Copyright © 2023, Emerald Publishing Limited. This author accepted manuscript is deposited under a Creative Commons Attribution Non-commercial 4.0 International (CC BY-NC) licence (https://creativecommons.org/licenses/by-nc/4.0/). This means that anyone may distribute, adapt, and build upon the work for non-commercial purposes, subject to full attribution. If you wish to use this manuscript for commercial purposes, please contact permissions@emerald.com (see: https://www.emeraldgrouppublishing.com/publish-with-us/author-policies/our-open-research-policies#green).

Emerald Information Technology & People

How TalkTalk did the walk-walk: Strategic reputational repair in a cyber-attack

Journal:	*Information Technology & People*
Manuscript ID	ITP-08-2022-0589.R4
Manuscript Type:	Article
Keywords:	Risk < Theoretical concept, Strategy < Management practices < Practice, Decision making < Phenomenon, Information strategy < IT/IS management < Practice, IT strategy < IT/IS management < Practice, Management practices < Practice

SCHOLARONE™
Manuscripts

How *TalkTalk* did the *walk-walk*: Strategic reputational repair in a cyber-attack

Abstract

Purpose — Cyber-attacks that generate technical disruptions in organisational operations and damage the reputation of organisations have become all too common in the contemporary organisation. This paper explores the reputation repair strategies undertaken by organisations in event of becoming victims of cyber-attacks.

Design/methodology/approach — Developing our contribution in the context of the internet service providers' industry, we draw on a qualitative case study of TalkTalk, a British telecommunications company providing B2B and B2C internet services, which was a victim of a 'significant and sustained' cyber-attack in October 2015. Data for the enquiry is sourced from publicly available archival documents such as newspaper articles, press releases, podcasts, and parliamentary hearings on the TalkTalk cyber-attack.

Findings — Our findings suggest a dynamic interplay of technical and rhetorical responses in dealing with cyber-attacks. This plays out in the form of marshalling communication and mortification techniques, bolstering image, and riding on leader reputation—which serially combine to strategically orchestrate reputational repair and stigma erasure in the event of a cyber-attack.

Originality — Analysing a prototypical case of an organisation in dire straits following a cyber-attack, the paper provides a systematic characterisation of the setting-in-motion of strategic responses to manage, revamp, and ameliorate damaged reputation during cyber-attacks, which tend to negatively shape the evaluative perceptions of the organisation's salient audience.

Keywords: Cyber-attack, information technology, organisational reputation, stigma, TalkTalk

Introduction

Recent years have seen a marked growth in malicious cyber-attacks that seek to obtain classified information, purloin intellectual property and users' personal details, and generate other disruptive activities (Pinguelo and Muller, 2011). Citing cases of successful cyber-attacks penetrating some of the most secured cyber-security systems, notable attacks include Toyota, Amazon, Vodafone, and the Ukrainian power grid. Thus, reliance on interconnected cyber-technologies, particularly in the management of information systems, poses an existential threat to organisations, their customers, and the wider public, and has come to represent a contemporary risk in today's high-velocity business environment (Żebrowski et al., 2022). When news of a company falling victim to a successful cyber-attack is released to the public, the state of uncertainty characterising the attack also breeds doubts about the company’s ability to protect personal and confidential information. The attacked organisation may therefore become stigmatised and suffer reputational damage, as it receives discrediting judgements from the audiences that its core activities must satisfy.

In light of the negative impact of cyber-attacks on organisational performance and the overwhelming costs they impose on the attacked organisation (Agrafiotis et al., 2018; Haislip et al., 2019; Patè-Cornell et al., 2018), several scholars have sought to provide some valuable insights into various methodological tools for analysing risk, and for designing countermeasures and defence infrastructure that organisations can employ to protect their cyber systems from cyber-attacks (Rios Insua et al., 2021). More recently, a framework for quantitative cyber-risk assessment and management has been developed to pre-empt cyber-attacks (Żebrowski et al., 2022). However, given that cyber-risk has become an inexorable part of contemporary organisations, we ask the enduring question: how do organisations (re)construct their flawed reputation in the event of a cyber-attack? We argue that there is still very little explicit illustration of how organisations may go about dealing with such events, and most importantly how they manage to repair their often-damaged reputation. In our view, such issues may have been side-stepped due to complexity in mapping out the actions and activities undertaken by attacked firms within the contingencies of responding to the threats. Therefore, this study makes an important step towards addressing this lacuna by providing a practical understanding of how organisations could effectively deal with the fallouts from cyber-attacks and the damaging effect on their reputations, which has the potential to extend our understanding of managing cyber-risks in organisations.

To achieve this objective, we focus on a British telecommunications company, TalkTalk, which was a victim of consistent cyber-attacks on the 21st of October 2015. The attacks allowed hackers to gain access to various customer personal data, and the data breach affected 4% of TalkTalk customers, triggering a

£400,000 fine—the largest in the history of the UK Information Commissioner's Office—for failure to address vulnerabilities in its IT security systems. The company's compromised information system left customers in a state of uncertainty, which led to the organisation being stigmatised as unreliable and thereby facing a crisis of reputational damage. In probing the puzzle of reputational repair and stigma erasure in this discrediting predicament, we rely on data sourced from newspaper articles, the company's press releases, parliamentary hearings, and podcasts on the TalkTalk cyber-attack. We then draw on the sociological concept of stigma (Goffman, 1963) as a theoretical frame to inductively explore how the organisation, entangled in a series of cyber-risks and attacks, came to be a target of stigmatisation as a result of its damaged reputation. What is particularly distinctive about our theoretical sensitivity to *stigma*, however, is its usefulness in capturing the relationship between the reactive social evaluations underpinning reputation and the survival of an organisation dealing with reputational repair. Hence, we draw our analysis explicitly on acts of stigma erasure enacted by the company during the cyber-attack to shore up reputation amongst its customers, regulators, and the wider public. Positioning our arguments at the intersection of the stigma and crisis management literatures, we go on to unpack in fine detail the reputational repair strategies adopted by the company.

Our explication of the set of rhetorical and technical responses adopted by TalkTalk to survive the cyber-attack generates three main contributions. First, while extant research has focused on cyber-security tools that can identify potential threats, develop countermeasures, and manage risks (Paté-Cornell et al., 2018; Żebrowski et al., 2022), we present an important point of departure for understanding how the management of such discrediting events is orchestrated in practice. We provide a systematic characterisation of the setting in motion of strategic responses to manage, revamp, and ameliorate damaged reputation during cyber-attacks, which tend to negatively shape perceptions held about the organisation's salient activities. Second, this study underlines that although image and reputation repair during cyber-attacks may be conceived as a collective organisational action, the organisational leaders' crisis management efforts, in their bid to 'save face', also become critical to the re-construction of organisational reputation. Specifically, the study draws attention to how astute and resilient leadership musters important values that are relevant to undertaking image repair strategies that resonate with the organisational audience in order to redress stigmatising labels. Third, by analysing a prototypical case of an organisation in dire straits following cyber-attacks, and facing a crisis of reputational damage and stigmatisation, we extend the literature on cyber-risk management with a first-hand account that epitomises the actions and activities undertaken to respond to such threats and crisis.

The remainder of the paper is organised as follows. In the next section, we present a brief discussion on cyber-risk, after which the concept of stigma is explored to understand why organisations facing cyber-attacks may become targets of stigmatisation. Next, we explore and complement the literature on stigma management with that of crisis management to delineate some potential reputational and image repair strategies. The following section provides insights into our methodological approach and present a chronological account of the TalkTalk cyber-attack. Next, we provide a detailed description of how the empirical data for the study was sourced and analysed to develop our contribution. The penultimate section explicates our findings from the analytical process. Finally, we discuss our findings and close the paper by delineating the implications of our study for both theory and management practice, paying particular attention to unlocking the dynamics of cyber-risk management and image repair strategies.

Cyber-risk and security

Akin to any other systems that are prone to failure, vulnerabilities in cyber-systems also pose risk to organisations, as they become susceptible to exploitation by malicious users and cyber-criminals (Ransbotham et al., 2016; Warkentin and Willison, 2009). Unleashing this challenging predicament, which imposes overwhelming costs on individuals and organisations (Ekelund and Iskoujina, 2019; Paté-Cornell et al., 2018), the malicious attacker may adopt different methods to compromise cyber-security systems. A widely recognised approach in the literature is when the attacker probes IT systems and firewalls to identify vulnerabilities that could be exploited and delivers malware to compromise the system and steal confidential information in order to victimise the organisation, often demanding a ransom (Al-rimy et al., 2018; Allodi and Massacci, 2017). Given the myriad attack designs employed to penetrate and compromise cyber-systems, the extant literature on cyber-security has provided classifications for cyber-risks in order to build a clear picture of the different patterns of attack. Chakrabarti and Manimaran (2002), for example, approached this classification taxonomically, and, largely focusing on the exploitable vulnerabilities in IT systems, defined four main classifications of cyber-threats, namely DNS hacking, routing table poisoning, packet mistreatment, and denial-of-service (DOS) attacks. Ransbotham and Mitra (2009) extended this knowledge by developing a conceptual model which provides a typological distinction between attacks that are 'targeted' and 'nontargeted', either of which may arise out of a deliberate attempt or reconnaissance activities by the attacker. These varying threats to cyber systems thus raise an important concern about the existential threats of cyber-criminal activities and ways to ensure user safety and protection from such attacks.

In this respect, cyber-security has become a subject of intensive research amongst scholars, who are continuously providing countermeasures, including models and technologies, that will complement efforts to secure cyber networks and database systems and detect risks in order to reduce the likelihood and severity of cyber-attacks (Ransbotham and Mitra, 2009; Sarathy and Muralidhar, 2002). Amongst the widely adopted techniques to assess cyber-risk and design countermeasures is the use of matrices to estimate multiple risks that may compromise cyber-security systems and prioritising the most imminent risks to counter (Żebrowski et al., 2022). Also, Factor Analysis of Information Risk (FAIR) is a widely used method which relies on a combination of algorithms and quantifiable risk factors to estimate cyber-security risk in order to provide a proportionate response (Wang et al., 2020; Wangen et al., 2018). Equally popular in the literature is a technique that involves identifying vulnerabilities in cyber-security systems and sequentially modelling the possible paths that an attacker may adopt to breach the security system—which are widely known as attack graphs or trees (Nandi et al., 2016; Żebrowski et al., 2022). Other risk-mitigating methods, however, employ automated tools that mine cyber-systems to identify, evaluate and caution imminent or ongoing attacks. More recently, the National Institute for Standards and Technology (NIST) has also become a widely used cyber-security risk management tool (Gordon et al., 2020). Nonetheless, some scholars have argued that deriving appropriately comprehensive countermeasures requires both expert insights and analysis of the likelihood and impacts of cyber-attacks (Ceric and Holland, 2019; Żebrowski et al., 2022). As such, recent studies have directed attention to developing exact algorithms to mitigate the multitudes of risks and adopting techniques that combine quantitative risk analysis with expert judgment to develop optimal portfolios of cyber-security countermeasures (Goodall et al., 2009; Nandi et al., 2016; Żebrowski et al., 2022). Other studies have sought to design sophisticated frameworks and cyber-attack simulations that would help to improve response times and eliminate threat (Armenia et al., 202; Spyridopoulos et al., 2013).

Although these cyber-security tools are perceived to be convenient for understanding or anticipating the most likely or possible risk within the portfolio of attacks available to cybercriminals and developing improved defensive systems (Wang et al., 2020), there remain contentions about whether these tools are sufficiently robust for protection (Allodi and Massacci, 2017; Cox, 2008), particularly in an era where cyber-attacks have become more complex and the attack modes are more difficult to decipher, thereby rendering the assessment, prevention, and management of cyber-risks very challenging. Despite the painstaking efforts toward addressing cyber-risks, catalysing technological breakthroughs that provide advanced cyber defence systems, incidents of cyber-attacks persist even in the most secured systems (Kemmerer and Vigna, 2002). In this regard, many of today's organisations cannot assume away the threat of organisations becoming victims of cyber-attacks, suffering loss in reputation and eventually being stigmatised for failure to protect the valuable information of their customers and other stakeholders (Kamiya et al., 2021). Repairing reputational damage during such attacks is critical, beyond technically containing the attack, meaning that cyber-security risk issues are not only the prerogative of technology experts but also of management (Al-rimy et al., 2018; Haislip et al., 2021; Higgs et al., 2016). In this regard, there is a compelling need to understand how reputational repair in the event of a cyber-attack can be strategically designed to protect organisational reputation and erase stigma in order to maintain competitive position in the market. Against this background, we now explore the concept of *stigma* (Goffman, 1963) as a coherent theory to delineate how the image and reputation of organisations involved in cyber-attacks may come to be blemished and the repair strategies to survive such conditions.

