Cybersecurity and Social Amplification of Risk in Financial Systems

Danilo Dias

Thesis to obtain the Master of Science Degree in

Information Security and Cyberspace Law

Supervisors: Dr. José Luís Brinquete Borbinha
Dr. Pedro Filipe Xavier Mendonça

Examination Committee

Chairperson: Dr. Carlos Manuel Costa Lourenço Caleiro
Supervisor: Dr. José Luís Brinquete Borbinha
Member of the Committee: Dr. Ricardo Jorge Fernandes Chaves

September 2021

Acknowledgements

I am profoundly grateful to Professor José Borbinha and Professor Pedro Mendonça for their support during this project. Their invaluable guidance was responsible for opening my mind to a range of research topics I was not familiar with. That was crucial to the realization of this work and my development as a researcher.

I would also like to thank Banco Central do Brasil for the financial support that made this research possible, and my co-workers for their encouragement.

Ultimately, I would like to dedicate the work done to my wife Simonne, my daughter Betina and my son Dante.

Abstract

Cyber risk is now considered a significant threat to financial stability since it is conceivable that a cyber incident could halt critical economic functions or cause an extreme loss of confidence in the financial system. Financial authorities should be prepared for a systemic crisis caused by a cyber source with appropriate risk management and effective methodologies for risk analysis. The prospect of reputational contagion events should be particularly considered since confidence in institutions is a crucial factor for the stability of financial systems. This work explores the hypothesis that the Social Amplification of Risk Framework and the Situational Crisis Communication Theory can be relevant foundations for a codebook to analyse cyber incidents that may generate a reputational contagion effect and trigger a systemic crisis. Directed content analysis is performed in a data corpus built from 148 news articles published by CNBC about the Equifax data breach announced in September 2017 and the Capital One data breach announced in July 2019. After a cross-case analysis, this work indicates some of the most relevant social amplification factors that may be responsible for sustained media coverage, the amplification of risk perception and the generation of secondary impacts and ripple effects. Finally, further research is suggested to link these factors to a potential systemic crisis.

Keywords: Crisis communication, cybersecurity, social amplification of risk, systemic risk, risk communication, risk perception.

Resumo

O risco cibernético tem sido considerado uma ameaça significativa à estabilidade financeira, pois é concebível que um incidente cibernético possa interromper funções econômicas críticas ou causar uma perda de confiança extrema no sistema financeiro. As autoridades financeiras devem estar preparadas para uma crise sistêmica causada por uma fonte cibernética com gestão de risco adequada e metodologias eficazes para análise de risco. A perspetiva de eventos de contágio de reputação deve ser especialmente considerada, uma vez que a confiança nas instituições é um fator crucial para a estabilidade dos sistemas financeiros. Este trabalho explora a hipótese de que o “Social Amplification of Risk Framework” e a “Situational Crisis Communication Theory” podem ser fundamentos relevantes para um livro de código para analisar incidentes cibernéticos que podem gerar um efeito de contágio de reputação e desencadear uma crise sistêmica. Uma análise de conteúdo dirigida é realizada em um corpus de dados construído a partir de 148 artigos de notícias publicados pela CNBC sobre as violações de dados que afetaram a Equifax e a Capital One, anunciadas em setembro de 2017 e julho de 2019, respetivamente. Após uma análise cruzada dos estudos de casos, este trabalho indica alguns dos fatores de amplificação social mais relevantes que podem ser responsáveis pela cobertura mediática sustentada, a amplificação da perceção de risco e a geração de impactos secundários e efeitos em cascata. Finalmente, sugere-se que novas pesquisas liguem esses fatores a uma potencial crise sistêmica.

Palavras-chave: Amplificação social do risco, cibersegurança, comunicação de crise, comunicação de risco, perceção de risco, risco sistêmico.

Index

List of figures

List of tables

List of acronyms

AWS	Amazon Web Services
CEO	Chief Executive Officer
CERC	Crisis & Emergency Risk Communication
CFPB	Consumer Financial Protection Bureau
CIISI-EU	Cyber Information and Intelligence Sharing Initiative – European Union
CNBC	Consumer News and Business Channel
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPMI	Committee on Payments and Market Infrastructures
CRI	Cyber Risk Institute
CROE	Cyber Resilience Oversight Expectations
EBA	European Banking Authority
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ERM	Enterprise Risk Management
ESRB	European Systemic Risk Board
EU	European Union
FBI	Federal Bureau of Investigation
FI-ISAC	Financial Institutes – Information Sharing and Analysis Centre
FS-ISAC	Financial Services Information Sharing and Analysis Center
FTC	Federal Trade Commission
G7	Group of Seven
G20	Group of Twenty
ICC	Integrated Crisis Communication
IDEA	Internalization, Distributions, Explanation, and Action
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
IRT	Image Restoration Theory
IT	Information Technology
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OFR	Office of Financial Research
SARF	Social Amplification of Risk Framework
SCCT	Situational Crisis Communication Theory
SIPA	School of International and Public Affairs at Columbia University
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIBER-EU	Threat Intelligence Based Ethical Red Teaming – European Union
US	United States of America

1 Introduction

The European Central Bank defines financial stability as “a condition in which the financial system – which comprises financial intermediaries, markets and market infrastructures – is capable of withstanding shocks and the unravelling of financial imbalances” (European Central Bank 2021). Additionally, the European Parliament and the Council (2010) defines systemic risk as “a risk of disruption in the financial system with the potential to have serious negative consequences for the internal market and the real economy”.

