

# UNIVERSITA' DEGLI STUDI DI VERONA

*DIPARTIMENTO DI*

*SCIENZE ECONOMICHE*

*SCUOLA DI DOTTORATO DI*

*SCIENZE GIURIDICHE ED ECONOMICHE*

*DOTTORATO DI RICERCA IN*

*ECONOMICS AND MANAGEMENT*

CICLO/ANNO

30°/2014

TITOLO DELLA TESI DI DOTTORATO

Managing cyber risk in organizations and supply chains

S.S.D. SECS-P/08

Coordinatore: Prof. Roberto Ricciuti

Tutor: Prof.ssa Barbara Gaudenzi

Dottorando: Dott.ssa Giorgia Giusi Siciliano

Contents	
Introduction.....	4
1. Just do it. Managing IT and Cyber Risks to Protect the Value Creation.....	28
1.1 Introduction.....	28
1.2 Literature review.....	30
1.2.1 Information technology and cyberspace .....	30
1.2.2 Managing IT and cyber risks to protect the value creation.....	31
1.3 Methods and data.....	32
1.3.1 The method .....	32
1.3.2 Research sample and data collection.....	33
1.3.3 Variable descriptions.....	34
1.3.4 Fuzzy solution generation .....	35
1.4. Results.....	37
1.4.1 Descriptive statistics: IT and cyber risk perceptions.....	37
1.4.2 Fuzzy analysis: Risk management solutions to protect the value creation .....	38
1.4.3 A proposed framework for managing IT and cyber risks. ....	39
1.5. Discussion.....	40
1.6. Conclusions.....	43
References.....	44
2. Managing IT and Cyber Risks in Supply Chains.....	53
2.1 IT risks and Cyber risks: real threats for all supply chains....	53
2.2 How external Cyberspace and IT tools generate risks. ....	55
2.3 Managing IT and Cyber risks in supply chains: A practical framework.....	57
2.4 Practical evidence from a European sample of companies. ...	61
2.5 Conclusions.....	68

References.....	70
3. Effects of data breaches from user-generated content: A corporate reputation analysis.....	77
3.1 Introduction.....	78
3.2 Literature review and theoretical development.....	81
3.2.1 Corporate reputation .....	81
3.2.2 Data breaches .....	82
3.2.3 Social media.....	83
3.2.4 Situational crisis communication theory.....	84
3.3 Methodology .....	85
3.3.1 Sampling .....	85
3.3.2 Research design.....	88
3.3.3 Latent Dirichlet allocation... ..	89
3.3.4 Content and valence analysis of user-generated content.....	90
3.4	
Results.....	91
3.4.1 Dimensions of reputation for intentional and internal data breaches.....	94
3.4.2 Dimensions of reputation for unintentional and internal data breaches.....	97
3.4.3 Dimensions of reputation for intentional and external data breaches.....	99
3.5 Discussion... ..	103
3.5.1 When and how customers react to data breaches?.....	104
3.5.2 When and how customers pay attention to firms' ability to protect their privacy .....	106
3.5.3 Customers' perceptions and valence across industries .....	107
3.6 Contributions.....	108
3.7 Conclusions.....	109
References.....	111

Appendices.....	122
Conclusions.....	128
References.....	130

# INTRODUCTION

## INTRODUCTION

The academic literature has extensively confirmed that firms and their supply chains (SCs) are vulnerable to a wide range of risks (Zsidisin, 2003). From a single firm perspective, the risk management discipline has evolved from a traditional, defensive approach focused on the prevention of and protection against adverse financial and operational consequences (Gaudenzi and Borghesi, 2006) to the more proactive enterprise risk management (ERM) approach (Gatzert and Martin, 2015) and the wider concept of resilience in SC networks (Christopher, 2016; Ponomarov and Holcomb, 2009).

An emerging risk for firms and SCs is cyber risk, whose occurrence has dramatically increased over the last years, jumping from fourth to second place in the most-reported types of economic crime in 2016 (PWC Global Economic Crime Survey of 2016).

The digitalization and extensive use of information technology (IT) represents a fertile field for both malevolent actors and unintentional cyber-related mistakes that lead to business disruption and damages to tangible and intangible corporate assets, such as financial and reputational drawbacks (Amin, 2017; Martin et al., 2017; Martin and Murphy, 2017; Eling and Schnell, 2016; Romanosky, 2016).

The IT literature has shown great interest in cyber risk, mainly identifying technical solutions to face these emerging risks.

Nonetheless, cyber risks require a major integration between technical solutions and strategic management. Recently, the risk management domain and the SC literature have provided studies about how an effective cyber risk management process should be planned to improve firmal resilience and prevent financial drawbacks.

The risk management process consists of two main phases: (i) the risk assessment, comprising the risk identification, risk analysis and risk evaluation and (ii) the risk treatment (ISO 31000, 2009).

The risk assessment process is a set of systematic activities that provide rigorous identification, measurement, quantification and evaluation for each risk (Haines, 2015; Zsidisin et al., 2004;

Zsidisin et al., 2000). Risk treatment, on the other hand, is the process of taking a specific course of action to reduce the probability and impact of risks and to transfer the financial consequences of negative events to third parties (Pritchard, 2014; Chopra and Sodhi, 2004).

In such a context, a thorough cyber risk assessment should consider the inherent characteristics of cyber risks so that firms are sure to allocate specific investments accordingly (PWC, 2014).

In particular, two major characteristics of cyber risk have been ascertained in the literature: (i) the probability of occurrence and (ii) its different sources (Eling and Schnell, 2016; Biener et al., 2015; Refsdal et al., 2015).

With respect to the probability of occurrence, cyber risks may be distinguished between ‘black swans’, or incidents that occur as a complete surprise (Ab Rahman et al., 2016; Refsdal et al., 2015; Higgins, 2014; Coburn et al., 2013) and ‘grey swans’, which are incidents that could be anticipated (Ab Rahman et al., 2016; Refsdal et al., 2015; Coburn et al., 2013).

Furthermore, both management practitioners and academicians have tried to categorise the different types of cyber risk (Table 1).

The Privacy Rights Clearinghouse (<https://www.privacyrights.org>) provides a fairly comprehensive database in which data breaches since 2005 are categorised across two dimensions: the level of intentionality characterising the cyber issue and whether cyber risks may stem from inside or outside the company.

The management literature has confirmed this categorization. In particular, a cyber risk may be caused accidentally by actors within the firm (Furnell et al., 2017; Eling and Schnell, 2016; Hall, 2016; Sen and Borle, 2015; Pearson et al., 2014; Strand, 2014; Jaeger, 2013) or deliberately by internal or external actors to damage companies (Kude et al., 2017; Eling and Schnell, 2016; Manworren et al., 2016; Refsdal et al., 2015; Sen and Borle, 2015; Srinidhi et al., 2015).

<p style="text-align: center;"><b>INTENTIONALITY</b></p> <p style="text-align: left;"><b>PLACE</b></p>	<p style="text-align: center;"><b>INTENTIONAL</b></p>	<p style="text-align: center;"><b>UNINTENTIONAL</b></p>
<p style="text-align: center;"><b>OUTSIDE THE ORGANIZATION</b></p>	<p>1. Malware, hacking, phishing, denial of service attacks, click fraud, privacy breaches, frauds, violation of digital property rights (Kude et al., 2017; Eling and Schnell, 2016; Mauworrren et al., 2016; Refsdal et al., 2015; Sen and Borle, 2015; Srinidhi et al., 2015)</p>	
<p style="text-align: center;"><b>INSIDE THE ORGANIZATION</b></p>	<p>2. Someone with legitimate access intentionally breaches information (e.g., an employee or contractor) (Sen and Borle, 2015; Srinidhi et al., 2015)</p>	<p>3. Sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, sending in an email, sending in a mailing or sending via fax Jaeger, 2013; Pearson et al., 2014; Strand, 2014; Sen and Borle, 2015; Eling and Schnell, 2016; Hall, 2016; Furnell et al., 2017</p>

**Table 1. Categorization of cyber risks**

Despite advances in categorizing these vulnerabilities, cyber risk assessment still appears to be challenging. In fact, the current guidelines for defining likelihood, a key point in the risk assessment phase, may be of little help in identifying and predicting black swans, but may be well suited to cope with so-called ‘grey swans’ (Refsdal et al., 2015).

In this phase, studies stress the relevance of involving experts in the field, as their experience may help in assessing present and future cyber-related threats (Amin, 2017; Caldwell 2017; Biener et al., 2015).

With respect to risk treatment, particularly risk treatment solutions, the literature highlights that a sustainable cyber insurance market is still in its infancy, and there is a need to improve the competitiveness of the cyber insurance market (Marotta et al., 2017; Eling and Schnell, 2016; Romanosky, 2016; Biener et al., 2015; Yang and Lui, 2014).

Cyber risk transfer has played only a minor role because of a lack of data; the dynamicity of cyber risks – namely, the high risk of change; and information asymmetry problems (Marotta et al., 2017; Eling and Schnell, 2016; Biener et al., 2015). Moreover, the literature highlights that market offerings to cover malicious cyber risk are more developed than those for non-

malicious events (Franke, 2017).

The extant cyber insurance literature suggests systematic data collection to capture the dynamic changes affecting the cyber insurance market and to provide a path for improving insurance coverage. Moreover, Woods et al. (2017) stress the relevance of the policy maker's involvement to avoid disparity between insurance practices and IT best practices.

Romanosky (2016) points out that not every data breach is dramatic, such as the one Target suffered that exposed the personal data of 70 million customers in 2013 (Martyn, 2015). A scarce range of cyber insurance policies may consequently be due to the generally moderate business costs stemming from the occurrence of cyber risk. Eling and Schnell (2016) only partially agree with this view, suggesting that while the costs and detrimental effects cyber risk causes must be critically questioned, the major part of these detrimental effects is indirect (e.g. reputation, loss of trust). Moreover, given a globally connected economy and society, the potential consequences of cyber risks for companies and individuals are considerable, leading to enormous accumulations risk insurers should consider.

Yang and Lui (2014) underline how decisions about investing in cyber insurance stem from an interdependent process where security investments made by one node of the business network can affect the security risk of the others. In this context, companies' prevention measures depend on the security policies of their partners and customers; they are as exposed as their weakest link is (Khan and Estay, 2015). Thus, the presence of insurance policies that cover various levels of the business network's nodes may be a positive incentive for security adoption (Yang and Lui, 2014).

In spite of its increasing relevance for firms, cyber risk research is still limited. The majority of research can be found in the information management and technology domain, with few studies in the management and economics literature (Eling and Schnell, 2016; Biener et al., 2015). From an SC perspective, cyber risks are among the inherent risks of a more volatile business environment. For example, 600 million Samsung Galaxy phones were recently discovered to have a major security flaw originating from one of Samsung's keyboard software suppliers, and the 2013 Target breach stemmed from a hacker attack on one of Target's multinational vendors (Martyn,

2015).

In this context, Christopher (2016) stresses how studies have shifted from a mainly operational approach (Yang et al., 2017; McNeil et al., 2015; Stevenson and Hojati, 2007) to a more strategic one focused on value creation and delivery (Christopher, 2016; Bromiley et al., 2015; Gatzert and Martin, 2015). This means the literature is abandoning the logistics lens when studying SCs and now considers them complex networks made up of 'multiple suppliers and, indeed, suppliers to suppliers as well as multiple customers and customers' customers' (Christopher, 2016, Inp. 3). As these relationships are increasingly interdependent, the main goal cannot be cost minimisation or service optimisation, but rather implementing strategic actions, such as encouraging more collaborative work, in order to achieve greater visibility of upstream and downstream risk profiles and a shared involvement in managing those risks (Christopher, 2016; Ponomarov and Holcomb, 2009). With particular respect to cyber risks, Khan and Estay (2015) highlight that modern SCs are a lucrative and easy target for cyber criminals because of the amount of strategic information they share. The authors suggest developing superior resilience, which refers to the SC's ability to cope with unexpected disturbances, and recognising the paramount importance of companies developing cyber-resilience, defining it as 'the capability of a SC to maintain its operational performance when faced with cyber-risk' (p. 7).

The related literature suggests that, to improve cyber-resilience, strategic actions should involve government entities and boost business-to-business (B2B) and business-to-government (B2G) data sharing (Urciuoli, 2015). In general, SC cyber-resilience requires shifting from mere technological solutions to a more holistic approach (Boyes, 2015) in which information, visibility and transparency are implemented both upstream and downstream (Davis, 2015).

However, Khan and Estay (2015) stress that there is a lack of theoretical and empirical research to address cyber risks within SCs.

From a single firm perspective, the management literature mainly focuses on the customer-related drawbacks a cyber breach causes, drawing from the concepts of data privacy management and reputation management (Martin, 2018; Ferrell, 2017; Kashmiri et al., 2017; Martin and Murphy, 2017; Martin

et al., 2017; Manworren et al., 2016).

Studies ascertain that customers respond negatively to data breaches, producing a range of negative emotional and cognitive responses against the firm (Martin et al., 2017). What is more, the increasing prominence of social media and digital evolution represent additional threats to firms, amplifying such negative effects on reputation (Gatzert, 2015) and financial performance (Martin et al., 2017).

However, the aforementioned research fails to capture other equally relevant effects, such as corporate reputation harm.

Management studies also highlight that the role of management is of paramount importance in training employees (Soomro et al., 2016; Strand, 2014), to facilitate the upstream reporting of issues and to engage in efficient and clear communication with customers (Soomro et al., 2016). Investing in human capital and training should lead to greater awareness. In fact, most people are trained to keep their firewalls and anti-virus software updated (Hall, 2016; Strand, 2014), but data breaches often occur due to negligence, ignorance, apathy or resistance (Safa et al., 2015).

Nonetheless, there is a lack of research providing guidance on and frameworks about how to boost a cyber security culture that renders cyber risk management procedures fully understood and accepted (Ferrell, 2017; Manworren et al., 2016).

As shown above, there have been significant descriptive studies documenting data security issues. However, cyber risk actors must be further analysed, and the implications for customers, employees and critical assets like corporate reputation should be addressed (Ferrell, 2017; Martin et al., 2017).

### **Scope of the research and publications**

During the Ph.D. program, a comprehensive analysis of the potential effects of cyber threats was conducted within single companies and along networks of relationships in a wider SC perspective.

As a consequence, three studies have been developed to investigate cyber risk management, adopting two different units of analysis: the single firm and the SC.

The three studies aim at addressing the following research questions, which encompass several theoretical and managerial implications:

- How do managers perceive and define cyber risk? What is the difference from IT risk?
- How does cyber risk represent a threat to the value creation of a single company?
- When and how does cyber risk affect the continuity and vulnerability of the SC?
- When and how does cyber risk affect the reputation of the downstream SC?

**Gaudenzi, B., & Siciliano, G. (2017). Just do it. Managing IT and Cyber Risks to Protect the Value Creation. Journal of Promotion Management, 1-14**

The paper is published in the Journal of Promotion Management, a peer-reviewed publication indexed in Scopus. The research was developed in collaboration with Prof. Barbara Gaudenzi.

The focus of the research is two-fold.

The first aim of this research is to study cyber risk as a business disruptor and its differences with respect to IT operational risks. In fact, the literature provides scant contributions that define cyber risk, which have mainly related to IT risk (Ward, 2012; Sheriff et al., 2011; Melville, 2010) and have sometimes used cyber risk as its synonym (Schryen, 2013; Smirnov et al., 2013; Von Solms and Van Niekerk, 2013; Mithas et al., 2011).

The second goal of this empirical analysis is to provide in-depth insights into how managers plan an efficient and effective risk management process.

Considering the novelty of the investigation and the need to use an inductive approach that builds theory from data (Eisenhardt and Graebner, 2007; Suddaby, 2006), the study addressed a questionnaire to 15 companies, grounding it in the literature. In particular, the study is grounded in the dynamic capabilities perspective (Teece, Pisano, & Shuen, 1997; Eisenhardt & Martin, 2000; Winter, 2003; Teece, 2007) in order to analyse how relational, firmal and technical capabilities should be integrated (Eisenhardt & Martin, 2000; Teece, 2007) to better manage IT and cyber risks.

In this perspective, the authors highlight that the (risk) perceptions of individual actors in different functions of the firm should be well aligned to make good decisions (Ambrosini &

Bowlman, 2009; Li & Liu, 2014; Helfat & Peteraf, 2015).

This process led to interviews with 15 security/risk managers of European firms, whose answers were then analysed through a fuzzy set qualitative comparative analysis (fsQCA) (Fiss, 2011; Ragin and Fiss; 2008; Rihoux, 2006; Ragin and Pennings, 2005).

This qualitative methodology has been increasingly used in management studies (Kraus et al., 2017) because of its main advantage in that it provides configurations of the solutions subjects use to reach a specific goal (Tóth et al., 2017; Yu et al., 2016; Rihoux, 2006). In this case, the implementation of the fsQCA methodology was particularly fitting, as it highlighted the different cyber risk management solutions managers adopt to reach the same goal – superior firm performance.

The findings reveal that IT risks are categorised as vulnerabilities stemming from firms' offline activities, while cyber risks are considered third-party intrusions. Moreover, the results highlight that cyber risks are still far from being considered more than mere technological issues and stress the need to go beyond the traditional risk management process.

Therefore, the study proposes a framework grounded in the dynamic capabilities theory for managing cyber risk through a holistic approach in the protection of value creation. In particular, the study advances the notion that cyber risks are not merely a matter of technological measures to be adopted. Cyber risks require the development of strong dynamic capabilities to better sense emerging cyber threats and to develop the resilience and capacity to continuously adjust and adapt strategic directions to keep creating value for a company, despite external and internal threats. Thus, for cyber risk issues, the study confirms the need to improve the 'sensing, seizing, and transforming' capabilities suggested by the pillars of the dynamic capabilities theory (Teece et al, 2016; Teece, 2007; Winter, 2003; Eisenhardt & Martin, 2000; Teece, Pisano, & Shuen, 1997). In particular, dynamic capabilities should involve the identification, development, co-development and assessment of technological threats; the investment of resources to address threats while capturing value ('seizing'); and the promotion of evolution ('transforming' or 'shifting') (Teece & Leih, 2016; Teece et al., 2016; Fawcett et al., 2011;). The aforementioned framework highlights a link rarely explored before: the role of

firmal and managerial implications when guiding an enterprise under conditions of emergent risks.

**Gaudenzi, B., & Siciliano, G. (2018). Managing IT and Cyber Risks in SC. In SC Risk Management (pp. 85-96). Springer, Singapore**

The second study was published as a chapter in SC Risk Management, published by Springer in 2018. The research was developed in collaboration with Prof. Barbara Gaudenzi, who supervised the entire publication process.

The research question the study aims to address is: When and how does cyber risk affect the continuity and vulnerability of the SC?

The study aims to fill a gap in the SC and risk management literature where there seems to be scarce theoretical frameworks that link risk-management processes to cyber risk throughout the SC. Therefore, an SCRM framework is provided that considers how to assess and mitigate cyber risks and failures, such as piracy and theft, product shortages and safety and security, across SC processes.

Moreover, the chapter fills the gap in the current literature about how the characteristics of companies comprising the SC influence cyber risk management. In fact, most risk management literature shares the idea that small and mid-sized companies lack the awareness, resources and skills to prevent and mitigate cyber activities, while larger firms might be more effective in tackling these emergent risks (Berry & Berry, 2018; Low, 2017; Epstein, 2014). Moreover, the European Political Strategy Centre (2017) stresses that there is a lack of information on the status quo of cyber security among European companies, in contrast to other countries such as the US. The report highlights how this under-reporting ‘represents a major hurdle to better understanding and addressing cyber threats and provides scope for new vulnerabilities to spread more widely’ (European Political Strategy Centre, 2017, p.4).

In consideration of the above insights, the study aims to investigate whether size is relevant for not only cyber risk management in a single company but also when the unit of analysis is the risk management process of the entire SC. Moreover, it focuses on Europe to unveil the state of cyber security. Thus, the sample involves European companies and

their SCs. In particular, it includes one small, local company with a revenue under €1 million and between 10 and 100 employees; seven mid-sized companies with revenues between €1 million and €500 million and less than 50,000 employees and that represent various interests internationally; and seven large companies with revenues exceeding €10 billion and more than 50,000 employees, which were evenly distributed in their level of internationalization.

Even though the study's narrow focus on 15 companies precludes the generalization of its findings, some general outcomes may be obtained. In particular, it confirmed that from an SC perspective, cyber risk may dramatically affect SC business continuity and is not a mere technological issue. The results stress a lack of information sharing and visibility in the relationship between the focal firm and its suppliers as well as an insufficient number of cyber risk measures implemented. As security investments made by one node of the business network can affect the security risk of the others, resulting in exposure at the business's weakest link (Khan and Estay, 2015; Yang and Lui, 2014), the interdependency among firms exacerbates cyber risk issues in SCs. Another meaningful finding shows that managers perceive cyber risks as reputational threats toward customers. This is because a breach of personal information is considered less tolerable than threats to B2B partners.

This study's main contribution has been the design of a framework for managing cyber risk in SCs, adopting the following risk management measures.

First, it suggests enhancing the levels of compliance with security regulations. In fact, a wide range of policies and procedures has been provided concerning the use of IT by all users and protections against external hackers. Compliance with policies such as COBIT, 2000; ISO 31000, ISO/IEC 27001 (Biener et al., 2015; Mangalaraj et al., 2014; Mukhopadhyay et al., 2013; Shackelford, 2012; Von Solms, 2005) is considered an internationally accepted best practice to ensure the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people, etc.), and it is therefore an essential requirement for good corporate governance.

Failure to comply might exacerbate vulnerability and exposure to various drawbacks. In fact, the adoption of formal regulations would not only protect from cyber risks, but also prevent other

actors in the chain from adopting a negative attitude toward the non-compliant company.