Organisational stigma

Tracing the etymology of the word ‘stigma’ takes a curious mind on a retrospective journey to an era where the word was used to identify bodily marks such as cuts, scars, or burns. These marks were often associated with individuals with lower social status, such as slaves, traitors, criminals, those with physical deformities, and even migrants (Isaakyan and Triandafyllidou, 2019; Pescosolido and Martin, 2015). This allegorical use of the word ‘stigma’, however, resonated with some scholars who have found relevance for the word as a concept to explore the emergence and enactment of identities that are perceived by some social audiences as deviating from the expected social identity (Ashforth and Kreiner, 1999; Sutton and Callahan, 1987; Goffman, 1963). Thus, the term has come to represent a devaluation of identity in the form of discrediting predicaments, physical abnormalities, social disapproval, moral suspicions, or prejudice (Hudson, 2008; Paetzold et al., 2008; Wang et al., 2021; Wiesenfeld et al., 2008). Goffman (1963), for example, provided a fine articulation of this concept, which has remained influential in the contemporary study of stigma. According to Goffman, society attributes labels to individuals with distinctive characteristics, some of which are deeply discrediting. In this regard, stigma is conceived as that which devalues "a whole and usual person to a tainted, discounted one” (Goffman, 1963, p. 3). Further providing a comprehensive characterisation of stigmatising conditions, Goffman identified three categories of stigma: (a) stigma associated with physical deformities, such as missing a limb or having an illness; (b) stigma accorded to an individual’s conduct, influenced by beliefs and vices, such as being a drug addict or having a mental disorder; and (c) stigma related to ‘tribal’ factors such as gender, religion, and ethnicity.

Although this Goffmanian sentiment on stigma was conceived within the domain of individual social relationships, his arguments reserve a core set of general understanding that can be applied to the organisational. Thus, recent studies have established a fine link between Goffman's conceptualisation of human stigma and organisations that are characterised by flaws to establish how stigma becomes a useful theoretical concept that can travel easily across levels of analysis. Devers et al. (2009, p. 157), for example, defined organisational stigma as “a label that evokes a collective stakeholder group-specific perception that an organisation possesses a fundamental, deep-seated flaw that deindividuates and discredits the organisation”. Thus stigmatisation, which symbolises taint on organisational reputation and legitimacy, is a socially constructed label which indicates that an organisation is flawed or undeserving of approval (Devers et al., 2009; Hampel and Tracey, 2019; Tracey and Phillips, 2016). Thus, the underlying assumption here is that just as individuals are stigmatised by their perceived social audiences, organisational activities are also evaluated by organisational audiences such as customers, regulators, and the wider public (Wang et al., 2021; Wiesenfeld et al., 2008). Highlighting the stigmatising conditions of organisations, Hudson (2008) argued that organisational stigmas can be event-related, occurring as a result of an infraction made by the organisation itself. Here, inappropriate patterns of action change how external audiences perceive the organisation, thereby leading to stigmatisation. Also, core-related stigmas may arise when external entities perceive the presence of an engrained defect in the way an organisation conducts its operations. Thus, an organisation may be stigmatised based on the behaviour of its leader(s), by virtue of the setting or value networks in which they operate, or due to the organisation’s involvement in unethical activities (Boakye et al., 2022a; Kvåle and Murdoch, 2021; Durand and Vergne, 2015; Wiesenfeld et al., 2008). Organisations that do not fall within the stigma domain tend to avoid interactions with those that are stigmatised due to the fear of ‘stigma transfer’ (Hudson and Okhuysen, 2009).

On this basis, we observe that the social-psychological concepts of stigma, organisational reputation and image are mutually related in terms of their practical exposition. As Rindova et al. (2005) aptly argued, organisational reputation consists of multiple stakeholders' perceived evaluations of the organisation on a specific attribute, and its prominence in the specific organisational field. Therefore, the concept of organisational reputation generally encompasses the concept of organisational identity or image, which also refers to the perceptions of those who belong to the organisation with respect to the external audience's perceptions about the organisation (Dutton et al., 1994). Organisational reputation thus resides not only in the consensual interpretative schemas of its members, but also those of the perceived audiences whom their activities are expected to satisfy (Carmeli and Tishler, 2005). These audiences enact relationships and evaluate salient organisational activities in ways that cumulatively shape the perceived image they hold about the organisation (Gioia et al., 2000; Ravasi and Schultz, 2006;). Therefore, the organisational audience form impressions, which in turn establish the espoused reputation of the organisation (Paetzold et al., 2008; Fombrun et al., 2000). Any discrediting marker that creates a disconnect between impressions formed and actual experiences of the audience therefore has the potential to taint the organisational reputation (Kvåle and Murdoch, 2021; Paetzold et al., 2008). As a result, negative reactions that are triggered among these audiences lead to disengagement, thereby creating a hostile organisational–audience relationship (Pollock et al., 2019). Therefore, stigma markers emerge through the organisational audience's perceptive evaluations, which have direct impact on organisational reputation, image, and identity. Any anomalous event that generates a hostile audience can thus be conceived as a crisis event that has the potential to tarnish the organisational image and reputation and construct stigmatising labels (Coombs, 2007).

Stigma repair and crisis management

In responding to the audiences whose evaluation of organisational activities can problematise organisational reputation and stigma labelling, the extant literature offers some important lines of approach. Prior studies have found that when organisations are entangled in anomalous situations, they attempt to repair their image by providing alternative accounts of the discrediting event and decoupling stigmatising labels from their general activities (Elsbach and Sutton, 1992; Sutton and Callahan, 1987). Also, organisations that embattle what Hudson (2008) labels 'core stigma' adopt a strategy of 'shielding' to conceal or lessen the fallout from stigma (Hudson and Okhuysen, 2009). Other scholars have also argued that organisations attenuate the effect of stigma by using 'straddling' to convey the positivity connected to their activity and 'co-opting' to exploit the stigma to gain attention and resources (Durand and Vergne, 2015; Helms and Patterson, 2014; Paetzold et al., 2008). Altogether, these studies highlight how organisations manage events and core stigmas.

Insights from the literature on crisis management also become instructive in the management of stigma, as both concepts bear practical coherence, particularly during the unfolding moments of discrediting events. In this perspective, the organisational leaders occupy a central position as crisis managers who spearhead efforts to set right the operational errors that led to the crisis and frame the legitimacy of the organisation to its audience (Koehn, 2020; Pearson and Clair, 1998; Wu et al., 2021). Prior research suggests that organisational executives' perceptions and preparedness to commit resources to manage the crisis are the underlying factors that determine whether effective responses can be unleashed to save the organisation (Mitroff et al., 1996; Pearson and Clair, 1998). Also, in designing the response to crisis, Benoit (1997) highlighted key communication strategies for crisis management and image repair, which may take one of five forms: denial of involvement in the crisis, evasion of responsibility, reducing offensiveness, corrective action to repair image, and mortification in the form of accepting responsibility and rendering an apology. Coombs (1998) also classified crisis management based on the underlying intents of the strategies, including defensive strategies, which aim to save the image of the organisation; and accommodative strategies, and which are enacted with the intention to give out relevant information needed to reduce the concerns of the victims. This set of instructive and adjustive mechanisms therefore constitutes an effective approach to dealing with the complexity of safeguarding the organisational image while making the audiences privy to key information to help them adjust to the uncertainty of the situation. As such, efforts are made to shift the potentially negative evaluations towards a more positive perception as the audiences observe the organisation effectively managing the crisis (Desai, 2011; Sturges, 1994). In this regard, the effectiveness of the responses depends on the ability of the organisational leaders to develop contingency plans, identify the nature and locus of the crisis, and determine how best to channel communication to the audience (Coombs and Schmidt, 2000; Kent et al., 2003).

Against this background, we submit that the internet and cyber-related service providers industry presents an organising context that is at constant risk of reputational damage and stigmatisation, as their operations are constantly exposed to cyber threats and attacks (Deloitte, 2020). More importantly, the core activities in this industry are enacted within a value network that is steeped in the "principle of confidentiality and integrity" (Chakrabarti and Manimaran, 2002, p. 13). Thus, failure to protect personal and confidential data of the organisation and its customers not only triggers a contestation of operational competence—which might be due to a singular anomalous event bounded in epochal significance (Hudson and Okhuysen, 2009)—but also leads to reputational damage and engrained stigma markers. Specifically, these IT and telecommunications businesses are at risk of reputational damage and stigmatisation within their ordered interactions with customers, regulators and the wider public. In this respect, we argue that technical capability in managing cyber-attacks may be a necessary condition to surviving in this context but not sufficient to erase the stigma that may scar the attacked organisation, as organisations battling a cyber-attack may fall short of social and regulatory support as well as operational credibility among the wider stakeholders (Boakye et al., 2022b; Hampel and Tracey, 2017; Hudson, 2008). Thus, the everyday organisational experience in this context must be interlaced with the constant design of both technically and socially validated strategies that can be coalesced to provide an effective response to manage the crisis ensuing from a cyber-attack. Such responses require the use of intelligible techniques to influence the ways in which external and internal audiences react to the event in order to break out of the state of crisis, repair damaged reputation, and ensure erasure of stigmatising markers. In the subsequent sections, we draw on these insights from the literature to inform our explication of TalkTalk's strategic responses to its cyber-attack.

Research methods

The research method we employ here is one that draws on an exceptional case study to provide rich insights into a phenomenon and allow for further useful inferences to be drawn (Hampel and Tracey, 2017; Siggelkow, 2007). This approach recognises that managerially relevant knowledge can be acquired from unique organisational realities that are construed in specific events and occurrences (Gibbert, 2008). We were therefore attracted to the case of the TalkTalk cyber-attack, which represents a prototypical case of an organisation that is entangled in a crisis of reputational damage and threat of being stamped with stigmatising labels. More importantly, much as this case allows us to explore how cyber-attack as a discrediting event may lead to an organisation becoming a target of stigmatisation, it also provides a practical diagnosis that is illustrative (Siggelkow, 2007) of how organisations could strategically navigate such crisis to shore up their reputation and image among their audiences. Furthermore, the TalkTalk case seeded several debates and led to new regulatory reforms that would allow the ICO to increase levels of fines for data breaches, as well as legislative instruments to establish stricter controls on the telecommunication and other cyber-related industries (Doward et al., 2015; ICO, 2022a; Parliament, 2016b). We now present a brief overview of the case.

The TalkTalk cyber-attack

TalkTalk is a British company owned by the Telecom Group PLC. Its establishment can be traced to 1995, when Opal Telecoms was created by the Telecom Group to provide fixed line voice services to corporations (TalkTalk Group, 2022). Opal Telecoms was purchased by Carphone Warehouse in 2002 and extended its services by providing both fixed line voice services and internet services to corporate customers. In 2003, TalkTalk was launched as a new consumer telecommunications brand after the Communication Act—

which aimed to spur innovation, encourage competition, and catalyse interoperability in the telecommunications market—was passed by the United Kingdom government (TalkTalk Group, 2022a). Between 2004 and 2006, TalkTalk acquired other broadband service providers to expand its assets and reinforce its operational capacity to introduce competitive offers to its customers. Furthermore, in an effort to cement its status as the biggest supplier of broadband in the UK and strengthen its operational ties with IT customers and the wider public, the company, in 2009, invested in a sponsorship deal for one of the UK's biggest and most popular entertainment programmes, 'The X Factor' (TalkTalk Group, 2022a). In 2010, TalkTalk demerged from Carphone Warehouse and became an independent company, trading on the London Stock exchange as TalkTalk Telecom Group PLC (TalkTalk Group, 2018a). Employing efficient fibre technology to provide an array of low-cost services to its customers, TalkTalk is touted as a leading provider of voice, internet, TV and mobile services to UK homes and businesses, despite its relatively short history. The company currently has over four million broadband customers and controls approximately 96% of fixed-line broadband in UK homes, thus reserving a reputable status within the UK telecommunications industry (TalkTalk, 2018b, 2022b).

The unfortunate event which generated hostile reactions amongst TalkTalk customers, regulators and the public occurred on Wednesday 21st October 2015. What began as difficulties in accessing the company's website, and seemed to be a mere technical issue, turned out to be a dangerous cyber-attack that risked compromising customers' personal details (Johnston, 2015). Despite efforts by the company to take its internal systems offline in order to safeguard customers' data, the cyber-attack was successful (Ahmed and Thomas, 2015). The total number of customers affected by the attack was 569,959, representing 4% of the four million TalkTalk customers (Farrell, 2015; Khomami, 2015b; Rodionova, 2016). Of this number, those whose personal bank details were hacked or compromised totalled 15,656, while 15,000 had their date of birth exposed (Farrell, 2016; Gayle, 2015; ICO, 2016; TalkTalk, 2015e). Also, the company confirmed that it had received a ransom demand from an unidentified person or group who claimed to be responsible for the attack (Khomami, 2015a, 2015b). As news of the attack was made public, TalkTalk faced a crisis of reputational damage and stigmatisation, which led to the company's share price plummeting by 10% (BBC, 2015a; Waller, 2015). The company was also forced to suspend its advertising and X Factor sponsorship for two weeks (Spanier, 2015; Waller, 2015). Given the customer dissatisfaction and public outrage, the UK parliament's Culture, Media and Sport Committee initiated investigations into the attack, inviting Baroness Dido Harding, who was the Chief Executive Officer (CEO) of TalkTalk at the time, to provide evidence on how the attack had occurred and what measures were being put in place to contain the threat (ICO, 2016; Parliament, 2015, 2016a). Also, TalkTalk reported the cyber-attack to the Information Commissioner's Office (ICO), an independent regulatory body set up to enforce information laws in the UK (ICO, 2022b).