A stable financial system is critical to society since it performs several functions that are vital to the economy, such as intermediating payments and clearing, allocating credit, transferring risk, and providing liquidity. A significant deficiency in any of these core functions can cause serious consequences to the real economy. Therefore, financial authorities pursue the conservation of financial stability and the mitigation of systemic risk.

Traditional threats to financial stability include financial, reputational, and operational risks. More recently, there is a growing concern with cyber risk, since malicious actors have been using cyber capabilities to threaten financial institutions, investors, and the public, and it is conceivable that a cyber incident could evolve into a systemic crisis (European Systemic Risk Board 2020).

Recognizing that, researchers are looking for the links between cyber risk and financial stability. Studies identify several ways cybersecurity incidents could threaten financial stability, also known as transmission channels (European Systemic Risk Board 2020; Healey et al. 2021; Office of Financial Research 2017). Essentially, a cyber incident might cause a systemic crisis by disrupting vital financial functions (operational disruption effect) or triggering an extreme loss of confidence in the financial system (reputational contagion effect).

For some years, authorities and private entities have fostered initiatives to improve the cyber resilience of critical infrastructures and essential services of the financial services industry. Cybersecurity legislation, frameworks, guides, simulation exercises, and information-sharing are some of the efforts that have been made recently (Healey et al. 2018). These initiatives enable the continuous improvement of the financial sector’s cyber resilience, mitigating cyber risks, particularly those related to operational crises.

However, that might not be enough to manage the risk of widespread loss of confidence in financial systems caused by a cyber source. Traditional risk assessment strategies may not be suitable to analyse those risks, and a different approach must be considered.

This work aims to contribute to the advance of the state of the art of systemic risk research by exploring tools to analyse cyber risks that may generate a reputational contagion effect in the financial system and cause a systemic crisis.

The remainder of this chapter states the scope of this work, defines the research problem and questions, and then presents the research approach and a summary of results. The last session describes the structure of this document.

1.1 Scope

This work focuses on the financial services sector and is interested in systemic risk, which may be understood as a risk of disruption of an entire financial system, as opposed to breakdowns in individual financial institutions (Kaufman and Scott 2003).

Regarding the source of risk, this work is concerned with risks originated by cyber threats, which have specific characteristics that fundamentally differentiate cyber risk from other sources of risks – such as traditional financial or operational risk.

In that scope, this investigation focuses on the specific type of cyber incident that is a data breach - which happens when information is taken from a system without the authorization of the organization or person that owns the data -, and on the possibility that such an incident might generate a widespread loss of confidence in financial institutions.

In summary, the scope of this work embraces financial systemic risk originated by a cyber source through a data breach that might cause a reputational contagion effect in the financial system.

The next session defines the research problem.

1.2 Problem definition

Risk analysis can be defined as “a process to comprehend the nature of risk and to determine the level of risk” (International Organization for Standardization 2009), and typically consists of estimating the likelihood of events and the nature and magnitude of their consequences. This general approach is not appropriate to assess systemic risk, characterized by extremely unlikely risk events that have a huge impact on society, which renders the quantification of likelihood and consequence impractical.

Also, analysing cyber risks requires a comprehensive understanding of the cyber threat landscape, since there are fundamental differences from cyber to traditional risk (Bank for International Settlements and International Organization of Securities Commissions 2016; European Systemic Risk Board 2020; Healey et al. 2018).

Moreover, analysis of risks that potentially cause a widespread loss of confidence in the financial system brings unique challenges, since psychological, social, and cultural factors must also be considered to understand the spread of risk across society.

This work addresses these challenges by investigating techniques to analyse how cyber incidents can endanger financial stability by causing a widespread loss of confidence in the financial system.

The following session narrows the problem down to define the set of research questions that were the focus of this work.

1.3 Research questions

To analyse the risk of a reputational contagion event caused by a cyber source, it is critical to understand the factors that may amplify risk perception during a cyber crisis. One major aspect is the level of media

coverage. A high volume of news stories published by media outlets is correlated with the amplification of perceived risk, and so it is important to investigate which characteristics of the cyber event are related to sustained media coverage.

However, research shows that a high volume of information by itself does not necessarily amplify the audience's risk perception. Another key point is to understand what are the relevant social amplification factors concerning cyber incidents affecting financial institutions, including the qualitative properties of the risk event, the attributes of the information flow, and the social response mechanisms of society.

A third aspect to be studied is how the relevance of these social amplification factors changes over time, and what is their relation to the incidence of ripple effects that might generate a systemic crisis.

Finally, another research topic is the relation of the crisis communication strategies used by the affected institutions with the potential attenuation of perceived risk, and, as a result, of its consequences.

To address these research questions, a specific category of cyber events was selected: a data breach affecting a financial services institution.

Therefore, this work proposes the following research questions:

When a major data breach affects a financial services institution:

Research Question 1 (RQ1): Which risk event characteristics relate to sustained media coverage?

Research Question 2 (RQ2): What social amplification factors may be relevant concerning those risk events?

Research Question 3 (RQ3): How does the relevance of these social amplification factors and the incidence of ripple effects change over time?

Research Question 4 (RQ4): How do crisis communication strategies used by the affected institutions relate to the attenuation of perceived risk?