Second, the framework promotes the implementation of cyber risk assessment and prevention procedures that might include a cost-benefit analysis of the cyber risk exposure, assessing the current insurance coverage and systematically calculating the probabilities of a cyber event to detect and prevent attacks as they occur and, when possible, before the data breach can be launched ((Biener et al., 2015; Shackelford, 2012; Mukhopadhyay et al., 2013; Dondossola et al., 2009; Von Solms, 2005).

This would require a revolution in SC security culture, as in every company, the back-office IT, maintenance, operations, consumer-facing systems, management, and the board would be involved. Moreover, it should strengthen cybersecurity capabilities, including identity and access management, data protection and encryption, design and application security and security awareness (PWC, 2016).

Third, should a risk occur, the framework stresses the relevance of structured SC risk mitigation strategies. Some of the variables that enable risk mitigation are information sharing, aligning incentives and risk sharing (Christopher & Gaudenzi, 2015; Gaudenzi, 2009; Zsidisin & Ritchie, 2009), and the literature suggests these measures should not be used in isolation, but rather in concert one with one another (Faisal et al., 2006).

Fourth, the framework underlines also the importance of IT governance, which is ‘the firmal capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT’ (Mangalaraj et al., 2014; De Haes & Van Grembergen, 2004; Webb et al., 2006).

In this context, the study highly recommends that managers better define and communicate the company’s level of appetite and tolerance for cyber risk. The presence of IT governance in the framework stresses the relevance of specific training programs for human resources at all levels.

The implementation of the framework should lead to at least three advantages for the whole SC, namely strategic benefits, such as controlling the level of risk for the entire SC and standardising compliance to legal requirements; reputation protection, which would prevent reputation crises and reinforce cooperation and SC relationships; and business continuity,

which involves decreasing the severity of disruptions and controlling costs.

The main contribution of the study is a framework relevant to both managers and academicians. From a practical perspective, the framework promotes a formal and systematic mitigation plan, suggests a strong commitment from top management and clarifies the company's real risk appetite and tolerance. From an academic perspective, the proposed cyber risk management framework seems to fill a gap in the literature and addresses how systematic IT and cyber risk management may enhance the ability to share information and better manage SC processes.

**Giorgia G Siciliano, Ilenia Confente, Barbara Gaudenzi and Matthias Eickhoff (2017). Effects of data breaches from user-generated content: A corporate reputation analysis (under review for European Management Journal)**

The third study is under review for the European Management Journal, a flagship international scholarly journal with an impact factor of 2.608. The research was developed in collaboration with Prof. Barbara Gaudenzi, Prof. Ilenia Confente and Ph.D. candidate Matthias Eickhoff.

The aim is to discover how reputational dimensions change before and after a cyber risk occurs as well as the differences among the types of data breaches and industries.

Reputation is considered a strategic intangible asset for companies because it substantially contributes to a competitive advantage (Gatzert and Schmit, 2016; Gatzert, 2015; Rindova and Fombrun, 1999).

However, gaining from connectivity without losing trust is a delicate balancing act (PWC, 2016) that a cyber breach may compromise. In fact, the Global Economic Crime Survey of 2016 reports that reputational damage to both employees and external stakeholders is the most damaging effect of a cyber breach.

Corporate reputation literature infers different dimensions composing a company's reputation, which stem from the different perceptions of customers, suppliers, (potential) employees, investors and local communities (Eckert, 2017; Gatzert, 2015; Wepener and Boshoff, 2015; Walker, 2010; Walsh et al., 2009; Walsh and Beatty, 2007).

While the negative influence of cyber risks on corporate

reputation seems clear, little is said about which reputational dimensions are mainly eroded by these threats or the effects of the redundancy of these scandals on social media.

The study uses a mixed methods approach, following the suggestions of the recent literature (Golicic and Davis, 2012; Spens and Kovacs, 2012; Seuring, 2011) that encourage the combination of qualitative and quantitative methods within a single SC study to provide multiple perspectives on the phenomenon under investigation. In particular, the paper analyses 250,000 social media posts generated by users, or user-generated content (UGC), for a sample of 35 data breach incidents between 2013 and 2016, triangulating a content analysis with the latent Dirichlet allocation (LDA) analysis. This latter method is part of the topic model methods and is particularly fitting for the scope of the research. It allowed the researchers to ascertain the corporate latent reputation dimensions that consumers do not explicitly mention (Tirunillai and Tellis, 2014), but that are in fact the main topic of the social media posts they write.

The literature review and data collection phase were conducted at the University of Göttingen, Faculty of Economic Sciences, under the supervision of Prof. Jan Muntermann, chair of electronic finance and digital markets.

The results reveal that, compared with the antecedent period, a greater number of reputational dimensions emerged after critical events and provide key insights for academia and industry to understand large-scale data breaches and the reputational drawbacks after such critical incidents.

This study provides both academic and practical contributions to the literature. With respect to the theoretical perspective, the study contributes to the crisis communication research field (Coombs and Holladay, 2002), risk management literature (Gatzert, 2015) and reputation research (Wepener and Boshoff, 2015; Walsh et al., 2009; Walsh and Beatty, 2007), as it is one of the first studies to test corporate reputation dimensions in a data breach crisis context (Martin and Murphy, 2017; Martin et al., 2017).

The managerial implications of this study lie both in the categorization of the main reputational drivers that managers should consider when designing a communication recovery response and in the suggestion of a methodology – an LDA analysis triangulated with a content and valence investigation –

that may be implemented to unveil the corporate reputation dimensions that emerge in rich UGC after a data breach.

### **3. Research in progress**

Two research projects are in progress.

With respect to the first, a study is currently being conducted to provide an illustrative case study of an firm's practices in mitigating cyber risk and its influence on SC financial structures. The study aims to fill a gap in the literature regarding the integration of risk management and SC finance, an area that demands further definition and conceptual foundation (Gelsomino et al., 2016; Pfohl and Gomm, 2009; Wuttke et al., 2013).

The research is in collaboration with George Zsidisin, professor of SC management at Virginia Commonwealth University, and Prof. Barbara Gaudenzi.

The study has been accepted for publication in *SC Finance: Solutions for Financial Sustainability, Risk Management and Resilience in the SC*, an edited collection published by Kogan Page.

The second planned study is in collaboration with Prof. Jan Muntermann, chair of electronic finance and digital markets at the University of Göttingen. The study focuses on the public announcements firms release regarding the implementation of cyber risk management procedures after cyber breaches. In particular, it will investigate the impact of these announcements on UGC produced by customers on social media. The method of synthetic control will be used to construct a counterfactual (synthetic) brand to verify whether the implementation of the aforementioned measures positively contributes to restoring benevolent aspects in customer relationships, filling a gap in the marketing and management literature (Martin et al., 2017; Tirunillai and Tellis, 2017).

### **4. Future research directions**

The literature needs further observations of when and how cyber data breaches affect relationships with stakeholders (Krafft et al., 2017; Rasoulilian et al., 2017; Schneider et al., 2017; Stewart et al., 2017; Markos et al., 2016). In this context, I intend to conduct future research to develop a taxonomy of situational

factors that influence stakeholders' behaviours and perceptions. A regression model may measure the impact of some contingences, such as the crisis history of a firm (Rasoulilian et al., 2017) or the firm's sharing of stakeholders' data with external partners (Schneider et al., 2017). Moreover, while the third study mentioned above focused on users' perceptions after cyber-related scandals in European countries, it would be beneficial to expand the number of countries studied in order to ascertain whether there is a continuum of countries with different levels of cyber-related privacy concerns (Krafft et al., 2017; Markos et al., 2016).

## References

- Ab Rahman, N. H., Glisson, W. B., Yang, Y., & Choo, K. K.R. (2016). Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Computing*, 3(1), 50-59.
- Amin, Z. (2017). A practical road map for assessing cyber risk. *Journal of Risk Research*, 1-12.
- Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, 8(1), 1-10.
- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance Issues and Practice*, 40(1), 131-158.
- Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, 5(4), 28.
- Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long range planning*, 48(4), 265-276.
- Caldwell, T. (2017). The UK's £ 1.9 bn cyber-security spend—getting the priorities right. *Computer Fraud & Security*, 2017(3), 12-20.
- Chopra, S., & Sodhi, M. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review*, 46(1), 53–61
- Christopher, M. (2016). *Logistics & supply chain management*. Pearson UK.
- Christopher, M., & Gaudenzi, B. (2015). Managing risks in sustainable supply chains. *Sinergie Italian Journal of Management*, 57-74.

Coburn, A., Ralph, D., Tuveson, M., Ruffle, S., & Bowman, G. (2013). A taxonomy of threats for macro-catastrophe risk management. Centre for Risk Studies, Cambridge: University of Cambridge, Working Paper, July, 20-24.

Higgins D M., (2014),"Fires, floods and financial meltdowns: black swan events and property asset management", *Property Management*, Vol. 32 Iss 3 pp. 241 – 255.

Davis, A. (2015). Building cyber-resilience into supply chains. *Technology Innovation Management Review*, 5(4), 19.

De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal*, 1, 27-33.

Dondossola, G., Garrone, F., & Szanto, J. (2009, March). Supporting cyber risk assessment of power control systems with experimental data. In *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES* (pp. 1-3). IEEE.

Eckert, C. (2017). Corporate reputation and reputation risk: Definition and measurement from a (risk) management perspective. *Journal of Risk Finance*, 18(2), 145–158.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal*, 50(1), 25-32.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*, 17(5), 474-491.

EPSC Strategic Notes, Building an Effective European Cyber Shield Taking EU Cooperation to the Next Level [http://ec.europa.eu/epsc/sites/epsc/files/strategic\\_note\\_issue\\_2\\_4.pdf](http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_2_4.pdf)

Epstein, A. J. (2014). Thinking strategically about cyber risk. *NACD Directorship*, 32-35.

Fawcett, S. E., Wallin, C., Allred, C., Fawcett, A. M., & Magnan, G. M. (2011). Information technology as an enabler of supply chain collaboration: a dynamic-capabilities perspective. *Journal of Supply Chain Management*, 47(1), 38-59.

Ferrell, O. C. (2017). Broadening marketing's contribution to data privacy. *Journal of the Academy of Marketing Science*, 45(2), 160–163.

Fiss, P. C. (2011). Building better causal theories: A fuzzy set approach to typologies in organization research. *Academy of Management Journal*, 54(2), 393-420.

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security*, 68, 130-144.

- Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, 2017(2), 5-10.
- Gatzert, N. (2015). The impact of corporate reputation and reputation damaging events on financial performance: Empirical evidence from the literature. *European Management Journal*, 33(6), 485–499.
- Gatzert, N., & Martin, M. (2015). Determinants and value of enterprise risk management: empirical evidence from the literature. *Risk Management and Insurance Review*, 18(1), 29-53.
- Gatzert, N., and Schmit, J. (2016). Supporting strategic success through enterprise-wide reputation risk management. *Journal of Risk Finance*, 17(1), 26–45.
- Gaudenzi, B. (2009). Assessing risks in projects and processes. In *Supply Chain Risk* (pp. 67-82). Springer, Boston, MA.
- Gaudenzi, B., & Borghesi, A. (2006). Managing risks in the supply chain using the AHP method. *The International Journal of Logistics Management*, 17(1), 114-136.
- Gelsomino, L.M., Mangiaracina, R., Perego, A., Tumino, A., 2016. Supply Chain Finance: a literature review. *International Journal of Physical Distribution and Logistics Management*, 46(4), 1–19.
- Glaser, Barney G. and Anselm L. Strauss (1967), *The Discovery of Grounded Theory: Strategies for Qualitative Research*, New York: Aldine De Gruyter.
- Global Economic Crime Survey of 2016, Retrieved from <http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html> Accessed 20/08/2017
- Golicic, S. L., and Davis, D. F. (2012). Implementing mixed methods research in supply chain management. *International Journal of Physical Distribution and Logistics Management*, 42(8/9), 726-741.
- Haimes, Y. Y. (2015). *Risk modeling, assessment, and management*. John Wiley & Sons.
- Hall, M. (2016). Why people are key to cyber-security. *Network Security*, 2016(6), 9-10.
- ISO 31000:2009 Risk management -- Principles and guidelines Retrieved from <https://www.iso.org/standard/43170.html> Accessed 02/10/2016
- Jaeger, J. (2013). Human error, not hackers, cause most data

- breaches. *Compliance Week*, 10(110), 56-57.
- Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, 45(2), 208-228.
- Khan, O., & Estay, D. A. S. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*, 5(4).
- Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission Marketing and Privacy Concerns—Why Do Customers (Not) Grant Permissions?. *Journal of Interactive Marketing*, 39, 39-54.
- Kraus, S., Ribeiro-Soriano, D., & Schüssler, M. (2017). Fuzzy-set qualitative comparative analysis (fsQCA) in entrepreneurship and innovation research—the rise of a method. *International Entrepreneurship and Management Journal*, 1-19.
- Kude, T. H., Hoehle & Sykes, T. A. (2017). Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *International Journal of Operations & Production Management*, 37(1), 56-74.
- Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security*, 2017(4), 18-20.
- Mangalaraj, G., Singh, A., & Taneja, A. (2014). IT governance frameworks and COBIT-a literature review.
- Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, 59(3), 257-266.
- Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. *Journal of Public Policy & Marketing*, jppm-15.
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*.
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135-155.
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58.
- Martyn P., (2015). Risky Business: Cybersecurity And Supply Chain Management. *Forbes*. Retrieved from

<https://www.forbes.com/sites/paulmartyn/2015/06/23/risky-business-cyber-security-and-supply-chain-management/#1b62cef55543> Accessed 30/06/2017

McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management: Concepts, techniques and tools*. Princeton university press.

Melville, N. P. (2010). Information systems innovation for environmental sustainability. *MIS Quarterly*, 34(1), 1–21.

Mithas, S., Ramasubbu, N., & Sambamurthy, V. (2011). How information management capability influences firm performance. *MIS Quarterly*, 35(1), 237–256.

Mohd Nishat Faisal, D.K. Banwet, Ravi Shankar, (2006) "SC risk mitigation: modelling the enablers", *Business Process Management Journal*, Vol. 12 Issue: 4, pp.535-552.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not?. *Decision Support Systems*, 56, 11-26.

Pearson, N. (2014). A larger problem: financial and reputational risks. *Computer Fraud & Security*, 2014(4), 11-13.

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The international journal of logistics management*, 20(1), 124-143.

Pritchard, C. L., & PMP, P. R. (2014). *Risk management: concepts and guidance*. CRC Press.

Privacy Rights Clearinghouse database. Retrieved from <https://www.privacyrights.org> Accessed 10/01/2017

PWC, 2014 “Prioritising your investment” Retrieved from <https://www.pwc.com/sg/en/risk-assurance/assets/cyber-risk-sg-2014.pdf> Accessed 1/11/2017

PWC 2016, Aviation Perspectives: Volume 4.2 - Cybersecurity prevention June 2016, Retrieved from <https://www.pwc.com/us/en/industries/industrial-products/library/airline-industry-perspectives-cybersecurity-prevention.html> Accessed by 02/10/2017

PWC, 2016 “Gaining from connectivity without losing trust” Retrieved from <https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2017/gx/trust.html> Accessed 5/09/2017

Ragin, C. C., and Fiss, P. C. (2008). Net effects versus configurations: An empirical demonstration. In C. C. Ragin (Ed.), *Redesigning social inquiry: Fuzzy sets and beyond* (pp. 190–212). Chicago: University of Chicago Press.

Ragin, C. C., and Pennings, P. (2005). Fuzzy sets and social

research. *Sociological Methods and Research*, 33(4), 423–430.

Rasoulilian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2017). Service crisis recovery and firm performance: insights from information breach announcements. *Journal of the Academy of Marketing Science*, 1-18.

Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In *Cyber-Risk Management* (pp. 33-47). Springer International Publishing.

Rihoux, B. (2006). Qualitative comparative analysis (QCA) and related systematic comparative methods recent advances and remaining challenges for social science research. *International Sociology*, 21(5), 679–706.

Rindova, V. P., and Fombrun, C. J. (1999). Constructing competitive advantage: The role of firm-constituent interactions. *Strategic Management Journal*, 20(8), 691–710.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121-135.

Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*.

SANS Institute InfoSec Reading Room, *Combatting Cyber Risks in the Supply Chain* <https://www.sans.org/reading-room/whitepapers/analyst/combating-cyber-risks-supply-chain-36252>

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons*, 55(4), 349-356.

Schryen, G. (2013). Revisiting IS business value research: What we already know, what we still need to know, and how we can get there. *European Journal of Information Systems*, 22(2), 139–169.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314–341.

Seuring, S. (2011). Supply chain management for sustainable products—insights from research applying mixed methodologies. *Business Strategy and the Environment*, 20(7), 471-484.

Sheriff, A., Bouchlaghem, D., El-Hamalawi, A., & Yeomans, S. (2011). Information management in UK-based architecture and engineering organizations: Drivers, constraining factors, and barriers. *Journal of Management in Engineering*, 28(2), 170–180.

Smirnov, A., Sandkuhl, K., & Shilov, N. (2013). Multilevel self-

organisation of cyber-physical networks: synergic approach. *International Journal of Integrated Supply Management*, 8(1–2–3), 90–106.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.

Spens, K., and Kovacs, G. (2012). Mixed methods in logistics research: the use of case studies and content analysis. *International Journal of Physical Distribution and Logistics Management*, 42(3).

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, 75, 49-62.

Stevenson, W. J., & Hojati, M. (2007). *Operations management* (Vol. 8). Boston: McGraw-Hill/Irwin.

Stewart, D. W. (2017). A comment on privacy. *Journal of the Academy of Marketing Science*, 45(2), 156-159.

Strand, C. (2014). Challenging confidence in cyber-security. *Computer Fraud & Security*, 2014(12), 12-15.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of management journal*, 49(4), 633-642.

Teece, D., & Leih, S. (2016). Uncertainty, innovation, and dynamic capabilities: An introduction. *California Management Review*, 58(4), 5-12.

Teece, D., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. *California Management Review*, 58(4), 13-35.

Tirunillai, S., & Tellis, G. J. (2014). Mining marketing meaning from online chatter: Strategic brand analysis of big data using latent Dirichlet allocation. *Journal of Marketing Research*, 51(4), 463–479.

Tirunillai, S., & Tellis, G. J. (2017). Does offline TV advertising affect online chatter? Quasi-experimental analysis using synthetic control. *Marketing Science*.

Tóth, Z., Henneberg, S. C., & Naudé, P. (2017). Addressing the ‘Qualitative’ in fuzzy set Qualitative Comparative Analysis: the generic membership evaluation template. *Industrial Marketing Management*, 63, 192-204.

Urciuoli, L. (2015). Cyber-resilience: a strategic approach for

supply chain management. *Technology Innovation Management Review*, 5(4), 13.

Von Solms, S. B. (2005). Information Security Governance—compliance management vs operational management. *Computers & Security*, 24(6), 443-447.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.

Walker, K. (2010). A systematic review of the corporate reputation literature: Definition, measurement, and theory. *Corporate Reputation Review*, 12(4), 357–387.

Walsh, G., and Beatty, S. E. (2007). Customer-based corporate reputation of a service firm: Scale development and validation. *Journal of the Academy of Marketing Science*, 35(1), 127–143.

Walsh, G., Mitchell, V. W., Jackson, P. R., & Beatty, S. E. (2009). Examining the antecedents and consequences of corporate reputation: A customer perspective. *British Journal of Management*, 20(2), 187-203.

Ward, J. M. (2012). Information systems strategy: Quo vadis?. *The Journal of Strategic Information Systems*, 21(2), 165–171.

Webb, P., Pollard, C., & Ridley, G. (2006, January). Attempting to define IT governance: Wisdom or folly?. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on* (Vol. 8, pp. 194a-194a). IEEE.

Wepener, M., and Boshoff, C. (2015). An instrument to measure the customer-based corporate reputation of large service organizations. *Journal of Services Marketing*, 29(3), 163–172.

Woods, D., Agrafiotis, I., Nurse, J. R., & Creese, S. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, 8(1), 8.

Yang, S. O., Hsu, C., Sarker, S., & Lee, A. S. (2017). Enabling Effective Operational Risk Management in a Financial Institution: An Action Research Study. *Journal of Management Information Systems*.

Yang, Z., & Lui, J. C. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, 74, 1-17.

Yu, X., Krause, R. A., Bell, G., & Bruton, G. D. (2016, January). A Configurational Exploration of Family Relationships, Corporate Governance, and Firm Performance. In *Academy of Management Proceedings* (Vol. 2016, No. 1, p. 10063). Academy of Management.

- Zsidisin, G. (2003) "Managerial perceptions of risk", *Journal of Supply Chain Management*, Vol. 39, pp. 14–25.
- Zsidisin, G. A., Ellram, L. M., Carter, J. R., & Cavinato, J. L. (2004). An analysis of supply risk assessment techniques. *International Journal of Physical Distribution & Logistics Management*, 34(5), 397-413.
- Zsidisin, G. A., Panelli, A., & Upton, R. (2000). Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study. *Supply Chain Management: An International Journal*, 5(4), 187-198.
- Zsidisin, G. A., & Ritchie, B. (2009). Supply chain risk management—developments, issues and challenges. In *Supply Chain Risk* (pp. 1-12). Springer, Boston, MA.

# **1. Just do it. Managing IT and Cyber Risks to Protect the Value Creation**

**Gaudenzi, B., & Siciliano, G**

## Abstract

The purpose of this paper is to analyze how IT and cyber risks are currently perceived by companies. These risks may have critical impacts on the protection of organizational value creation in many industries. We developed a qualitative study, using a grounded-theory approach, involving European organizations. We elaborated the data through a fuzzy set Qualitative Comparative Analysis (fsQCA). The findings reveal that companies rely mainly on risk mitigation measures, showing little awareness about what these threats are. However, the fsQCA correlates an effective protection of value creation to a holistic IT and cyber risk management, together with a thorough cross-functional communication.

