple aspects of the crisis, the most important being the lateness of response by Yahoo despite the company likely having known about the breach for quite some time. Several user-comments addressed this point of critique:

Thereallordbaal:

"Marissa Mayer should now get fired. They knew about it 2 years ago, and didn't say anything."

(as commented on CNET, 22-09-2016)

susndee4:

"Why didn't you tell us sooner? By now if they wanted our information they have it. It was 2 years ago!!!! Unacceptable!!!"

(as commented on CNET, 22-09-2016)

This same point of critique got reinforced by security experts as the most prominent critique stated in their comments echoed the same:

Richard Cassidy, UK cyber security evangelist at Alert Logic:

If initial reports that Yahoo experienced this particular breach back in 2014, and its only now coming to light, then this raises serious concerns for consumers of Yahoo products or services, and questions need to be answered on why external communication has been withheld for so long.

(ITSecurityGuru, 23-09-2016)

[8] An overview of all CNET-comments is available on request, the sources of incorporated quotes are referenced and included in the bibliography. The articles containing the industry-professional reactions will also be referenced and included in the bibliography

However, this was not the only critique Yahoo received from users and professionals alike. Another often stated critique was focused on Yahoo's use of the *Scapegoat*-strategy:

Chris Hodson, EMEA CISO at Zscaler:

"With no technical details included in Yahoo's report about how the data was exfiltrated, just that it was, it's impossible to assess credibility of the 'state sponsored' claim without this. In this instance, we can only speculate that the 'state sponsored actor' claim was made with a view to placating the general public."

(ITSecurityGuru, 23-09-2016)

Paul Farrington, manager of EMEA solution architects at Veracode:

"The company tells us that hack was performed by a state-sponsored actor. It's interesting that this is given prominence in the press release whilst other details remain undisclosed."

(Pudwell, 23-09-2016)

Thereallordbaal:

"And how do they know it was state sponsored?"

(as commented on CNET, 22-09-2016)

Finally, the company also received some critique on its decision to offer no compensation.

haud_termino:

"where is the compensation for all the users ?"

(as commented on CNET, 22-09-2016)

Adobe

In Adobe's case, the main criticism on its response mainly cited by user-comments was focussed on the company's attempted instances of *Denial* of risk

Mark Smith:

" "..there is no "increased risk to customers as a result of this incident."

There is no risk because it´s not Adobe´s president credit card numbers..."

(as commented on CNET, 03-10-2013)

gork_platter:

"Sure there is increased risk. Now hackers have the luxury of examining the code for vulnerabilities, and either use it to build the next lineup of viruses or surreptitiously plant a few lines, then rebuild and post them on torrents. Trust is GONE."

(as commented on CNET, 03-10-2013)

This same critique was, albeit to a lesser extent, repeated by industry-professionals:

Troy Gill, Senior Security Analyst at AppRiver:

> *According to initial reports, the attackers were also able to exfiltrate a great deal of source code for major Adobe products. This will almost certainly lead to an increase in malicious actors exploiting vulnerabilities in Adobe software to infect users systems with malware. Of course it will depend on what the attackers do with the information from here, but we have to assume they won't be kind and drop it in the shredder.*

(HelpNetSecurity, 04-10-2013)

Another, often repeated, critique on Adobe focussed on the company's compensation offer. Users stated that it, in its current form, was a cheap attempt by Adobe to mitigate blame for the crisis:

Snth:

" "...of enrolling in a one-year complimentary credit monitoring membership where available"

Such generosity is unheard of. Why didn't they also throw in an air guitar?"

(as commented on CNET, 03-10-2013)

Model Bravo:

What a joke! Adobe probably has a deal with the credit monitoring service so their "free" service offering for their own lack of sufficient security appears to be a good deal but it really isn't. Adobe's hoping people will easily dismiss their serious security short comings. If I were an Adobe customer (of which I am not thankfully) I would be pissed and sue their pant's off. There is no excuse for this; especially from a software company of Adobe's size.

(as commented on CNET, 03-10-2013)

Industry professionals criticized the compensation effort on the same basis of being insufficient with regard to the crisis, however it was still deemed better than nothing:

Troy Gill, Senior Security Analyst at AppRiver:

> *While the offer of "one year of free credit monitoring" at Adobe's expense may seem like a too-little-too-late proposition, go ahead and take advantage of it.*

(HelpNetSecurity, 04-10-2013)

Marriott

Critique outed on Marriott was, in contrast to the other two cases, reasonably mild. The main points of critique expressed by user comments focussed on the fact that Marriott unnecessarily collected user data without managing to defend it from attackers:

Bob-Marley-Is-Alive:

"These large companies have data breaches where Joe Consumer is left having to change passwords on all of their devices, all the while no penalties whatsoever with the culprit. Put legislation forward with stiff penalties and fines, and these companies will not be so careless with our data."

(as commented on CNET, 30-11-2018)

Tillited:

"It's back to the basic, If the company didn't retain so much personal information about a person the hack wouldn't be so worrisome."

(as commented on CNET, 04-01-2019)

Industry-professional opinions on the other hand were relatively positive of Marriot's handling of the crisis. There were however two main critiques that were evident from these opinions. Firstly, as in the Adobe case, while the compensation was deemed better than nothing, it was also criticized for being inadequate in relation to the extensiveness of the crisis:

> Joseph Carson, Chief Security Scientist at Thycotic:
>
> *"The major problem of such data breaches in the past is that those companies who have been entrusted to protect their customer data have only offered up to one year of identity theft protection. But, many of the identity information that is stolen typically can last between 5-10 years such as drivers licenses and passports. So while victims may get some protection, they are at serious risk for years unless they actively replace compromised identity documents which is done at a cost."*
>
> (Zorz, 30-11-2018)

Secondly, Marriott was criticized for the pre-crisis aspects of the case. This critique mainly focussed on the fact that Marriott was unable to detect the breach in a timely manner. While this is not related to the response-strategies employed by Marriott, it does illustrate the workings of blame attribution with regard to security failures:

> James Hadley, CEO at Immersive Labs:
>
> *"[...] what's more concerning is that this has been happening since 2014. This clearly demonstrates that something is off in the company's approach to security and urgently needs to be re-assessed."*
>
> (Zorz, 30-11-2018)

> Trevor Reschke, Threat Intelligence Officer, at Trusted Knight:
>
> *"We have been shown again and again that organisations do not take the security of their customer data seriously – and such unauthorised access going unnoticed for four years is a prime example of this. We don't know yet how this breach happened, but whatever the cause, it's simply unacceptable that it went undetected for so long."*
>
> (Zorz, 30-11-2018)

Despite these criticisms however, Marriott also received praise for its response from industry-professionals, which distinguishes it from the other two cases:

> Colin Bastable, CEO at Lucy Security:
>
> *"Kudos to Marriott for getting the news out as soon as they learned about the breach. [...] Marriott's fast reporting shows some other recent cyberattack victims up in a bad light; they clearly had a plan in place for such a situation and executed on it."*
>
> (Zorz, 30-11-2018)

Conclusion on response critique

The evaluation of critiques allows for a general indication of where the blame attribution in the three crises lies. This evaluation led to several interesting findings.

First and foremost the apparent importance of a timely response must be noted as this was the primary critique in the Yahoo case. It seems that the timeliness of the response, while being separate from the traditional response-strategies, has a noteworthy impact on the blame attribution and subsequent reputational damage in a case.

Furthermore, it must be noted that while offering compensation was theoretically considered to be adequate in itself, it seems that the nature of the *Compensation* is equally important. If the *Compensation* is deemed insufficient or unfitting, the positive effects stemming from offering

Compensation may be diminished.

What is also interesting is that the critiques mainly focus on the inadequately applied response-strategies. Yahoo, for instance, was criticized for its lack of offering *Compensation* and its unwarranted use of the *Scapegoat*-strategy. Similarly, the main point of critique in the Adobe-case was its initial incorrect attempts to *Deny* any risk to users or its products. While these critiques therefore seem to validate the set of theoretically adequate response-strategies, it is important to note that there was no mention of Yahoo's missing *Apology* or the inadequate attempts to employ an *Excuse*-strategy.

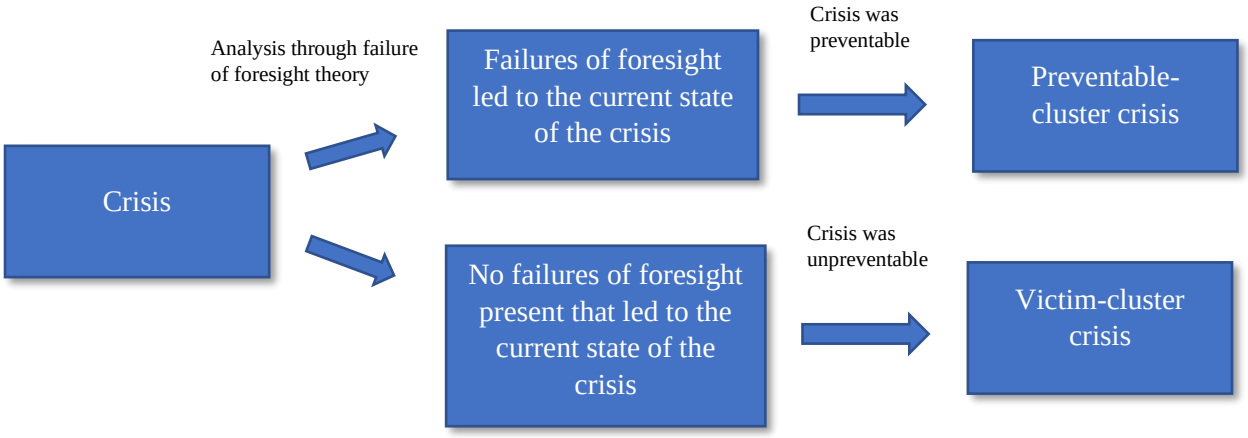
While these critiques provide a valuable insight into the nature of the blame attributed to the companies and the opinions regarding their response-strategies, such insights are unfortunately not sufficient to scientifically validate the theoretically adequate set of response-strategies. This is due to the fact that the number of relevant responses is simply too low and many of the professional critiques stem from different secondary sources.

VI. Discussion and Limitations

6.1 Discussion on the nature of the research

This research project has sought to build upon existing crisis communication research and fill in numerous gaps in relation to modern crises such as data breaches. Where previous research attempts into this field often based their crisis-type assessment on arbitrary rational reasoning, this study proposes a more objective model to determine the crisis-type and the adequate crisis response-strategies following this type. This *preventability-model* fuses Turner's *Failure of Foresight*-theory (1976) with Coombs' SCCT (2007) and its recommendations into a model that aims to determine the preventability of certain crises based on the presence of failures of foresight. By utilising this model the theoretical discussion on whether a data breach is a victim-cluster crisis or a preventable-cluster crisis can be solved through an objective form of analysis. The way this *preventability-model* functions is illustrated in the following simplified graphic:

Model 2: Preventability-model



Determining the crisis-type allowed this research to determine, on the basis of pre-existing crisis response recommendations, what the theoretically most adequate crisis response would have been (Coombs & Holladay, 2011). This in turn allowed for an analysis and subsequent assessment of the response-strategies in three recent high-profile data breach cases. Thus providing insight in the actual employment of the theoretically adequate set of response-strategies and enabling an evaluation of the response efforts of the three cases. Finally, this research sought to fill an important knowledge gap that plagued numerous researchers in the field of crisis communication such as Benoit (1997) Krishna & Vibber (2017) and Wang & Park (2017). All these researchers struggled with adequately determining the crisis outcome in terms of measuring reputational damage. By investigating three distinct components of the outcome this research sought to provide a more holistic way of determining outcome and determine the practical validity of the theoretically adequate set of response-strategies. By failing in scientifically determining such an outcome however, this research has instead managed to provide insight into the issues that plague such efforts and brought to light the complex nature of determining reputational damage as a variable.