To support this investigation, two cyber events were chosen as case studies, as described in the next session.

1.4 Research approach

The Equifax data breach announced in September 2017 and the Capital One data breach announced in July 2019 are among the largest in history, affecting private information from more than one hundred million consumers each. These two cyber incidents were chosen as case studies since both affected financial services institutions with the same order of magnitude considering the number of affected individuals, but at the same time had significant differences in terms of media exposure and consequences to the affected companies.

The analysis was based on 131 articles about the Equifax cyber breach published between 7 September 2017 and 10 February 2020, and 17 articles about the Capital One breach published between 29 July 2019 and 17 December 2019, all retrieved from the CNBC website (Consumer News and Business Channel 2021).

A directed approach was used for content analysis (Hsieh and Shannon 2005). Therefore, existing literature and theory were used to create a structured codebook prior to the start of coding.

To develop the codebook, this work used the Social Amplification of Risk Framework (SARF) proposed by Kasperson et al. (1988) and the Situational Crisis Communication Theory (SCCT) proposed by Coombs and Holladay (2002). The coding system consisted of three main themes: social amplification factors, impacts, and crisis communication strategies. The coding of social amplification factors and impacts were based on SARF, while the coding of crisis communication strategies used SCCT.

Subsequently, this work analysed the sequence of episodes of each case study identifying and quantifying the relevant characteristics over time. Then, a cross-case analysis was performed, and the similarities and differences between the two risk events were discussed. As a result of this discussion, this work indicates some of the most relevant social amplification factors that may be responsible for sustained media coverage, the amplification of risk perception and the generation of secondary impacts and ripple effects.

The next session depicts a summary of this work's main results.

1.5 Summary of results

Based on the analysed data, this work found that the "dread risk" and "unknown risk" factors may be related to sustained media coverage of data breaches affecting financial services institutions. Other social amplification factors that seem to be relevant in this context are the extent of risk exposure, the volume of information, and social distrust of responsible institutions.

Moreover, the chronological analysis showed that although the absolute frequency of social amplification factors greatly reduces after 30 days, the same does not happen with the relative frequency, with some of the amplification factors increasing over time (for instance, the "dread risk" and "unknown risk" factors intensified in one of the case studies). This fact may promote the continuous generation of secondary impacts and ripple effects in the medium and long term.

Finally, analysis of the crisis communication strategies used by the affected companies showed that the "rebuild" strategy - commonly used when the organization is the main responsible for the incident - may not be enough to attenuate perceived risk, while the "diminish" strategy seems to be of importance in such events.

The next session displays the document structure.

1.6 Document structure

This document follows with exploring the fundamentals concepts of “risk management”, “financial system”, and “systemic risk” (Chapter 2). Then an analysis of recent research on cyber risk to financial stability is made, including studies on the context and assessment of systemic cyber risk, and a synthesis of measures that have been taken to treat this risk by public and private entities (Chapter 3). Furthermore, this work examines research dedicated to risk perception and the concept of social amplification of risk (Chapter 4) and discusses studies about risk and crisis communication (Chapter 5).

Chapter 6 describes the data analysis method used in this research, including the data collection, the codebook development, and the coding and analysis procedures. Chapters 7 and 8 report the analysis results of the two selected cases studies, with chronological analyses and the quantification of social amplification factors. In Chapter 9, this work discusses the results and answers the research questions.

Chapter 10 presents the conclusions, limitations, and suggestions for future work. Finally, the Bibliography is enumerated, and the Appendix portrays the list of the data corpus news articles and corresponding social amplification factors that were found during the content analysis.

2 Core concepts

To treat cyber risk to financial stability, it is crucial to comprehend “risk management” principles and available techniques. Moreover, management of this type of risk requires a clear understanding of the concepts of “financial system” and “systemic risk”. This chapter explores these topics.

2.1 Risk management

Risk management is part of everyday life. Every person is continually managing risks throughout hundreds of little decisions made each day. The same happens with enterprises. To achieve their objectives and make informed decisions, enterprises must manage risk, which may be defined as “the effect of uncertainty on objectives” (International Organization for Standardization 2018).

Many frameworks were developed to support effective risk management in enterprises. COSO ERM is one of the most known and motivated the proliferation of enterprise risk management frameworks, and ISO 31000 helped the development of the field, defining general principles and a process for risk management that can be used in any domain or application (Vieira 2016).

According to ISO31000:2018, an organization should initially establish the scope, the context, and risk criteria to implement a risk management process. Then, risks must be identified, analysed, and evaluated – the three stages of risk assessment -, so they can be properly treated under the organization’s objectives, risk criteria and available resources. Risk communication should be present throughout all these stages (International Organization for Standardization 2018).

For the remainder of this session, the main steps of a risk management process are examined.

Scope, context, and risk criteria

To customize the risk management process to the organization’s needs, the first step is to define the scope of the risk management activities. This includes the process’ objectives, outcomes, required resources, responsibilities, and specific inclusions and exclusions. The scope should also include what are the risk assessment tools and techniques that will be used when executing the process.

The next step is understanding the external and internal context in which the organization operates, and more specifically what is the environment of the risk management activity within the defined scope. That includes examining social, cultural, and political factors; key drivers and trends affecting the objectives of the organization; and stakeholders’ perceptions, values, needs and expectations.

Risk criteria should also be established at the beginning of the risk management process. The criteria to evaluate risks should consider the nature and types of risks; how consequences and likelihood will be defined and measured; consistency in the use of measurement; and how to determine the level of risk.