## *1.1 Introduction*

A survey conducted by PWC in 2014 (PWC, 2014) found that average financial losses attributed to Information Technology (IT) and cyber security incidents increased up to 18% in 2013 over the previous year, and big liabilities increased up to 51% over 2011.

This information reveals that in today's world, both internal IT risks and external cyber attacks may have critical impacts on the value creation in many industries (Aon Risk

Solutions, 2015; Jajodia, Liu, Swarup, & Wang, 2010; Lee, Koo, & Nam, 2010; Mithas, Ramasubbu, & Sambamurthy, 2011; Wang, Liang, Zhong, Xue, & Xiao, 2012). Aon (2015), in particular, ranked these risks as two of the major threats associated with rapid technological changes. However, as threats become more frequent and severe, investments in security initiatives seem to decrease (PWC Reports, 2015).

The study is grounded in the dynamic capabilities perspective (Teece, Pisano, & Shuen, 1997; Eisenhardt & Martin, 2000; Winter, 2003; Teece, 2007), in order to analyze how relational, organizational, and technical capabilities should be integrated (Eisenhardt & Martin, 2000; Teece, 2007) for better managing IT and cyber risks. In this perspective, authors highlighted that (risk) perceptions of individual actors in different functions of the organization should be well aligned to take good decisions (Ambrosini & Bowlman, 2009; Li & Liu, 2014; Helfat & Peteraf, 2015).

Considering the complexity and dynamism of IT and cyber risks (Leuprecht, Skillicorn, & Tait, 2016), their management require both technical e.g. software, insurance, investments in IT assets) and organizational (team work, human IT resources) capabilities (Lim, Stratopoulos, & Wirjanto, 2011; Mithas, Tafti, Bardhan, & Goh, 2012; Schryen, 2013; Lee, DeLone, Tan, & Corrales, 2014) to

protect the capability of the company to create value.

To the best of our knowledge, in the management field there is a lack of investigation about how these new threats are currently perceived (Järveläinen, 2013) and should be managed to protect the value creation. In order to fill this gap, we developed an empirical research based on 15 European organizations, using a fuzzy set Qualitative Comparative Analysis (fsQCA) (Fiss, 2011). Results provide a picture of how managers perceive these risks with respect to the internal and external environment. Finally, the study proposes a managerial framework for deploying companies' dynamic capabilities to manage IT and cyber risks.

## *1. 2. Literature review*

### *1.2.1 Information technology and cyberspace*

In the literature of the last five years, the terms Information Technology (IT) and cyberspace have often been related (Melville, 2010; Sheriff, Bouchlaghem, El-Hamalawi, & Yeomans, 2011; Ward, 2012) and sometimes used interchangeably (Mithas et al., 2011; Schryen, 2013; Smirnov, Sandkuhl, & Shilov 2013; Von Solms & Van Niekerk, 2013). For example, Melville (2010) defined IT as the technological foundation of the information systems and cyberspace, Sheriff et al. (2011) considered IT an infrastructure, while, Schryen (2013), stated IT has not been yet properly theorized.

Cyberspace has been described as an integration of “complex networks into a global Internet” (Choucri & Goldsmith, 2012; Phister, 2010), characterized by low price of entry, anonymity, and asymmetries in vulnerability (Nye, 2011). It has been defined as a synonym for IT (Smirnov et al., 2013) or for the “e-commerce space” (Lee et al., 2010). Others have considered hardware, software and data to be “cyber assets” (D’Amico, Buchanan, Goodall, & Walczak, 2010).

### *1.2.2 Managing IT and cyber risks to protect the value creation*

The Global State of Information Security Survey 2015 (PWC Reports, 2015) found that, in 2015, there were 117,339 incoming attacks per day, every day, consisting in events such as identity and intellectual property theft or competitors disrupting business to gain competitive advantage (Von Solms & Van Niekerk, 2013; Bailey, Miglio, & Richter, 2014). Despite the complexity and recent evolution of the above-mentioned threats, cyber security has been only partially investigated in management studies, particularly in relation to social issues (Benson, Saridakis, & Tennakoon, 2014; Vladlena, Saridakis, Tennakoon, & Ezingard, 2015), smart grids (Nazir, Hamdoun, Alzubi, & Alzubi, 2015), data protection (Howell, 2015) and governmental issues (Von Solms & Van Niekerk, 2013).

With respect to IT risks, the literature of the last five years has focused primarily on technical solutions (Järveläinen, 2013; Biener, Eling, & Wirfs, 2015; Tøndel, Meland, Omerovic, Gjære, & Solhaug, 2015, Leuprecht et al., 2016; Young, Lopez, Rice, Ramsey, & McTasney, 2016), while investments in other security initiatives are decreasing (Järveläinen, 2013). (When dealing with technological issues, the dynamic capability view suggests to integrate and orchestrate managerial capabilities with organizational and technical processes (Eisenhardt & Martin, 2000; Teece, 2007; Kor & Mesko, 2013, Vogel & Güttel, 2013) in order to protect value in “rapidly changing environments” (Teece et al., 1997, p. 516). The risk management literature suggests an effective protection towards dynamic key risks such as those related to information technology (Gaudenzi & Borghesi, 2006; Silva et al., 2014) and the cyberspace (Boyson, 2014) may be achieved through proper risk prevention, assessments, and mitigation.

To examine these issues, we built an empirical study comprising leader European organizations, in order to conduct a preliminary investigation on the state of practice in managing IT and cyber risks.

### *1.3 Methods and data*

#### *1.3.1 The method*

In this research we adopted a fuzzy set Qualitative

Comparative Analysis (fsQCA) for interpreting the qualitative data collected in this study.

It provides all the possible mix of inputs that lead to a desired outcome (Rihoux, 2006), which—in this study—means obtaining all the various combinations of risk assessment, risk prevention, risk mitigation, risk compliance and risk governance that may impact on the value creation. Values between 1 and 5 were assigned in order to obtain a single value representing the overall mean for both the input variables (the risk management measures) and the outcome variable (the financial performance, which is our selected proxy for the value creation).

The subsequent calibration process (Ragin & Pennings, 2005), provided the final fuzzy set scale, assuming the following continuous values: 0.05 for a low level of value creation, 0.50 for an average level of value creation, and 0.95 for a high level of value creation, as shown in Table 1.

### *1.3.2 Research sample and data collection*

In order to gain an in-depth understanding of the various approaches that firms can take in managing IT and cyber

risks, we select the sample shown in Table 2.

Table 1. Variables and values after

VARIABLES	INITIAL VALUES			FUZZY VALUES			FUZZIFICATION PROCESS
Risk Assessment	Values from 1 to 5			Values from 0.05 to 0.95			Calibration process
Risk Prevention	Values from 1 to 5			Values from 0.05 to 0.95			Calibration process
Risk Mitigation	Values from 1 to 5			Values from 0.05 to 0.95			Calibration process
Risk Compliance	Values from 1 to 5			Values from 0.05 to 0.95			Calibration process
Risk Governance	Values from 1 to 5			Values from 0.05 to 0.95			Calibration process
Dimension	Values from 1 to 5			Values from 0.05 to 0.95			Directly assigned
Internationalization	Values from 1 to 5			Values from 0.05 to 0.95			Directly assigned
Financial Performance	Small	Medium	Large	0.95	0.75	0.5	Directly assigned

The units of analysis are the firms’ IT and cyber risk practices of assessment, mitigation, and governance. An heterogeneous sample has been selected, for two reasons. First, similar dynamic capabilities can be better identified when the analysis is conducted with different companies (Ambrosini & Bowlman, 2009). Second, heterogeneous samples allow a clearer observation (Martin & Eisenhardt, 2010) capturing different viewpoints (Gibbert & Ruigrok, 2010).

The respondent we identified in each organization was the security manager or the risk manager at the director level. In consultant companies, we involved the IT risk consultant or business continuity consultant, who lead consultant projects within client firms. In all of the organizations, our key respondents were able to provide us with all the information needed to complete the questionnaires. We terminated the sampling process after achieving a point of theoretical saturation following our 15th interview.

### *1.3.3 Variable descriptions*

At the best of our knowledge, the literature of the last 5 years does not provide surveys or items related to IT and cyber risk management. Thus, we were unable to test variables that were already present in academic studies. For this reason, we decided to propose a managerial framework, and to develop and test items mainly according to risk management literature and standards (ISO 31000, 2009; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010, Yildirim, Akalp, Aytac, & Bayram, 2011; Ifinedo, 2012; Järveläinen, 2013; Boyson, 2014; Feng, Wang, & Li, 2014; Silva et al., 2014; Biener et al., 2015; ISO 27001, 2013). We also included 8 general questions to deepen interviewees' answers (Rubin & Rubin, 2011). As shown in Table 3, we selected 14 items, describing 5 input variables, and 1 item indicating the output variable (financial performance).

### *1.3.4 Fuzzy solution generation*

The use of a fsQCA software generates an evaluation of the potential relationships between an outcome (such as—in our case—the financial performance) and all the possible combinations of 'predictors' (the input variables) (Longest & Vaisey, 2008). The method also clusters input variables information into different paths

Table 2. Sample characteristics.

FIRMS	SECTOR	FINANCIAL PERFORMANCE (2012–2014)		SIZE	ROLE OF KEY INFORMANT	LEVEL OF INTERNATIONALIZATION
		100 K < x < 1 MM: poorly performing companies	1 MM < x < 500 MM: average-performing companies			
C1	Apparel	High		Large	Security manager	Very High
C2	Metacasting	Medium		Medium	Risk manager	Low
C3	Services	Medium		Medium	IT risk consultant	Very Low
C4	Services	High		Large	IT risk consultant	Medium
C5	Oil and Gas	High		Large	IT risk and business continuity consultant	Very High
C6	Finance	High		Large	IT risk and business continuity consultant	High
C7	Software	Low		Small	Risk management consultant	Low
C8	Healthcare	Medium		Medium	Risk Manager and CEO	High
C9	Apparel	Medium		Medium	Security manager	Very High
C10	Healthcare	Medium		Medium	Business manager and IT manager	High
C11	Finance	Medium		Medium	Business manager and IT security manager	Low
C12	Tobacco	High		Large	IT manager	Very High
C13	High Technology	High		Large	IT manager	High
C14	Heating	Medium		Medium	Quality manager and IT manager	Medium
C15	Food Products	High		Large	CEO	Very High

Table 3. Variables

Input variables	Main references
<b>1. Risk Assessment</b>	
1. Unauthorized changes to system hardware or software	Yildirim et al. (2011)
2. Piracy	Biener et al. (2015)
3. Devices breakdowns	Järveläinen, (2013)
4. Procedures failing	
5. Specific budget for IT security management	
6. Investments in risk assessment	
7. Consulting projects	
<b>2. Risk Prevention</b>	
8. Hardware, software and insurance expenses	Infredo, (2012) Järveläinen, (2013) <sup>7</sup> Yildirim et al. (2011) Biener et al. (2015) Boyson, (2014) Silva et al. (2014)
<b>3. Risk Mitigation</b>	
9. Insurance	Biener et al. (2015)
10. Secure areas	Silva et al. (2014) Feng et al., 2014 Yildirim et al. (2011)
<b>4. Risk Governance</b>	
11. Organization's risk attitude	Järveläinen, (2013)
12. Human resources	Yildirim et al. (2011) Boyson, (2014) Infredo, (2012) Johnston & Warkentin (2010) Biener et al. (2015)
<b>5. Risk Compliance</b>	
13. Recognition of the organization's vulnerability toward IT and Cyber risks	Yildirim et al. (2011) Infredo, (2012)
14. Risk appetite of an organization	Bulgurcu et al. (2010) Feng et al., 2014 Biener et al. (2015) Boyson, (2014)
<b>Output Variable</b>	
15. Financial performance	Venanzi (2011) Lavie (2007).

toward that outcome (Schneider & Wagemann, 2010). We set the fsQCA software in order to generate solutions with the maximal level of parsimony, which means we did not consider some cases that may exist logically, but that have not been observed in the data (Rihoux, 2006).

Finally, software results are evaluated considering how each solution can explain the dependent variable (Longest & Vaisey, 2008; Schneider & Wagemann, 2010).

#### *1.4 Results*

##### *1.4.1 Descriptive statistics: IT and cyber risk perceptions*

Our results show significantly different managers' perceptions and meanings of the two types of risks. Looking at descriptive statistics, 40% of the sample believed that IT risks manifest in the "offline" world, impacting only internal dimensions (e.g., business continuity, compliance, and procedures) while cyber risks consist of intrusions from third parties through the web, emails, and smartphones. In some cases, these risks were not perceived as real threats, and hence not monitored. On the other hand, one out of three of the organizations considered cyber risks to be a subcategory of IT risks; these interviewees suggested that managing only the latter may be sufficient to protect against the former.

The role of the key informant influenced his or her IT and

cyber risk perceptions: risk and security managers showed to know the two types of risk, while half of the sample of IT corporate managers did not, with consequent scarce investments in training for employees at all levels. When discussing the relevance of managing both types of risks, a paradox emerges: while roughly 50% of the sample saw effective management as extremely relevant, one out of three managers admitted that their companies behaved as if they had very high risk appetites.

#### *1.4.2 Fuzzy analysis: Risk management solutions to protect the value creation*

Looking at the results emerged from the fuzzy analysis, it emerged that there are four possible ways in which the risk management process can generate value. Table 4 shows these using Ragin and Fiss's (2008) notation system: each column represents a combination of conditions and a correlated outcome, such that full circles (●) indicate the presence of a condition and empty cross circles (○) indicate its absence.

Solution 1 suggests none of the above-mentioned measures impacts the protection of value creation of bigger and international companies; Solution 2 focuses on local, non-international companies, whose IT and cyber risk management strategies are limited to mitigation in cases of concrete threats; Solution 3 shows also international companies rely solely on mitigation strategies, accompanied

by the compliance to official information security standards; while Solution 4 proposes a complete IT and cyber risk management leads international companies to greater financial performance. However, among these, only the latter is able to explain the 32% of the value creation of companies, while, the others just the 0.6%.

Table 4. Results of the fuzzy set qualitative

Solutions Variables	Solutions			
	Solution 1	Solution 2	Solution 3	Solution 4
Risk Assessment	⊖	⊖	⊖	•
Risk Prevention	⊖	⊖	⊖	•
Risk Mitigation	⊖	•	•	•
Risk Compliance	⊖	⊖	•	•
Risk Governance	⊖	⊖	⊖	•
Dimension	•	⊖	•	•
Internationalization	•	⊖	•	•
Consistency	0.91	1.00	1.00	1.00
Raw Coverage	0.16	0.17	0.20	0.46
Unique Coverage	0.06	0.06	0.06	0.32
Solution Consistency	0.98			
Solution Coverage	0.66			

Note. Legend.

• = Core causal condition present.

⊖ = Core causal condition absent.

#### 1.4.3 A proposed framework for managing IT and cyber risks

In Table 5 we show how managers perceive and describe a good risk management process. All the respondents spontaneously highlighted that it should start with the systematic identification and measurement of potential sources of IT and cyber risks.

Since risks can arise at any point in time, managers confirm that a formal plan of mitigation strategies should be created

and systematically updated to take into consideration the urgency—and, thus, the time pressure—related to each given risk (Ward, 1999).

In Figure 1 we propose a framework for managing IT and cyber risks as emerged during the interviews.

### 1.5 Discussion

This study answers to the call for a deeper understanding of IT and cyber-related issues at a more granular level (Bauer & Bernroider, 2015; Асина, 2016), by considering all types of

IT and Cyber Risk Assessment	<p>C1: We informed employees about some IT and cyber security practice, such as usage of passwords and codes, but they hardly could assess any IT and cyber risk. However, the CEOs shows the greatest lack of awareness about proper IT and cyber risk assessment procedures, even if they do not ignore them intentionally...simply, there is not consciousness.</p> <p>C2: The dedicated budget is not adequate still, but it is growing.</p> <p>C7: The IT and cyber official standards are not mandatory for our company, but we look at them when we need some hint about the correct risk assessment procedures...then we adapt them on our best practices.</p>
IT and Cyber Risk Prevention	<p>C3: We have an IT and cyber plan of prevention, but it is not so specific, defined and sophisticated yet. It is in development as we know prevention has to be a part of the architecture and a part of all layers when creating, developing or changing a solution.</p> <p>C3: Almost 100% of the budget is invested in technical preventive measures.</p> <p>C14: The company is experiencing a moment of changing and there is awareness that great effort should be put in training and information.</p>
IT and Cyber Risk Mitigation	<p>C2: We are working on physical entry controls, secure areas, equipment security level. Moreover we stipulated contractual agreements with suppliers, which have coverage clauses.</p> <p>C4: We would like to invest more on insurance, but there is low offering. We rely on software but nobody cares about the performances. We also rely on cloud solutions.</p>
IT and Cyber Risk Compliance	<p>C8: We informally follow more than one Standard, but we have best practices above all.</p>
IT and Cyber Risk Governance	<p>C7: Our risk appetite is low at the moment, we hope to be able to align the strategic risk appetite with the IT risk appetite</p> <p>C15: We are working to have a good IT and cyber risk governance: some companies failed sometimes. We also had problems with media and press because of these risks.</p> <p>C2: For CEOs is an important but not an essential area. I have the feeling the attention changes in relation to how the theme is treated: if we say there is some business interruption, there is great alarm, when speaking about IT everybody is indifferent...they just do not link the two things.</p>

Table 5. Evidence from the case

event (malicious vs. accidental), their sources (internal vs. external) and the perceptions companies have about their impact on the protection of value creation.

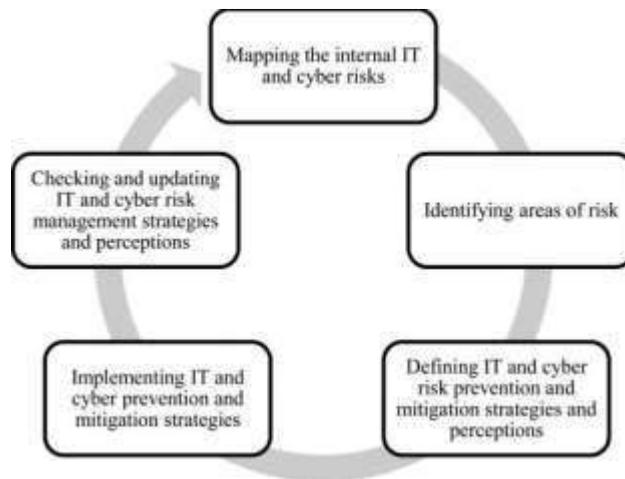


Figure 1. IT and cyber risk management framework.

The fsQCA results reveal there are four ways in which risk management measures can be combined to enhance the value protection.

The best solution is reached when the entire IT and cyber risk management process is put in place.

A second option suggests that international companies that do not implement any risk management measure have still acceptable results. This is probably due to the high level of financial, economic, and human resources they have in place

and their widespread geographic presence, which may mitigate the impacts of some manifestations of IT or cyber threats. However, the importance of an holistic IT and cyber risk management process suggests that international companies are nowadays still relying on “parachutes,” which may become insufficient soon.

With respect to the last two solutions, they massively rely on some risk mitigation strategy, primarily insurance and technical solutions. One possible interpretation of these results is that such companies operate instable industries that rarely experienced IT or cyberspace breaches. However, the always increasing number of breaches suggests that IT and cyber risks will play as a “black swan”: though they may not be an everyday challenge, when they do manifest, they are difficult to recover from.

In conclusion, our results contradict studies that focus merely on technical solution, such as technological approaches (Leuprecht et al., 2016) and insurance (Biener et al., 2015; Tøndel et al., 2015, Young et al., 2016). In fact, while technical solutions are surely important to protect the value creation, the findings seem to confirm the existing literature on the dynamic capability view which highlights the relevance of a major integration among relational, organizational, and technical capabilities (Eisenhardt & Martin, 2000; Teece, 2007) when dealing with technological issues (Vogel & Götzel, 2013). We propose this could be

achieved implementing a systematic risk management process, reactive to the dynamic nature of IT and cyber risks, as suggested by Boyson (2014), Biener et al. (2015), and Teece et al. (2016).

Moreover, we found that a thorough management of IT and cyber risks may protect the value creation in any type of industries, in line with that part of the literature that states dynamic capabilities exhibit commonalities across different firms in terms of efficiency and value creation (Peteraf, Di Stefano, & Verona, 2013; Breznik & Hisrich, 2014; Di Stefano, Peteraf, & Verona, 2014).

The findings also propose organizations should foster radical changes to company culture, confirming the learning process as a core topic of the dynamic capabilities view (Vogel & Gittel, 2013). In fact, there seems to exist a general lack of knowledge and awareness across employees at different levels (e.g., corporate and local) about what IT and cyber risks are. This seems to require a more open communication and a clear leadership about the management of IT and cyber risks.

### *1.6 Conclusions*

The most important strategic action regarding IT and cyber risks for to protect value creation of both multinational and local companies seems to be the implementation of a holistic IT and cyber security management system. Information sharing, technology managerial process integration, and

investments to create a common culture among employees at all levels can help managers enhance the creation of value in the long term. Effective IT and cyber risk management yields critical advantages; thus, its implementation should rely on scientific research.

This study contains a number of limitations that may be addressed in future research. First, the limited number of companies does not allow generalizability. Future research could use a wider sample, in terms of company size, location and type of industry. Second, while our suggestion to implement an IT and cyber risk management and to foster a deeper cross-functional communication has its merits, future efforts should investigate which are the specific mechanisms to put in place from a dynamic capability perspective.