TalkTalk's internal investigations, and its collaboration with the Metropolitan Police (MP) to identify the nature and extent of the attack (BBC News, 2015; TalkTalk Group, 2015a, 2015d), revealed that the malware used in the attack was a Distributed Denial of Service (DDOS) attack combined with a Structured Query Language (SQL) attack, which was aimed to collect customers' personal data (Ahmed and Thomas, 2015; ICO, 2016; Parliament, 2015). Generally, such DDOS attacks occur when a significant number of packets are sent into the same network from computers in different locations, with the aim of flooding the network systems and taking them offline (Specht and Lee, 2003). The purpose of the packets is to make identification of the source of the attack particularly difficult. The computers used as means to perform such attacks are generally infected by specific viruses or remotely controlled by intruders. The effect of the DDOS is complemented by SQL attacks, which are designed to penetrate the query language in order to extract data from databases (Specht and Lee, 2003). The DDOS attack in the case of TalkTalk was used by the hackers as a tool of distraction to pursue an SQL injection (Hern, 2016; ICO, 2016). Despite the sophistication in this type of the attack, the hackers only managed to break into the website and not into the core system of the company (TalkTalk Group, 2015b). Therefore, the intruders gained access to steal a limited amount of users' personal data, and later demanded a ransom (Khomami, 2015a; TalkTalk Group, 2015e). Table 1 presents a summary of events characterising the TalkTalk cyber-attack.

--
Insert Table 1 about here
--

It was estimated that the cost of the cyber-attack amounted to £77m and that the company lost about 101,000 customers (Lyons, 2018). According to the ICO, TalkTalk had no excuse for failing to prevent the attack, as the company had not fully encrypted its customer database, even though it was expected to safeguard its customers by resolving the vulnerabilities in its systems (BBC, 2016a; Gayle, 2015; ICO, 2016). On 5th October 2016, the ICO announced that it had fined TalkTalk £400,000—the largest fine in the history of the ICO—for failure to address vulnerabilities in its IT security systems which allowed previous attempts and the current attackers to easily penetrate their system (BBC, 2016a; Hern, 2016; ICO, 2016). The CEO of TalkTalk collaborated willingly with the authorities leading the investigation and promoted a high level of transparency with regard to the operations and measures undertaken by the company. In her efforts to save the company's reputation, Baroness Harding led the charge in reassuring customers by communicating what the company was doing to protect them and educating them on ways to be cyber-security conscious (Parliament, 2015; TalkTalk Group, 2016).

Data sources

In gathering data to unpack this guiding phenomenon presented by the TalkTalk case, we relied on a broad range of webpage archives, including media articles, parliamentary hearings, podcasts, and the websites of TalkTalk and the ICO as sources of data. This type of publicly available archival data has been previously used in similar studies to provide accurate and robust analysis of organisational phenomena (see Aversa et al., 2021; Boakye et al., 2022a). Also, our approach is consistent with the existing protocols on conducting social science research using internet-based data (Arora et al., 2016). We began our data search and selection process by employing *Google* as the primary search engine and applied the following search phrases: (“TalkTalk cyber-attack*” OR “TalkTalk ransomware*” OR “ICO investigations*” AND “TalkTalk” OR “parliamentary inquiry*” AND “TalkTalk” OR “TalkTalk CEO” AND “response*” OR “TalkTalk fine*”). The initial search directed us to five (5) major news portals, namely The Guardian, BBC News, The Mirror, The Independent, and The Financial Times. These online news outlets altogether provided nineteen (19) articles on the TalkTalk cyber-attack between 2015 and 2016. We further accessed the official website of TalkTalk to retrieve twelve (12) press releases and obtained the historical background of the company.

In addition, the search results directed us to the ICO’s website, where one (1) document highlighting the key events during the attack, from 2015 to 2016, was identified. Furthermore, the official link to the UK parliament also appeared in the search results, leading us to retrieve one (1) video recording of Baroness Harding appearing before the Culture, Media and Sport Committee and a parliamentary report on the case. A formal request was sent to the ‘Parliamentary TV’ channel to request access to the hearing, which was held on 15th December 2015. The search further led us to identify a podcast on SoundCloud where Baroness Harding delivered a lecture as part of the University of the West of England's Annual Bolland Lecture Series. Although the purpose of the lecture was not to address issues related to the cyber-attack, questions posed by participants required the Baroness to provide some insightful comments on the crisis. All the audio-visual recordings were transcribed verbatim. Cumulatively, a total of 33 internet-based qualitative data were triangulated to construct an accurate contextual backdrop and chronological narrative of the case.

Data analysis

Following an inductive approach, which allowed us to interactively examine the dataset in tandem with our theoretical readings on stigma and crisis management (Mantere and Ketokivi, 2013), we proceeded with our data analysis in two stages. First, we thoroughly studied the entire dataset to compile an event-history database and build insights needed to construct a whole narrative of the case. We systematically mapped out specific events, actions, reactions, and responses into various analytical contents (see table 2). For instance, the event of the cyber-attack triggered hostile actions by their audience, while TalkTalk reactively adopted communication techniques to address the public and to offer safety measures to help protect their data, which was well received by their customers. Delving into an unfolding crisis that was chronologically marked by a series of critical events and responses, we were prompted to adopt the 'temporal bracketing' technique (Langley et al., 2013) to collapse the dataset into phases, namely the *attack phase* and the *reputational repair phase*. However, after discussing and comparing emerging ideas on TalkTalk's response to the crisis, we identified that there was a contemporaneous execution of both technical responses to contain the attack and reputational repair strategies during the crisis: hence, this approach was less useful. Progressing with our new understanding, concerns surfaced about the reliability of our initial inferences drawn from the case (Cornelissen et al., 2014; Wang et al., 2021). To address this, we invited involvement from a certified crisis management professional and a cyber-security expert, who examined the dataset to refine our understanding and explanation of the data. Drawing on their insights, we proceeded to re-position our analytical frames to view the case as one which is characterised by a cumulative set of transient crisis events draped in durationally indivisible strategic responses. This helped us to vividly capture the overall dynamics of how the cyber-attack and the orchestration of strategic reputational repair responses by the company, as well as the CEO as a 'protagonist', unfolded (Kvåle and Murdoch, 2021).

Considering the potential for spontaneous and non-deliberate actions of the company and CEO to elastically stretch the analysis beyond our adopted theoretical frames (Sutton and Callahan, 1987), the analysis progressed to the second stage where we turned our gaze to what responses and countermeasures were undertaken, the outcomes of those actions, and the changing patterns of evaluations enacted by the organisational audiences. Thus, we were able to zoom in on how the specific stigma and image repair actions were strategically enacted to counter negative assertions about the company in order to protect or save its reputation. Further situating our analysis at the intersection of the crisis management, stigma and reputational repair literature, we developed a mid-range explanatory theme to label the identified dynamics of reputational repair strategies that came to influence the patterns of evaluations espoused by TalkTalk's audiences, including *marshalling communication and mortification techniques, bolstering image,* and *riding on leader reputation*. By casting a re-reading mechanism on the insights from the analytical process, we realised we had reached the point of theoretical saturation where no new patterns of repair strategies could be identified and labelled (Hampel and Tracey, 2019). Given that these themes cumulatively captured strategies at play to repair reputation and erase stigma during the attack, they were finely aggregated and stylised: *How TalkTalk did the walk-walk*.

Insert Table 2 about here

Before we present the core findings, we wish to reflect on our analytical process. The analysis revealed some practical insights which suggest that reputational repair strategies are mapped out and made sense of within the emerging sequence of responses designed to manage and erase stigma. Thus, the retrospective case analysis employed to unpack the reputational repair strategies of TalkTalk underscores the significance of real-time meaning-making actions, social construction of meaning through communication, and leader-driven collective commitments to (re)frame public evaluations of organisations' core activities in reputation-damaging events. Interestingly, successfully shaping the perceptive evaluations of an organisation in reputational crisis does not solely depend on mere communications and figure representations that trigger favourable emotional contagion among audiences, but also that of deliberate efforts made to 'walk the talk'.

How TalkTalk did the walk-walk

The in-depth analysis of the dataset revealed that in addition to the disruptions in operations and the financial cost in containing the attack and honouring its fines, TalkTalk faced an even greater challenge of losing the trust of customers, business partners, and other stakeholders. When news of the attack was made public, the loss of confidential information impelled customers to contemplate the ability of the company to protect their personal data and interests. This damage to the organisational image and reputation also led other organisations to disengage from collaborating with TalkTalk to avoid the transfer of the stigmatising markers (Hudson and Okhuysen, 2009; Kvåle and Murdoch, 2021), notably their marketing deal in the X Factor sponsorship. A technology correspondent for the BBC, Rory Cellan-Jones, succinctly captured this concern:

> For TalkTalk, the cost to its reputation is likely to be very serious. Now it is going to have to reassure its customers that its security practices are robust enough to regain their trust (BBC, 2015a).

As the cyber-attack led to a breakdown in TalkTalk's operations, thereby causing negative evaluations, its primary audience—the customers—began to develop hostilities towards the company, as it had failed to meet their expectations. Some news articles reported the views of concerned TalkTalk customers who expressed displeasure and criticism. The following quotes illustrate these concerns:

> I don't know if I should cancel my account with them so that I'm not a victim of further attacks, or if I should stay with them now that the damage is done, and they may be able to rectify anything that could happen to me as a result (BBC, 2015c).
>
> I'm very concerned that my bank details may have been taken but didn't want to have to change all bank details. It's a lot of hassle doing so but now it looks like I will have to after the disgusting customer service. I was angry enough being on hold that long but to then be cut off is terrible (Johnston, 2015).

The incident further attracted the attention of regulators, specifically the ICO and the UK's parliamentary committee on Culture, Media, and Sport, to conduct investigations. The ICO investigations, for instance, concluded that TalkTalk had "failed to take appropriate measures against the unauthorised or unlawful processing of personal data" (ICO, 2016), thereby leading to their issuance of a £400,000 fine to the company. In a statement issued by the ICO after its investigations, it was reported that:

> TalkTalk had failed to remove, or otherwise make secure, the webpages that enabled the attackers to access the underlying database. The investigation also highlighted that the

> database software in use was outdated […]. For no good reason, TalkTalk appears to have overlooked the need to ensure it had robust measures in place despite having the financial and staffing resources available (ICO, 2016).

Unpacking how TalkTalk designed and executed its reputational repair strategies to help reshape these evaluations of the company's core activities, we first present a graphical overview of the cyber-attack as a crisis event and the induced responses identified from our data in Figure 1. The figure highlights that the occurrence of the cyber-attack was rooted in vulnerabilities in TalkTalk's cyber-security systems. The attack triggered a series of crisis events in which TalkTalk experienced a breakdown in its operations, plummeting stock value, diminishing competitive advantage, regulatory scrutiny and fines, and the loss of nearly 101,000 customers. This led to negative assertions about the company's core operations, thereby impairing its reputation. As a result, hostile evaluations including criticism and distrust were developed and enacted by TalkTalk's customers, the public, and regulators. The crisis therefore created a discrediting marker which disconnected the perceived evaluations of the stakeholders from their actual experience with the company, thereby rendering TalkTalk a target of event-related stigmatisation (Hudson, 2008). These unfolding conditions then induced the company's strategic design of both technical responses to contain the attack and image repair activities to shore up its reputation among its audiences (Zavyalova et al., 2012). A fine-grained explication of how TalkTalk executed these strategic responses is now presented.

--
Insert Figure 1 about here
--

Marshalling communication and mortification techniques

Erasing the stigma marker as an internet service provider operating an inefficient cyber-security system had become a daunting objective for TalkTalk to achieve. The company acknowledged that getting a measure of the attack and designing appropriate countermeasures and communication techniques to reinstate confidence in its audiences needed to be at the fore of its scale of operational objectives. Thus, immediate efforts were made to identify the nature of the attack, after which the company took down its website, replacing it with a holding page (BBC, 2015a; ICO, 2016). As being open and transparent about what was happening, collaborating with regulatory bodies, and giving out frequent updates to the public tend to be significant techniques when containing a crisis (Coombs and Schmidt, 2000; Desai, 2011), TalkTalk adopted various communication channels, predominantly press releases, to inform its customers about the cyber-attack (see, for example, TalkTalk, 2015g, 2015i). Appearing on the BBC news channel a day after the attack, the CEO of the company, Baroness Dido Harding, addressed customers, saying:

> The attack happened yesterday. We brought down all our websites yesterday lunchtime and have spent the last 24 hours investigating with the metropolitan police and various security advisors to understand the scale of the attack and what had actually happened. And we've taken the decisions this evening, although it's too early to know what has been attacked and what data has been stolen, that we wanted to take the precaution of contacting all of our customers as fast as possible. Hence […] why I am appearing on the BBC News channel tonight as one of the fastest ways of reaching all of our customers [...]. Potentially [the attack] could affect all of our customers, which is why we are [also] contacting them all by email and we will write to them as well. (BBC, 2015).