6.2 Limitations

As with all research projects, this research has encountered several limitations. While the majority of these limitations have already been discussed in the previous chapters, it is imperative for the accessibility of these limitations that they are also addressed here.

Firstly, while the determination of the crisis type of the different cases on the basis of the *preventability-model* allows for the distinction between preventable- or victim-cluster to be made, it does not account for the third cluster that is described by Coombs: the accidental-cluster. This is primarily due to the fact that accidental-cluster crises are often self-evident as they mainly consist of

mechanical or technical errors. Nevertheless, further efforts to incorporate crises of this cluster-type into the model should be recommended.

Furthermore, regarding the content analysis aspect(s) of this research, it is important to mention that any form of content analysis may carry the risk of reliability issues such as cherry-picking, coder-bias and unreliability of the documents that are analysed. In order to diminish these issues, strict codebooks were created and followed and randomly selected documents were re-coded at later times to ensure coder-reliability. The risk of unreliable documents is negated in this research as the documents used are primary sources and thus directly indicate the intentions and strategies of their authors. This use of primary sources however does limit the scope of this research as any crisis-response efforts made outside of the official statements were not analysed. Additionally, due to the objective nature of a content analysis, indications of intentions and response-strategies that were found as implicit statements, could not be coded as such unless they fell within the coding indicators or coding rules.

Moreover, since this research only covered three distinct cases, it is difficult to generalise its results to all corporate crisis-response efforts, as every crisis case carries distinct inherent differences by nature. However, the cases did prove to be similar enough to determine a general recommended set of response-strategies and evaluate which mistakes in terms of crisis-response may be present in corporate crisis responses and should thus be avoided.

Finally, the most important limitation that must be discussed is the fact that the outcome of the cases that were analysed was found to be undeterminable which leads to a lack of practical validation for the adequate response-strategies. This is due to several factors. Firstly, despite academic claims that market effects indicate reputational effects, the market effects that were found followed mostly random, volatile patterns and provided no clear indication regarding to what extent the effects could be attributed to reputational damage. Secondly, while a comment analysis might be a valid way to indicate reputational damage, this is only the case if a large number of comments that are evenly distributed throughout sources are found. However, in the cases central to this research, such sources with large, evenly distributed comment-pools did not exist, making the comment analysis unreliable. Thirdly, a similar issue existed with regard to the response-critique component of the outcome, if a large number of expressions of critique had existed this could have been a potentially viable way to determine the nature of reputational damage. However, due to the lack of such an amount the response analysis is limited to functioning more as an indication of which parts of a response generated criticisms. Nevertheless, the attempts to determine the outcome of the cases did manage to provide an approximation of the different outcomes and are useful as an illustration of the issues that exist within the field of crisis communication.

VII. Conclusion

In recent years cyber-related crises such as data breaches have risen to relevance and cyber-attacks have become one of the most frequent modern forms of crime (Bissell, LaSalle & Cin, 2019). Despite this rise in importance, companies affected by such crises are often found dealing with such crises without a proper response-plan (Ponemon Institute, 04-2019). In order to further the knowledge of what would constitute such a proper response-plan, this research sought to answer the following question:

> *''To what extent can corporate communication response to cybersecurity breaches be deemed adequate?''*

In order to answer this question it was split into four distinct sub-questions which were each answered chronologically:

1. *How can the theoretically adequate crisis response regarding cybersecurity breaches be determined?*
2. *To what extent can the crisis communication efforts in the cases be deemed theoretically adequate?*[9]
3. *To what extent can the cases be compared in terms of the theoretical adequateness of their crisis communication efforts?*
4. *To what extent can the theoretically adequate strategies be validated by the outcome?*

In order to answer the first sub-question, a model consisting of a fusion between pre-existing theories was created. This *Preventability*-model allows for determining whether a crisis was preventable or not and enabled an application of recommendations from SCCT to determine what a theoretically adequate crisis response would have been.

By applying the model to three recent, high-profile data breach-cases, being the Yahoo 2016 data breach, the Adobe 2013 data breach and the Marriott 2018 data breach, it was found that all three cases contained failures of foresight enabling their respective crises thus proving that all three cases were preventable-cluster crises. By applying SCCT's recommendations to these preventable-cluster cases the theoretically adequate set of response-strategies for each of the cases was determined as being a *Base response*, supplemented by *Rebuild*-strategies in the form of an *Apology* and *Compensation*, to which optional *Bolstering strategies* and if necessary *Deny*-strategies could be added.

Through a qualitative content analysis of the official crisis response-statements in each of the three cases, it was found that the responses of the three cases differed in their adequacy. While Marriott fully adhered to the adequate response-strategies, Adobe added unwarranted response-strategies into its statements and Yahoo neglected the prerequisites for an adequate response altogether. This meant that on a theoretical basis, Marriott had been the most adequate in its crisis-response, Yahoo had been the least adequate and Adobe fell in between with a somewhat adequate response.

In order to validate these results, attempts were made to compare the outcome of the three cases. Since earlier studies within the field of crisis communication are lacking in their attempts to determine the outcome of analysed cases, this research decided to employ three different components to determine the outcome, being *market effects*, *public response* and *response critique*. However, due to the unpredictability of market effects and the lack of available data with regard to public responses, these efforts failed to scientifically determine an outcome in the form of clear reputational effects. This attempt did however manage to provide insights into the difficulties that plague the field of crisis communication and an approximation of the outcome of the different cased based on the data that was

[9] See the Theory and Methods chapters for a full explanation

available.

Overall, this research managed to provide the field of crisis communication with a method to determine the crisis-cluster of data breaches, it managed to evaluate three modern, high-profile data breach cases through applying theories that were seldom to never applied to such cases and it provided valuable insights into the existing gaps of knowledge present in the field of crisis communications. Based on these existing gaps of knowledge further research into ways to measure reputational damage is recommended as it would lead to a better validation of the theoretical conclusions.