Third, we focused on the IT and cyber risk management impact on one dimension, namely the protection of the value creation. However, other aspects, such as the reputation, may be worth studying.

## References

- Acuna, D. C. (2016). Enterprise computer security: A literature review. *Journal of the Midwest Association for Information Systems*, 2016(1), 37–53.
- Ambrosini, V., & Bowman, C. (2009). What are dynamic capabilities and are they a useful construct in strategic

management?. *International Journal of Management Reviews*, 11(1), 29–49. Aon Risk Solutions. (2015). *Global risk management survey*. Retrieved from [www.aon.com/2015GlobalRisk](http://www.aon.com/2015GlobalRisk)

Bailey, T., Miglio, A. D., & Richter, W. (2014). The rising strategic risks of cyberattacks. *McKinsey Quarterly*, 2(2014), 17–22.

Bauer, S., & Bernroider, E. W. (2015, August). *The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring*. In T. Tryfonas & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust, HAS2015. Lecture notes in computer science* (Vol. 9190, pp. 154–164). Cham, Switzerland: Springer International Publishing.

Benson, V., Saridakis, G., & Tennakoon, H. (2014). Purpose of social networking use and victimisation: Are there any differences between university students and those not in HE?. *Computers in Human Behavior*, 51, 867–872.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance Issues and Practice*, 40(1), 131–158.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), 342–353.

Breznik, L. D., & Hisrich, R. (2014). Dynamic capabilities vs. innovation capability: Are they related?. *Journal of Small Business and Enterprise Development*, 21(3), 368–384.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523–548.

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, 68(2), 70–77.

D'Amico, A., Buchanan, L., Goodall, J., & Walczak, P. (2010, April). *Mission impact of cyber events: Scenarios and ontology to express the relationships between cyber assets, missions, and users*. In Proceedings of 5th International Conference on Information Warfare and Security (pp. 8–9). Dayton, OH: Academic Conferences International.

Di Stefano, G., Peteraf, M., & Verona, G. (2014). The organizational drivetrain: A road to integration of dynamic capabilities research. *The Academy of Management Perspectives*, 28(4), 307–327.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they?. *Strategic management journal*, 21(10–11), 1105–21.

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, 256, 57–73.

Fiss, P. C. (2011). Building better causal theories: A fuzzy set approach to typologies in organization research. *Academy of Management Journal*, 54(2), 393–420.

Gaudenzi, B., & Borghesi, A. (2006). Managing risks in the supply chain using the AHP method. *The International Journal of Logistics Management*, 17(1), 114–136.

Gibbert, M., & Ruigrok, W. (2010). The "what" and "how" of case study rigor: Three strategies based on published research. *Organizational Research Methods*, 13(4), 710–737.

Helfat, C. E., & Peteraf, M. A. (2015). Managerial cognitive capabilities and the microfoundations of dynamic capabilities. *Strategic Management Journal*, 36(6), 831–850.

Howell, D. (2015). Building better data protection with SIEM. *Computer Fraud & Security*, 2015 (8), 19–20.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95.

ISO 31000 (2009). *Risk management—Principles and guidelines*. Geneva: International Standards Organisation.

ISO 31000. (2013). *Risk management ISO/IEC 27001. Information technology - Security techniques - Information security management systems - Requirements*. Geneva: International Standards Organisation.

Jajodia, S., Liu, P., Swarup, V., & Wang, C. (2010). *Cyber situational awareness*. New York, NY: Springer.

Järvelin, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, 33 (3), 583–590.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, 34(3), 549–566.

Kor, Y. Y., & Mesko, A. (2013). Dynamic managerial capabilities: Configuration and orchestration of top executives' capabilities and the firm's dominant logic. *Strategic Management Journal*, 34(2), 233–244.

- Lavie, D. (2007). Alliance portfolios and firm performance: A study of value creation and appropriation in the US software industry. *Strategic Management Journal*, 28(12), 1187–1212.
- Lee, G., DeLone, W., Tan, M., & Corrales, M. (2014). Special issue on leveraging the IS organization for business value creation. *Journal of Information Technology*, 29(2), 111–3.
- Lee, S. G., Koo, C., & Nam, K. (2010). Cumulative strategic capability and performance of early movers and followers in the cyber market. *International Journal of Information Management*, 30(3), 239–255.
- Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the castle model of cyber-risk and cyber-security. *Government Information Quarterly*, 33(2), 250–257.
- Li, D. Y., & Liu, J. (2014). Dynamic capabilities, environmental dynamism, and competitive advantage: Evidence from China. *Journal of Business Research*, 67(1), 2793–99.
- Lim, J. H., Stratopoulos, T. C., & Wirjanto, T. S. (2011). Path dependence of dynamic information technology capability: An empirical investigation. *Journal of Management Information Systems*, 28(3), 45–84.
- Longest, K. C., & Vaisey, S. (2008). Fuzzy: A program for performing qualitative comparative analyses (QCA) in Stata. *Stata Journal*, 8(1), 79.
- Martin, J. A., & Eisenhardt, K. M. (2010). Rewiring: Cross-business-unit collaborations in multi-business organizations. *Academy of Management Journal*, 53(2), 265–301.
- Melville, N. P. (2010). Information systems innovation for environmental sustainability. *MIS Quarterly*, 34(1), 1–21.
- Mithas, S., Ramasubbu, N., & Sambamurthy, V. (2011). How

information management capability influences firm performance. *MIS Quarterly*, 35(1), 237–256.

Mithas, S., Tafti, A. R., Bardhan, I., & Goh, J. M. (2012). Information technology and firm profitability: Mechanisms and empirical evidence. *MIS Quarterly*, 36(1), 205–224.

Nazir, S., Hamdoun, H., Alzubi, J. A., & Alzubi, O. A. (2015). Cyber attack challenges and resilience for smart grids. *European Journal of Scientific Research*, 134, 111–120.

Nye, J. S. (2011). *The future of power*. London. PublicAffairs.

Peteraf, M., Di Stefano, G., & Verona, G. (2013). The elephant in the room of dynamic capabilities: Bringing two diverging conversations together. *Strategic Management Journal*, 34(12), 1389–1410.

Phister, Jr., P. W. (2010). Cyberspace: The ultimate complex adaptive system. *The International C2 Journal*, 4(2), 1–32.

PWC Report. (2014). *Managing cyber risks with insurance. Key factors to consider when evaluating how cyber insurance can enhance your security program. The Global State of Information Security<sup>®</sup> Survey 2014*. Retrieved from <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/managing-cyber-risks-with-insurance.html>

PWC Report. (2015). *Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security<sup>®</sup> Survey 2015*. Retrieved from <http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>

- Ragin, C. C., & Fiss, P. C. (2008). Net effects versus configurations: An empirical demonstration. In C. C. Ragin (Ed.), *Redesigning social inquiry: Fuzzy sets and beyond* (pp. 190–212). Chicago: University of Chicago Press.
- Ragin, C. C., & Pennings, P. (2005). Fuzzy sets and social research. *Sociological Methods & Research*, 33(4), 423–430.
- Rihoux, B. (2006). Qualitative comparative analysis (QCA) and related systematic comparative methods recent advances and remaining challenges for social science research. *International Sociology*, 21(5), 679–706.
- Rubin, H. J., & Rubin, I. S. (2011). Preparing follow-up questions. In *Qualitative interviewing: The art of hearing data* (3rd edition) (pp. 149–168). Thousand Oaks, CA: Sage Publications.
- Schneider, C. Q., & Wagemann, C. (2010). Standards of good practice in qualitative comparative analysis (QCA) and fuzzy-sets. *Comparative Sociology*, 9(3), 397–418.
- Schryen, G. (2013). Revisiting IS business value research: What we already know, what we still need to know, and how we can get there. *European Journal of Information Systems*, 22(2), 139–169.
- Sheriff, A., Bouchlaghem, D., El-Hamalawi, A., & Yeomans, S. (2011). Information management in UK-based architecture and engineering organizations: Drivers, constraining factors, and barriers. *Journal of Management in Engineering*, 28(2), 170–180.
- Silva, M. M., de Gusmao, A. P. H., Poletto, T. E., Silva, L. C., & Costa, A. P. C. S. (2014). A multi-dimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, 34(6), 733–

740.

Smirnov, A., Sandkuhl, K., & Shilov, N. (2013). Multilevel self-organisation of cyber-physical networks: synergic approach. *International Journal of Integrated Supply Management*, 8(1–2–3), 90–106.

Teece, D., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility. *California Management Review*, 58(4), 13–35.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319–50.

Tøndel, I. A., Meland, P. H., Omerovic, A., Gjære, E. A., & Solhaug, B. (2015). Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research. Technical report SINTEF A27298. Retrieved from <https://www.sintef.no/globalassets/sets/sintef-ikt/kst/insecurance/sintef-a27298-insecurance-2015.pdf>

Venanzi, D. (2011). *Financial performance measures and value creation: The state of the art*. Berlin: Springer Science & Business Media.

Vladlena, B., Saridakis, G., Tennakoon, H., & Ezingear, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social networking users. *International Journal of Human-Computer Studies*, 80, 36–44.

Vogel, R., & Götzel, W. H. (2013). The dynamic capability view in strategic management: A bibliometric review. *International*

- Journal of Management Reviews*, 15(4), 426–446.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.
- Wang, N., Liang, H., Zhong, W., Xue, Y., & Xiao, J. (2012). Resource structuring or capability building? An empirical study of the business value of information technology. *Journal of Management Information Systems*, 29(2), 325–367.
- Ward, J. M. (2012). Information systems strategy: Quo vadis?. *The Journal of Strategic Information Systems*, 21(2), 165–171.
- Ward, S. C. (1999). Assessing and managing important risks. *International Journal of Project Management*, 17(6), 331–6.
- Winter, S. G. (2003). Understanding dynamic capabilities. *Strategic Management Journal*, 24(10), 991–5.
- Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, 31(4), 360–5.
- Young, D., Lopez, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14, 43–57.

## **2. Managing IT and Cyber Risks in Supply Chains**

**Gaudenzi, B., & Siciliano, G.**

### Abstract

This chapter describes the potential impact of Information Technology (IT) and Cyber risks on the continuity and vulnerabilities of the supply chain. We propose a theoretical framework and direction to help organizations to manage these risks. The evidence gleaned from an empirical investigation will illustrate how organizations actually perceive, control, and manage IT and Cyber risks within the supply chains. The findings will underline that managers tend to invest in few mitigation strategies; hence, they take risks that are much higher than their declared risk appetites. In addition, managers denounce a general lack of awareness regarding the effects that IT and Cyber risks may have on supply operations and relationships.

Keywords: IT risk, Cyber risk, security, supply chain risk management

### *2.1. IT risks and Cyber risks: real threats for all supply chains*

Global trends, such as digitalization and servitization, have caused an evolution in all conventional supply chains whose structures have switched from a “web of disconnected islands”

to a network of interconnected processes, which are strongly oriented toward flexibility, efficiency, and resilience.

In this context, Internet platforms assure operational benefits, such as cost reduction, inventory pooling, postponement, a reduction of the bullwhip effect, and shorter lead times, to allow for faster information sharing across different organizations. For example, supply chain leaders such as Wal-Mart, Warner-Lambert, Procter & Gamble, and Levi Strauss, have achieved great benefits from their investments in Information Technology (IT) tools such as the Enterprise Resource Planning (ERP). In particular, these companies have improved their performances in demand planning and scheduling production, which have created better coordination with their key suppliers.

However, the use of IT tools and Internet platforms generates new forms of supply chain vulnerability and new risks, which may affect the supply chain's continuity and performance. Managers should recognize these new threats as critical issues, that may exacerbate the other supply chain risks throughout interdependencies (Gaudenzi and Borghesi, 2006). However, recent reports (PWC Report, 2014; PWC, 2015a) show that the awareness of these risks is still low: among security incidents across geographic regions, IT and Cyber breaches are rising significantly in Europe, which reported a 41% jump over the previous year. Thus, supply chain managers need to focus more attention on the management of all risks that may be generated

by IT tools, such as ERP or any vertical software, and external Cyberspace.

## *2.2 How external Cyberspace and IT tools generate risks*

A McKinsey report (Bailey et al., 2014) considers “Cyberattacks” to be events such as fraud, identity or intellectual property theft, and political statements made by hacktivists. A PWC report (2015b) sees IT as a tool and an enabler of seamless and real-time interconnectivity across the entire network.

Part of the literature considers the two risks related and even occasionally exchangeable. Both are not easily predictable, and they always imply a violation of three key properties: confidentiality, availability, and integrity.

Some authors consider IT as the foundation of Cyberspace (Melville, 2010), while others consider it a mere infrastructure, where hardware, software, and external data represent “Cyber assets” (D’Amico et al., 2010). Cyberspace is typically considered an external environment with low entry barriers, which have an ambiguity characterized by a certain risk exposure.

In practice, IT risks seem strictly technical: they stem from failures of ERP/IT systems and impact only on the flow of information itself. Here, the control of technical features and procedures plays a key role in assuring information security.

Cyber risks go beyond mere IT disruptions; they are linked to human Cyberattacks, where hackers intentionally access an organization or a network with the goal of either gaining an economic advantage or causing sabotage. These actions are typically linked to Cyber bullying, Cyber terrorism, or political issues (Garfinkel, 2012; von Solms and van Niekerk, 2013).

In 2014, McKinsey found that, while IT and Cyber-related breaches are occurring with growing regularity, executives perceive that they are not quickly responding with adequate tools (Bailey et al., 2014). In the Global Risk Management Report (Aon, 2015), “Cyberattacks” were listed in the top 10 threatening risks for organizations and networks.

Despite these perceptions, Cyber security and IT security remain the areas of risk management with the largest gap between the level of threat and the amount of resources invested. Several studies (Bandyopadhyay et al., 2010; Kong et al., 2012; Gao and Zhong, 2015; Gao et al., 2015; PWC Report, 2015a) have revealed that, as these threats become more frequent and severe, investments in security initiatives decrease. Even with this attention on IT and Cyber security management, recent literature has mainly focused on managerial perceptions, technical aspects, or legislative perspectives (Ellison and Woody, 2010; Ozkan and Karabacak, 2010; Huang et al., 2011; Markmann et al., 2012; Brender and Markov, 2013; Mukhopadhyay et al., 2013; Yang et al., 2013; Biener et al., 2015). From the supply chain risk management perspective, authors only recently

investigated the impacts of IT risks and Cyber risks on supply chains (Olson and Wu, 2010; Järveläinen, 2013; Bartol, 2014; Boyson, 2014; Khan and Estay, 2015; Gaudenzi and Siciliano, 2016).

Therefore, supply chain managers should carefully focus on two critical points:

1. Information security should not be considered as a technology investment itself. Instead, decisions should be made that involve all the actors in the supply chain, create an awareness about IT and Cyber risks, and define clear procedures to identify these threats to protect the supply chain from these vulnerabilities.
2. Managing IT and Cyber risks may increase the overall performance, which will augment the sharing of information and collaboration as well as the efficient management of processes across the supply chain.

### 2.3 Managing IT and Cyber risks in supply chains: A practical framework

We propose a supply chain risk management framework that may guide managers to assess and manage IT and Cyber risks in protecting supply chain processes. We addressed key risks, such as IT failures, piracy and thefts, product shortages, safety and security, inventory levels, and supplier dependence, which may significantly affect strategic, financial, and operational

performances of all actors in a supply chain. Nonetheless, to the best of our knowledge, there are very few theoretical frameworks (Khan and Estay, 2015) that link the supply chain risk management process to IT and Cyber risks throughout the entire value chain.

To fill this gap, we adapted a framework based on Fawcett et al. (2011), whose objective was to study the effective deployment of IT by analyzing why some types of investments are more successful than others. We aimed to enlarge the abovementioned scope by considering how systematic IT and Cyber risk management may enhance the ability to share information and better manage supply chain processes. The proposed framework is shown in Figure 1, and represents how the key steps of a risk management process (risk assessment, risk treatment, risk governance, and risk compliance) should be adapted to IT and Cyber risks.

A robust IT and Cyber risk management program may protect the strategic goals of the supply chain, preventing business disruptions and protecting the reputation of all actors involved. Firstly, managing IT and Cyber risks would have the strategic benefits of enhancing the firms' capability to guarantee a tolerable level of overall risk for all actors involved and consistently do so within their real risk appetite. Thus, managers should monitor if and how IT and Cyber risks may threaten relevant assets and relationships with upstream and downstream supply chain partners.

Secondly, IT failures, piracy, thefts, and Cyberattacks are listed among the major causes of reputation crises and losses of reputation value. Protecting the supply chain against those risks requires stable relationships amongst supply chain members and fostering collaboration.

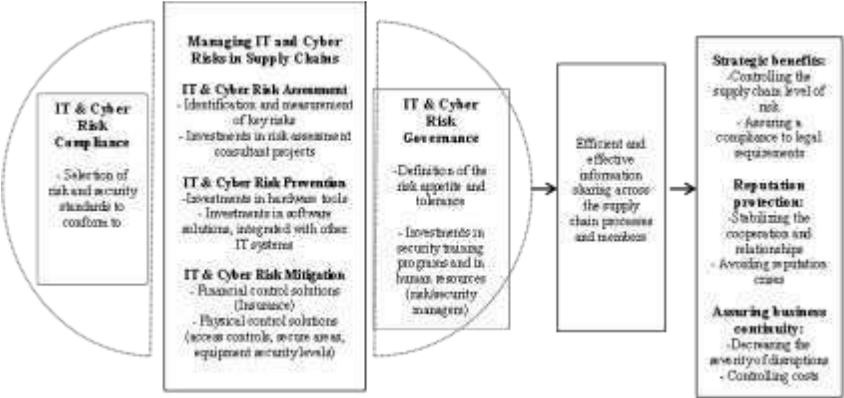


Figure 1. A framework for managing IT and Cyber risks in supply chains

Thirdly, IT failures and Cyberattacks may cause business interruptions, which in turn may damage suppliers’ and customers’ operational and financial performances.

The risk management process should therefore start with a careful assessment of the sources of IT and Cyber risks amongst all supply chain members. In companies that lack awareness of these risks, the role of the “channel captain” is essential. These supply chain leaders should, for example, lead supply chain risk management projects or include them in their contractual agreements or sourcing strategies’ ad hoc requirements regarding investments in IT and Cyber risk consultancy projects.

After the assessment (identification, measurement, and evaluation) of these risks, each supply chain member should decide the nature and amount of investments in risk prevention strategies, such as investments in hardware and software, which they plan to implement. Risk mitigation strategies reduce the severity of disruptions, control costs, and assure continuity of supplies. Risk mitigation comprises both financial controls (IT and Cyber risk insurance programs) and physical controls (investing in access control, secure areas, equipment security levels).

This framework offers a holistic risk management process, in which the abovementioned strategies, processes, technologies, and human resources should be aligned in coherence with the governance of each organization and of the supply chain as a whole. Several variables will influence the implementation of the risk management process such as the position of the supply chain captain (i.e., a manufacturer or a retailer), strategic priorities (i.e., efficiency vs. responsiveness), the industry/markets (there are different security standards to conform to, such as ISO/IEC 27001:2013, depending on the sector/markets), and organizations' dimensions. The final result should be a supply chain where the actors share more information throughout the whole process, which guarantees strategic benefits, reputation protection, and business continuity. Notably, empirical studies have demonstrated that IT-enabled information sharing promotes advantages, such as logistics

integration and agility, which has a positive impact on operational, strategic, and financial performances (Trkman et al., 2010; Dewan and Ren, 2011; Giannakis and Louis, 2011; Mithas et al., 2011; Tallon and Pinsonneault, 2011; Prajogo and Olhager, 2012; PWC Report 2015b). Thus, companies that show a real commitment to safeguarding the entire value chain from IT and Cyber risks have greater control over the supply chain's level of risk, build solid reputations, and assure business continuity.

#### *2.4 Practical evidence from a European sample of companies*

Recent literature has poorly investigated the perceptions and decision-making processes regarding the management of IT and Cyber risks within the supply chain (Benlian and Hess, 2011; Yildirim et al., 2011; Pezderka and Sinkovics, 2011). This led us to conduct an empirical investigation of European organizations that rely on security and risk management standards in order to choose the drivers of systematic IT and Cyber risk management (risk assessment, risk prevention, risk mitigation, risk compliance, and risk governance), as shown in Table 1.