After establishing the risk management process scope, context, and risk criteria, the risk assessment and treatment processes may be conducted.

Risk assessment, treatment, and communication

The risk assessment process consists of the activities of risk identification, analysis, and evaluation. Risk identification is a process to find, recognize, and describe significant risks considering the established scope and context. To identify risk events, assessors must understand the threat landscape, the existing vulnerabilities, and the consequences of potential events on the organization's objectives.

During risk analysis, the nature of each identified risk and its characteristics should be comprehended, and, where appropriate, the level of risk may be estimated. Risk analysts usually determine the level of each risk as a function of its likelihood and consequence. Sometimes, these factors can be deduced mathematically based on past events. For example, the likelihood of an event might be inferred from the number of past events by year, and the consequences could be estimated from financial losses resultant from past occurrences.

Nevertheless, every so often there is not enough data to measure the level of risk based on past events. Therefore, it may not be possible to determine the likelihood and consequence quantitatively, and a qualitative approach must be taken. So, risk analysis usually depends on subjective evaluations based on the experience and expertise of relevant stakeholders. That is one of the reasons why understanding risk perception is crucial.

Risk perception may be defined as the "stakeholder's view on a risk", reflecting his or her "needs, issues, knowledge, belief and values" (International Organization for Standardization 2009). The stakeholders' perceptions must be considered not only in the risk analysis phase, but also when selecting risk treatment options, and even before, as part of understanding the external and internal context (International Organization for Standardization 2018).

High uncertainty of some risk events brings another layer of complexity to risk analysis. That is the case with very unlikely events of large magnitudes, such as those known as "black swan" events. Quantifying the likelihood and consequence of such events might be unfeasible, and other techniques and approaches may be needed.

Risk evaluation is the last step of risk assessment and serves to determine if any action is required, comparing the results of risk analysis with the established risk criteria. Some of the possible decisions are doing nothing, considering risk treatment options, and undertaking further analysis.

For each assessed risk, if the estimated level is higher than the organization's risk tolerance according to established criteria, risk treatment options must be selected and implemented. Possible options include avoiding the risk by interrupting the related activity, mitigating the risk to change its likelihood or consequence, sharing the risk with insurers, and accepting the risk by informed decision.

Another important activity of the risk management process is communication with external and internal stakeholders. Risk assessment should use the best available information, and for that effective communication with stakeholders is essential. Communication should be a two-way process where risk experts assist stakeholders in understanding risk, while stakeholders provide information and feedback that are useful to risk assessment and decision-making.

Risk communication should ensure that different views and perceptions are considered throughout different steps of the risk management process, bringing different areas of expertise together, and building a sense of inclusiveness among those affected by the risk.

In the next session, the concept of “financial systems” is examined.

2.2 Financial systems

Financial systems are described and analysed in different ways in the literature. One way to describe them is the institutional approach, which considers the financial system as the formal financial services sector, i.e., the set of institutions that provides financial services, such as banks, financial markets, insurance companies, investment and pension funds, and central banks.

The institutional approach lacks a comprehensive view of the functions a financial system should perform. The functional approach was developed as an alternative, where the financial system is described by the functions it provides. Six functions of the financial system are proposed by Merton and Bodie (1995):

- Clearing and settling payments
- Pooling resources and subdividing shares
- Transferring resources across time and space
- Managing risk
- Providing information
- Dealing with incentive problems

The functional approach presupposes those functions are separable, and since it abstracts institutional detail, in some cases it is not effective to analyse real financial systems where there are interrelationships between the different functions and complementarity between different institutions.

The systemic approach aspires to accomplish that and describes the financial system as a set of complementary elements or subsystems (Schmidt and Tyrell 2005). Examples of these elements are the role of banks and financial markets, the financing patterns and governance structure of corporations, the structure of the pension system, and parts of the legal system.

In line with the more comprehensive systemic approach, Schmidt and Tyrell (2005) propose a broad definition of the financial system: “the interaction between the supply of and the demand for the provision of capital and other finance-related services”. One important note is that this definition includes the demand side, such as households that accumulate wealth or firms which need capital for investing, even when they do not use the formal financial services sector.

By this definition, the financial system of a country includes:

- The formal financial services sector.
- The state, in its role of legislating, organizing, regulating, and supervising the financial sector.
- Households and other surplus units.

- Firms and other deficit units.
- The corporate governance system.

The broad definition of the financial system proposed by Schmidt and Tyrell (2005) may be appropriate when managing systemic risk, since vulnerabilities that may affect financial stability may be found outside the formal financial sector, especially if we consider the risk of a general loss of confidence in the financial system.

The next session examines the concept of systemic risk.

2.3 Systemic risk

Regarding the financial services sector, the systemic risk may be understood as the risk that affects the entire financial system, rather than just one or a few institutions (Bartholomew and Whalen 1995, as cited in Kaufman and Scott 2003). Systemic risk events may be originated by direct causation effects referred to as chain-reactions, or by indirect causation effects known as common-shocks.

A chain-reaction occurs when the failure of one participant of the financial system causes its creditors to default, and so on down the transmission chain (Bank for International Settlements 1994). It is considered a direct effect since the consequences derive from concrete capital and liquidity shortage caused by insolvent institutions that do not settle their commitments.