TalkTalk had at this initial stage assumed a worst-case scenario that all the personal data relating to their customers could have been compromised (Khomami, 2015b). Their communication strategy to keep customers informed about the attack and its scale served as a way to establish an interactional relationship in which the audiences perceived the company to be keen on helping to protect their interests. Also, in order to retain public confidence in the face of this discrediting attack, this approach underpinned efforts to alter the audiences' negative evaluation of the company's capability to protect customers. Furthermore, in its subsequent press release, the company provided details on the potential data breach, actions being taken to contain the attack, and what its customers could do to protect themselves, as well as details of helplines and cyber-security awareness information. An excerpt from the statement reads:

> Today […] a criminal investigation was launched by the Metropolitan Police Cyber Crime Unit following a significant and sustained cyberattack on our website yesterday. That investigation is ongoing, but unfortunately there is a chance that some of the following data has been compromised: names, addresses, date of birth, phone numbers, email addresses, TalkTalk account information, credit card details and/or bank details. We are continuing to

> work with leading cybercrime specialists and the Metropolitan Police to establish exactly what happened and the extent of any information accessed (TalkTalk, 2015a).

Here, the company strategically made symbolic references to the MP as an institution whose credibility would resonate well with its customers and the wider public. By highlighting its collaboration with the MP in conducting investigations into the attack, TalkTalk provided reassurance that its technical responses to the attack were reliable. It therefore reactively provided responses to fill the reputational vacuum that had led to the formation of negative evaluations, which were degenerating into stigmatising markers. The company adopted this approach of intense communication and regulator-backed information delivery to its customers on actions being taken in order to re-shape the discrediting frames which were directly shaping the perceptions of its customers and the wider public. This strategy was also reinforced in a series of apologies, which were rendered through the CEO:

> On behalf of everyone at TalkTalk, I would like to apologise to all our customers. We know that we need to work hard to earn back your trust and everyone here is committed to doing that (TalkTalk, 2015f).

Similar comments we made when Baroness Harding appeared before the UK parliament's inquiry to provide a factual account of how and why the cyber-attack had occurred. The Baroness began her response to the first question by saying:

> Before I directly answer your question, Chairman, could I just begin by apologising again to all of TalkTalk's customers for the concern and the inevitable uncertainty that this event has caused all of them? (Parliament, 2015).

From this set of statements, TalkTalk demonstrated an acceptance of responsibility for not being able to pre-empt the attack, given that it had previously experienced such threats (ICO, 2016). This technique to acknowledge the company's vulnerable position in the interactional relationship with its audiences served as a sentimental tool for influencing the underlying evaluation schemas of the customers and the wider public. As such, the company intervened in the ostensibly descriptive crisis events that had sparked the hostile reactions through emotional persuasions to constitute a web of opposing subjectiveobjective evaluations. Again, TalkTalk exhibited its defensive skill by highlighting the pervasiveness of cyber-threats as well as the company's own evaluations of the event. The following quotes by Baroness Harding observed:

> I am not in any way pretending that I think TalkTalk is perfect, and clearly there is a lot more that we can do and will do going forward. But I would just say that we are far from alone in having had cyber-attacks. The PwC report done for BIS showed that nine out of 10 large companies have been the victim of a successful cyber-attack in the course of the last 12 months. GCHQ say that they are dealing with 200 active cyber-attacks every month in corporate Britain. I would love to say that this is just a TalkTalk problem, but I am afraid it isn't. This is something that is much broader…The only way you can be 100% confident that you are not at risk of cybercrime is not to operate in the digital space, and that is the wrong answer (Parliament, 2015).
>
> With the benefit of hindsight, were we doing enough? Well, you've got to say that we weren't and obviously we will be looking back and reviewing that extremely seriously (Khomami, 2015b).

TalkTalk's efforts to characterise the attack as a pervasive challenge in the industry enabled it to dispose its audience to perceive TalkTalk as a victim, rather than negatively assessing the company as an incompetent operator for allowing such mishap to occur (Mishina et al., 2012). This therefore created a mechanism for the company to perpetually hold onto its subtle control over the perceptual evaluation patterns of its audiences. As the CEO recounted:

> The one thing that I would not change is being open and honest. We think it saved our company. Our customers tell us, 'We didn't really trust you before, we don't think it is your fault. We don't think we trust you now. We rather admire the fact that you tried to help us in difficult time' (Harding, 2016).

This reflective comment suggests that the communication and mortification strategy enabled TalkTalk to sustain customers' support and trust, as it projected to the audience its thoughtful responses to the crisis and its decision to build a more robust cyber-security system. Thus, carving trust out of this discrediting predicament meant that TalkTalk ensured an interactional outcome that distilled blame and generalised the potential risk of cyber-attacks, and underlined that its counter-security efforts to protect customers were not random but calculated.

Bolstering image

The company proceeded to enact an image repair strategy by offering premium service packages at no extra costs for all existing customers, including new TV content for adults and children, mobile SIMs with monthly allowances of texts, calls and data, and broadband health checks from engineers (TalkTalk, 2015h). In addition, TalkTalk embarked on a mission to offer cyber-security awareness information to its customers and the wider public, encouraging them to report scam calls to the police, double-check the phone numbers from which they were receiving phone calls, and report suspicious numbers to a specific team at TalkTalk (TalkTalk, 2015c, 2015e, 2015i). Furthermore, the company announced its support for the 'Safer Internet Day 2016' initiative and actively participated in the foundation of 'Internet Matters', a non-profit organisation which aims to help parents to understand the behaviour that children have when using the internet (TalkTalk, 2016b). Also, TalkTalk participated in the Telegraph Cyber Security Conference, where the director of Corporate Affairs and Regulation presented what they called 'lessons of the cyber-attack' (TalkTalk, 2016c). These ceremonial activities helped TalkTalk to reinforce its interactional structure with the public, which also had the potential to make its customers feel that they had a stake in the survival of the company. In effect, TalkTalk kept reminding the audience about the uniqueness of the company and emphasising its commitment towards protecting their interests (Sutton and Callahan, 1987; Zavyalova et al., 2012). In one of company's press releases, it reaffirmed this commitment, stating:

> TalkTalk is well established as the value for money provider in the fast-growing quad play market and, notwithstanding the recent attack, remains well positioned to deliver strong and sustainable long-term growth (TalkTalk, 2015h)

TalkTalk also managed to exploit the crisis to reinforce its competitive position in the industry, as it became positioned as a model survivor of a cyber-attack. Thus, the series of actions helped to serve as a deflective mechanism designed to influence the performance evaluation actioned by its audiences. And in a bid to attenuate further stigmatising conditions and markers, TalkTalk presented an alternative perspective of the cyber-attack to influence the general evaluations of the crisis (Goffman, 1963; Zavyalova et al., 2012). This was actively executed by asserting the crisis as one that had helped the company to muster expertise and improved its technical knowledge on cyber-security issues. Its expositions on the attack were therefore designed to highlight its salience, presenting it as a 'necessary evil' to strengthen the company's security systems and improve service delivery. For instance, the following quotes by the CEO during the parliament inquiry and her message in the company's 2016 annual report illustrate that the crisis was emergently framed as an opportunity for the company to improve its operations:

> I am confident that we had a very robust, very clear plan. But clearly you have to look back with the benefit of hindsight and say, "If I had the time again, would I have done more, would the company have done more on security, knowing what we know today?" I think the only logical conclusion you can take is of course we would. Would that have prevented the attack? I do not know at this stage, but I think the thing our customers would expect us to say—and as I say, I think it is the only logical conclusion—is that of course we need to do more, and I would be surprised if any chief executive of any company does not say that to you today (Parliament, 2015).
>
> Equally the learnings from our detailed review of systems and processes following the cyber-attack have helped us to prioritise elements of our trading approach and strategy, which will help us deliver material improvements in profitability in FY17 (TalkTalk, 2016a).

Furthermore, TalkTalk presented its cyber-security system as one which was intricately robust and sensitive to the nature of the attack that it experienced, given that the hackers only manage to gain access to a fraction of the customers' personal information (Parliament, 2015). This defensive tactic, designed to protect its reputation and anticipatively aimed at erasing stigmatising markers, was also markedly demonstrated when concerns were raised at the parliamentary inquiry that the company's failure to encrypt customer data had led to the attackers having access to such information (BBC, 2015c). Baroness Harding responded by saying:

> […] I think there is a temptation for people to assume that encryption is a sort of silver bullet—that if you encrypt all the data, everything will be okay, whereas for some sorts of data, encryption is not a high enough security standard. One of the reasons why none of our customers' credit card details were stolen in a usable form was because they were not encrypted; they were what is called tokenised, which means you block out completely—you erase—the six digits in the middle of the credit card. So even if that is stolen there is no key that can unlock it. The six digits don't exist anymore. The way we look at things is that

> we use different security tools for different data […]. What we look at is different forms of security, of which encryption is one, to do what is right for that specific piece of data (Parliament, 2015).

In this regard, the company effortfully revised the reputational damage and stigma associated with the cyber-attack. It came to gain broader acceptance from its audience by illustrating its ability to protect customers against potential attacks and competence in providing secure services. Thus, despite the disruption in TalkTalk's operations, the company's strategic effort to construct favourable perceptive evaluations among the audience was leveraged to maintain its competitive advantage and accrue high financial performance benefits. An excerpt from TalkTalk's 2016 annual report reads:

> The actions we took following the cyber-attack to focus on our existing customers and to restore normality have more than mitigated any lasting impact on the business. This focus, together with the customer experience benefits of MTTS, helped us to stabilise the broadband base in Q4; drive strong growth in Revenue Generating Units (RGUs); and deliver the lowest ever churn in our history (1.3%) […]. The Board has recommended a final dividend of 10.58p, taking the full year dividend to 15.87p, 15% higher year on year, and in line with our commitment (TalkTalk, 2016a).

The purposive engineering of these prescient responses to the attack enabled TalkTalk to into its stride the collective evaluations actioned by the audiences, which were meant to impair its reputation. In this regard, the company demonstrated a subtle sway over the audiences' evaluative meanings and interpretations of the crisis. By first understanding that the cyber-attack had violated the organisational audiences' expectations of the company, it managed to cast a positive perception regardless of the discrediting event that had occurred.

Riding on leader reputation

Amidst the heightened contingencies of restraining the diffusion of adverse evaluation of TalkTalk's operations amongst its audiences, the CEO, by virtue of her functional role in the crisis management, was also central to reorienting such collective evaluations towards a more positive realm (Cellan-Jones, 2015). We find that her utilisation of communication skills, eliciting both a defensive and a mortification stance, were key to the positive outcomes of the company's reputational repair strategies (Wiesenfeld et al., 2008).

Baroness Harding's active involvement in the execution of TalkTalk's response to the attack came to represent the effortful accomplishment of the company in resolving the disruptions caused by the attack. This leader-driven approach to reputational repair served as a pragmatic mechanism for establishing stable control over the discrediting interpretations of what had happened. For instance, being aware of the tendency of the audiences to assume that the company had been irresponsible in paying attention to cyber-security issues, Baroness Harding defined its organising structures, saying:

> I would also say that security in a telecoms company is a lot more than the direct security team, so all of our systems, network and processes can work together to improve our customers' security […] the line responsibility for keeping our customers' data safe is split across a number of teams, so the accountability for security policies, the accountability for security audit, the accountability for security best practice, knowledge and dissemination within the organisation sits with the security function. The implementation of systems and processes that comply with those policies sits with my technology function. The implementation of the human elements of security—safe passwords, usage, complying with call centre policies—sits within my operations function (Parliament, 2016a).

As this quote indicates, the CEO explained how cyber-security issues are constitutive of the company's day-to-day operations. More so, Baroness Harding underscored the seriousness of cyber-security at TalkTalk as a shared responsibility of the board (Haislip et al., 2021), and that although there are operational teams handling various aspects of cyber-security, she as the CEO could be appropriately deemed responsible for the security failure (Cellan-Jones, 2015; Parliament, 2016a). While this exposition had the potential to trigger public reactions that may have compromised her role as the CEO, such reactions were accommodated by the notion that she was only 'responsible by virtue of her position' but not because she was directly responsible for preventing the cyber-security breaches. Here, the effectiveness of the strategy relied on the distributed nature of cyber-security at every aspect of the company's operations, thereby rendering it difficult to emphatically attribute blame to individual(s) or a department. These conditions thus meant that the entire security systems of the company were inefficient and thus the company as whole was responsible, as was noted in the ICO's report (ICO, 2016). Again, the reputation of the CEO and other high-ranking members of the board helped sway this perception. Baroness Harding again recounted:

> On the TalkTalk board we are very lucky to have a number of non-executive directors who have direct experience. You have seen that we launched an independent review with the board, led by James Powell, who is one of our independent non-executive directors, who is currently the chief technology officer of Nielsen and previously was the chief technology officer of Thomson Reuters, so he is one of the most experienced CTOs in the world (Parliament, 2015).