Table 1. IT and Cyber risk management constructs

Risk Management Process	Main references
<b>Risk Assessment</b>	
<ul style="list-style-type: none"> <li>- Identification and measurement of key risks</li> <li>such as:               <ul style="list-style-type: none"> <li>- Inadvertent breaches</li> <li>- Deliberate attacks</li> <li>- Asset thefts</li> <li>- Equipment failures</li> <li>- Backup failures</li> <li>- Data thefts</li> <li>- Site disasters</li> <li>- Copyright infringements</li> </ul> </li> <li>- Presence of a dedicated budget for IT security management</li> <li>- Investments in risk assessment consulting projects</li> </ul>	Yildirim, E. et al. (2011) Biener, C. et al. (2015) Järveläinen, J. (2013)
<b>Risk Prevention</b>	
<ul style="list-style-type: none"> <li>- Investments in hardware tools</li> <li>- Investments in software solutions integrated with other IT systems</li> </ul>	Ifinedo, P. (2012) Järveläinen, J. (2013) Yildirim, E. et al. (2011) Biener, C. et al. (2015) Boyson, S. (2014) Silva, M. et al. (2014)
<b>Risk Mitigation</b>	
<ul style="list-style-type: none"> <li>- Financial control solutions (insurance)</li> <li>- Physical control solutions (access controls, secure areas, and equipment security levels)</li> </ul>	Biener, C. et al. (2015) Silva, M. et al. (2014) Feng, N. et al. (2014)

	Yildirim, E. et al. (2011)
<b>Risk Governance</b>	
<ul style="list-style-type: none"> <li>- Defining the organization's risk appetite and tolerance</li> <li>- Investments in ad hoc training programs in security</li> <li>- Investments in organizational human resources (risk manager, security manager, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Järveläinen, J. (2013)</li> <li>Yildirim, E. et al. (2011)</li> <li>Boyson, S. (2014)</li> <li>Ifinedo, P. (2012)</li> <li>Johnston, A. et al. (2010)</li> <li>Biener, C. et al. (2015)</li> </ul>
<b>Risk Compliance</b>	
<ul style="list-style-type: none"> <li>- Perception of the organization regarding exposure and vulnerability toward IT and Cyber risks</li> <li>- Risk appetite of an organization</li> </ul>	<ul style="list-style-type: none"> <li>Yildirim, E. et al. (2011)</li> <li>Ifinedo, P. (2012)</li> <li>Bulgurcu, B. et al. (2010)</li> <li>Feng, N., et al. (2014)</li> <li>Biener, C., et al. (2015)</li> <li>Boyson, S. (2014)</li> </ul>

To investigate whether or not the perceptions and management of these risks vary, depending on the industry, performance, and globalization choices of organizations, we considered heterogeneity with regard to the industries they operate in, their size, and their level of internationalization (Martin and Eisenhardt, 2010). The sample involved several European companies including: one small, local company, with a revenue under €1 million, which had between 10 and 100 employees; seven medium companies, with revenues between €1 million and €500 million, less than 50 thousand employees, and that represented various interests internationally; and seven large

companies, which were evenly distributed throughout their level of internationalization, with revenues exceeding €10 billion and more than 50 thousand employees.

We interviewed more than one key informant, including CEOs, supply managers, risk managers, and/or IT managers, within the same organization to consider whether or not their role might impact the way IT and Cyber risks are seen and faced. This process allowed us to reach the point of theoretical saturation with fifteen organizations.

Some evidences from our research are summarized in Table 2. The sample revealed that managing IT risks and Cyber risks positively influences reputation toward both the upstream and downstream actors of the supply chain. However, the commitment to managing these risks and protecting reputation varied by the dependence of the supply chain under observation: IT and Cyber risk management toward the upstream supply chain was almost non-existent, while a higher commitment was seen toward clients and customers. In fact, managers perceived breaches to private and personal information as less tolerable than threats to business-to-business partners.

Table 2. Some evidences from the interviews

IT and Cyber Risk Assessment	<i>C1: When we analyze risks, what we measure is the reputational damage. We also address the economic damage for the company, but the reputational damage is our priority, as it is knowable to anybody and it takes time to reabsorb.</i>
------------------------------	---

	<p><i>C2: We assess risks through daily antivirus scanning and we keep ourselves updated about the possible IT and Cyber risks through specialized journals and blogs.</i></p> <p><i>C1: In the last 24 months we suffered from inadvertent breaches, deliberate attack, asset theft, equipment failure, backup failure, copyright and compliance infringement. We focus our risk assessment on these risks.</i></p>
IT and Cyber Risk Prevention	<p><i>C7: We do not have a dedicated budget for IT and Cyber risk prevention. The problem is that there are urgent needs, and we invest only on emergencies. In this way, sometimes we spend more than we would if we were investing in formal prevention plan.</i></p> <p><i>C3: We get there only when it is too late, when the damage has been done. There is little strategy and a lot of tactics, and little prevention.</i></p> <p><i>C14: Only a careful training could improve the efficacy and the efficiency of the IT Risk Prevention.</i></p>
IT and Cyber Risk Mitigation	<p><i>C2: The back-up procedures (for IT risk) are formal and these are able to reconstruct the history of up to three years. The back-up is on a daily base, business continuity is excellent. The disaster recovery is great and there are two separate sites. However all of this is just for IT risks, not cyber risks.</i></p> <p><i>C4: On average we realize we had an intrusion 180 days later, and between 70% and 80% of internal fraud are discovered only by informers. So our mitigation strategy is not efficient yet.</i></p>
IT and Cyber Risk Compliance	<p><i>C8: We decided not to follow some specific Information Security Standard. We just follow our best practices.</i></p>

IT and Cyber Risk Governance	<p><i>C7: The Risk Manager is also responsible for IT risk, but he cannot be good in everything! He assigns priorities to the problems to solve.</i></p> <p><i>C15: Top managers consider themselves completely risk adverse. Nonetheless, they do not care sufficiently about IT risks.</i></p> <p><i>C2: We do not have systematic training on IT and Cyber Risk Management. We rely just on our perceptions.</i></p> <p><i>C7: The IT manager is not in the management committee, and his language is too technical to deal with the top management. There is a communication problem.</i></p>
------------------------------	---

Strategic and operational advantages related to careful IT and Cyber risk management currently lack acknowledgement. Thus, managers usually neither stipulate contractual agreements with key suppliers nor implement systematic plans for disaster recovery, business continuity, or the backup of sensitive data. Moreover, there is a low commitment at the corporate level: risk and security managers show a greater awareness about IT and Cyber risks, while top managers do not prioritize their management. The consequence is a scarce effort in building a deeper awareness among employees through systematic training.

Regarding risk assessment, IT and Cyber risks were systematically assessed by more than half of the sample, who also had a dedicated budget. However, the identification and measurement of key risks appeared to be far from effective:

three out of four of the respondents had faced some IT and Cyber breaches in the last 24 months.

Investments in risk assessment consulting projects were low for the majority of larger, multinational organizations, which used consultancy “on demand” for testing protection systems (penetration intrusion test), disaster recovery, and backup systems.

Regarding risk treatment, mitigation strategies were widely used, even if the majority was exclusively dedicated to IT risks. More than half of the sample had a budget solely dedicated to software, hardware, insurance, physical entry controls, secure areas, and equipment security levels. Interestingly, managers appeared genuinely convinced that effective IT and Cyber risk management was possible solely through these types of investments. Risk prevention rarely accounted for ad hoc investments by most of the organizations. Thus, they seemed somewhat disoriented by the breaches from which they suffered; a third of the sample admitted that companies tend to be high-risk takers, with a dramatic number of IT and Cyber breaches discovered roughly six months after the fact.

In general, risks were assessed by only one out of three organizations. Interestingly, the majority of them were medium and small companies, which invested in protection, disaster recovery, and backup consultancy services. The only exception to this trend was represented by multinational operations in the financial and oil industries, which invested significantly in risk

assessment consulting projects. However, they often required consultancy services exclusively to assess Cyber risks and rarely for IT risks.

Efforts in IT and Cyber risk prevention were performed systematically by all the multinational companies and by the small organization, which operates in the software industry. As mentioned earlier, roughly all the sample companies implemented systematic mitigation strategies. The only striking exceptions were the small organization and all those operating in the healthcare industry.

The majority of the medium and small companies perceived low exposure and vulnerability toward IT and Cyber risks, while risk appetite was declared to be very low throughout all companies and industries. Roughly all the companies invested in ad hoc training programs in security, but they were only directed toward the risk and security managers, never to all the employees.

In general, finance and high technology industries showed the most careful and systematic IT and Cyber risk management processes, while the healthcare sector implemented only occasional measures.

## *2.5 Conclusions*

The pervasive use of Internet throughout the entire value chain may assure significant advantages to organizations, particularly

in terms of resilience. To investigate how companies in practice perceive IT and Cyber risks and whether they include them in their decision-making process, we conducted an exploratory survey among different European companies, leaders in their industries. The findings show a lack of awareness at different organizational levels. Employees seem to be unprepared to deal with these risks and with their effects onto processes and operations. From the top management perspective, managers seem to dedicate insufficient efforts and investments particularly in IT and Cyber risk mitigation strategies, mainly using reactive approaches instead of proactive ones.

The proposed risk management framework seems to fill an existing gap in the literature, addressing how systematic IT and Cyber risk management may enhance the ability to share information and better manage supply chain processes. From a practitioner perspective, the framework addresses those risks – such as IT failures, piracy and thefts, product shortages, safety and security, inventory over-stocks, and supplier dependence – which may significantly affect supply chain performances. In practice, this approach may guide managers to formally assess and manage IT and Cyber risks in order to protect supply chain processes. Moreover, the framework promotes a formal mitigation plan to update systematically, in order to respond to IT and Cyber risks, considering the time pressure these new threats impose to all the actors of the supply chain. These risk management process should be constantly supported by strong

commitment from top management, especially in conforming to the ad hoc security standards and the definition of the real risk appetite and tolerance of the company. Managers should also be engaged in promoting an overall “IT and Cyber culture” transversally in the entire supply chain, because IT and Cyber risks represent significant threats for both the upstream and downstream supply chain.

### **References**

Aon Risk Solutions, Global Risk Management Survey 2015 Available at: <http://www.aon.com/2015GlobalRisk/> [Accessed 04 April 2016].

Bailey, T., Miglio, A. D., & Richter, W. (2014). The rising strategic risks of Cyberattacks. *McKinsey Quarterly*, 2(2014), 17-22.

Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. *Information Technology and Management*, 11(1), 7-23.

Bartol, N. (2014). Cyber supply chain security practices DNA—Filling in the puzzle using a diverse set of disciplines. *Technovation*, 34(7), 354-361.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, 52(1), 232-246.

- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis†. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1), 131-158.
- Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), 342-353.
- Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International journal of information management*, 33(5), 726-733.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.
- D'Amico, A., Buchanan, L., Goodall, J., & Walczak, P. (2010, April). Mission impact of Cyber events: scenarios and ontology to express the relationships between cyber assets, missions and users. In *International Conference on Information Warfare and Security* (p. 388). Academic Conferences International Limited.
- Dewan, S., & Ren, F. (2011). Information technology and firm boundaries: Impact on firm risk and return performance. *Information Systems Research*, 22(2), 369-388.
- Ellison, R. J., & Woody, C. (2010, January). Supply-chain risk management: Incorporating security into software development. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pp. 1-10. IEEE.

Fawcett, S. E., Wallin, C., Allred, C., Fawcett, A. M., & Magnan, G. M. (2011). Information technology as an enabler of supply chain collaboration: a dynamic-capabilities perspective. *Journal of Supply Chain Management*, 47(1), 38-59.

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information sciences*, 256, 57-73.

Gao, X., & Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, 235(1), 277-300.

Gao, X., Zhong, W., & Mei, S. (2015). Security investment and information sharing under an alternative security breach probability function. *Information Systems Frontiers*, 17(2), 423-438.

Garfinkel, S. L. (2012). The cybersecurity risk. *Communications of the ACM*, 55(6), 29-32.

Gaudenzi, B., & Borghesi, A. (2006). Managing risks in the supply chain using the AHP method. *The International Journal of Logistics Management*, 17(1), 114-136.

Gaudenzi, B., & Siciliano, G. (2016). "Just do it. Managing IT and cyber risks to create value" in 6<sup>th</sup> Global Innovation and Knowledge Academy (GIKA) Conference, 21-23 March 2016, Valencia, Spain.

Giannakis, M., & Louis, M. (2011). A multi-agent based framework for supply chain risk management. *Journal of Purchasing and Supply Management*, 17(1), 23-31.

Huang, S. M., Hung, W. H., Yen, D. C., Chang, I. C., & Jiang, D. (2011). Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems*, 50(4), 692-701.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.

ISO/IEC 27001:2013 Information technology-Security techniques-Information security management systems-Requirements Available at: [http://www.iso.org/iso/catalogue\\_detail?csnumber=54534](http://www.iso.org/iso/catalogue_detail?csnumber=54534) [Accessed 04 April 2016].

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, 33(3), 583-590.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Khan, O., & Estay, D. A. S. (2015). Supply Chain CyberResilience: Creating an Agenda for Future Research. *Technology Innovation Management Review*, 5(4), 6-12.

- Kong, H. K., Kim, T. S., & Kim, J. (2012). An analysis on effects of information security investments: a BSC perspective. *Journal of Intelligent Manufacturing*, 23(4), 941-953.
- Markmann, C., Darkow, I. L., & von der Gracht, H. (2013). A Delphi-based risk analysis—Identifying and assessing future challenges for supply chain security in a multi-stakeholder environment. *Technological Forecasting and Social Change*, 80(9), 1815-1833.
- Martin, J. A., & Eisenhardt, K. M. (2010). Rewiring: Cross-business-unit collaborations in multibusiness organizations. *Academy of Management Journal*, 53(2), 265-301.
- Melville, N. P. (2010). Information systems innovation for environmental sustainability. *MIS quarterly*, 34(1), 1-21.
- Mithas, S., Ramasubbu, N., & Sambamurthy, V. (2011). How information management capability influences firm performance. *MIS quarterly*, 35(1), 237-256.
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not?. *Decision Support Systems*, 56, 11-26.
- Olson, D. L., & Dash Wu, D. (2010). A review of enterprise risk management in supply chain. *Kybernetes*, 39(5), 694-706.
- Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management*, 30(6), 567-572.

Pezderka, N., & Sinkovics, R. R. (2011). A conceptualization of e-risk perceptions and implications for small firm active online internationalization. *International Business Review*, 20(4), 409-422.

Prajogo, D., & Olhager, J. (2012). Supply chain integration and performance: The effects of long-term relationships, information technology and sharing, and logistics integration. *International Journal of Production Economics*, 135(1), 514-522.

PWC Report (2014). Information Security Breaches Survey 2014 Technical Report. Available at: <http://www.pwc.co.uk/services/audit-assurance/insights/2014-information-security-breaches-survey.html> [Accessed 04 April 2016].

PWC Report (2015a). Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015. Available at: [www.pwc.com/gsis2015](http://www.pwc.com/gsis2015) [Accessed 04 April 2016].

PWC Report (2015b). Reinventing Information Technology in the Digital Enterprise. PwC's New IT Platform: Achieve High Velocity IT in a Digital World. Available at: <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/new-it-platform.html> [Accessed 04 April 2016].

- Silva, M. M., de Gusmão, A. P. H., Poletto, T., e Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, 34(6), 733-740.
- Tallon, P. P., & Pinsonneault, A. (2011). Competing perspectives on the link between strategic information technology alignment and organizational agility: insights from a mediation model. *Mis Quarterly*, 35(2), 463-486.
- Trkman, P., McCormack, K., De Oliveira, M. P. V., & Ladeira, M. B. (2010). The impact of business analytics on supply chain performance. *Decision Support Systems*, 49(3), 318-327.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.
- Yang, Y. P. O., Shieh, H. M., & Tzeng, G. H. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Information Sciences*, 232, 482-500.
- Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, 31(4), 360-365.

### **3. Effects of data breaches from user-generated content: A corporate reputation analysis**

**Siciliano G., Confente I., Gaudenzi B. & Eickhoff M.**

#### Abstract

This paper investigates the effects of data breaches on corporate reputation. Prior research indicates that these new and unpredictable threats may have significant drawbacks for vital corporate dimensions. Further, in the Industry 4.0 era, the redundancy of these scandals on social media can exacerbate negative effects. In this context, the study conducted Latent Dirichlet Allocation analysis on social media user-generated content for a sample of 35 firms in nine industries that had a data breach incident between 2013 and 2016. The aim was to discover how reputational dimensions changed before and after these critical events, as well as the differences among the types of data breaches and industries.

The results reveal that, compared with the antecedent period, more reputational dimensions emerged after critical events. Three of these dimensions—perceived quality, customer orientation and corporate performance—emerged for all three types of breach. However, if there was a identified responsible party for the data breach, users focused more on the role of firms' human resources management, whereas if users did not identify a responsible party, users focused more on privacy drawbacks.

These findings provide key insights for the research and industry to understand large-scale data breaches and reputational drawbacks after such incidents.

**Keywords:** Corporate Reputation, Data Breach, User-Generated Content, Latent Dirichlet Allocation

### *3.1 Introduction*

Reputation is considered a strategic intangible asset for companies because it substantially contributes to giving them a competitive advantage (Gatzert, 2015; Gatzert & Schmit, 2016; Rindova & Fombrun, 1999).

Data breaches represent a significant threat to companies' reputation. Cybercrime has become the second most reported cause of economic crime (KPMG, 2016; PwC, 2016). For example, in May 2017, the WannaCry ransomware attack seized hundreds of thousands of computer systems around the world (Sanger, Chan, & Scott, 2017). Recently, marketing studies (Ferrell, 2017; Hille, Walsh, & Cleveland, 2015; Kashmiri, Nicol, & Hsu, 2017; Martin & Murphy, 2017; Martin, Borah, & Palmatier, 2017) and management studies (Kude, Hoehle, & Sykes, 2017; Gatzert, 2015; Gatzert & Schmit, 2016) have focused their attention on such events.

Data breaches are unpredictable, often low-probable and high-impacting, like "black swans" (Gaudenzi & Siciliano, 2017), and they can be categorized into three groups (Sen & Borle, 2015): intentional and internal (e.g., malicious employees

stealing customers' data), unintentional and internal (e.g., incorrect security settings that expose private information), and external and intentional (e.g., ransomware infecting companies' software).

In this context, the Situational Crisis Communication Theory (SCCT) (Coombs, 2007, 2016) assumes that corporate reputation can be threatened by crises through the creation of negative perceptions (Coombs, 2007; Coombs & Holladay, 2002). To capture and to understand such perceptions online data analysis provide a global and valuable feedback (Wang, Wan, Zhang, Li, & Zhang, 2016). In particular, user-generated content (UGC) (Tirunillai & Tellis, 2014), which is defined as content that is created and shared by users (Kumar, Bezawada, Rishika, Janakiraman, & Kannan, 2016), is considered a valid representation of the "wisdom of the crowds" (Tirunillai & Tellis, 2014, p. 464).

Few marketing and management studies have examined the effect of different data breaches (Kashmiri et al., 2017) on vital corporate dimensions, such as reputation (Ferrell, 2017; Manworren, Letwat, & Daily, 2016), in different industries (Kashmiri et al., 2017; Sen & Borle, 2015).

To fill this gap, this study's three research questions focus on consumers' reactions to data breaches by analysing UGC extracted from social media:

What is the main UGC topic related to company reputation dimensions? Do the dimensions vary after data breaches? If so, how?

How does UGC related to company reputation dimensions vary depending on the type of data breach?

How does UGC related to company reputation dimensions change in relation to different industries?

The unit of analysis in this study is UGC around companies, which was analysed using the Latent Dirichlet Allocation (LDA) automated method (Blei, Ng, & Jordan, 2002). Potential implications of LDA in management research have been studied recently (George, Osinga, Lavie, & Scott, 2016) and adopted by marketing studies to ascertain implicit and intangible dimensions such as quality (Tirunillai & Tellis, 2014), consumers' attitudes and behaviour in social media (Langley, Hoeve, Ortt, Pals, & van der Vecht, 2014; Zhang, Moe, & Schweidel, 2017) and purchase predictions (Jacobs, Donkers, & Fok, 2016).

In addition, qualitative data analysis was implemented to ascertain the content and valence characterizing the dimensions extracted through the LDA analysis.

The rest of the article is organized as follows. Section 2 presents a literature review of the main concepts of corporate reputation, data breaches, UGC and SCCT. Sections 3 and 4 describe the method and results respectively. Section 5 presents the findings

and implications, and Section 6 discusses limitations and future research directions.

### *3.2 Literature review and theoretical development*

#### *3.2.1 Corporate reputation*

Fombrun (2012) highlighted that “a corporate reputation is a collective assessment of a company’s attractiveness to a specific group of stakeholders relative to a reference group of companies with which the company competes for resources” (p. 100). Thus, reputation is largely perceived as a multidimensional construct in which perceptions of customers, suppliers, (potential) employees, investors and local communities converge (Eckert, 2017; Gatzert, 2015). In line with this stream of literature, Walsh and Beatty (2007), Walsh, Mitchell, Jackson and Beatty (2009), and Wepener and Boshoff (2015) recommended further investigation of customers’ perceptions, which are the primary and most challenging revenue driver.

Reputation has been described as a fragile construct because of potential adverse changes in stakeholders’ perceptions (Gatzert, 2015). Reputation is largely considered an asset that is exposed to several risks, and companies consider reputational risk in their risk management agenda (Gaudenzi, Confente, & Christopher, 2015).

Gatzert (2015) categorized the events that may damage corporate reputation and financial performance. However,

Eckert (2017) noted that there is a lack of in-depth understanding of the effect of stakeholders' perceptions on the different dimensions of corporate reputation in the case of critical events.

### *3.2.2 Data breaches*

Access to consumers' personal information enables firms to better personalize products and services (Hofacker, Malthouse, & Sultan, 2016), as well as prices (Wedel & Kannan, 2016). However, this access has led to firms facing new threats, which are represented by data breaches that may stem from external and intentional attacks (KPMG, 2016), as well as employees (PwC, 2016).

While a growing number of firms in various industries (KPMG, 2016; Martin & Murphy, 2017; PwC, 2016) have suffered from data breaches, the literature seems to focus on single incidents; thus, broader investigations are needed (Kashmiri et al., 2017; Knittel & Stango, 2014).

The literature on information systems and management highlights the relevance of investments in enhancing technical preventive measures (August, Niculescu, & Shin, 2014; Järveläinen, 2013; Nazareth & Choi, 2015), protecting data privacy (Martin & Murphy, 2017) and boosting cultural change (Gaudenzi & Siciliano, 2017). Moreover, studies in management and risk propose reputation risk insurance solutions (Gatzert, 2015; Gatzert & Schmit, 2016; Scandizzo,

2011). However, efforts towards mitigation strategies often remain partially implemented because of the lack of a holistic understanding of the damage caused by data breaches on firms. Thus, there is a need to investigate the erosion of firms' reputations (Ferrell, 2017) across industries (Kashmiri et al., 2017; Sen & Borle, 2015), as well as types of data breaches (Kashmiri et al., 2017).