The common-shock or reassessment-shock effect happens when participants withdraw funds from - or refuse to lend to - institutions that have similar risk-exposure profiles to that of the initially affected unit. (Kaufman and Scott 2003). It is an indirect effect since solvent institutions are impacted for their potential of being subject to adverse effects from the same shock.

As the crisis advances, accurate information on the causes or the magnitude of the initial shock or the risk exposures of other institutions may not be readily available, rendering analysis of which units are at risk of insolvency challenging. At this stage, common-shock contagion may become indiscriminate, with a general loss of confidence in all institutions. This random contagion, based on actions by uninformed agents, is likely to be broader and more difficult to contain (Kaufman and Scott 2003).

Past systemic crises have mostly been triggered by participants of the financial system or by macroeconomic policy changes. Since specific triggers of systemic crises are hard to predict, financial stability analysts mainly focus on identifying and mitigating vulnerabilities and propagation mechanisms that make the system unstable in the first place (Healey et al. 2018).

Three main characteristics of financial systems are important when assessing risks to financial stability: leverage, maturity/risk transformation, and procyclicality of the price of risk. The risk of a systemic crisis is higher when the level of leverage, the degree of maturity transformation, and the price of risky assets are high (Healey et al. 2018).

To mitigate systemic risk, one commonly used measure is deposit insurance to prevent bank runs. Other relevant measures are specific requirements for banks, such as minimum capital ratios, minimum liquid asset holdings, and maximum leverage, such as those defined by the Third Basel Accord (Basel III) that

was developed after the 2007-2009 financial crisis. A process that is used to assess systemic risk is stress testing, where hypothetical adverse economic scenarios are tested on banks under the supervision of financial public authorities.

The next chapter examines the cyber risk to financial stability, which may be considered a special category of systemic risk that is originated by cyber threats.

3 Cyber risk to financial stability

Several studies have examined the possibility of a systemic crisis caused by a cyber source. This chapter summarizes recent research which indicates the context of systemic cyber risk and proposes assessment techniques. Then, current measures taken by public and private entities to treat cyber risk to financial stability are reviewed. Finally, based on the concepts and research presented so far, this work discusses strategies for the management of systemic cyber risk and points to the need for further investigation concerning reputational contagion events caused by cyber threats.

3.1 The context of systemic cyber risk

To manage cyber risk to financial stability, risk managers should understand its context. For that, it is important to recognise the differences between cyber risks and the traditional risks financial systems face, and the transmission channels by which cyber risks could be transmitted, potentially leading to financial crises.

Differences between cyber and traditional risks to financial stability

When analysing systemic cyber risk, it is important to understand the special characteristics of cyber threats. Healey et al. (2018) identify three main differences: timing, complexity, and adversary intent. The timing of cyber-attacks may be chosen by the adversary, while traditional financial crises' triggers usually occur at random. The complexity of cyberspace adds new challenges to risk analysts, with its interconnections not completely mapped or understood. Finally, a key difference is adversary intent, since cyber risks can be imposed and initiated by deliberate actions, which is not expected in traditional financial risks.

Bank for International Settlements and International Organization of Securities Commissions (2016) indicate other specific characteristics of cyber risk. The persistent nature of certain cyber-attack campaigns makes them difficult to identify or fully eradicate. There is a broad range of entry points through which institutions could be compromised, including clients, linked institutions, service providers, vendors, vendor products, and insiders. Besides, some risk management and business continuity arrangements are ineffective against certain types of cyber-attacks – e.g., data replication may fuel the propagation of malware and corrupted data.

European Systemic Risk Board (2020) highlights other key features that fundamentally differentiate cyber risk from other sources of operational risk: the speed and scale of its propagation. Furthermore, it is important to note that adversaries may use cyber capabilities not only to initiate a financial crisis but also to exacerbate one that is already in progress, and there is the possibility of slow-burn crises, when adversaries may cause long-term high impact with a sum of low-impact cyber-attacks – e.g., ransomware, distributed denial-of-service, or data leaks (Healey et al. 2018).

In short, the specific properties of cyber threats indicate the need for specialized analysis of cyber risks by financial stability risk managers. One important step is to identify the transmission channels.

Transmission channels

Transmission channels are the ways cybersecurity incidents could threaten financial stability. The US Department of the Treasury's Office of Financial Research (OFR) indicates what could be some of these transmission channels: (i) lack of substitutability, (ii) loss of confidence and (iii) loss of data integrity (Office of Financial Research 2017).

- Lack of (financial) substitutability: On financial systems, some key hubs perform a vital function for the entire industry, like interbank payments and the custody and exchange of securities. These functions are not easily substituted, and since they rely heavily on IT infrastructure, a major cyber incident on one of these key hubs can raise stability concerns.
- Loss of confidence: A wide range of attacks could trigger an extreme loss of confidence in financial systems, causing bank runs and potential financial instability. Examples are large-scale ATM hacks or account takeovers, takedowns of trusted institutions, hacker-induced flash-crashes, and releases of compromising messages from authorities or bankers.
- Loss of data integrity: Ransomware and other cyber-attacks can cause loss of financial data, slowing or even halting financial transactions and the flow of funds. In a report from 2020, the European Systemic Risk Board (ESRB) considered that the destruction or alteration of data related to value has the most potential for serious negative consequences for the real economy (European Systemic Risk Board 2020).