In a more practical sense, based on the theoretical results and practical approximation of the outcome between the different cases, recommendations for the private sector can be made. These recommendations apply to corporations that suffer a preventable data breach and focuses on several aspects, being; proper timing and taking responsibility by apologizing and adequately compensating affected stakeholders. In terms of timing, as has been shown by the negative fallout Yahoo received, corporations that suffer preventable data breaches would do well to issue a timely response and avoid waiting to disclose the breach. This is shown in the critique that Yahoo received as stakeholders attributed blame to Yahoo based on its failure to immediately disclose the breach. Marriott, who disclosed its breach relatively quickly, received less negative fallout and was praised for its quick disclosure and handling of the crisis. Additionally, corporations that suffer preventable data breaches would do well to show their stakeholders that they take responsibility for the crisis and the subsequent theft of data, instead of attempting to avoid responsibility and blame. They may do so by issuing apologies, offering compensation that is in line with the scope of the consequences for their stakeholders, and abstaining from unwarranted *Diminish*- and *Deny*-strategies. This recommendation is supported by the fact that both Yahoo and Adobe got called out on their attempts to employ *Denial*- and *Scapegoat*-strategies and, based on what is known, received more negative fallout than Marriott, who immediately took responsibility by apologizing and offering compensation. What must be added to this recommendation, is that simply offering any form of compensation might not be sufficient. Offering a compensation that is deemed inappropriate in relation to the extent of the crisis may lead to its own blame attribution, as is seen from the critiques on both the Marriott and Adobe cases. What constitutes an appropriate compensation warrants additional research however, as it seems dependent on the scale and consequences of a suffered breach. Nevertheless, following these different recommendations might allow corporations that suffered a preventable data breach to limit reputational damage and save face in the cyber-age.

VIII Bibliography

Adobe. (03-10-2013[a]). *Illegal access to Adobe source code*. From: https://blogs.adobe.com/security/2013/10/illegal-access-to-adobe-source-code.html [Accessed 10-04-2020]

Adobe. (03-10-2013[b]). *Important customer security announcement*. From: https://theblog.adobe.com/important-customer-securitys-announcement/ [Accessed 15-04-2020]

Adobe. (15-10-2018). *Customer security alert.* From: https://helpx.adobe.com/x-productkb/policy-pricing/customer-alert.html [Accessed 16-04-2020]

Ashford, W. (30-11-2018). *Marriott data breach highlights basic failings.* From: https://www.computerweekly.com/news/252453521/Marriott-data-breach-highlights-basic-failings. Computer Weekly. [Accessed 22-06-2020]

Bartlett, L., & Vavrus, F. (2016). Rethinking case study research: A comparative approach. Taylor & Francis.

Bennett, A. (2004). Case study methods: Design, use, and comparative advantages. Models, numbers, and cases: Methods for studying international relations, 19-55.

Benoit, W. (1997). Image repair discourse and crisis communication. Public Relations Review, 23(2), 177-186.

Berg-Schlosser, D., & Meur, G. (2009). Comparative research design: Case and variable selection. In Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques (p. Configurational comparative methods: qualitative comparative analysis (QCA) and related techniques).

Bissell, K., LaSalle, R., & Cin, P. D. (2019). Ninth Annual Cost of Cybercrime Study. Ponemon Institute: Dublin, Ireland, 6.

Bitglass. (2019). Kings of the Monster breaches. Retrieved from: https://www.bitglass.com/blog/monster-sized-breaches-spell-disaster-for-enterprise

Carnegie Mellon University. (31-12-2008). *MD5 vulnerable to collision attacks: vulnerability note VU#836068*. From: https://www.kb.cert.org/vuls/id/836068 [Accessed 20-06-2020]

CNET, (03-10-2013). *Adobe hacked, 3 million accounts compromised.* From: https://www.CNET.com/news/adobe-hacked-3-million-accounts-compromised/#comments [Accessed: 01-07-2020]

CNET, (22-09-2016). *Yahoo hit in worst hack ever, 500 million accounts swiped*. From: https://www.CNET.com/news/yahoo-500-million-accounts-hacked-data-breach/#comments [Accessed: 01-07-2020]

CNET, (30-11-2018). *Senators call for data security law in wake of Marriott breach*. From: https://www.CNET.com/news/lawmakers-call-for-data-security-legislation-in-wake-of-marriott-breach/#comments [Accessed 22-06-2020]

CNET, (04-01-2019). *Marriott says hackers stole more than 5 million passport numbers*. From: https://www.CNET.com/news/marriott-says-hackers-stole-more-than-5-million-passport-numbers/#comments [Accessed 22-06-2020]

Collier, D., & Mahoney, J. (1996). Insights and pitfalls: Selection bias in qualitative research. World Politics, 49(1), 56-91.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. Corporate reputation review, 10(3), 163-176.

Coombs, W. T., Frandsen, F., Holladay, S. J., & Johansen, W. (2010). Apologizing in a globalizing world: Crisis communication and apologetic ethics. Corporate Communications: An International Journal.

Coombs, W. T., & Holladay, S. J. (Eds.). (2011). The handbook of crisis communication (Vol. 22). John Wiley & Sons.

Claeys, A. S., & Cauberghe, V. (2012). Crisis response and crisis timing strategies, two sides of the same coin. Public Relations Review, 38(1), 83-88.

Cyber Risk Analytics. (08-2019). 2019 MidYear Quickview Data Breach Report. *RiskBased Security*

Cygilant. (25-11-2013). *Facts about the Adobe Data Breach.* From: https://blog.cygilant.com/blog/bid/326184/Facts-About-the-Adobe-Data-Breach. [Accessed 29-05-2020].