The CEO demonstrated that the company had executive members who were involved in issues of cyber-security, suggesting that it was indeed running a robust cyber-security system and thus that the cyber-attack was an unfortunate event which should rather be linked to the sophisticated nature of attack. She added:

> We had, and have, a detailed cybersecurity plan, using the "10 Steps to Cyber Security" framework that Government encourages companies to use, and because we are a telecoms company, I think compared to many other large companies—and certainly compared to small companies—we have had a lot of external support and advice in pulling that security plan together. Personally, I sit on TISAC, the Telecoms Industry Security Advisory Committee, and one of the things that TISAC has done has been benchmarking the various members of TISAC on the "10 Steps to Cyber Security" process. We had a lot of both external and internal scrutiny on that plan and continue to do so (Parliament, 2015).

The CEO's emphasis on her privileged position as a member of the Telecoms Industry Security Advisory Committee (TISAC) was to demonstrate that the company had all it takes to run a secure cyber system. Thus, given the intertwining relationship between CEO's personal reputation and that of the company (Deutsch and Ross, 2003; Gioia et al., 2014), her role in the process of salvaging TalkTalk's reputation was pronounce. Following the series of investigations which led to arrests made by the MP, and the steps that were undertaken to boost cyber-security, Baroness Harding confidently noted that she took a firm stance towards going public despite the MP opposing such decision (Harding, 2016). Although she indicated that the MP had supported the company in managing the consequences of going public, her mentioning of such backstage discussions underlined how challenging it was to engage in such disclosure.

This helped TalkTalk to eliminate existing or impending stigmas, as it signalled to the organisational audiences that it had prioritised protecting customers' safety and interest during the attack. As such, the interactional relationship between the company and its audiences was bolstered with the notion that the company had provided the best possible form of protection during the attack.

Discussion and Conclusion

Following and extending recent studies on cyber-attack as a pervasive threat to the contemporary organisation (Tounsi and Rais, 2018), the purpose of this study has been to constructively tease out how organisations involved in cyber-attacks could effectively repair their reputational damage during such discrediting events. Yet, in contrast to prior research, which has largely focused on the technical responses to cyber-attacks (see, for example, Spyridopoulos et al., 2013; Żebrowski et al., 2022), this paper has extended our understanding beyond the existing boundaries of thought by providing insights into comprehensive strategies adopted to repair the collateral loss in organisational reputation and erase stigma markers during cyber-security incidents. Specifically, we drew on the case of a telecommunications company, TalkTalk, which suffered a significant and sustained cyber-attack, to explicate the processes through which the paradoxical tension of technically containing the attack and preserving or repairing organisational reputation is achieved. The TalkTalk case attracted the largest fine in the history of the ICO and sparked debates among experts and policymakers alike on the need for stricter legislative instruments and institutional arrangements to control organising practices within the telecommunications and other cyber-related industries (Doward et al., 2015; ICO, 2022a; Parliament, 2016b). This case therefore aptly offered analytical avenue for generating our contribution on the reputational damage and stigma that a cyber-attack could evoke, and how such crises are managed.

Our findings suggest that the company judiciously employed technical and rhetorical strategies which were contemporaneously executed during the crisis to shore up reputation among its audiences. TalkTalk undertook a calculated step to understand the scope and magnitude of the attack in order to engage with appropriate regulatory institutions, their customers and the wider public. In a bid to repair their eluding reputation as negative evaluations began to erupt, the company strategically contrived perceptual frames for controlling its audiences' meaning-making and interpretations of the event. The use of various communication channels and skills, rendering an apology, funding and engaging in cyber-security education programs to bolster its image, and riding on the reputation of its leader to reinforce trust in its responses, constituted an active framework for assuaging the negative evaluations of the company's operations. As we unpacked these responses, we found consistency with extant studies which suggest that corrective actions to repair reputation resides in efficient information flows between the organisation and its audiences, which are geared toward casting the company in a more positive light (e.g., Desai, 2011; Sturges, 1994).

Furthermore, an important insight that emerged in the TalkTalk case is the picturesque illustration of how ensuring a close-knit interaction with security agencies or institutions that are recognised by the public as credible is instrumental to retaining trust and bolstering organisational reputation, helping to assure audiences about the efficacy of the organisation's actions to contain the attack. Again, this insight complements studies that underscore how an organisation's reputational repair and stigma erasure efforts become contingent on third-party endorsements, which help to re-establish trust and legitimacy (Rhee and Valdez, 2009). TalkTalk working hand-in-glove with the MP and the ICO provided much-needed public comfort in the measures that were being rolled out to contain the attack. In this respect, what the study has found to be significant is the proposition that in the event of a cyber-security crisis, the ongoing attempts to contain an attack and minimise its impact is to gain credibility through the public acknowledging that the countermeasures are not mere 'self-correcting fallacy'. Rather, new knowledge and expertise, which are usually perceived by the audience as superior, are infused in the steps towards protecting stakeholders' interests.

Theoretical contribution

The analysis we have presented offers three important theoretical contributions to the discourse on cyber-risk management and reputational repair. First, our study suggests that organisational audiences may question an organisation's fundamental operations, enact distrust, and generate and signal negative evaluations to the wider public in the event of a cyber-attack. The enactment of these reputational damaging evaluations may, however, persist, thereby leading to the attachment of stigmatising markers to the organisation. In this regard, we submit that surviving a cyber-attack is contingent on an interplay between robust technical countermeasures and judicious social defence acts to influence the perceptual evaluations of organisational audiences. Thus, a collective socio-technical response to a cyber-attack allows the organisation to hold together and pursue its technical response while at the same time limiting the fleeting tendencies of public perceptions, which may in turn lead to difficulty in bouncing back from the attack.

Second, the study indicates that the organisational leader's role as a representative figure in the management of a crisis is essential for coordinating the strategic response to the attack and the reputational repair efforts. Thus, in the event of what we conceive as a *fragile reputational condition dominated by unfavourable appraisal of organisational operations*, the attributive link between organisational leader(s)' reputation and the organisation they control (Love et al., 2017; Men, 2012) becomes critical in the management of such events. As such, our emphasis on the role of organisational leaders at the centre-stage of reputational repair strategies draws in complementary insights from the crisis leadership literature (Wu et al., 2021) to suggest that theory development on reputational repair could benefit from appreciating organisational leaders' engagement in industry-wide activities such as committees and sub-institutions that are set up to enhance the operational efficiency of the industry. This is important because, as this study reveals, their active participation in such arrangements helps to establish the organisation's prominence in their competing fields. The core relevance of this effort in the management of a cyber-attack, therefore, is the nurturing of positive perceptions of the organisation and its leader, thereby helping to build credibility and trust as they spearhead active image repair strategies in reputation-damaging incidents.

Third, our study extends efforts to define a fundamental relatedness, rather than contrast, between organisational reputation and stigma. Specifically, our exposition of stigma and reputation as mutually related concepts within the rising tensions of failing to meet the expectations of the organisational audience captures how the (re)construction and/or protection of organisational reputation is rooted in an arduous attempt to avoid stigma—which sits at the dark side of the social evaluation continuum (Devers et al., 2009). Thus, embedded in the strategic efforts to repair reputation in a crisis event is an ardent urge to evade stigmatising labels, which not only trigger dissociating responses from other organisations due to stigma transfer, but also could limit agents' ability to move across and between institutions. On this basis, an obscured psychological dynamic takes hold to shape modes of response to reputational threats as well as patterns of narratives to facilitate recovery from such crisis events (Bundy et al., 2017). The significance of the psychodynamics of reputational repair efforts is the explication of the mechanism through which individual affectivity interacts with and reinforces the organisational response to a crisis and enacts stigma erasure.

Practical Implications

Our study also has practical implications for the study and management of cyber-attacks in contemporary organising. Beyond the theoretical specification of strategic reputational repair strategies, we reveal pragmatic approaches to engaging with and managing cyber-attacks within the interacting tensions of technical and social responses. We begin by converging upon a set of insights from the study, which, contrary to the existing often-descriptive approaches (Rosanes, 2022), provides a practical guide for organisations to conceive and implement in event of cyber-attack. With insights from the findings of the study, we capture and label this guiding model as *speed*, *timing*, *assurances*, and *remedy* (STAR), in addition to some corresponding actions. Here, we propose that the speed or swiftness of identifying the nature and magnitude of the cyber-attack is the foremost element of the reputational repair process. The TalkTalk case revealed that taking measure of the attack is a fundamental step on which all other response strategies are conceived and enacted. Next, it is imperative that key stakeholders, including regulators, customers and business partners, are informed about the attack and offered cyber-security information to help maintain awareness, cope with, and prevent activities that may further compromise cyber-security systems (Jaeger and Eckhardt, 2021). This also implies that appropriate communication channels are utilised to go public with news of the attack. Elements of apology and transparency in activities undertaken to protect customers are, however, to be contained in such communiqués. Also, it is important to cooperate with recognised security agencies and regulatory bodies whom the organisational audience deem to possess valuable and credible identities (Paetzold et al., 2008) to help contain the attack and to provide assurances to stakeholders about the effectiveness of the countermeasures being undertaken. Finally, to further eliminate stigmatising markers on the organisation, efforts ought to be made to publicly provide an account of the effectiveness of the security measure taken during the attack, highlighting the improvement to the cyber-security systems and engaging cyber-related educational programs. We summarise this into a response-action heuristic model (Table 3) to help organisations deal with cyber-attacks.

Insert Table 3 about here

Second, given that the negative perceptive evaluations that underpin reputational loss may persist over the interstices of identifying an attack and actioning cyber-security measures, this study underlines the need for organisations to nurture foresightfulness, through anticipation and designing incident response plans (Bundy et al., 2017; Ceric and Holland, 2019; Cynet, 2022). This is important because stigma markings that the watching public may imprint on the attacked organisation take effect right from when the incident has occurred and become known. Thus, effective reputational repair in the event of a cyber-attack is dependent on pronto strategic responses that are designed, from the onset at least, to shape the understanding and interpretation of the incident and hence the perceptive evaluations of the organisational audience. Thus, we offer insights for managers to conceive that cyber-risk is almost ubiquitous in today's high-velocity digital business environment. Hence, reputational repair is a strategic competence that rests in the development of a visioning mode of organisational foresight (e Cunha et al., 2006; Sarpong et al., 2013) to condition the audience's perceptions such that they view the diverging gap between expectations and actual experiences as anomalous.

Limitations and future research

Despite the progress made in this study in unpacking and delineating what we describe as strategic reputational repair after cyber-attack, we acknowledge two main limitations in our study, which, in turn, open up opportunities for future research. First, although the TalkTalk cyber-attack is a unique case that provides an illustrative account of how cyber-attacks are contained beyond the technical responses, it remains an exceptional case of an organisation whose core operational activities are rooted in the provision of cyber-related products and services. Yet, given the existing business environment, where digital transformation has become critical to organisational survival, we are of the view that the intricacies and dynamics of an industry that is evaluated based on operational parameters other than the capability to protect customer data may not require such extreme measures in its reputational repair efforts. In this regard, we encourage future research into cross-industrial comparisons to identify the uniqueness of reputational repair strategies, in order to provide an extended framework for generalising such strategies. Second, the study narrowly focuses on reputation salvaging and stigma erasure, and thus fails to conceive the potential of the cyber-attack to trigger relational disequilibrium within the organisation. As prior research suggests, post-crisis effects may manifest in the form of cognitive effects, which could impact work relationships and organisational performance (Kahn et al., 2013; Bechky, 2006). As such, we urge future research to embark on longitudinal studies to provide insights into how organisations manage the internal disturbances that result from social tensions and psychological ambiguities that may arise among organisational members after the attack has been contained.

Conclusion

Thus far, the discourse on cyber-risk and security has been dominated by studies focusing on technological responses to cyber-attacks and the financial costs incurred to contain such threats. This has led to limited insights into how the attacked firm may suffer reputational damage during such incidents, which has implications for organisational survival and competitiveness. We have in this paper attempted to address this lacuna by analysing the case of TalkTalk's cyber-attack and the reputational repair strategies enacted to salvage the organisation from the crisis. While the insights presented here may not be exhaustive, we hope that the study offers the beam compass needed to trace and extend theoretical and practical insight into the discourse on cyber-risk management and reputational repair strategies in this digital era.

References

Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. and Upton, D. (2018), A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, Vol. 4 No. 1, p. 6. https://doi.org/10.1093/cybsec/tyy006

Ahmed, M. and Thomas, D. (2015), "TalkTalk cyber-attack: what we know about the hack", available at: https://www.ft.com/content/9bfb4e72-7965-11e5-a95a-27d368e1ddf7. [Accessed 1 May 2018].

Al-rimy, B.A.S., Maarof, M.A. and Shaid, S.Z.M. (2018), Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. *Computers & Security*, Vol. 74, pp. 144-166. https://doi.org/10.1016/j.cose.2018.01.001

Allodi, L. and Massacci, F. (2017), Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis*, Vol. 37 No. 8, pp. 1606-1627. https://doi.org/10.1111/risa.12864

Alsop, R.J. (2004), *The 18 immutable laws of corporate reputation: creating, protecting, and repairing your most valuable asset*, The Free Press, New York, NY.