Expanding this work from OFR, the Project on Cyber Risk to Financial Stability of the School of International and Public Affairs at Columbia University (SIPA) identifies two additional transmission channels: lack of IT substitutability and interconnectedness (Healey et al. 2018, 2021).

- Lack of IT substitutability: Some IT companies concentrate a large portion of the world's computing and storage, and their failure could cause a huge impact on the operations of many firms including financial institutions. Also, a critical vulnerability on widely used software or network protocols may be used to cause harm to many firms at once, impacting the entire financial system.
- Interconnectedness: The fast technological advance of financial services makes the financial system and IT infrastructure further intertwined, and not all interconnections are easily identified or understood.

On another approach, the ESRB, in a 2020 report concerning systemic cyber risk, identifies three channels through which cyber-attacks could harm the real economy (European Systemic Risk Board 2020):

- Operational disruption channel: the severe disruption of critical economic functions by cyber threat actors.
- Operational contagion channel: the spread of disruption to other critical economic functions not initially targeted by the attackers.

- Reputational contagion channel: the loss of public and market confidence, triggering financial contagion channels, and resulting in a liquidity crisis or the insolvency of major financial institutions.

After establishing the context, systemic risk managers should define the tools and techniques for risk assessment. The next session examines research on the assessment of systemic cyber risk.

3.2 Systemic cyber risk assessment

The first step of risk assessment is the identification of potential risk events. Regarding cyber risk to financial stability, recent research has shed some light on the risk identification phase, with the proposal of two frameworks that may be used to identify cyber risk events with possible systemic effects, and the documentation of several generic risk scenarios that may be used as a basis of the identification process.

Frameworks to support the identification of systemic cyber risk

Some frameworks were proposed to link cyber risks to financial stability. Healey et al. (2021) propose an analytical framework to map cyber risks to the transmission channels through which incidents may affect financial stability, or to analyse a particular aspect of the financial system, identifying its major cyber risks. The framework also includes the assessment of the impact of amplifiers and dampeners on the system, such as new technologies like blockchain.

European Systemic Risk Board (2020) proposes a conceptual model – developed by ESRB's European Systemic Cyber Group - with four stages to assist in the identification of cyber incidents that may grow into a systemic crisis. The four stages are (i) context, (ii) shock, (iii) amplification, and (iv) systemic event. The context phase describes specific cyber risks in terms of threats, vulnerabilities, assets, countermeasures, and the starting point. In the shock phase, immediate consequences of the cyber risk are identified, using traditional business impact analysis. The amplification phase consists of identifying the interactions between the affected institution and other parts of the financial system, using the concept of amplifiers and contagion channels. Finally, the systemic event phase examines the point at which the system can no longer absorb the shock, using the concept of impact tolerance and absorptive capacity.

Cyber event scenarios

Some researchers have identified potential cyber event scenarios that may generate a systemic crisis in the future. Boer & Vazquez (2017) describe four types of scenarios that could have systemic repercussions, based on the transmission channels identified by the OFR: (i) attacks on financial market infrastructures, (ii) corruption of data, (iii) failure of wider infrastructure, and (iv) loss of confidence.

Kaffenberger & Kopp (2019) goes one step further and propose a list of actual and prospective future cyber risk scenarios that can be used by financial stability analysts, divided into three categories.

- High-impact operational risk scenarios: ransomware attack on a large bank, large wire transfer fraud, data breach on a rating agency, malware in trading systems, large-scale attacks on a global messaging network, and simultaneous attacks on systemically important institutions.
- Upstream infrastructure scenarios: disruptions to central clearing, disruptions to payment-processing gateways, massive malware infection on network routers, failure of a cloud provider, and disruptions on electricity or telecom utilities.
- External shock scenarios: sanctions retaliation via cyber-attacks and armed conflict.

European Systemic Risk Board (2020) stresses three hypothetical scenarios that could cause financial instability using its proposed framework: incapacitation of a large domestic bank's payment system, malicious destruction of account balance data, and scrambling of price and position data.

Identified risk events need to be analysed so they can be properly evaluated and compared to established risk criteria. For the remainder of this session, this work examines some of the challenges of systemic cyber risk analysis.

Systemic cyber risk analysis

Quantifying systemic risk events with a cyber source is not an easy task, since (Boer and Vazquez 2017; Kopp, Kaffenberger, and Wilson 2017; Office of Financial Research 2017):

- There is a lack of standardized and empirical data about cyber incidents.
- Financial firms may avoid reporting incidents due to reputation concerns.
- Unlike traditional financial risks, such as credit or market risk, cyber risk cannot easily be modelled, measured, or hedged based on past performance due to the evolving nature of cyber-attacks.
- Given individual firms' limited visibility and understanding of broader systemic effects, risk management in financial institutions has been focused on idiosyncratic risk.
- There is significant uncertainty surrounding the potential financial impact of cyber events, particularly indirect costs.
- Firms cannot reliably judge the risk to infrastructure the firm's operations rely on.

With the intent of supporting individual financial institutions on considering systemic cyber risk in their risk assessment process, Bouveret (2018) proposes a framework to estimate aggregate losses due to cyber risk that includes a contagion factor based on the probability that cyber-attacks may affect one or several firms.