Datanyze, (2020). *Market share: graphics: united states.* From: https://www.datanyze.com/market-share/graphics--462/United%20States?page=1 [Accessed 09-07-2020]

Decuypere, A. & Van de Water, D. (2020). Content Analysis: Final Assignment. Available on: https://1drv.ms/b/s!Ar3fB4iy7FcjoQ0heqCVWzhkRI6S?e=VlmGXS

Dibazar, A. A., Yousefi, A., Park, H. O., Lu, B., George, S., & Berger, T. W. (2011). Intelligent recognition of acoustic and vibration threats for security breach detection, close proximity danger identification, and perimeter protection. University of South California: Los Angeles

Ducklin, P. (04-11-2013). *Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder.* From: https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/. Naked Security by Sophos. [Accessed 25-05-2020]

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. Journal of advanced nursing, 62(1), 107-115.

Evans, M., McIntosh, W., Lin, J., & Cates, C. (2007). Recounting the courts? Applying automated content analysis to enhance empirical legal research. Journal of Empirical Legal Studies, 4(4), 1007-1039.

Finkle, J. (29-10-2013). *Adobe data breach more extensive than previously disclosed*. From: https://www.reuters.com/article/us-adobe-cyberattack/adobe-data-breach-more-extensive-than-previously-disclosed-idUSBRE99S1DJ20131029. Reuters. [Accessed 25-05-2020]

Forman, J., & Damschroder, L. (2007). Qualitative content analysis. In Empirical methods for bioethics: A primer. Emerald Group Publishing Limited.

Fox, L. (01-03-2019). Marriott data security breach costs the company $28M so far. From: https://www.phocuswire.com/marriott-full-year-results-2018 [Accessed 25-05-2020]

Fruhlinger, J. (12-02-2020). Marriott data breach FAQ: How did it happen and what was the impact? From: https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html [Accessed 24-5-2020]

Goodin, D. (01-11-2013). *How an epic blunder by Adobe could strengthen hand of password crackers.* From: https://arstechnica.com/information-technology/2013/11/how-an-epic-blunder-by-adobe-could-strengthen-hand-of-password-crackers/. Ars Technica. [Accessed 05-06-2020]

Goodin, D. (22-09-2016). *Yahoo says half a billion accounts breached by nation-sponsored hackers.* From: https://arstechnica.com/information-technology/2016/09/yahoo-says-half-a-billion-accounts-breached-by-nation-sponsored-hackers/. Ars Technica. [Accessed 29-05-2020]

Graham, M. W., Avery, E. J., & Park, S. (2015). The role of social media in local government crisis communications. Public Relations Review, 41(3), 386-394.

Gressin, S. (04-12-2018). The Marriott data breach. From: https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach Published on order of the US Federal Trade Commission. [Accessed 24-05-2020]

Harrington, E. K., Gordon, D., Osgood-Roach, I., Jensen, J. T., & Aengst, J. (2015). Conceptualizing risk and effectiveness: a qualitative study of women's and providers' perceptions of nonsurgical female permanent contraception. Contraception, 92(2), 128-134.

HelpNetSecurity. (03-10-2013). *Reactions from the security community to the Adobe breach.* From: https://www.helpnetsecurity.com/2013/10/04/reactions-from-the-security-community-to-the-adobe-breach/ [Accessed 01-07-2020]

Holsti, O. R. (1969). Content analysis for the social sciences and humanities. *Reading. MA: Addison-Wesley (content analysis)*.

Huffman, M. (11-11-2016). *Adobe settles 2013 data breach with 15 states*. From: https://www.consumeraffairs.com/news/adobe-settles-2013-data-breach-with-15-states-111116.html [Accessed 08-03-2020]

Inside Privacy. (25-01-2013). *ICO fines Sony £250,000 following the 2011 Playstation Network Platform data breach*. From: https://www.insideprivacy.com/data-security/ico-fines-sony-250000-following-the-2011-playstation-network-platform-data-breach/ [Accessed 07-03-2020]

ICO. (09-07-2019). *Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach.* From: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/. [Accessed 25-06-2020]

ITSecurityGuru. (23-09-2016). *Yahoo! hack – Industry reactions.* From: https://www.itsecurityguru.org/2016/09/23/yahoo-hack-industry-reactions/ [Accessed: 01-07-2020]

Keane, J. *Adobe agrees to pay $1 million across 15 states after being hacked in 2013*. From: https://www.digitaltrends.com/computing/adobe-hack-1-million-fine/. Digital Trends. [Accessed 05-06-2020]

Kilgore, T. (30-11-2018). *Marriott's stock sinks after disclosing data breach affecting up to 500 million guests.* Published by Market Watch. From: https://www.marketwatch.com/story/marriotts-stock-sinks-after-disclosing-data-breach-affecting-up-to-500-million-guests-2018-11-30 [Accessed 09-07-2020]

Kim, B., Johnson, K., & Park, S. Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. Cogent Business & Management, 4(1), 1354525.

Kocieniewski, D. (03-10-2013). *Adobe announces security breach*. In: *The New York Times* from: https://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html [Accessed 07-03-2020]

KrebsonSecurity. (03-10-2013). *Adobe to announce source code, customer data breach.* From: https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/ [Accessed 07-03-2020]

KrebsonSecurity. (17-11-2016). *Adobe Fined $1M in Multistate Suit Over 2013 Breach; No Jail for Spamhaus Attacker.* From: https://krebsonsecurity.com/2016/11/adobe-fined-1m-in-multistate-suit-over-2013-breach-no-jail-for-spamhaus-attacker/. [Accessed 05-06-2020]

Krishna, A., & Vibber, K. S. (2017). Victims or conspirators? Understanding a hot-issue public's online reactions to a victim cluster crisis. Journal of Communication Management.

La Monica, P. R. (12-11-2013). *Adobe hacked. Wall Street doesn't care.* Published by: The Buzz. From: https://buzz.money.cnn.com/2013/11/12/adobe-stock-hacking/ [Accessed 09-07-2020]

Libin, C. A. I., & Xiaotong, Z. H. U. (2019). Research on the Image Restoration Strategy of Tourism Destination Identity under the Network Public Opinion Crisis based on SCCT: Taking the Incident of Disfigurement in Lijiang as an Example. Tourism and Hospitality Prospects, 3(1), 21-42.