### *3.2.3 Social media*

Social media includes platforms where big data can be analysed in high volume, velocity and variety (Hofacker et al., 2016). Big data represents a twofold channel of interaction whereby firms can post firm-generated content (Kumar et al., 2016; Kumar, Choi, & Greene, 2017) and customers can create and share UGC with firms and people (Kumar et al., 2016; Tang, Fang, & Wang, 2014; Tirunillai & Tellis, 2014).

Studies have investigated customers' motivations in creating UGC (Presi, Saridakis, & Hartmans, 2014; Sun, Dong, & McIntyre, 2017), the change in users' perceptions following exposure to UGC (Marchiori & Cantoni, 2015), and the credibility of travel-related UGC such as TripAdvisor (Ayeh, Au, & Law, 2013) and restaurant recommendations (Salehi-Esfahani, Ravichandran, Israeli, & Bolden, 2016), as well as customers' propensity and involvement to post online (Ahn, Duan, & Mela, 2015; Shriver, Nair, & Hofstetter, 2013), engage publicly with a brand (Chiagouris & Williams, 2014; Malthouse,

Calder, Kim, & Vandenbosch, 2016) and make purchase decisions online (Ludwig et al., 2013).

In relation to UGC as a tool to measure firms' dimensions, studies have ascertained implicit and intangible dimensions such as quality (Tirunillai & Tellis, 2014), predicted purchases (Jacobs et al., 2016), users' behaviour (Thakur, Summey, & John, 2013), quantified firms' return on sales (Kumar et al., 2016; Leeflang, Verhoef, Dahlström, & Freundt, 2014; Tang et al., 2014) and firm value (Leeflang et al., 2014). Extant literature suggests that UGC should be monitored in crises contingencies (Hsu & Lawrence, 2016; Sung & Hwang, 2014) because customers may erode a firm's reputation when discussing critical events (Eckert, 2017; Gatzert, 2015; Leeflang et al., 2014).

#### *3.2.4 Situational crisis communication theory*

Coombs' (2007) SCCT states that a firm's reputation is a valued asset that is threatened when stakeholders start to have negative perceptions of the firm's actions (Coombs, 2007; Coombs & Holladay, 2002). SCCT links different crisis communication strategies to different types of crises, which are categorized as intentional and internal, intentional and external, unintentional and internal, and unintentional and external (Coombs & Holladay, 1996, 2001).

The theory has been enriched through investigations into the effect of previous crises on a current crisis (Coombs & Holladay,

2004) and the role of firms' reputation in mitigating the current threat (Coombs & Holladay, 2006), as well as the effects of crisis communication on brand equity (Hegner, Beldad, & Kamphuis op Heghuis, 2014), people's risk perceptions and perceived safety (Liu, Kim, & Pennington-Gray, 2015; Liu, Pennington-Gray, & Krieger, 2016).

However, there has been little consideration of the role of different reputational dimensions in designing the appropriate crisis communication strategy. Thus, this study explores whether and how different dimensions of reputation change when different types of data breaches occur.

### *3.3 Methodology*

#### *3.3.1 Sampling*

To analyse the relationship between data breaches and corporate reputation, firms in the sample had to meet the following criteria. First, firms had to suffer from a data breach in the previous three years, because the social media monitoring tool (SDL SM2) used for the subsequent extraction of the social media posting related to each firm did not allow data to be gathered beyond this period. To identify the firms, the study relied on Privacy Rights Clearinghouse (<https://www.privacyrights.org>), which is an open-source database that contains news on data breaches. The database only includes firms whose headquarters are in the United States.

Three researchers independently integrated the list of firms with a manual search of data breach scandals that occurred worldwide in the previous three years. The unit of analysis was UGC related to firms that suffered from data breaches; thus, the sample was extracted by the social media monitoring tool SDL SM2. This enabled 250,000 postings about the same firm to be gathered for the period 2013–2016 from the following social media platforms: blogs, video microblogs (e.g., Twitter), social networks (e.g., Facebook), online message boards, wikis, photo sharing and classified/review sites. Next, the SDL SM2 search query was based on the firm name and refined by setting two parameters: English language and date range. For each company, social media data were collected considering the 15 days before and after the data breach (as well as the date of the event publication) to capture the feelings stemming from the scandal. In this phase, no keywords (e.g., “data breaches”, “cyberattack”, “hacker”) were used to filter the search to avoid constraints in the overall picture regarding what users discussed soon after a scandal.

The final sample was composed of 35 firms in nine industries (Appendix A) that had a data breach between 1 January 2013 and 30 November 2016. To answer the first and second research questions, firms in the sample were grouped according to the type of data breach (Appendix A).

Three researchers independently read news about data breaches relating to the sample firms and categorized them according to

the crises groups provided by the SCCT (Coombs & Holladay, 1996, 2001) (Table 1).

**Table 1. Classification of data breach types from the Privacy Rights Clearinghouse database**

<b>Intentional and internal</b>	<b>and</b>	<b>Unintentional and internal</b>	<b>Intentional and external</b>
<p><b>Insider:</b> Someone with legitimate access intentionally breaches information (e.g., employee, contractor or customer).</p> <p><b>Data and device theft:</b> Includes paper documents (non-electronic), laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape and stationary computers.</p>		<p><b>Unintended disclosure:</b> Disclosure not involving hacking, intentional breach or physical loss (e.g., sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, sending in an email, sending in a mailing or sending via fax).</p> <p><b>Data and device losses:</b> Includes paper documents (non-electronic), laptop, PDA, smartphone, memory stick, CDs, hard drive and data tape.</p>	<p><b>Payment card fraud:</b> Fraud involving debit and credit cards that is not accomplished via hacking.</p> <p><b>Hacking or malware:</b> Hacked by outside party or infected by malware.</p> <p><b>Data and device theft:</b> Includes paper documents (non-electronic), laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape and stationary computers.</p>

The protagonists of the first and second categories of data breach were employees, who “accounted for 59% of security incidents in 2014, and in U.S. companies alone, the unauthorized use of computers by employees accounted for \$40 billion in losses” (Manworren et al., 2016, p. 264). The study examined cases in which employees deliberately breached information, because white-collar crimes can be devastating for companies (Ferrell, 2017; PwC, 2016). Further, cases in which employees unintentionally spread sensitive information in their activities of receiving and replying to email, as well as working with cloud

technologies and mobile devices, are particularly susceptible to cyberattacks (Manworren et al., 2016; PwC, 2016). The third category gathered data on intentional and external attacks (KPMG, 2016).

To answer the first and third research questions, firms in the sample were classified according to their industry (Appendix A).

### 3.3.2 Research design

To answer the research questions, this study used the social media text-mining approach showed in Figure 1, based on recent applications in the information technology (IT) and marketing literature (Calheiros, Moro, & Rita, 2017; Moro, Cortez, & Rita, 2015). Each phase of the analysis is described in depth in Sections 3.2.1 and 3.2.2. This section briefly illustrates the overall process, which consisted of two analyses. First, LDA analysis was conducted on the social media posts to extract the latent dimensions of the reputation. The process followed the steps illustrated by Tirunillai and Tellis (2014), so it began with pre-processing the textual information of the posts to transform an unstructured set of data into a structured list of words. The output is the corpus with all conjunctions and other basic and common terms removed that would not have provided any significant content to the study (e.g., “and”, “while”). Lastly, reputational dimensions were extracted from the corpus. Once the dimensions were extracted, they represented the input for the

second analysis, which conducted a detailed study of the content of the quotes representing the different dimensions and the valence characterizing each one. The qualitative data analysis software package NVivo 11 was used to conduct the analysis, categorize the quotes into the different dimensions extracted and value the related valence.

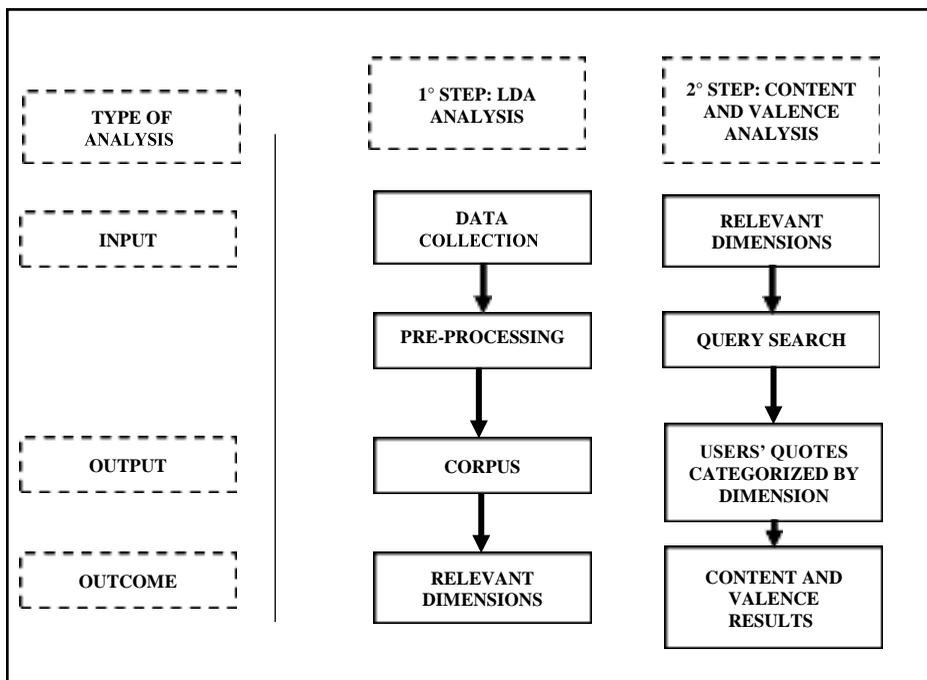
### *3.3.3 Latent Dirichlet allocation*

This study extracted the reputational dimensions expressed in UGC using one of the base models in the family of “topic models” (Blei, 2012) represented by the LDA (Blei, Ng, & Jordan 2003), which can efficiently analyse big, sparse data (Tirunillai & Tellis, 2014). As highlighted by Tirunillai and Tellis (2014), text needs to be pre-processed to remove all words that do not provide meaningful content. This includes breaking text down into individual words (tokenizing) (Blei et al., 2002), removing non-word content (e.g., punctuations) and stopwords (e.g., pronouns), and reducing remaining words to the word they stemmed from (e.g., from “feelings” to “feel”) (Porter, 1980). After estimating the model and extracting the dimensions, it was important to give them appropriate labels by selecting top-ranked words for relative importance in the given dimension (Tirunillai & Tellis, 2014). The word(s) that had the highest relative importance in each dimension could provide labels for the given dimension (Tirunillai & Tellis, 2014).

Labels were assigned considering the top five words for each topic (see Tables 3, 5 and 7 and Appendix B) and excluding words pertaining to industry-specific issues of the sample firms. These issues were too context specific and were not in line with the study's goal of investigating corporate reputation dimensions (Tirunillai & Tellis, 2014).

### 3.3.4 Content and valence analysis of user-generated content

**Figure 1. Proposed approach**



Given that the LDA model does not provide assumptions about the structure of the text (Tirunillai & Tellis, 2014), this study used text-mining analysis to gain a deeper understanding of the

content of the posts on social media and the valence associated with them.

The analysis was conducted using NVivo 11, which is a qualitative data analysis software package that supports the identification, categorization and analysis of words and sentences forming the emerged dimensions (Bazeley & Jackson, 2013). Recent studies in the management literature have used NVivo (Aitken & Paton, 2016; Hodges & Howieson, 2017; Taj, 2016; Vernuccio & Ceccotti, 2015) because it provides rigour and traceability in unstructured qualitative data (Ananthram & Chan, 2013). In particular, this study implemented the latest version of the software (NVivo 11 Plus), which works efficiently with large amounts of data to provide insights into text content not only by theme (in this study, the corporate reputation dimensions), but also by sentiment (in this study, the valence characterizing a dimension).

In relation to the content analysis, after the dimensions were established, a query search based on each one was performed. The analysis was conducted using two levels of specificity. In the first level, categorization was set to provide the exact dimensions identified by the LDA and supported by the literature—in particular, Walsh and Beatty's (2007) customer-based reputation dimensions. In this case, the query search was set to find the dimensions' exact match (e.g., search for "customer orientation", find "customer orientation"). In the second level of analysis, Walsh and Beatty's (2007) customer-

based corporate reputation factors were inserted into the query search (Table 2).

**Table 2. NVivo query search**

<b>Walsh and Beatty (2007) Corporate reputation factors</b>	<b>Wepener and Boshoff (2015) Corporate reputation factors</b>	<b>Walker (2010) Corporate reputation factors</b>	<b>Fombrun, Gardberg, &amp; Sever (2000) Corporate reputation factors</b>	<b>Synonyms set in the NVivo 11 query search</b>
Customer Orientation	Emotional Appeal	–	Emotional Appeal	Customer Care; Customer Service
Good Employer	Good Employer	Employee Treatment	Workplace Environment	Employee Training; Management; Good Employee; Experience; Skill; Working Conditions; Salary
Reliable and Financially Strong Company	Corporate Performance	Profitability; Corporate Governance	Financial Performance; Vision and Leadership	Investment; Fund; Corporate Performance
Product and Service Quality	Service Points	Product Quality	Products and Services	Service Quality; Product Quality; Innovation
Social and Environmental Responsibility	Social Engagement	Environmental Responsibility; Social Responsibility	Social and Environmental Responsibility	Society; Ethics

Once NVivo 11 provided the different users’ quotes categorized by dimension, it was set to analyse the tone characterizing the posts in the categories using the command “identify sentiment per phrase”. NVivo 11 provided four types of sentiment: very negative, moderately negative, very positive and moderately positive.

Given that the investigation was conducted in the 15 days after a scandal, there was a high chance that the “very positive” and “moderately positive” quotes were ironic; therefore, hiding a

“negative” or “neutral”. Thus, the three researchers independently coded the same users’ sentences and subsequently compared and discussed how they categorized the sentences to maximize reliability (Ananthram & Chan, 2013).

### *3.4 Results*

This study used LDA analysis to extract and label the dimensions of reputation across all UGC for each of the 35 firms in the sample using the procedure suggested by Tirunillai and Tellis (2014). Moreover, LDA analysis was integrated with content and valence analysis to provide in-depth information regarding the dimensions that emerged.

Tables 3, 5 and 7 provide snapshots of the top five words with the highest relative frequency relating to each dimension for the three types of data breach before and after the critical event. The labels were supported by the literature and assigned as follows. The first column of Table 3 shows the words “hire”, “skill”, “team”, “employee” and “work”, which can be referred to the employers of the firm, that can be labelled as “firm as employer”, consistently with the extant literature (Walker, 2010; Walsh & Beatty, 2007). Similarly, the second column characterizes firms’ corporate performance and the convenience of investing in them (“invest”, “financial”, “equity”, “investment”, “investors”). Thus, “corporate performance” is an appropriate label (Walker, 2010; Walsh & Beatty, 2007). “Customer orientation” refers to firms’ efforts to fulfil

customers' needs (Patel, Manley, Hair, Ferrell, & Pieper, 2016; Walsh & Beatty, 2007). "Social responsibility" considers firms' responsibility in relation to social issues (Patel et al., 2016; Walker, 2010; Walsh & Beatty, 2007), and "perceived quality" concerns customers' perceptions of the quality of firms' products and services (Walker, 2010; Walsh & Beatty, 2007). In addition, Tables 4, 6 and 8 outline the content and valence analysis implemented by NVivo 11. The LDA results of Tables 4, 6 and 8 answer the first research question and show that UGC varied before and after a data breach occurred. In general, before a critical event, users discussed about one main topic: the perceived quality of a firm's offer. Three additional dimensions then emerged—each characteristic of a specific type of data breach. Therefore, the second research question was addressed.

#### *3.4.1 Dimensions of reputation for intentional and internal data breaches*

Table 3 shows that when an intentional and internal data breach manifested, the "customer orientation" reputation dimension emerged through discussions about how much firms care about customers' needs ("care", "support") and their ability to target ("custom") assistance and provide it in a good way ("friendly") given the apprehension caused by the event ("concern").

**Table 3. Dimensions of reputation for intentional and internal data breaches**

	PRE-CRISIS			POST-CRISIS		
Employer	Corporate performance	Perceived quality	Customer orientation	Employer	Corporate performance	Perceived quality
Hire	Invest	Perform	Care	Employer	Dividend	Service
Skill	Financial	Quality	Support	Employee	Share	Quality
Team	Equity	Service	Custom	Compensation	Equity	Complaint
Employee	Investment	Value	Concern	Training	Investment	Weakest
Work	Investor	Product	Friendly	Responsible Investor		Worry

The second dimension that emerged (“employer”) relates to users’ interest in firms’ human resources management. From a comparison between the top five words before and after the data breach, the focus switched from general employees’ treatment (e.g., “hire”, “skill”) to specific aspects such as “compensation” and “training”. Further, the intentional nature of the scandal was reaffirmed (“responsible”).

The third dimension discussed after an intentional and internal data breach was firms’ “corporate performance”, which appears to have been discussed even before the event. In both periods, users commented on firms’ financial decisions (“invest”, “investment”) and the subsequent results (“equity”, “dividend”, “share”).

Finally, users discussed firms’ “perceived quality”, which was discussed before the critical event, but in different ways. In fact, before an intentional and internal data breach, the topics relate

to the performance (“perform”) and the value of the offer (“value”), while in the period after the event, the LDA analysis caught words related to users’ attitudes (“complaint”, “worry”) because of changes in the offer (“weakest”).

Table 4 presents the results of the LDA analysis to provide a more in-depth answer to the second research question. First, users focused on firms’ customer service (“customer orientation”), “perceived quality” of firms’ products and services, and “corporate performance”. Valence is characterized by two extremes: if users perceived improvements in these dimensions, the tone was positive; otherwise, they valued firms’ efforts in a “negative” way.

In “firm as employer” content analysis, “negative” tones were used to complain about the lack of training, with users hypothesizing the presence of resentful employees (an example of quote is the following: “Disgruntled ex-employee, maybe?”).

<b>Corporate reputation dimension</b>	<b>Company</b>	<b>Example</b>	<b>Valence</b>
Customer orientation	Capital One Financial Corp	@CapitalOneUK Found out that my CC is hacked! Capital One— excellent as always!! Helpful and courteous. Superb security. Highly recommended.	Very positive
	AT&T Inc.	God knows this is probably the worst example of customer service I have come across!	Very negative
Firm as employer	AT&T Inc.	I don’t have anything good to say about AT&T. They not only have very poor customer service, they have poor employee training and poor follow up to complaints.	Negative

	Sage Group PLC	Sage says it doesn't know how much data ... Disgruntled ex-employee, maybe?	Negative
Corporate performance	AT&T Inc.	Good job, I hope your shareholders are happy.	Negative
	Morgan Stanley	WOW! Time to divest yourself from Big Oil: Morgan Stanley's #Renewable #Energy Stock Picks for 2015.	Positive
Perceived quality	Federal Deposit Insurance Corporation (FDIC)	I like how the Federal Deposit Insurance Corporation (FDIC) is going out to collect customer #feedback.	Positive
	AT&T Inc.	Day 5 and counting, but my U-verse Internet service has STILL not been fixed by #AT&T. They are the worst provider on earth. I'm switching.	Very Negative

**Table 4. Content categorization and valence analysis for intentional and internal data breaches**

### *3.4.2 Dimensions of reputation for unintentional and internal data breaches*

Table 5 presents the LDA results for unintentional and internal data breaches. The top five words for the dimension labelled “customer orientation” show that users showed “concern” and discussed whether firms are oriented towards customers’ needs (“care”, “support”), focusing on firms’ ability to be effective (“helpful”) while expecting regrets (“apologize”). The second dimension relates to the convenience of investing in firms suffering from a data breach (“stock”, “equity”). Moreover, users discussed firms’ respect of rules and standards (“governance”, “compliance”).

**Table 5. Dimensions of reputation for unintentional and internal data breaches**

<b>PRE-CRISIS</b>		<b>POST-CRISIS</b>		
<b>Perceived quality</b>	<b>Customer orientation</b>	<b>Corporate performance</b>	<b>Perceived quality</b>	<b>Social responsibility</b>
Delivery	Concern	Finance	Service	Government
Quality	Helpful	Governance	Angry	Social
Product	Support	Stock	Innovative	Penalty
Great	Care	Compliance	Bad	Occupational
Service	Apologize	Equity	Quality	Educational

Users also discussed the quality of firms’ products and services. This dimension was discussed before the critical event and, also in the case of unintentional and internal data breaches, the dynamics of the dimension show changes in users’ attitudes (“angry”) and in the quality of the offer (“bad”). Finally, users cared about the effect of unintentional and internal data breaches on society, discussing a “penalty”, the role of the “government”, and the “social”, “occupational” and “educational” aspects. Table 6 presents the content and valence analysis, which shows that the “customer orientation” dimension was characterized by a “negative” to “very negative” valence. The “corporate performance” dimension was characterized by genuine questions about firms’ ability to deal with cyber-related issues in the future and by ironic quotes that hide negative valence. Users negatively welcomed decreasing quality of firms’ products and services and focused on the ethical implications of the internal and unintentional data breach—namely, “social responsibility”.