Kaffenberger & Kopp (2019) propose a framework for assessing systemic financial risk on the national level. It is based on the country's: (i) cyber risk exposure (dependence on technology and degree of connectivity), (ii) cybersecurity preparedness, and (iii) resilience to financial shocks. To estimate each one of these indices, the authors use public data such as the share of the population that utilizes digital payments (cyber risk exposure), the Global Cybersecurity Index from the International Telecommunication Union (cybersecurity preparedness) and the banking system's regulatory capital buffers (shock resilience).

Healey et al. (2021) propose a model which gauges the severity of the risks by their consequence, vulnerability, probability, and outrage ("how upset it's likely to make people"), which ties to loss of confidence. The inclusion of an "outrage" metric draws attention to a factor that may be overlooked by many risk managers: the social, cultural, and psychological factors that may influence people's perception of risk events.

The next step after the assessment is risk treatment. Public and private entities have been taken actions to treat systemic cyber risks, such as cybersecurity regulation, guides and frameworks, information-sharing arrangements, and cybersecurity testing. Some of these measures are presented in the next session.

3.3 Systemic cyber risk treatment

A key measure to mitigate cyber risk to critical services is to promote the improvement of the cyber resilience of the organizations that provide those services. Recognizing that, in February 2013 the US White House issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (The White House 2013), which directed the development of a voluntary framework for reducing cyber risks to critical infrastructure. This framework was developed by the National Institute of Standards and Technology (NIST), with version 1.0 published in February 2014, and the current version (1.1) published in April 2018 (National Institute of Standards and Technology 2018).

In European Union (EU), a different approach has been chosen. The European Parliament and the Council have published a mandatory legislative framework, known as the NIS Directive (The European Parliament and the Council 2016a). This Directive became the foundation of the Member States cybersecurity frameworks, laws and strategies that have been developed since then. In 2020, a new proposal for a revised NIS 2 Directive was adopted by the European Commission (EC) to include new critical sectors, eliminate the distinction between operators of essential services and digital service providers, strengthen security requirements for the companies, and enhance the role of the Cooperation Group (European Commission 2020b).

Following the SWIFT Network cybersecurity incidents in 2016 (Reuters 2016), financial sector organizations have been adopting specific frameworks to address cyber risk – in distinction from the generic operational risk frameworks that were used before.

In June 2016 the Committee on Payments and Market Infrastructures (CPMI) of the Bank for International Settlements and the Board of the International Organization of Securities Commissions (IOSCO) published the "Guidance on cyber resilience for financial market infrastructures" (Bank for International Settlements and International Organization of Securities Commissions 2016). Even though it is specific to one sector of the financial services industry, its principles can be expanded to any critical

operator on the financial system. In October 2016 the Group of Seven (G7)[1] reached a consensus on a set of 8 key elements to be pursued by entities in the financial sector to reduce the risk of a significant impact caused by a cyber incident (Group of Seven 2016).

Following the publication of the CPMI/IOSCO Guidance and the G7 Elements, many other frameworks and guides were developed in the financial sector, such as the CROE (European Central Bank 2018a), the EBA Guidelines (European Banking Authority 2019), and the CRI Cyber Profile (Cyber Risk Institute 2020).

Meanwhile, financial public authorities from several countries published new regulations concerning cyber risk to the financial sector (World Bank Group 2020), and the Group of Twenty (G20)[2] requested the Financial Stability Board to perform a stocktake on cybersecurity regulations (Financial Stability Board 2017). The proliferation of national regulatory initiatives and supervisory approaches were considered suboptimal by the European Commission since cyber risks and financial systems have a cross-border nature, and the lack of coordination results in overlaps, inconsistencies, duplicative requirements, and high administrative and compliance costs. So, in 2020, the EC adopted a proposal for a new regulation on digital operational resilience for the financial sector to harmonise cyber resilience requirements for the EU financial entities (European Commission 2020a).

Additional measures to treat systemic cyber risk are cyber information-sharing and cybersecurity testing. Several information-sharing initiatives have been implemented in the financial sector, such as the US FS-ISAC, the European FI-ISAC, and the CIISI-EU (European Central Bank 2020; European Union Agency for Cybersecurity 2021; Financial Services Information Sharing and Analysis Center 2021).

Concerning cybersecurity testing, the G7 published a guide for financial entities and authorities (Group of Seven 2018), and the European Central Bank has developed the TIBER-EU framework to assist national monetary authorities to implement programs to test and improve resilience against sophisticated cyber-attacks targeting the financial sector (European Central Bank 2018b). Meanwhile, the US financial sector, including industry, government, and academy, has been performing exercises to improve the capacity of the service sector in responding to incidents with systemic impacts, such as the Quantum Dawn and the Hamilton series (Boer and Vazquez 2017).

Finally, recognizing that systemic cyber risk treatment should be coordinated at a global level, the Carnegie Endowment for International Peace published the “International Strategy to Better Protect the Financial System Against Cyber Threats” with recommendations to global leaders on how the international community could better protect the financial system against cyber threats (Maurer and Nelson 2020). The Strategy’s priority areas include clarifying roles and responsibilities, strengthening

[1] The Group of Seven (G7) is an international intergovernmental economic organization consisting of the seven major developed countries: Germany, Canada, the United States, France, Italy, Japan and the United Kingdom.

[2] The Group of Twenty (G20) is an intergovernmental forum comprising 19 countries and the European Union which addresses major issues related to the global economy, such as international financial stability.

the collective defence and response of the financial sector, reinforcing international norms to clarify what is inappropriate behaviour from nation-states, and building the cybersecurity workforce.