Lien, T. (23-07-2014). *Sony agrees to $15M settlement in 2011 data breach class action*. Published on Polygon. From: https://www.polygon.com/2014/7/23/5931793/sony-2011-data-breach-class-action-lawsuit [Accessed 08-03-2020]

LogicMonitor. (13-12-2017). *Cloud Vision 2020: The Future of the Cloud.* From: https://www.logicmonitor.com/resource/the-future-of-the-cloud-a-cloud-influencers-survey/?utm_medium=pr&utm_source=businesswire&utm_campaign=cloudsurvey [Accessed 04-03-2020)

Marriott. (30-11-2018[a]). *Original Notice from November 30, 2018*. From: http://starwoodstag.wpengine.com/wp-content/uploads/2019/05/us-en_First-Response.pdf. [Accessed 09-05-2020]

Marriott. (30-11-2018[b]). *Marriott Announces Starwood Guest Reservation Database Security Incident.* From: https://marriott.gcs-web.com/news-releases/news-release-details/marriott-announces-starwood-guest-reservation-database-security. [Accessed 09-05-2020]

Marriott. (04-01-2019). *Marriott Provides Update on Starwood Database Security Incident.* From: https://news.marriott.com/news/2019/01/04/marriott-provides-update-on-starwood-database-security-incident#:~:text=Marriott%20Provides%20Update%20on%20Starwood%20Database%20Security%20Incident,-January%204%2C%202019&text=Marriott%20today%20is%20providing%20an,company%20on%20November%2030%2C%202018. [Accessed 09-05-2020]

Marriott. (09-07-2019). *Marriott International Update on Starwood Reservation Database Security Incident.* From: https://news.marriott.com/news/2019/07/31/marriott-international-update-on-starwood-reservation-database-security-incident. [Accessed 09-05-2020]

Mattila, A. S. (2009). How to handle PR disasters? An examination of the impact of communication response type and failure attributions on consumer perceptions. Journal of Services Marketing.

Mayring, P. (2004). Qualitative content analysis. A companion to qualitative research, 1(2004), 159-176.

McDonald, L., & Härtel, C. E. (2000). Applying the involvement construct to organisational crises (pp. 799-803). Faculty of Business & Economics, Monash University.

McMillan, R. (02-12-2018). *Marriott's Starwood missed chance to detect huge data breach years earlier, cybersecurity specialists say.* From: https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659. The Wall Street Journal. [Accessed 20-06-2020]

Menn, J., Finkle, J. & Volz, D. (18-12-2016). *Yahoo security problems a story of too little, too late*. From: https://www.reuters.com/article/us-yahoo-cyber-insight/yahoo-security-problems-a-story-of-too-little-too-late-idUSKBN1470WT [Accessed 19-05-2020]

Mitroff, I. I., Shrivastava, P., & Udwadia, F. E. (1987). Effective crisis management. Academy of Management Perspectives, 1(4), 283-292.

Moynihan, D. P. (2009). The network governance of crisis response: Case studies of incident command systems. Journal of Public Administration Research and Theory, 19(4), 895-915.

NBC. (22-09-2016) Yahoo Says 'State-Sponsored Actor' Hacked 500M Accounts. From: https://www.nbcnews.com/tech/tech-news/your-yahoo-account-was-probably-hacked-company-set-confirm-massive-n652586 [Accessed 02-02-2020]

Nohe, P. (22-03-2019). Autopsying the Marriott Data Breach: This is why insurance matters. From: https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ [Accessed 25-05-2020]

Nolter, C. (23-12-2016). *Why Yahoo!'s Latest Breach Is More Serious Than Its Previously Disclosed One*. Published by The Street. From: https://www.thestreet.com/investing/stocks/yahoo-shares-fall-as-company-discloses-another-one-billion-accounts-were-hacked-13926474 [Accessed 09-07-2020]

OAIC[10]. (01-06-2015). *Adobe Systems Software Ireland Ltd: Own motion investigation report.* From: https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/adobe-systems-software-ireland-ltd-own-motion-investigation-report/ [Accessed 08-03-2020]

O'Flaherty, K. (11-03-2019). Marriott CEO Reveals New Details About Mega Breach. From: https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#50c97dac155c [Accessed 24-05-2020]

Oleinik, A. (2011). Mixing quantitative and qualitative content analysis: Triangulation at work. Quality & Quantity, 45(4), 859-873.

Pauli, D. (17-08-2015). *Adobe pays USD 1.2M plus settlements to end 2013 breach class action*. From: https://www.theregister.co.uk/2015/08/17/adobe_settles_claims_for_data_breach/ [Accessed 08-03-2020]

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. Academy of management review, 23(1), 59-76.

Perlroth, N. & Goel, V. (28-09-2016). *Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say*. From: https://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html. The New York Times.[Accessed 16-05-2020].

Picchi, A. (15-10-2019). *How to get up to $358 in the Yahoo data breach settlement* by CBS News. From: https://www.cbsnews.com/news/yahoo-data-breach-settlement-how-you-can-get-up-to-358-in-the-yahoo-data-breach-settlement/ [Accessed 08-03-2020]

Ponemon Institute. (04-2019). The Fourth Annual Study on: The Cyber Resilient Organisation

[10] Office of the Australian Information Commissioner of the Australian Government

Ponemon, L. (23-07-2019). *What's New in the 2019 Cost of a Data Breach Report*. From: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/ [Accessed 04-03-2020]

Pudwell, S. (23-09-2016). *Yahoo data breach: Industry reaction and analysis*. From: https://www.itproportal.com/news/yahoo-data-breach-industry-reaction/ Published by ITProPortal. [Accessed 01-07-2020]

Ramakrishna, A. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. Journal of Information Privacy & Security, 8, 33–56

Reuters. (15-12-2016). *Here's How Much Yahoo Shares Are Dropping After Latest Hack Reveal*. Published by Fortune. From: https://fortune.com/2016/12/15/yahoo-shares-hack/ [Accessed 09-07-2020]

Scheerens, J., & Creemers, B. P. (1989). Conceptualizing school effectiveness. International journal of educational research, 13(7), 691-706.