Armenia, S., Angelini, M., Nonino, F., Palombi, G. and Schlitzer, M.F. (2021), A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, Vol. 147, p. 113580. https://doi.org/10.1016/j.dss.2021.113580

Arora, S.K., Li, Y., Youtie, J. and Shapira, P. (2016), Using the wayback machine to mine websites in the social sciences: a methodological resource. *Journal of the Association for Information Science and Technology*, Vol. 67 No.8, pp. 1904-1915. https://doi.org/10.1002/asi.23503

Ashforth, B.E. and Kreiner, G.E. (1999), "How can you do it?": Dirty work and the challenge of constructing a positive identity. *Academy of Management Review*, Vol. 24 No. 3, pp. 413-434. https://doi.org/10.5465/amr.1999.2202129

Aversa, P., Huyghe, A. and Bonadio, G. (2021), First impressions stick: market entry strategies and category priming in the digital domain. *Journal of Management Studies*, Vol. 58 No. 7, pp. 1721-1760. https://doi.org/10.1111/joms.12712

Bechky, B.A. (2006), Gaffers, gofers, and grips: role-based coordination in temporary organizations. *Organization Science*, Vol 17 No 1, pp. 3-21. https://doi.org/10.1287/orsc.1050.0149

BBC (2015a), "TalkTalk cyber-attack: website hit by 'significant' breach", available at: http://www.bbc.co.uk/news/uk-34611857. [Accessed 17 April 2022]

BBC (2015b), "TalkTalk cyber-attack: boss 'receives ransom email'", available at: http://www.bbc.co.uk/news/uk-34615226. [Accessed 20 April 2022].

BBC (2015c), "TalkTalk cyber-attack: your views", available at: https://www.bbc.co.uk/news/uk-34615260. [Accessed 11 May 2022].

BBC (2015d), "TalkTalk hack to cost up to £35m", available at: https://www.bbc.co.uk/news/uk-34784980. [Accessed 12 May 2022]

BBC (2016a), "TalkTalk fined £400,000 for theft of customer details", available at: http://www.bbc.co.uk/news/business-37565367. [Accessed 27 April 2022]

BBC (2016b), "Boy, 17, admits TalkTalk hacking offences", available at: https://www.bbc.co.uk/news/uk-37990246. [Accessed 1 June 2022].

Benoit, W.L. (1997), Image repair discourse and crisis communication. *Public Relations Review*, Vol. 23 No. 2, pp. 177-186. https://doi.org/10.1016/S0363-8111(97)90023-0

Boakye, D., Siaw, D. and Sarpong, D. (2022a), The Airbus bribery scandal: a collective myopia perspective. *European Management Review*, Vol. 19 No. 4, pp. 654-670. https://doi.org/10.1111/emre.12511.

Boakye, D., Sarpong, D. and Mordi, C. (2022), Regulatory review of new product innovation: Conceptual clarity and future research directions. *Technological Forecasting and Social Change*, Vol. 175, p. 121419. https://doi.org/10.1016/j.techfore.2021.121419

Bundy, J., Pfarrer, M. D., Short, C. E. and Coombs, W. T. (2017), Crises and crisis management: Integration, interpretation, and research development. *Journal of management*, Vol. 43, p. 1661-1692.

Cantril, H. (1947), *Gauging public opinion*, Princeton, NJ: Princeton University Press.

Carmeli, A. and Tishler, A., (2005), Perceived organizational reputation and organizational performance: an empirical investigation of industrial enterprises. *Corporate Reputation Review*, Vol. 8 No. 1 pp. 13-30. https://doi.org/10.1057/palgrave.crr.1540236.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2005), The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, Vol. 16 No. 1, pp. 28-46. https://doi.org/10.1287/isre.1050.0041.

Cellan-Jones, R. (2015), "Questions for TalkTalk", available at: https://www.bbc.co.uk/news/technology-34636308. [Accessed 1 May 2022].

Ceric, A. and Holland, P. (2019), The role of cognitive biases in anticipating and responding to cyberattacks. *Information Technology & People*, Vol. 32 No. 1, pp.171-188.

Chakrabarti, A. and Manimaran, G. (2002), Internet infrastructure security: a taxonomy. *IEEE network*, Vol. 16 No. 6, pp. 13-21. https://doi.org/10.1109/MNET.2002.1081761

Coombs, W.T. (1998), An analytic framework for crisis situations: better responses from a better understanding of the situation. *Journal of Public Relations Research*, Vol. 10 No. (3), pp. 177-191. https://doi.org/10.1207/s1532754xjprr1003_02

Coombs, T. and Schmidt, L. (2000), An empirical analysis of image restoration: Texaco's racism crisis. *Journal of Public Relations Research*, Vol. 12 No. 2, pp. 163-178. https://doi.org/10.1207/S1532754XJPRR1202_2

Coombs, W.T. (2007), Protecting organization reputations during a crisis: the development and application of situational crisis communication theory. *Corporate Reputation Review*, Vol. 10 No. 3, pp. 163-176. https://doi.org/10.1057/palgrave.crr.1550049

Cornelissen, J.P., Mantere, S. and Vaara, E. (2014), The contraction of meaning: the combined effect of communication, emotions, and materiality on sensemaking in the Stockwell shooting. *Journal of Management Studies*, Vol. 51 No. 5, pp. 699-736. https://doi.org/10.1111/joms.12073

Cox, A. L. (2008), What's wrong with risk matrices? *Risk Analysis*, Vol. 28 No. 2, pp. 497-512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Cynet (2022). "Incident response plan", available at: https://www.cynet.com/incident-response/#:~:text=An%20incident%20response%20plan%20is,pressure%20of%20an%20actual%20cyberattack. [Accessed 20 December 2022]

Deloitte (2020), "Global cyber executive briefing", available at: https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/High- Technology-Sector.html. [Accessed 12 June 2022].

Desai, V. M. (2011), Mass media and massive failures: determining organizational efforts to defend field legitimacy following crises. *Academy of Management Journal*, Vol. 54 No2, pp. 263-278. https://doi.org/10.5465/amj.2011.60263082

Deutsch, Y. and Ross, T.W. (2003), You are known by the directors you keep: reputable directors as a signaling mechanism for young firms. *Management Science*, Vol. 49 No. 8, pp. 1003-1017. https://doi.org/10.1287/mnsc.49.8.1003.16399

Devers, C.E., Dewett, T., Mishina, Y. and Belsito, C.A. (2009), A general theory of organizational stigma. *Organization Science*, Vol. 20 No. 1, pp. 154-171. https://doi.org/10.1287/orsc.1080.0367

Doward, J., Tims, A. and Boffey, D. (2015), TalkTalk cyber-attack sparks calls for new regulatory powers, Available at: https://www.theguardian.com/business/2015/oct/24/talktalk-cyber-attack-new-powers-regulators-hacking. [Accessed 01 April 2023].

Durand, R. and Vergne, J.P. (2015), Asset divestment as a response to media attacks in stigmatized industries. *Strategic Management Journal*, Vol. 36 No. 8, pp. 1205-1223. https://doi.org/10.1002/smj.2280

Dutton, J.E., Dukerich, J.M. and Harquail, C.V. (1994), Organizational images and member identification. *Administrative Science Quarterly*, pp. 239-263. https://doi.org/10.2307/2393235

e Cunha, M.P., Palma, P. and da Costa, N.G. (2006), Fear of foresight: knowledge and ignorance in organizational foresight. *Futures*, Vol. 38 No. 8, pp. 942-955. https://doi.org/10.1016/j.futures.2005.12.015

Ekelund, S. and Iskoujina, Z. (2019), Cybersecurity economics–balancing operational security spending. *Information Technology & People*, Vol. 32 No. 5, pp. 1318-1342. https://doi.org/10.1108/ITP-05-2018-0252

Elsbach, K.D. and Sutton, R.I. (1992), Acquiring organizational legitimacy through illegitimate actions: z marriage of institutional and impression management theories. *Academy of Management Journal*, Vol. 35 No. 4, pp. 699-738. https://doi.org/10.5465/256313

Farrell, S. (2015), “Nearly 157,000 had data breached in TalkTalk cyber-attack”, available at: https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack. [Accessed 27 April 2022].

Farrell, S. (2016), “TalkTalk counts costs of cyber-attack”, available at: https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave. [Accessed 1 May 2018].

Fombrun, C.J., Gardberg, N.A. and Sever, J.M. (2000), The Reputation Quotient SM: a multi-stakeholder measure of corporate reputation. *Journal of Brand Management*, Vol. 7 No. 4, pp. 241-255. https://doi.org/10.1057/bm.2000.10

Gayle, D. (2015), “TalkTalk cyber-attack not as bad as first thought, company says”, available at: https://www.theguardian.com/business/2015/oct/24/talktalk-attack-government-urged-to-do-more-on-cybercrime. [Accessed 1 May 2022].

Gibbert, M., Ruigrok, W., & Wicki, B. (2008), What passes as a rigorous case study? *Strategic Management Journal*, *29*(13), 1465-1474.

Gioia, D.A., Schultz, M. and Corley, K.G. (2000), Organizational identity, image, and adaptive instability. *Academy of Management Review*, Vol. 25 No. 4pp. 63-81. https://doi.org/10.5465/amr.2000.2791603

Gioia, D.A., Hamilton, A.L. and Patvardhan, S.D. (2014), Image is everything: reflections on the dominance of image in modern organizational life. *Research in Organizational Behavior*, Vol. 34, pp. 129-154. https://doi.org/10.1016/j.riob.2014.01.001

Goodall, J.R., Lutters, W.G. and Komlodi, A. (2009) Developing expertise for network intrusion detection. *Information Technology & People*, Vol. 22 No. 2, pp. 92-108. https://doi.org/10.1108/09593840910962186

Gordon, L.A., Loeb, M.P. and Zhou, L. (2020) Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, Vol. 6 No. 1, p. tyaa005. https://doi.org/10.1093/cybsec/tyaa005

Goffman, E. (1963), *Stigma: notes on the management of spoiled identity*, Prentice Hall: Englewood, NJ.

Haislip, J., Lim, J. H. and Pinsker, R. (2021), The impact of executives' IT expertise on reported data security breaches. *Information Systems Research*, Vol. 32 No. 2, pp. 318-334. https://doi.org/10.1287/isre.2020.0986

Hampel, C.E. and Tracey, P. (2017), How organizations move from stigma to legitimacy: the case of Cook's travel agency in Victorian Britain. *Academy of Management Journal*, Vol. 60 No. 6, pp. 2175-2207. https://doi.org/10.5465/amj.2015.0365

Hampel, C. and Tracey, P. (2019), Introducing a spectrum of moral evaluation: integrating organizational stigmatization and moral legitimacy. *Journal of Management Inquiry*, Vol. 28 No. 1, pp.11-15. https://doi.org/10.1177%2F1056492618790897

Harding, D. (2016), "Bristol Distinguished Address Series", available at: https://soundcloud.com/uwebristol/baroness-dido-harding. [Accessed 30 May 2018]

Helms, W.S. and Patterson, K.D. (2014), Eliciting acceptance for "illicit" organizations: the positive implications of stigma for MMA organizations. *Academy of Management Journal*, Vol. 57 No. 5, pp. 1453-1484. https://doi.org/10.5465/amj.2012.0088

Hern, A. (2015), "TalkTalk hit with record £400k fine over cyber-attack", available at: https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine- over-cyber-attack. [Accessed 27 May 2022].

Higgs, J.L., Pinsker, R.E., Smith, T.J. and Young, G.R. (2016), The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, Vol. 30 No. 3, pp. 79-98. https://doi.org/10.2308/isys-51402

Hudson, B.A., (2008), Against all odds: a consideration of core-stigmatized organizations. *Academy of Management Review*, Vol. 33 No. 1, pp. 252-266. https://doi.org/10.5465/amr.2008.27752775

Hudson, B.A. and Okhuysen, G.A. (2009), Not with a ten-foot pole: core stigma, stigma transfer, and improbable persistence of men's bathhouses. *Organization Science*, Vol. 20 No. 1, pp. 134-153. https://doi.org/10.1287/orsc.1080.0368

Information Commissioner's Office (2016), "TalkTalk cyber attack – how the ICO's investigation unfolded", available at: https://ico.org.uk/about-the-ico/news-and-events/talktalk- cyber-attack-how-the-ico-investigation-unfolded/. [Accessed: 9 May 2022].

Information Commissioner's Office (2022a), Guide to enforcement processes, available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-le-processing-1-1.pdf. [Accessed: 6 April 2023]

Information Commissioner's Office (2022b), "Who we are", available at: https://ico.org.uk/about- the-ico/who-we-are/ [Accessed 9 May 2022].