**Table 6. Content categorization and valence analysis for unintentional and internal data breaches**

<b>Corporate reputation dimension</b>	<b>Company</b>	<b>Example</b>	<b>Valence</b>
Customer orientation	Aflac Inc.	Why is this Aflac commercial so funny?	Negative
	HSBC Holdings PLC	@HSBC_UAE_Help HSBC customer service is an absolute disgrace! Rightly negative called the worst bank in terms of the customer experience. #avoidHSBC.	Very
Corporate performance	Cisco Systems Inc.	Can Cisco alone create a brighter future for IoT security?	Neutral
	HSBC Holdings PLC	#HSBC Chairman getting very tired with a shareholder listing all the bank's failures. I can sympathise, it's taking forever!	Negative
Perceived quality	Toyota Motor Corp	Someone hacked my account "Toyota" and stole my rsn. How do I recover it?	Negative
	Bank of America Corp	Bank of America: hard to believe account security is your priority when you send a new card every 3 months because your database was compromised.	Very
Social responsibility	Google Inc.	Ethicists concerned after records show US government may wield troubling influence over how Google runs the country.	Neutral
	HSBC Holdings PLC	Finally closed my account with HSBC and switched to a more ethical bank :) it's very important to think about stuff like this people!	Positive

### *3.4.3 Dimensions of reputation for intentional and external data breaches*

Table 7 shows that four dimensions emerged after an intentional and external data breach. The "customer orientation" reputational dimension focused on attributing responsibility ("blame", "complain") and how firms manage their responses ("communication", "rude", "customization"). The second dimension was the role of the "firm as the employer" (e.g.,

“work”, “salary”). There was also a focus on training activities.

Moreover, UGC presented arguments about firms’ management (“board”), financial results (“equity”, “bond”), and adherence to procedure and standards (“compliance”).

Finally, users valued the efficiency and reliability of firms’ products and services (“speed”, “unsafe”, “weak”). Table 8 shows that the general valence characterizing the emerged dimensions was “negative” or “very negative”. The tone was positive only when users perceived firms’ crisis management (an example of positive quote is the following one: “Tesco Bank have much better accounts than Barclays who also had a breach last year”) or initiatives (another example is “#Starbucks spends more on #employee #benefits each year than it does on #coffee. #interesting”) as effective.

**Table 7. Dimensions of reputation for intentional and external data breaches**

<b>PRE-CRISIS</b>		<b>POST-CRISIS</b>			
<b>Corporate performance</b>	<b>Perceived quality</b>	<b>Customer orientation</b>	<b>Employer</b>	<b>Corporate performance</b>	<b>Perceived quality</b>
Management	Useful	Rude	Work	Equity	Product
Finance	Original	Blame	Resume	Compliance	Speed
Acquisition	Special	Complain	Train	Board	Unsafe
Financial	Quality	Customization	Internship	Performance	Weak
Stock	Good	Communication	Salary	Bond	Quality

**Table 8. Content categorization and valence analysis for intentional and external data breaches**

<b>Corporate reputation dimension</b>	<b>CompanyExample</b>	<b>Valence</b>
Customer orientation	American Express Co. Skype Inc. @AskAmex ...no, it was fraud. I called American express disappointed yo never responded back...so much for assistance! #Skype has been hacked. Check your accounts, and good luck with customer support.	Negative
Firm as employer	theStarbucks Corp TalkTalk Telecom Group PLC #Starbucks spends more on #employee #benefits each year than it does on #coffee. #interesting. #victorialive it's best practice to encrypt all bank details. TalkTalk senior management should hire someone who understands security.	Positive Negative
Corporate performance	TalkTalk Telecom Group PLC #TalkTalk cyber-attack: Share price drops by 11%. Another example of the cost of poor reputation management.	Negative
	Yahoo STILL says a LOT about Yahoo's security practices. EVEN after the breach, why were they sitting smug? Sue the top executives.	Very negative
Perceived quality	Tesco Personal Finance PLC Tesco Bank have much better accounts than Barclays who also had a breach last year.	Positive
	LinkedIn Corp I might be more worried about the LinkedIn data breach if there was actually any value contained in my account.	Negative

The third research question of this study aimed to understand how UGC changes in relation to different industries. The study provides the top five words (Appendix B) and the dynamics of dimensions per industry (Appendix C). Overall, there is no a clear distinction among industries. However, users seem to discuss one main topic around companies of all the industries involved: “perceived quality”. Instead, after a data breach, users discussed firms’ corporate performance in most of the industries of the sample—particularly for “information technology”, “manufacturing”, “software & services” and “finance and insurance”. Owing to space limitations, Table 9 provides the best representative quote per industry to highlight the main valence of the quotes.

**Table 9. Content and valence analysis per industry**

Industry	Company	Quote examples	Valence
Accommodation and food services	Starbucks	Waking up to \$400 fraudulent charges to Starbucks on my credit card.	Negative
Arts, entertainment and Recreation	Disney	I would try to watch old Disney movies on my phone and it get hacked and my phone not work right.	Negative
Public benefits corporations	Kickstarter	Hackers broke in #Kickstarter this weekend. If you’ve used it, change your passwords :( #annoying.	Negative
Transportation and warehousing	United Airlines	United Airlines is annoying 😊. They don’t do nothing on time. I sprinted over here for nothing cus we still sitting here.	Negative
Information technology	TalkTalk Telecom Group PLC	Time to sack Chief Executive (Baroness) Dido (Diana) Harding for incompetence. lack of company knowledge and poor leadership of #TalkTalk.	Very negative
Manufacturing	American Apparel	HIS ACCOUNT GOT HACKED. Everyone keep supporting American	Positive

---

		Apparel. They do so much good work. Let's be patient while they deal with this. Just laugh at how silly/ridiculous the comics and hacker are, and not take it so seriously :).	
Technology hardware equipment	Cisco &	Thanks Cisco: I am now infinitely more alert and alarmed about shadowy hackers than I was 30. We have a new hero against video #piracy. Thank you Cisco!	Negative
Software services	&Dropbox	How can I be sure that my Dropbox account will not be compromised in the future? I've lost total confidence.	Very negative
Finance insurance	andHSBC Bank	@HSBC_UK_Help are you able to refund the money fraudulently taken from my bank account through HSBC's poor security?	Negative
	Tesco Bank	Tesco bank account breaches—significant reputational and financial loss!	Very negative

---

### 3.5 Discussion

A threat for a growing number of firms in various industries is the occurrence of different breaches of sensitive corporate data. These critical events represent vulnerability for firms' corporate reputation, whose multiple dimensions are affected by customers' negative perceptions in various ways. Some dimensions (e.g., "perceived quality", "customer orientation", "corporate performance") are important across different types of data breach and across industries, whereas other dimensions (e.g., "employer", "social responsibility") are important only for certain events and industries. Capturing such information and details represent a challenge for companies and represent a key finding of the present study. The following sections provide

insightful details related to when and how different corporate reputation vulnerabilities stem from different data breaches.

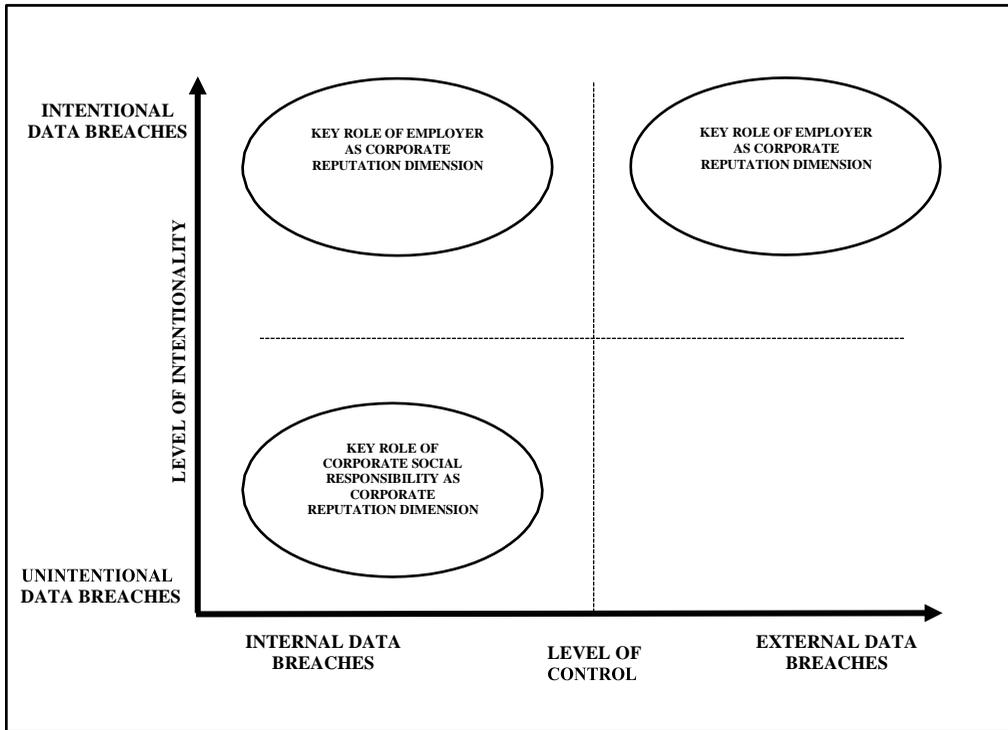
### *3.5.1 When and how customers react to data breaches?*

Figure 2 highlights that when a breach of sensitive data has been committed for malicious purposes (with a high level of intentionality), it leads to two negative reputational drawbacks. First, customers believe that firms are unable to train employees to prevent external hacks or to recognize/denounce colleagues who commit a cybercrime. Second, the lack of timely and meaningful information by customer service exacerbate customers' negative perceptions of customer orientation-related training. These negative drawbacks may be because of training programs that teach standardized customer care techniques, which may not fit with the extraordinary nature of data breaches. The result is that the “employer” corporate reputation dimension is negatively affected, and firms gain a reputation for lacking effective and systematic human resources management. This finding confirms studies in the relationship marketing literature that have found that timely and relevant communication forms positive perceptions in the consumer–brand relationship if it is “timely, meaningful, accurate, adequate, complete and credible” (Graca, Barry, & Doney, 2015, p. 807), and empathetic (Sarmiento, Simões, & Farhangmehr, 2015), especially in social media environments (Gensler, Völckner, Liu-Thompkins, &

Wiertz, 2013; Labrecque, von dem Esche, Mathwick, Novak, & Hofacker, 2013).

Further, this study integrates the notion that, in times of crises, employees show more commitment in delivering appropriate information to external stakeholders (van der Vegt, Essens, Wahlström, & George, 2015; Zhang & Venkatesh, 2013). In fact, their interest in performing well may be hindered by a lack of key information provided in a timely fashion, so they are unable to accomplish their assignments related to customer care. Thus, firms should prioritize timely access to salient information about the ongoing crisis because this plays a critical role in affecting employees' performance and, subsequently, firms' corporate reputation.

**Figure 2. Reputational dimensions characteristic of each data breach type**



*3.5.2 When and how customers pay attention to firms' ability to protect their privacy*

When a data breach stems from an unintentional error caused by a firm's internal employee, customers examine firms' cybersecurity measures and show concern about possible identity theft and online fraud. Further, they feel disappointed about how their personal information has been managed. This finding recalls the social contract theory (Donaldson & Dunfee, 1994; Ferrell, 2017), which notes that a moral contract drives

basic relationships between society and an individual. In a business context, this means that customers expect ethical and legal penalties for firms that have not protected their privacy rights within a society. Thus, an unintentional data breach sheds light on the “social responsibility” dimension of corporate dimension (Figure 2), and customers perceive that they are victims of an unfair error that could have been avoided with the implementation of systematic data privacy risk management.

This finding contrasts with prior literature, which has found that unintentional breaches should be perceived as minor transgressions when related to privacy concerns and ethical responsibilities in sharing sensitive information (Stewart, 2017). Conversely, this result confirms recent studies that have underlined the relevance of inserting firms’ use of consumer data into a larger societal picture (Ferrell, 2017; Martin & Murphy, 2017; Stewart, 2017).

### *3.5.3 Customers’ perceptions and valence across industries*

Contrary to previous studies on the effect of data breach announcements (Martin et al., 2017; Rosati et al., 2017), not all industries suffered from reputational drawbacks after a data breach. The discriminant lies in the role of sensitive data in each industry. If they are not the core business of the firms (e.g., manufacturing), corporate reputation is less vulnerable than in firms where consumers’ data are particularly sensitive (e.g., finance and insurance). In the latter, the results suggest that an

effective corporate communication strategy for external stakeholders should protect the “corporate performance” reputational dimension, which was negatively affected by data breach announcements in this study.

### *3.6 Contributions*

This study makes several academic and practical contributions to the literature. In relation to theoretical contributions, it complements crisis communication research by categorizing, in a different data breach context, stakeholders’ perceptions of firms’ ability to control the crisis, as well as the level of responsibility that stakeholders attribute to firms—the so-called “responsibility reputation” (Coombs & Holladay, 2002).

In addition, the research is informative for risk management literature (Gatzert, 2015) and reputation research (Walsh & Beatty, 2007; Walsh et al., 2009; Wepener & Boshoff, 2015) because it is one of the first studies to test corporate reputation dimensions in a data breach crisis setting (Martin & Murphy, 2017; Martin et al., 2017).

The managerial implications of this study are twofold. First, the investigation in nine industries enables some generalizations to be made about the main reputational drivers that managers should consider when designing a communication recovery response. Boosting a consumer-centric communication plan may be helpful to avoid damage to firms’ reputation. Thus, for instance, if the data breach stems from an unintentional error,

managers should explicitly share their efforts to improve voluntary security breach initiatives and their strict compliance with government guidelines. If, instead, the data breach is intentional, managers should encourage top-down communication to foster customer service employees' awareness about the ongoing crisis. In fact, an informed employee is more likely to provide effective and empathetic customer support.

Second, this study provides managers with a methodology—LDA analysis triangulated with a content and valence investigation—that comprises useful steps to unveil the corporate reputation dimensions that emerge in rich user-generated data after a data breach. This method also has scope to better assess data breach risks in firms' overall reputation risk management.

### *3.7 Conclusions*

This paper investigated the effect of data breaches on corporate reputation. Prior research has indicated that these new and unpredictable threats may have significant drawbacks for vital corporate dimensions. Further, in the Industry 4.0 era, conversations about these scandals on social media can exacerbate the negative effects. In this context, this study conducted LDA analysis on social media UGC for a sample of 35 firms in nine industries that suffered from a data breach incident in the period 2013–2016 to discover how reputational

dimensions change before and after these critical events, as well as the differences among the types of data breach and industries. Future research should better focus on the main differences among industries to understand the impact of data breaches on reputation dimensions.

Furthermore, this investigation considered what happens to customers' perceptions within a short period surrounding a data security event. Future research could complement this study by investigating how firms restore their reputation after these negative events, as well as which approach enables better recovery across industries and within a longer-term framework. Further, the study considered only one data breach event per firm, although some firms experienced the same type of breach multiple times. Future research could determine whether the presence of past crises plays a role in the formation of customers' perceptions and valence.

To conclude, this paper suggests that the analysis of a multidimensional construct such as reputation within a critical event is complex because it is influenced by several factors simultaneously. The holistic discussion provided by this research about the varying dynamics in different types of crisis and industry will help managers and researchers to better understand the common paths across firms and the distinctive threats of each event.

## References

- Ahn, D. Y., Duan, J. A., & Mela, C. F. (2015). Managing user-generated content: A dynamic rational expectations equilibrium approach. *Marketing Science*, 35(2), 284–303.
- Aitken, A., & Paton, R. A. (2016). Professional buyers and the value proposition. *European Management Journal*, 34(3), 223–231.
- Ananthram, S., & Chan, C. (2013). Challenges and strategies for global human resource executives: Perspectives from Canada and the United States. *European Management Journal*, 31(3), 223–233.
- August, T., Niculescu, M. F., & Shin, H. (2014). Cloud implications on software network structure and security risks. *Information Systems Research*, 25(3), 489–510.
- Ayeh, J. K., Au, N., & Law, R. (2013). “Do we believe in TripAdvisor?” Examining credibility perceptions and online travelers’ attitude toward using user-generated content. *Journal of Travel Research*, 52(4), 437–452.
- Bazeley, P., & Jackson, K. (Eds.). (2013). *Qualitative data analysis with NVivo*. Thousand Oaks, CA: Sage.
- Blei, D. M. (2012). Probabilistic topic models. *Communications of the ACM*, 55(4), 77–84.
- Blei, D. M., Ng, A. Y., & Jordan, M. I. (2002). Latent Dirichlet allocation. In T. G. Dietterich, S. Becker, & Z. Ghahramani (Eds.), *Advances in neural information processing systems* (pp. 601–608). Cambridge, MA: MIT Press.

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent Dirichlet allocation. *Journal of Machine Learning Research*, 3, 993–1022.

Calheiros, A. C., Moro, S., & Rita, P. (2017). Sentiment classification of consumer generated online reviews using topic modeling. *Journal of Hospitality Marketing & Management*. Advance online publication. <http://dx.doi.org/10.1080/19368623.2017.1310075>

Chiagouris, L., & Williams, M. (2014). If we build it will they stay? User generated content and website effectiveness. *Journal of Marketing Management*, 2(3 & 4), 1–14.

Coombs, W. T. (2007). Attribution theory as a guide for post-crisis communication research. *Public Relations Review*, 33(2), 135–139.

Coombs, W. T. (2016). Reflections on a meta-analysis: Crystallizing thinking about SCCT. *Journal of Public Relations Research*, 28(2), 120–122.

Coombs, W. T., & Holladay, S. J. (1996). Communication and attributions in a crisis: An experimental study in crisis communication. *Journal of Public Relations Research*, 8(4), 279–295.

Coombs, W. T., & Holladay, S. J. (2001). An extended examination of the crisis situations: A fusion of the relational management and symbolic approaches. *Journal of Public Relations Research*, 13(4), 321–340.

Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets: Initial tests of the situational crisis communication theory. *Management Communication Quarterly*, 16(2), 165–186.

Coombs, W. T., & Holladay, S. J. (2004). Reasoned action in crisis communication: An attribution theory-based approach to crisis management. In D. P. Millar & R. L. Heath R. L. (Eds.), *Responding to Crisis: A Rhetorical Approach to Crisis Communication* (pp. 95–115). Mahwah, NJ: Lawrence Erlbaum.

Coombs, W. T., & Holladay, S. J. (2006). Unpacking the halo effect: Reputation and crisis management. *Journal of Communication Management*, *10*(2), 123–137.

Coombs, W. T., Holladay, S. J., & Claeys, A. S. (2016). Debunking the myth of denial's effectiveness in crisis communication: Context matters. *Journal of Communication Management*, *20*(4), 381–395.

Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of Management Review*, *19*(2), 252–284.

Eckert, C. (2017). Corporate reputation and reputation risk: Definition and measurement from a (risk) management perspective. *Journal of Risk Finance*, *18*(2), 145–158.

Ferrell, O. C. (2017). Broadening marketing's contribution to data privacy. *Journal of the Academy of Marketing Science*, *45*(2), 160–163.

Fombrun, C. I. (2012). Corporate reputation: Definitions, antecedents, consequences. In M. L. Barnett and T. G. Pollock (Eds.), *The Oxford handbook of corporate reputation* (94–113). London, England: Oxford University Press.

Fombrun, C. J., Gardberg, N. A., & Sever, J. M. (2000). The Reputation Quotient<sup>SM</sup>: A multi-stakeholder measure of corporate reputation. *Journal of Brand Management*, *7*(4), 241–255.

Gatzert, N. (2015). The impact of corporate reputation and reputation damaging events on financial performance: Empirical evidence from the literature. *European Management Journal*, 33(6), 485–499.

Gatzert, N., & Schmit, J. (2016). Supporting strategic success through enterprise-wide reputation risk management. *Journal of Risk Finance*, 17(1), 26–45.

Gaudenzi, B., & Siciliano, G. (2017). Just do it: Managing IT and cyber risks to protect the value creation. *Journal of Promotion Management*. Advance online publication. <http://dx.doi.org/10.1080/10496491.2017.1294875>

Gaudenzi, B., Confente, I., & Christopher, M. (2015). Managing reputational risk: Insights from an European survey. *Corporate Reputation Review*, 18(4), 248–260.

Gensler, S., Völckner, F., Liu-Thompkins, Y., & Wiertz, C. (2013). Managing brands in the social media environment. *Journal of Interactive Marketing*, 27(4), 242–256.

George, G., Osinga, E. C., Lavie, D., & Scott, B. A. (2016). Big data and data science methods for management research. *Academy of Management Journal*, 59(5), 1493–1507.

Graca, S. S., Barry, J. M., & Doney, P. M. (2015). Performance outcomes of behavioral attributes in buyer-supplier relationships. *Journal of Business & Industrial Marketing*, 30(7), 805–816.

Hegner, S. M., Beldad, A. D., & Kamphuis op Heghuis, S. K. (2014). How company responses and trusting relationships protect brand equity in times of crises. *Journal of Brand Management*, 21(5), 429–445.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, 30, 1–19.

Hodges, J., & Howieson, B. (2017). The challenges of leadership in the third sector. *European Management Journal*, 35(1), 69–77.

Hofacker, C. F., Malthouse, E. C., & Sultan, F. (2016). Big data and consumer behavior: Imminent opportunities. *Journal of Consumer Marketing*, 33(2), 89–97.

Hsu, L., & Lawrence, B. (2016). The role of social media and brand equity during a product recall crisis: A shareholder value perspective. *International Journal of Research in Marketing*, 33(1), 59–77.

Jacobs, B. J., Donkers, B., & Fok, D. (2016). Model-based purchase predictions for large assortments. *Marketing Science*, 35(3), 389–404.

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, 33(3), 583–590.

Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: Intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, 45(2), 208–228.

Knittel, C. R., & Stango, V. (2014). Celebrity endorsements, firm value, and reputation risk: Evidence from the Tiger Woods scandal. *Management Science*, 60(1), 21–37.