Smits, R. (2015). The Crisis Response in Europe's Economic and Monetary Union: Overview of Legal Developments. Fordham Int'l LJ, 38, 1135.

Sisco, H. F., Collins, E. L., & Zoch, L. M. (2010). Through the looking glass: A decade of Red Cross crisis response and situational crisis communication theory. Public Relations Review, 36(1), 21-27.

Stempel, J. (09-04-2019). *Yahoo strikes $117.5 million data breach settlement after earlier accord rejected*. By Reuters. From: https://www.reuters.com/article/us-verizon-yahoo/yahoo-strikes-117-5-million-data-breach-settlement-after-earlier-accord-rejected-idUSKCN1RL1H1 [Accessed 08-03-2020]

Symanovich, S. (15-09-2018). *What is a security breach?* Norton. From: https://us.norton.com/internetsecurity-privacy-security-breach.html [Accessed 06-03-2020]

Trautman, L. J., & Ormerod, P. C. (2016). Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. Am. UL Rev., 66, 1231.

Turner, B. A. (1976). The organizational and interorganizational development of disasters. Administrative science quarterly, 378-397.

Van de Water, D. (2020). Air Crash-Communication. Available on: https://drive.google.com/file/d/12q0KE-Rb1EAdxSE6WIApH1Tch0aw6UT5/view?usp=sharing

Volodzko, D. (04-12-2018). Marriott Breach Exposes Far More Than Just Data. From: https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#7b5421c26297 [Accessed 25-05-2020]

Wang, P., & Park, S. (2017). Communication in Cybersecurity: A public communication model for business data breach incident handling. Issues in Information Systems, 18(2), 136-147

Way, B., Khan, F., & Veitch, B. (2013). Is reputational risk quantifiable. In The International Conference on Marine Safety and Environment (IMSE 2013), Kuala Lumpur, Malaysia.

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. Psychological review, 92(4), 548

Welch, C. (07-11-2013). *Over 150 million breached records from Adobe hack have surfaced online* From: https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online [Accessed 08-03-2020]

Whitney, L. (29-10-2013). *Adobe hack attack affected 38 million accounts* From: https://www.CNET.com/news/adobe-hack-attack-affected-38-million-accounts/ [Accessed 26-05-2020]

Woodrum, E. (1984). Mainstreaming Content Analysis in Social Science: Methodological Advantages, Obstacles, and Solutions. Social Science Research, 13(1), 1.

Yahoo. (22-09-2016[a]). *An important message about Yahoo user security*. From: https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security Written by CISO Bob Lord. [Accessed 24-05-2020]

Yahoo. (22-09-2016[b]). *Yahoo Security Notice September 22, 2016.* From: https://help.yahoo.com/kb/sln28092.html [Accessed 24-05-2020]

Yahoo. (14-12-2016). *Yahoo Security Notice December 14, 2016.* From: https://help.yahoo.com/kb/SLN27925.html [Accessed 24-05-2020]

Yahoo Finance. (n.d.[a]) Adobe Inc. (ADBE). From: https://finance.yahoo.com/quote/ADBE/history?period1=1373587200&period2=1386806400&interval=1d&filter=history&frequency=1d [Accessed 09-07-2020]

Yahoo Finance. (n.d.[b]) Marriott International, Inc. (MAR). From: https://finance.yahoo.com/quote/MAR/ [Accessed 09-07-2020]

Zhang, B., Kotkov, D., Veijalainen, J., & Semenov, A. (2016, September). Online stakeholder interaction of some airlines in the light of situational crisis communication theory. In Conference on e-Business, e-Services and e-Society (pp. 183-192). Springer, Cham.

Zorz, M. (30-11-2018). *Industry reactions to the enormous Marriott data breach.* Published by HelpNetSecurity. From: https://www.helpnetsecurity.com/2018/11/30/marriott-data-breach-reactions/ [Accessed 01-07-2020]

IX Annexes

Annex 1 – Content analysis codebook for strategy assessment

For use during the content analysis based on Coombs Situational Crisis Communication Theory (SCCT)(2007)

Research Question:

''What constitutes an effective communication response to cybersecurity breaches?''

Sub-questions to which this codebook applies:

1. *To what extent can the crisis communication efforts in the cases be deemed theoretically adequate?*[11]
2. *To what extent can the cases be compared in terms of the theoretical adequateness of their crisis communication efforts?*

Unit of Analysis: Paragraphs

Code	**Category**	**Definition**	**Indicators & Strategies** **(*type of statement made by organisation)***
1	Base response[1]	The organisation provides victims with instructions on how to act during the crisis, Expresses empathy and informs the victims of corrective actions	Statement providing information about the crisis / its effects (Crisis information) Or Statement providing instructions for victims how to act during and following the crisis (Crisis information) Or Statement expressing empathy for the victims (Display of Empathy / Care Response) Or Statement regarding corrective action and how the organisation aims to resolve the crisis or prevent another one