Isaakyan, I. and Triandafyllidou, A. (2019), Transatlantic repatriation: stigma management of second-generation Italian and Greek American women 'returning home'. *European Journal of Cultural Studies*, Vol. *22* No. 2, pp. 180-194. https://doi.org/10.1177%2F1367549418823058

Jaeger, L. and Eckhardt, A. (2021), Eyes wide open: the role of situational information security awareness for security-related behaviour. *Information Systems Journal*, Vol. 31 No. 3, pp. 429-472. https://doi.org/10.1111/isj.12317

Johnston, C. (2015), "TalkTalk customer data at risk after cyber-attack on company website", available at https://www.theguardian.com/business/2015/oct/22/talktalk-customer-data- hackers-website-credit-card-details-attack. [Accessed 9 May 2022].

Kahn, W.A., Barton, M.A. and Fellows, S. (2013), Organizational crises and the disturbance of relational systems. *Academy of Management Review*, Vol. 38 No. 3, pp. 377-396. https://doi.org/10.5465/amr.2011.0363

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M. (2021), Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, Vol. 139 No. 3, pp. 719- 749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kemmerer, R.A. and Vigna, G. (2002), Intrusion detection: a brief history and overview. *Computer*, Vol. 35 No. 4, pp. 27-l30. https://doi.org/10.1109/MC.2002.1012428

Kent, M.L., Taylor, M. and White, W.J. (2003), The relationship between web site design and organizational responsiveness to stakeholders. *Public Relations Review*, Vol. 29 No. 1, pp. 63-77. https://doi.org/10.1016/S0363-8111(02)00194-7

Khomami, N. (2015a), "TalkTalk hack could not have been prevented by government scheme", available at: https://www.theguardian.com/business/2015/dec/15/talktalk-hack- could-not-have- been-prevented-by-cyber-essentials. [Accessed 1 May 2018].

Khomami, N. (2015b), "TalkTalk cyber-attack: company has received 'ransom demand'", available at: https://www.theguardian.com/business/2015/oct/23/talktalk-cyber-attack- company-has-received-ransom-demand. [Accessed 20 May 2022]

Koehn, N., (2020), Real leaders are forged in crisis. *Harvard Business Review*, Vol. 3, pp. 1-6. https://hbr.org/2020/04/real-leaders-are-forged-in-crisis

Kvåle, G. and Murdoch, Z. (2021), Shame on you! Unpacking the individual and organizational implications of engaging with a stigmatized organization. *Journal of Management Studies,* Vol. 59. No. 8, pp. 2024-2066. https://doi.org/10.1111/joms.12743

Langley, A.N.N., Smallman, C., Tsoukas, H. and Van de Ven, A.H. (2013), Process studies of change in organization and management: unveiling temporality, activity, and flow. *Academy of Management Journal*, Vol. 56 No. 1, pp. 1-13. https://doi.org/10.5465/amj.2013.4001

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2021), Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, Vol. 105, p. 102248. https://doi.org/10.1016/j.cose.2021.102248

Love, E.G., Lim, J. and Bednar, M.K. (2017), The face of the firm: the influence of CEOs on corporate reputation. *Academy of Management Journal*, Vol. 60 No 4, pp. 1462-1481. https://doi.org/10.5465/amj.2014.0862

Lyonz, I. (2018), "TalkTalk hackers jailed for cyber cyber attack that cost company £77m", available at: https://www.telegraph.co.uk/news/2018/11/19/talktalk-hackers-jailed-18- months- 2015-cyber-attack [Accessed 15 June 2022].

Reise, S.P. and Waller, N.G. (2009), Item response theory and clinical measurement. *Annual Review of Clinical Psychology*, Vol. 5 No. 1, pp. 27-48. https://doi.org/10.1146/annurev.psych.56.091103.070137

Mantere, S. and Ketokivi, M. (2013), Reasoning in organization science. *Academy of Management Review*, Vol. 38 No. 1, pp. 70-89. https://doi.org/10.5465/amr.2011.0188

Meisenbach, R.J. (2010), Stigma management communication: a theory and agenda for applied research on how individuals manage moments of stigmatized identity. *Journal of Applied Communication Research*, Vol. 38 No. 3, pp. 268-292. https://doi.org/10.1080/00909882.2010.490841

Men, L.R. (2012), CEO credibility, perceived organizational reputation, and employee engagement. *Public Relations Review*, Vol. 38 No. 1, pp. 171-173. https://doi.org/10.1016/j.pubrev.2011.12.011

Mishina, Y., Block, E.S. and Mannor, M.J. (2012), The path dependence of organizational reputation: how social judgment influences assessments of capability and character. *Strategic Management Journal*, Vol. 33 No. 5, pp. 459-477. https://doi.org/10.1002/smj.958

Mitroff, I. I., Pearson, C. M. and Harrington, L. K. (1996), *The essential guide to managing corporate crises: a step-by-step handbook for surviving major catastrophes,* Oxford: Oxford University Press.

Nandi, A.K., Medal, H.R. and Vadlamani, S. (2016), Interdicting attack graphs to protect organizations from cyber attacks: a bi-level defender–attacker model. *Computers & Operations Research*, Vol. 75, pp. 118-131. https://doi.org/10.1016/j.cor.2016.05.005

Paetzold, R.L., Dipboye, R.L. and Elsbach, K.D. (2008), A new look at stigmatization in and of organizations. *Academy of Management Review*, Vol. 33 No. 1, pp. 186-193. https://doi.org/10.5465/amr.2008.27752576

Parliament. (2015), "Culture, Media and Sport Committee meeting: TalkTalk", available at: https://www.parliamentlive.tv/Event/Index/73368590-d756-4a37-badb-8174ac8ef239#p. [Accessed 9 May 2022]

Parliament. (2016a), "TalkTalk cyber-attack and response", available at: https://publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/14805.htm#footno te-054-backlink. [Accessed 5 May 2022]

Parliament. (2016b), "Written evidence submitted by TalkTalk plc (DEB 09)", Available at: https://websearch.parliament.uk/?q=Data%2Bbreach%2Breporting%2Bguidelines%2C+talktalk. [Accessed 1 April 2023]

Paté-Cornell, M.E., Kuypers, M., Smith, M. and Keller, P. (2018), Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, Vol. 38 No. 2, pp. 226-241. https://doi.org/10.1111/risa.12844

Pearson, C.M. and Clair, J.A. (1998), Reframing crisis management. *Academy of Management Review*, Vol. 23 No. 1, pp.59-76. https://doi.org/10.5465/amr.1998.192960

Pescosolido, B.A. and Martin, J.K. (2015), The stigma complex. *Annual Review of Sociology*, Vol 41, pp. 87-116. https://doi.org/10.1146%2Fannurev-soc-071312-145702

Pinguelo, F.M. and Muller, B.W. (2011), Virtual crimes, real damages: a primer on cybercrimes in the United States and efforts to combat cybercriminals. *Virginia Journal of Law and Technology*, Vol. 16, p. 116-189.

Pollock, T.G., Lashley, K., Rindova, V.P. and Han, J.H. (2019), Which of these things are not like the others? Comparing the rational, emotional, and moral aspects of reputation, status, celebrity, and stigma. *Academy of Management Annals*, Vol. 13 No. 2, pp. 444-478. https://doi.org/10.5465/annals.2017.0086

Ragins, B.R. (2008), Disclosure disconnects: antecedents and consequences of disclosing invisible stigmas across life domains. *Academy of Management Review*, Vol. 33 No. 1, pp. 194-215. https://doi.org/10.5465/amr.2008.27752724

Ransbotham, S. and Mitra, S. (2009), Choice and chance: a conceptual model of paths to information security compromise. *Information Systems Research*, Vol. 20 No 1, pp. 121-139. https://doi.org/10.1287/isre.1080.0174

Ransbotham, S., Fichman, R.G., Gopal, R. and Gupta, A. (2016), Special section introduction—ubiquitous IT and digital vulnerabilities. *Information Systems Research*, Vol. 27 No. 4, pp. 834-847. https://doi.org/10.1287/isre.2016.0683

Ravasi, D. and Schultz, M. (2006), Responding to organizational identity threats: exploring the role of organizational culture. *Academy of Management Journal*, Vol. 49 No. 3, pp. 433-458. https://doi.org/10.5465/amj.2006.21794663

Rhee, M. and Valdez, M.E. (2009). Contextual factors surrounding reputation damage with potential implications for reputation repair. *Academy of Management Review*, Vol. 34 No. 1, pp. 146-168. https://doi.org/10.5465/amr.2009.35713324

Rindova, V.P., Williamson, I.O., Petkova, A.P. and Sever, J.M. (2005), Being good or being known: an empirical examination of the dimensions, antecedents, and consequences of organizational reputation. *Academy of Management Journal*, Vol. 48 No. 6, pp. 1033-1049. https://doi.org/10.5465/amj.2005.19573108

Rios Insua, D., Couce-Vieira, A., Rubio, J.A., Pieters, W., Labunets, K. and G. Rasines, D. (2021), An adversarial risk analysis framework for cybersecurity. *Risk Analysis*, Vol. 41 No. 1, pp. 16-36. https://doi.org/10.1111/risa.13331

Rodionova, Z. (2016), "TalkTalk given record fine over data breach that led to data theft of nearly 157,000 customers", available at: https://www.independent.co.uk/news/business/news/talktalk- fine-data-breach-theft-customers-information-stolen-record-penalty-a7346316.html [Accessed 8 May 2022].

Rosanes, M. (2022), "Cybersecurity best practices – how should companies respond to a cyberattack?", available at: https://www.insurancebusinessmag.com/us/news/cyber/cybersecurity-best- practices--how-should-companies-respond-to-a-cyberattack-415154.aspx [Accessed 20 December 2022].

Sarathy, R. and Muralidhar, K. (2002), The security of confidential numerical data in databases. *Information Systems Research*, Vol. 13 No. 4, pp. 389-403. https://doi.org/10.1287/isre.13.4.389.74

Sarpong, D., Maclean, M. and Alexander, E. (2013), Organizing strategic foresight: a contextual practice of 'way finding'. *Futures*, Vol. 53, pp. 33-41. https://doi.org/10.1016/j.futures.2013.09.001

Siggelkow, N. (2007), Persuasion with case studies. *Academy of Management Journal*, Vol. 50 No. 1, pp. 20-24.

Spanier, G. (2015), "TalkTalk suspends advertising and X Factor sponsorship for second week", available at: https://www.campaignlive.co.uk/article/talktalk-suspends-advertising-x-factor- sponsorship-second-week/1370822 [Accessed 17 April 2022].

Specht, S. and Lee, R. (2003), Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. *CEL2003-03, Princeton University, Princeton, NJ, USA*.

Sturges, D.L. (1994), Communicating through crisis: a strategy for organizational survival. *Management Communication Quarterly*, Vol. *7* No. 3, pp. 297-316. https://doi.org/10.1177%2F0893318994007003004

Sutton, R.I. and Callahan, A.L. (1987), The stigma of bankruptcy: spoiled organizational image and its management. *Academy of Management Journal*, Vol. 30 No. 3, pp. 405-436. https://doi.org/10.5465/256007

Spyridopoulos, T., Karanikas, G., Tryfonas, T. and Oikonomou, G. (2013), A game theoretic defence framework against DoS/DDoS cyber attacks. *Computers & Security*, Vol. 38, pp. 39-50. https://doi.org/10.1016/j.cose.2013.03.014

TalkTalk Group (2022a), "Company history", available at: https://www.talktalkgroup.com/about-us/our-history [Accessed May 8, 2022].

TalkTalk Group. (2022b), "Annual report 2021", available at: https://www.talktalkgroup.com/annualreports [Accessed 5 May 2022].

TalkTalk Group (2015a), "Statement by TalkTalk PLC on cyber attack – Thursday October 22nd 2015", available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Statement-by-TalkTalk-PLC-on-Cyber-Attack---Thursday-October-22th-2015. [Accessed May 1, 2022]

TalkTalk Group (2015b), "Cyber attack update – Saturday October 24th, 2015", available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Cyber-Attack-update---Saturday-October-24th-2015. [Accessed 27 May 2022].

TalkTalk Group (2015c), "Cyber Attack update – Monday October 26th, 2015", available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Cyber-Attack-update---Monday-October-26th-2015. [Accessed 27 May 2022].

TalkTalk Group (2015d), "TalkTalk PLC responds to Metropolitan Police update", available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/TalkTalk-PLC-responds-to-Metropolitan-Police-update. [Accessed 27 May 2022].

TalkTalk Group (2015e), "Cyber Attack update – Tuesday October 27th, 2015". available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Cyber-Attack-update---Tuesday-October-27th-2015. [Accessed 30 May 2022].

TalkTalk Group (2015f), "Cyber Attack update – Friday October 30th 2015", available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Cyber-Attack-update---Friday-October-30th-2015. [Accessed 30 May 2022].

TalkTalk Group (2015g), "Cyber Attack update – Friday November 6th, 2015", available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Cyber-Attack-update---Friday-November-6th-2015. [Accessed 30 May 2022].

TalkTalk Group (2015h), "TalkTalk reaffirms commitment to customers", available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/TalkTalk-reaffirms-commitment-to-customers. [Accessed 3 June 2022].

TalkTalk Group. (2015i), "TalkTalk: serious about safety", available at: https://www.talktalkgroup.com/articles/talktalkgroup/TalkTalk-Group--moved-articles-/2016/TalkTalk--Serious-about-safety. [Accessed 1 May 2018].