KPMG. (2016). Consumer loss barometer. Retrieved from <https://info.kpmg.us/consumer-loss-barometer.html/> Accessed 20 April 2016.

Kude, T., Hoehle, H., & Sykes, T. A. (2017). Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *International Journal of Operations & Production Management*, 37(1), 56–74.

Kumar, A., Bezawada, R., Rishika, R., Janakiraman, R., & Kannan, P. K. (2016). From social to sale: The effects of firm-generated content in social media on customer behavior. *Journal of Marketing*, 80(1), 7–25.

Kumar, V., Choi, J. B., & Greene, M. (2017). Synergistic effects of social media and traditional marketing on brand sales: Capturing the time-varying effects. *Journal of the Academy of Marketing Science*, 45(2), 268–288.

Labrecque, L. I., vor dem Esche, J., Mathwick, C., Novak, T. P., & Hofacker, C. F. (2013). Consumer power: Evolution in the digital age. *Journal of Interactive Marketing*, 27(4), 257–269.

Langley, D. J., Hoeve, M. C., Ortt, J. R., Pals, N., & van der Vecht, B. (2014). Patterns of herding and their occurrence in an online setting. *Journal of Interactive Marketing*, 28(1), 16–25.

Leeflang, P. S., Verhoef, P. C., Dahlström, P., & Freundt, T. (2014). Challenges and solutions for marketing in a digital era. *European Management Journal*, 32(1), 1–12.

Liu, B., Kim, H., & Pennington-Gray, L. (2015). Responding to the bed bug crisis in social media. *International Journal of Hospitality Management*, 47, 76–84.

Liu, B., Pennington-Gray, L., & Krieger, J. (2016). Tourism crisis management: Can the extended parallel process model be used to understand crisis responses in the cruise industry? *Tourism Management, 55*, 310–321.

Ludwig, S., De Ruyter, K., Friedman, M., Brügger, E. C., Wetzels, M., & Pfann, G. (2013). More than words: The influence of affective content and linguistic style matches in online reviews on conversion rates. *Journal of Marketing, 77*(1), 87–103.

Malthouse, E. C., Calder, B. J., Kim, S. J., & Vandenberg, M. (2016). Evidence that user-generated content that produces engagement increases purchase behaviours. *Journal of Marketing Management, 32*(5–6), 427–444.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257–266.

Marchiori, E., & Cantoni, L. (2015). The role of prior experience in the perception of a tourism destination in user-generated content. *Journal of Destination Marketing & Management, 4*(3), 194–201.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58.

Moro, S., Cortez, P., & Rita, P. (2015). Business intelligence in banking: A literature analysis from 2002 to 2013 using text

mining and latent Dirichlet allocation. *Expert Systems with Applications*, 42(3), 1314–1324.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, 52(1), 123–134.

Patel, V. K., Manley, S. C., Hair, J. F., Ferrell, O. C., & Pieper, T. M. (2016). Is stakeholder orientation relevant for European firms? *European Management Journal*, 34(6), 650–660.

Porter, M. F. (1980). An algorithm for suffix stripping. *Program*, 14(3), 130–137.

Presi, C., Saridakis, C., & Hartmans, S. (2014). User-generated content behaviour of the dissatisfied service customer. *European Journal of Marketing*, 48(9/10), 1600–1625.

PwC. (2016). Global State of Information Security Survey 2016. Retrieved from <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html> Accessed 14/02/2017

Rindova, V. P., & Fombrun, C. J. (1999). Constructing competitive advantage: The role of firm-constituent interactions. *Strategic Management Journal*, 20(8), 691–710.

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, 49, 146–154.

Salehi-Esfahani, S., Ravichandran, S., Israeli, A., & Bolden III, E. (2016). Investigating information adoption tendencies based on restaurants' user-generated content utilizing a modified

information adoption model. *Journal of Hospitality Marketing & Management*, 25(8), 925–953.

Sanger, D. E., Chan, S., & Scott, M. (2017, May 14). Ransomware's aftershocks feared as U.S. warns of complexity. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html> Accessed 8/06/2017

Sarmiento, M., Simões, C., & Farhangmehr, M. (2015). Applying a relationship marketing perspective to B2B trade fairs: The role of socialization episodes. *Industrial Marketing Management*, 44, 131–141.

Scandizzo, S. (2011). A framework for the analysis of reputational risk. *Journal of Operational Risk*, 6(3), 41–63.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314–341.

Shriver, S. K., Nair, H. S., & Hofstetter, R. (2013). Social ties and user-generated content: Evidence from an online social network. *Management Science*, 59(6), 1425–1443.

Stewart, D. W. (2017). A comment on privacy. *Journal of the Academy of Marketing Science*, 45(2), 156–159.

Sun, Y., Dong, X., & McIntyre, S. (2017). Motivation of user-generated content: Social connectedness moderates the effects of monetary rewards. *Marketing Science*. 36(3), 329–337.

Sung, M., & Hwang, J. S. (2014). Who drives a crisis? The diffusion of an issue through social networks. *Computers in Human Behavior*, 36, 246–257.

Taj, S. A. (2016). Application of signaling theory in management research: Addressing major gaps in theory. *European Management Journal*, 34(4), 338–348.

Tang, T. Y., Fang, E. E., & Wang, F. (2014). Is neutral really neutral? The effects of neutral user-generated content on product sales. *Journal of Marketing*, 78(4), 41–58.

Thakur, R., Summey, J. H., & John, J. (2013). A perceptual approach to understanding user-generated media behavior. *Journal of Consumer Marketing*, 30(1), 4–16.

Tirunillai, S., & Tellis, G. J. (2014). Mining marketing meaning from online chatter: Strategic brand analysis of big data using latent Dirichlet allocation. *Journal of Marketing Research*, 51(4), 463–479.

Van der Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing risk and resilience. *Academy of Management Journal*, 58(4), 971–980.

Vernuccio, M., & Ceccotti, F. (2015). Strategic and organisational challenges in the integrated marketing communication paradigm shift: A holistic vision. *European Management Journal*, 33(6), 438–449.

Walker, K. (2010). A systematic review of the corporate reputation literature: Definition, measurement, and theory. *Corporate Reputation Review*, 12(4), 357–387.

Walsh, G., & Beatty, S. E. (2007). Customer-based corporate reputation of a service firm: Scale development and validation. *Journal of the Academy of Marketing Science*, 35(1), 127–143.

Walsh, G., Mitchell, V. W., Jackson, P. R., & Beatty, S. E. (2009). Examining the antecedents and consequences of

corporate reputation: A customer perspective. *British Journal of Management*, 20(2), 187–203.

Wang, S., Wan, J., Zhang, D., Li, D., & Zhang, C. (2016). Towards smart factory for Industry 4.0: A self-organized multi-agent system with big data based feedback and coordination. *Computer Networks*, 101, 158–168.

Wedel, M., & Kannan, P. K. (2016). Marketing analytics for data-rich environments. *Journal of Marketing*, 80(6), 97–121.

Wepener, M., & Boshoff, C. (2015). An instrument to measure the customer-based corporate reputation of large service organizations. *Journal of Services Marketing*, 29(3), 163–172.

Zhang, X., & Venkatesh, V. (2013). Explaining employee job performance: The role of online and offline workplace communication networks. *MIS Quarterly*, 37(3), 695–722.

Zhang, Y., Moe, W. W., & Schweidel, D. A. (2017). Modeling the role of message content and influencers in social media rebroadcasting. *International Journal of Research in Marketing*, 34(1), 100–119.

## Appendices

### Appendix A. Sample demographic and organizational characteristics

Type of breach	Company	Date made public	Industry	
Intentional and internal	Hilton Hotels	25/09/2015	Accommodation and Food Services	
	Morgan Stanley	05/01/2015	Finance and Insurance	
	Federal Deposit Insurance Corporation	24/10/2015	Finance and Insurance	
	Capital One Financial Corp	04/03/2014	Finance and Insurance	
	AT&T Inc.	08/04/2015	Information Technology	
	Sage Group PLC	11/08/2016	Software & Services	
	Unintentional and internal	Bank of America Corp	17/07/2014	Finance and Insurance
		Goldman Sachs Group Inc.	02/07/2014	Finance and Insurance
		Highmark Inc.	05/06/2014	Finance and Insurance
		HSBC Holdings PLC	13/01/2016	Finance and Insurance
Aflac Inc.		20/05/2016	Finance and Insurance	
Humana Inc.		09/10/2015	Finance and Insurance	
Google Inc.		06/05/2016	Software & Services	
Toyota Motor Corp		26/08/2016	Manufacturing	
Cisco Systems Inc.		25/10/2016	Technology Hardware & Equipment	
Intentional and external		Starbucks Corp	12/05/2015	Accommodation and Food Services
	Walt Disney Co	30/07//2016	Arts, Entertainment and Recreation	
	American Express Co	07/04/2014	Finance and Insurance	
	Tesco Personal Finance PLC	06/11/2016	Finance and Insurance	
	Skype Inc.	01/01/2014	Software & Services	
	Yahoo	22/09/2016	Software & Services	
	LinkedIn Corp	17/05/2016	Software & Services	
	eBay Inc.	21/05/2014	Software & Services	
	TalkTalk Group PLC	24/10/2015	Information Technology	
	Dropbox	27/08/2016	Software & Services	
	American Apparel (USA) LLC	20/02/2015	Manufacturing	
	Coca-Cola Co	24/01/2014	Manufacturing	

Kickstarter PBC	15/02/2014	Public-benefit Corporation
Myspace Inc.	31/05/2016	Software & Services
Snap Inc.	04/03/2016	Software & Services
Ashley Madison	19/07/2015	Software & Services
Foursquare Labs Inc.	21/10/2016	Software & Services
Adult FriendFinder	22/05/2015	Software & Services
United Airlines, Inc.	01/01/2015	Transportation and Warehousing
Uber Technologies Inc.	27/02/2015	Software & Services

**Appendix B**

**ACCOMMODATION AND FOOD SERVICES**

<b>PRE-CRISIS</b>	<b>POST-CRISIS</b>	<b>Perceived quality</b>
Perceived quality		
Coffee		Best
Tea		Great
Drink		Difficult
Hot		Fast
Food		Product

**INFORMATION TECHNOLOGY**

<b>PRE-CRISIS</b>	<b>POST-CRISIS</b>	<b>Perceived quality</b>
Perceived quality	Firm as employer	Corporate performance
Shipping	Employer	Finance
USD	Employee	Revenue
Feature	Working	Analyst
Storage	Worker	Financial
Software	Staff	CEO
		Device
		Repair
		Safe
		Infect
		Critical

**MANUFACTURING**

<b>PRE-CRISIS</b>	<b>POST-CRISIS</b>	<b>Perceived quality</b>
Perceived quality		Corporate performance
Apparel		Bank
Cotton		Prevent
Jacket		Investor Management
Clothing		Wrong
Leather		Process
		Perform

**SOFTWARE & SERVICES**

<b>PRE-CRISIS</b>	<b>POST-CRISIS</b>	<b>Perceived quality</b>
Perceived quality		Corporate performance
Resume		Finance
Recruiter		Execute
Candidate		Dividend
Interview		Chief
Experience		Executive
		Innovation
		Quality
		Improvement
		Exclusive
		Safe

**ARTS, ENTERTAINMENT, AND RECREATION**

**PRE-CRISIS**

**Perceived quality**

Princess  
Movie  
Film  
Character  
Studio  
New

**POST-CRISIS**

**Perceived quality**

Portable  
Convenient  
Brand  
Duration  
Unlimited  
Special

**FINANCE AND INSURANCE**

**PRE-CRISIS**

**Corporate performance**

Merge  
Debit  
Obligation  
Chairman  
Merger

**Perceived quality**

Expensive  
Best  
Best  
Specific  
Digital

**POST-CRISIS**

**Corporate performance**

Financial  
Prevention  
Administration  
Disclose  
Corporate

**Perceived quality**

Vulnerable  
Cheapest  
Shock  
Cheaper  
Quality

**PUBLIC- BENEFITS CORPORATIONS**

**PRE-CRISIS**

**Perceived quality**

Amazing  
Project  
Fun  
Goal  
Idea

**POST-CRISIS**

**Perceived quality**

Super  
International  
Support  
Humanity  
Quality

**TRANSPORTATION AND WAREHOUSING**

**PRE-CRISIS**

**Perceived quality**

Comfort  
Transport  
Travel  
Airport  
Nationwide

**POST-CRISIS**

**Perceived quality**

Safety  
Cheap  
Inspection  
Maintenance  
Complaint

**TECHNOLOGY HARDWARE AND EQUIPMENT**

**PRE-CRISIS**

**Perceived quality**

**POST-CRISIS**

**Perceived quality**

Solution  
Server  
Network  
Infrastructure  
Engineer

Password  
Threat  
Cloud  
USD  
Ability

**Appendix C. Dynamics of the dimensions of reputation before and after a data breach in different industries**

Industry	Product and service quality		Customer orientation		Firm as employer		Financial performance		Social responsibility	
	PRE	POST	PRE	POST	PRE	POST	PRE	POST	PRE	POST
Accommodation and food services	✓	✓								
Arts, entertainment and recreation	✓	✓								
Public benefits corporations	✓	✓								
Transportation and warehousing	✓	✓								
Information technology	✓	✓				✓		✓		
Manufacturing	✓	✓						✓		
Technology hardware & equipment	✓	✓								
Software & services	✓	✓						✓		
Finance and insurance	✓	✓					✓	✓		

## **Conclusions**

Modern firms are characterised by an intensive use of IT. The literature has extensively explored the advantages of such a technological progress, but research on its possible drawbacks appears scant. An emergent threat firms must face is cyber risks, whose occurrences have led to significant breaches involving entire supply chains. In 2013, Target experienced a significant breach involving the theft of roughly 70 million customers' data and at least 40 million payment cards (Manworren et al., 2016; Shackelford, 2015; Shackelford, 2012). The first victim of the cyber attack was a link in Target's company chain, the HVAC vendor Fazio Mechanical Services. The attackers stole network credentials from Fazio and used them to enter the Target network and eventually steal massive amounts of data over several months.

Home Depot, another large retailer, experienced a credit card breach in 2014. The company declared it was not a breach in the first place and that the breach stemmed from a third-party vendor (Shackelford, 2015).

In 2015, the U.S. Office of Personnel Management (OPM) revealed a massive breach of 22 million records, including sensitive data tied to numerous federal employees, contractors and military personnel (Shackelford, 2015).

The consequences of these emergent risks seem dramatic, and the risk management domain and the SC literature have reckoned that cyber risks may cause business disruptions and damages to tangible and intangible corporate assets and have provided studies about how an effective cyber risk management process should be planned to prevent and manage these cyber risks.

However, the aforementioned studies are mainly theoretical and there is still a significant lack of empirical studies in the management literature measuring the potential effects of cyber threats within single companies and along networks of relationships in a wider SC perspective.

The present thesis aims to fill some of these gaps in three empirical essays.

Through the lens of the dynamic capabilities theory, the first studies the risk management practices of 15 European firms through the fsQCA method, which allows the researchers to ascertain how managers perceive cyber risks. The study confirms the IT literature with regard to requiring technical solutions but suggests they be integrated with relational and firmal capabilities, in line with the dynamic capability literature. Dynamic capabilities theory can help managers shape the firm of SC relationships in order to invest in shared resources, aligned decision-making, common objectives and the transversal adoption of risk management procedures, which might also include insurance, hedging and buffer inventories. Moreover, a managerial framework is built that suggests implementing both technical (e.g. software, insurance and investments in IT assets) and firmal (e.g. team work, human IT resources) capabilities to protect the company's ability to create value.

The second essay extends the investigation of the drawbacks of cyber risks to SCs. An empirical investigation of several European firms is performed, providing evidence that investments in SC mitigation strategies are scant and that firms comprising SCs behave as if they have a high risk appetite, whereas managers declare they have a low risk-taking approach. Moreover, a general lack of awareness emerges regarding the

effects that IT and cyber risks may have on supply operations and relationships.

Thus, a framework drawing upon SC risk management is proposed, offering a holistic risk management process in which strategies, processes, technologies and human resources are aligned and cohere with the governance of each firm and of the SC as a whole.

The third essay draws on the situational crisis communication theory (SCCT) to ascertain whether and how different types of cyber breaches differently affect corporate reputation, defined as a multidimensional construct in which the perceptions of customers, suppliers, (potential) employees, investors and local communities converge. This is among the first studies to analyse the different reputational drawbacks these types of risk may cause.

The literature categorises breaches into three groups: intentional and internal to the firm (e.g. malicious employees stealing customers' data); unintentional and internal to the firm (e.g. incorrect security settings that expose private information); and intentional and external to the firm (e.g. ransomware infecting companies' software).

Moreover, the study considers that, in the industry 4.0 era, social media analysis may be of paramount importance for firms to understand the market.

In fact, UGC might help in understanding which dimensions of the corporation have been more attacked after a data breach. In this context, the study implements the LDA automated method, a base model in the family of 'topic models', to extract the reputational dimensions expressed in UGC from a sample of 35 firms in nine industries that had data breach incidents between

2013 and 2016. The results reveal that, in general, after a data breach three dimensions – perceived quality, customer orientation and corporate performance – are subject to debate for users. However, if the data breach was intentional and malicious, users focus more on the role of firms' human resource management, whereas if users do not identify the company as responsible, they focus more on privacy drawbacks.

The study complements crisis communication research by categorizing stakeholders' perceptions of a crisis in a data breach context. In addition, the research is informative for risk management literature and reputation research by analysing corporate reputation dimensions in a data breach crisis setting.

Further research should analyse the connections between how firms have to manage the SC and big data such as UGC in a cyber risk framework. The academic research should provide methods and guidelines on how to triangulate market data, sales, social media, demographic and direct data inputs to predict the occurrence of a cyber threat. Studies might also focus on the roles the Internet of Things (IoT) and machine learning might have in providing real-time data to predict unplanned downtimes.

Moreover, the study of big data such as UGC throughout the SC might help prevent or manage reputation drawbacks. In this context, further investigation should shed light on whether companies should rely on external insurance companies to manage breaches in corporate reputation or whether companies should manage drawbacks in their image due to cyber risks through a reputation framework.

The aforementioned insights provide a glimpse into the numerous gaps in the academic literature. The analysis of big

data sources throughout the SC might be a key tool to run at the same pace with fast, silent and damaging threats, such as cyber risks.

## References

- Christopher, M. (2016). *Logistics & supply chain management*. Pearson UK.
- Davis, A. (2015). Building cyber-resilience into supply chains. *Technology Innovation Management Review*, 5(4), 19.
- Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal*, 50(1), 25-32.
- Ferrell, O. C. (2017). Broadening marketing's contribution to data privacy. *Journal of the Academy of Marketing Science*, 45(2), 160–163.
- Gatzert, N. (2015). The impact of corporate reputation and reputation damaging events on financial performance: Empirical evidence from the literature. *European Management Journal*, 33(6), 485–499.
- Gatzert, N., & Martin, M. (2015). Determinants and value of enterprise risk management: empirical evidence from the literature. *Risk Management and Insurance Review*, 18(1), 29-53.

- Gatzert, N., and Schmit, J. (2016). Supporting strategic success through enterprise-wide reputation risk management. *Journal of Risk Finance*, 17(1), 26–45.
- Khan, O., & Estay, D. A. S. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*, 5(4).
- Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, 59(3), 257-266.
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135-155.
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58.
- PWC, 2014 “Prioritising your investment” Retrieved from <https://www.pwc.com/sg/en/risk-assurance/assets/cyber-risk-sg-2014.pdf> Accessed 1/11/2017
- PWC, 2016 “Gaining from connectivity without losing trust” Retrieved from <https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2017/gx/trust.html> Accessed 5/09/2017
- Ragin, C. C., and Fiss, P. C. (2008). Net effects versus configurations: An empirical demonstration. In C. C. Ragin (Ed.), *Redesigning social inquiry: Fuzzy sets and beyond* (pp. 190–212). Chicago: University of Chicago Press.
- Ragin, C. C., and Pennings, P. (2005). Fuzzy sets and social research. *Sociological Methods and Research*, 33(4), 423–430.
- Rihoux, B. (2006). Qualitative comparative analysis (QCA) and related systematic comparative methods recent advances and remaining challenges for social science research. *International Sociology*, 21(5), 679–706.
- Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons*, 55(4), 349-356.
- Shackelford, D. (2015). Combatting cyber risks in the supply chain. SANS. org.
- Tirunillai, S., & Tellis, G. J. (2014). Mining marketing meaning from online chatter: Strategic brand analysis of big data using latent Dirichlet allocation. *Journal of Marketing Research*, 51(4), 463–479.
- Walsh, G., and Beatty, S. E. (2007). Customer-based corporate reputation of a service firm: Scale development and validation.

Journal of the Academy of Marketing Science, 35(1), 127–143.  
Walsh, G., Mitchell, V. W., Jackson, P. R., & Beatty, S. E.  
(2009). Examining the antecedents and consequences of

corporate reputation: A customer perspective. *British Journal of Management*, 20(2), 187-203.

Wepener, M., and Boshoff, C. (2015). An instrument to measure the customer-based corporate reputation of large service organizations. *Journal of Services Marketing*, 29(3), 163–172.

Zsidisin, G. (2003) “Managerial perceptions of risk”, *Journal of Supply Chain Management*, Vol. 39, pp. 14–25.

Zsidisin, G. A., Ellram, L. M., Carter, J. R., & Cavinato, J. L. (2004). An analysis of supply risk assessment techniques. *International Journal of Physical Distribution & Logistics Management*, 34(5), 397-413.

Zsidisin, G. A., Panelli, A., & Upton, R. (2000). Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study. *Supply Chain Management: An International Journal*, 5(4), 187-198.