[11] See the Theory and Methods chapters for a full explanation

			(Corrective Action / Care Response)
2	Deny[2]	The organisation tries to deny its own blame and escape blame attribution through various means including denying the existence of the crisis or aspects of the crisis.	Statement attacking the actor that attributes blame to the organisation. (Attack the accuser) Or Statement denying the existence of the crisis or an aspect of the crisis. (Denial)[2] Or Statement trying to shift the blame for the crisis to an actor outside of the organisation[3] (Scapegoat)
3	Diminish	The organisation tries to minimize the perceived damage as a result of the crisis	Statement claiming there was nothing the organisation could have done to prevent the crisis or that the organisation never intended to do harm (Excuse) Or Statement claiming that actions leading to the crisis were for the right cause or that the damage is minimal in comparison to what is saved (Justification)
4	Rebuild	The organisation tries to rebuild its reputation and the trust stakeholders have in it	Statement regarding compensation for the victims or stakeholders (Compensation) Or Statement containing an apology from the organisation, a statement of regret for the crisis and/or a request for stakeholders to forgive the

			organisation[3] (Apology)
5	Bolstering[4]	The organisation tries to bolster its image by praising efforts and qualities before and during the crisis.	Statement praising the organisations qualities and good works before, during or after the crisis[4] (Reminder) Or Statement praising the stakeholders for their actions before, during or after the crisis (Ingratiation) Or Statement emphasizing the negative effects of the crisis for the organisation and the difficult nature of dealing with the crisis (Victimage)

Coding rules

General coding rules

- Units of Analysis that contain more than one indicators for different categories will be simultaneously coded under all these different categories.
- In order to provide overview, each category and its indicators will be linked to a different colour. This colour will, in turn, be used during the coding process to highlight indicators for different categories within a unit of analysis. The legend explaining which colour is linked to which category will be situated underneath each coding scheme and in each coded document.
- In order to guarantee objectiveness and reliability throughout the coding process, an indicator must be explicitly present. Implicit statements that are not guided by a coding rule will not be coded.
- Names and general company information listed at the bottom of the statement after its conclusion will not be coded.
- Sentences announcing a coming paragraph without content themselves will not be coded, however introductions directly leading to a quotation will be coded under the same indicator as the quote as these introductions are directly linked to the content of the quotes following them.
- Titles will not be coded as they carry no inherent content.
- The questions guiding the content in a FAQ-style statement will not be coded.
- A paragraph is defined as any text separated from another by a distinct space. In regular statements this separation can take the form of a singular white line, in FAQ-statements an answer to a question is regarded as a singular paragraph. Furthermore, bullet points or numbered statements falling under the same header such as *''Measures Taken''* are

considered a singular paragraph. However if such statements are separated by different headers they are considered separate paragraphs.

Category- and strategy-specific coding rules

[1]Base response

- If an organisation engages in self-promotion (For example: "use our … tool in order to minimize damage), it will be coded as Base response as long as it serves to resolve the crisis or minimize its consequences.
- Sentences that function as an introductory statement (for example: "we will be doing the following") will be coded as 'Base response*'* in the form of corrective action. As such they fall under the same indicator as the points following them.
- In cases where it is uncertain whether there is a crisis or not, a statement claiming signals of a crisis are being investigated to determine if a crisis is present will not be coded as *Corrective Action* but as *Crisis Information* as they only indicate the fact an organization is looking into a potential crisis not that it is addressing a current one.
- In cases where the existence of a crisis is already confirmed, statements regarding further investigation into the incident *are* coded as *Corrective Action* as in this stage the organization is actively trying to resolve the crisis by investigating it.

[2]Denial

- Whenever an organisations denies existence of the crisis or denies an aspect of the crisis, it will be coded as an instance of *'Denial'* whether the denial was rightful or not. The rightfulness of employed strategies will instead depend on the aspects of the crisis and will thus only be assessed after the coding process.
- Instances will only be coded as *'Denial'* if they are an initial denial dealing with disputed aspects of the crisis, updates stating that initially acknowledged aspects of the crisis no longer pose a risk will be coded as *'Crisis Information'* as it does not deny the previous truthfulness of the aspect but simply provides information on the current state of the aspect.

[3]Scapegoat

- Following SCCT, A scapegoat approach will be coded within the '*Deny'*-category if the organisation identifies an external actor to which it attributes the crisis or a part of the crisis without providing clear evidence of the actor's involvement.

[4]Bolstering

- A reminder of good works and qualities of the organization will only be coded as an indicator under the '*Bolstering*'-category if it expressively stresses positive aspects regarding the organizational pre-crisis reputation, actions taken during the crisis, engages in self-glorification or if positive words unnecessarily are used to describe actions or qualities. Indirect statements, such as "we are working with the relevant authorities ensure everything is handled well" are not coded as '*Bolstering'* as they signify corrective action and will thus be coded as a '*Base-response'* indicator. When such a statement is supplemented with an unnecessary positive adjective such as ''we are working *diligently*..'' the adjective is coded as an instance of bolstering.
- While Bolstering may occur in instances describing an ongoing process, it cannot occur in describing actions that still need to be performed, as those are considered promises, and should thus be coded as Base response in the form of corrective action.
- Bolstering through the use of unnecessary adjectives will not be coded under the '*Bolstering'* category if the adjective in question describes an action taken unrelated to the crisis.

Annex 2 – Thematic comment analysis codebook for public reaction assessment

For use during the Thematic Content Analysis

Dennis van de Water

Research Question:

''To what extent can corporate communication response to cybersecurity breaches be deemed adequate?''

Sub-questions to which this codebook applies:

1. *To what extent can the theoretically adequate strategies be validated by the outcome?*

Unit of Analysis: Comments

Code	Description/Indicator
Positive	An all-round positive statement towards the company is outed in the comment The company, or its actions, are defended in a comment, for instance against other commenters The comment expresses sympathy and understanding for the company and the crisis
Neutral	A comment is made that addresses both good and bad aspects of the company and does not lean in any particular way. A comment is made that does not concern the company, only security and breaches in a more general sense A non-related comment or response is made
Negative	A comment is made expressing negative feelings towards the company A comment is made replying negatively on a positive comment A comment is made claiming to not use the company or its services anymore

Coding rules

- A comment can only be coded under one category at a time
- Duplicate comments will not be coded
- Different comments from users that posted before will be coded as long as their contents differ from the earlier comments
- Obvious sarcasm in comments is assessed and coded as the indicated intention behind the comment
- Replies on comments are coded as their own comment