TalkTalk Group (2016a), "Annual report 2016", available at: https://www.talktalkgroup.com/annualreports. [Accessed 6 June 2022].

TalkTalk Group (2016b), "TalkTalk supports Safer Internet Day 2016", available at: https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2016/TalkTalk-Supports-Safer-Internet-Day-2016. [Accessed 1 May 2018].

TalkTalk Group (2016c), "Sharing lessons of the cyber-attack—telegraph cybersecurity conference", available at: https://www.talktalkgroup.com/article/talktalkgroup/2016/New-content/Launch-content/Sharing-the-lessons-of-the-cyber-attack---Telegraph-Cyber-Security-Conference. [Accessed 5 June 2022].

Tounsi, W. and Rais, H. (2018), A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, Vol. 72, pp. 212-233. https://doi.org/10.1016/j.cose.2017.09.001

Tovey, A. (2015), "TalkTalk claims cyber-attack hit just 4pc of customers", available at: https://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/telecoms/11979032/TalkTalk-claims-cyber-attack-hit-just-4pc-of-customers.html. [Accessed 1 May 2018].

Tracey, P. and Phillips, N. (2016), Managing the consequences of organizational stigmatization: Identity work in a social enterprise. *Academy of Management Journal*, Vol. 59 No. 3, pp. 740-765. https://doi.org/10.5465/amj.2013.0483

Waller, P. (2015), "TalkTalk suspends X Factor sponsorship as shares dive after cyber hack", available at: https://www.mirror.co.uk/news/business/talktalk-suspends-x-factor-sponsorship-6711474. [Accessed 8 May 2022].

Wang, M.S., Raynard, M. and Greenwood, R. (2021), From grace to violence: stigmatizing the medical profession in China. *Academy of Management Journal*, Vol. 64 No. 6, pp. 1842-1872. https://doi.org/10.5465/amj.2018.0715

Wang, J., Neil, M. and Fenton, N. (2020), A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, Vol. 89, p. 101659. https://doi.org/10.1016/j.cose.2019.101659

Wangen, G., Hallstensen, C. and Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, Vol. 17 No. 6, pp. 681-699. https://doi.org/10.1007/s10207-017-0382-0

Warkentin, M. and Willison, R. (2009), Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, Vol. 18 No. 2, pp. 101-105. https://doi.org/10.1057/ejis.2009.12

Wiesenfeld, B.M., Wurthmann, K.A. and Hambrick, D.C. (2008), The stigmatization and devaluation of elites associated with corporate failures: a process model. *Academy of Management Review*, Vol. *33* No. 1, pp. 231-251. https://doi.org/10.5465/amr.2008.27752771

Wu, Y.L., Shao, B., Newman, A. and Schwarz, G., 2021. Crisis leadership: a review and future research agenda. *The Leadership Quarterly*, Vol. *32 No.* 6, p. 101518. https://doi.org/10.1016/j.leaqua.2021.101518

Zavyalova, A., Pfarrer, M.D., Reger, R.K. and Shapiro, D.L. (2012) Managing the message: the effects of firm actions and industry spillovers on media coverage following wrongdoing. *Academy of Management Journal*, Vol. 55 No. 5, pp. 1079-1101. https://doi.org/10.5465/amj.2010.0608

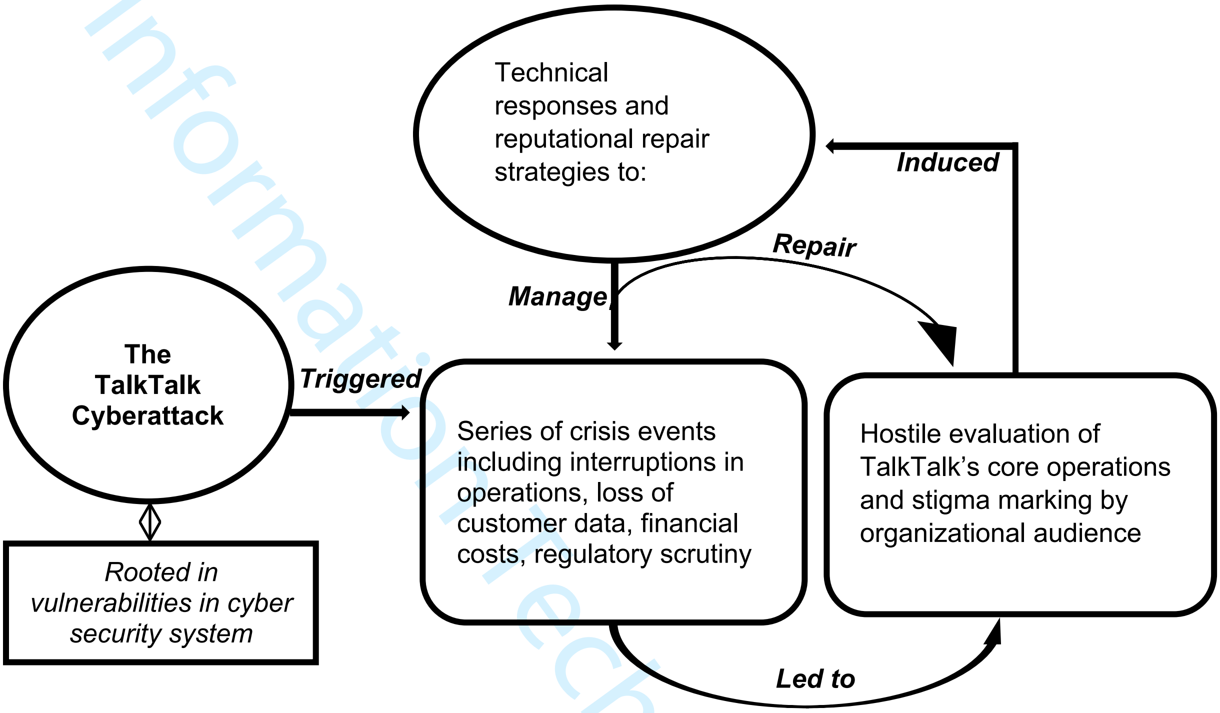
Żebrowski, P., Couce-Vieira, A. and Mancuso, A. (2022), A Bayesian framework for the analysis and optimal mitigation of cyber threats to cyber-physical systems. *Risk Analysis,* Vol. 42 No. 10, pp. 2275-2290. https://doi.org/10.1111/risa.13900

Appendix A: Data sources and weblinks

#	Data Sources	Weblink
1	Ahmed and Thomas (2015)	https://www.ft.com/content/9bfb4e72-7965-11e5-a95a-27d368e1ddf7
2	BBC (2015a)	http://www.bbc.co.uk/news/uk-34611857
3	BBC (2015b)	http://www.bbc.co.uk/news/uk-34615226
4	BBC (2015c)	https://www.bbc.co.uk/news/uk-34615260
5	BBC (2015d)	https://www.bbc.co.uk/news/uk-34784980
6	BBC (2016a)	http://www.bbc.co.uk/news/business-37565367
7	BBC (2016B)	https://www.bbc.co.uk/news/uk-37990246
8	Cellan-Jones, (2015)	https://www.bbc.co.uk/news/technology-34636308
9	Farrell, S. (2015	https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack
10	Farrell, S. (2016)	https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack
11	Gayle (2015)	https://www.theguardian.com/business/2015/oct/24/talktalk-attack-government-urged-to-do-more-on-cybercrime
12	Harding (2016)	https://soundcloud.com/uwebristol/baroness-dido-harding
13	Hern (2015)	https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack
14	ICO (2016)	https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded/
15	Johnston (2015)	https://www.theguardian.com/business/2015/oct/22/talktalk-customer-data-hackers-website-credit-card-details-attack
16	Khomami (2015a)	https://www.theguardian.com/business/2015/dec/15/talktalk-hack-could-not-have-been-prevented-by-cyber-essentials
17	Khomami, (2015b)	https://www.theguardian
18	Parliament (2015)	https://www.parliamentlive.tv/Event/Index/73368590-d756-4a37-badb-8174ac8ef239#p
19	Rodionova (2016a)	https://www.independent.co.uk/news/business/news/talktalk-fine-data-breach-theft-customers-information-stolen-record-penalty-a7346316.html
20	Spanier (2015)	https://www.campaignlive.co.uk/article/talktalk-suspends-advertising-x-factor-sponsorship-second-week/1370822

21	TalkTalk (2015a)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Statement-by-TalkTalk-PLC-on-Cyber-Attack---Thursday-October-22th-2015
22	TalkTalk (2015b)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Cyber-Attack-update---Saturday-October-24th-2015
23	TalkTalk (2015c)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles- /2015/Cyber-Attack-update---Monday-October-26th-2015
24	TalkTalk (2015d)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved- articles-/2015/TalkTalk-PLC-responds-to-Metropolitan-Police-update
25	TalkTalk (2015e)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Cyber-Attack-update---Tuesday-October-27th-2015
26	TalkTalk (2015f)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles- /2015/Cyber-Attack-update---Friday-October-30th-2015
27	TalkTalk (2015g)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/Cyber-Attack-update---Friday-November-6th-2015
28	TalkTalk (2015h)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles-/2015/TalkTalk-reaffirms-commitment-to-customers
29	TalkTalk (2015i)	https://www.talktalkgroup.com/articles/talktalkgroup/TalkTalk-Group--moved-articles- /2016/TalkTalk--Serious-about-safety.
30	TalkTalk (2016a)	https://www.talktalkgroup.com/annualreports
31	TalkTalk (2016b)	https://www.talktalkgroup.com/article/talktalkgroup/TalkTalk-Group--moved-articles- /2016/TalkTalk-Supports-Safer-Internet-Day-2016
32	TalkTalk (2016c)	https://www.talktalkgroup.com/article/talktalkgroup/2016/New-content/Launch-content/Sharing-the-lessons-of-the-cyber-attack---Telegraph-Cyber-Security-Conference
33	Tovey (2015)	https://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/telecoms/11979032/TalkTalk-claims-cyber-attack-hit-just-4pc-of-customers.html.

Figure 1: A framework of cyber-attack as reputational crisis


Technical responses and reputational repair strategies to:
Induced
Repair
Manage
The TalkTalk Cyberattack
Triggered
Series of crisis events including interruptions in operations, loss of customer data, financial costs, regulatory scrutiny
Hostile evaluation of TalkTalk's core operations and stigma marking by organizational audience
Rooted in vulnerabilities in cyber security system
Led to

Information Technology & People

Information Technology & People

Table 1: Main events characterizing the Talk-Talk cyber attack

	Date	Event
1	21 October 2015	The cyber-attack occurs
2	22 October 2015	The public is informed of the attack
3	23 October 2015	TalkTalk confirms they received an email from an anonymous entity demanding a ransom
4	06 November 2015	TalkTalk confirms that only 4% of its customers have been affected by the attack
5	15 December 2015	Dido Harding appears before the Parliamentary Select committee on Culture, Media, and Sports
6	May 2016	TalkTalk makes public the cost of the cyber-attack to the company
7	06 October 2016	The Information Commissioner Office fined TalkTalk £400,00 for the theft of customer details

Table 2: Quantitative details of data sources and contents

Data Sources	Analytical Content				
	TalkTalk's evaluation	*Audiences' evaluations*	*TalkTalk's Actions/responses*	*Nature of attack*	*Ransom demand/Cost*
News Articles (19):					
Ahmed & Thomas, 2015		*		*	
BBC, 2015a		*	*		
BBC, 2015b	*	*	*		*
BBC, 2015c		*			
BBC, 2015d			*		
BBC, 2016a		*	*		*
BBC, 2016b		*		*	*
Cellan-Jones, 2015		*	*	*	*
Farrell, 2015			*		*
Farrell, 2016			*		*
Gayle, 2015		*	*		
Hern, 2015			*		*
Johnston, 2015		*		*	*
Khomami, (2015a)	*	*	*	*	*
Khomami, 2015b	*		*		*
Rodionova, 2016			*		*
Spanier, 2015			*		*
Tovey, 2015	*				*

Waller (2015)		*			
Press Release (12):					
ICO, 2016	*	*	*	*	*
TalkTalk (2015a)	*		*		
TalkTalk, 2015b	*		*		
TalkTalk, 2015c			*		
TalkTalk, 2015d			*		
TalkTalk, 2015e			*		
TalkTalk (2015f)	*		*		*
TalkTalk (2015g)	*		*		*
TalkTalk (2015h)			*		
TalkTalk (2016a)	*				
TalkTalk (2016b			*		
TalkTalk, 2016c	*				
Parliamentary Hearing (1) and Podcast (1):	*	*	*	*	*

Table 3: A response-action heuristic model for managing cyberattacks

Response	Actions
Speed	Do not delay in identifying nature and magnitude of attack
Timing	Do no be hesitant to inform security agencies or industry regulators, and go public
Assurance	Accept guilt, render apology, communicate exactly what has happened but be succinct, and work with recognized security agencies
Remedy	Provide details on how the attack is/has been dealt with, engage in cyber-related social/educational events, highlight pre-emptive measures to avoid re-occurrence

Information Technology & People