Based on the core concepts and research presented so far, the next session discusses strategies to manage systemic cyber risk.

3.4 Discussion

Traditional systemic risk events are usually originated by chain-reactions – a direct effect – or common-shocks – an indirect effect -, as mentioned in Session 2.3. Likewise, potential systemic cyber risk events may be categorized into two major groups:

- Operational disruption events (direct effect): A cyber incident disrupts vital financial functions that are not easily substituted, causing a prolonged interruption of financial transactions and flow of funds, resulting in a chain-reaction systemic crisis.
- Reputational contagion events (indirect effect): A cyber incident triggers an extreme loss of confidence in the financial system, causing a common-shock systemic event, resulting in credit shortage, liquidity crunch, or bank runs.

The purpose of this proposed categorization scheme is to split the risk management problem in two since they need different approaches: (i) how to manage the risk of disruption of critical financial functions that are not easily substitutable, and (ii) how to manage the risk of a general loss of confidence in the financial system.

When addressing the risk of systemic operational disruption, financial stability risk managers should use a combination of strategies from financial systemic risk management, operational risk management, and cyber risk management. To support the risk identification process, it is possible to use the transmission channels documented by the OFR and SIPA (see Session 3.1), the frameworks proposed by European Systemic Risk Board (2020) or Healey et al. (2021), and the cyber event scenarios suggested by Kaffenberger and Kopp (2019) (see Session 3.2).

In the risk analysis phase, financial stress tests may be used to measure financial resilience and adequacy of capital and liquidity buffers considering the identified cyber event scenarios. The specific characteristics of cyber risk should be taken into account, since, for example, disruptions may occur at many institutions simultaneously, and be triggered at the worst time possible (see Session 3.1). Besides financial stress tests, cyber scenario-based exercises may be useful to comprehend the identified risk events and uncover resilience gaps, especially if the exercises are public-private and sector-wide (see Session 3.3).

Some of the potential risk treatment actions that should be considered are implementing new resilience schemes to not substitutable financial functions or IT infrastructure, improving the cyber resilience of critical institutions and service providers, and enabling cyber information-sharing and cooperation among the sector's participants (see Session 3.3).

Nevertheless, this work argues that the risk of a general loss of confidence in the financial system caused by a reputational contagion effect must be addressed differently, and possibly in a separate risk management process, since the scope, the context, risk criteria, and risk assessment techniques and tools should not be the same.

Beginning with the scope establishment, the definition of what is the financial system might not be necessarily the same in both processes. While in operational disruption risk management a narrower view of the financial system as a set of its institutions or functions may be sufficient, when we consider reputational contagion a more comprehensive definition of the financial system is necessary, such as the one proposed by Schmidt and Tyrell (2005). It follows that the risk management process scope should include not only the institutions that provide financial services, but also the state, households, and firms (see Section 2.2).

Moreover, it is not sufficient to include in the scope just the IT systems and infrastructure that are relevant to the financial sector. Traditional and social media companies, as well as cyber experts, opinion leaders and public officials, are examples of possible relevant actors that should be considered when identifying and analysing reputational contagion events.

Risk criteria and assessment tools must be carefully specified considering the specific characteristics of systemic reputational risk. In that matter, risk perception plays a central role. It is crucial to understand how employees and clients of the financial system would perceive a cyber risk event affecting the financial sector, to project possible reactions that might cause a systemic crisis.

Finally, when considering risk treatment options, risk and crisis communication is a central aspect, since the reaction of the financial system participants to a cyber risk event may be amplified by the lack of reliable information about which institutions may be affected and what is the absorptive capacity of the financial sector to that kind of risk. This becomes even more critical since it is common in cyber event scenarios that even the directly affected institutions do not know the cause, extent, and time to recover from the incident before a thorough investigation that may take a long time.

Table 1 summarizes some of the distinctions between the operational and reputational systemic cyber risk management processes.

Table 1 - Differences between operational and reputational systemic cyber risk management

Risk management phase	**Operational disruption event**	**Reputational contagion event**
Scope	The financial system may be defined as the set of its institutions or functions Critical IT systems and providers must be mapped	The financial system should also include the state, households, and firms Traditional and social media companies, cyber experts, opinion leaders, and public officials should be considered
Assessment	Financial stress tests and cyber scenario-based exercises	Techniques should include risk perception analysis tools
Treatment	Improving cyber resilience and information-sharing	Focus on risk and crisis communication plans

In summary, although there are many studies concerning the management of systemic cyber risk, and many measures have been implemented to mitigate operational disruption events, the tools and techniques for managing the risk of a widespread loss of confidence in the financial system caused by a cyber incident require further investigation, and the risk perception and communication research fields should be explored.

In the next chapter, research on the topic of risk perception is examined, including the concept of social amplification of risk, which may be used to understand the risk of a reputational contagion event in the financial system.

4 Risk perception and social amplification of risk

Earlier studies on risk perception found that there were significant biases in people's perceptions of risks. For example, comparing actual mortality rates for familiar causes of death with people's perceived mortality rates, there was an overestimation of well-publicized causes of death – such as botulism, tornadoes, and floods – and underestimation of chronic causes of death. Other characteristics that affected people's risk perception were if the hazard was catastrophic, new, or involuntary. One evidence of people's misperception of risks was that most drivers considered themselves to be safer than average, which means they probably underestimated the risk of car accidents when they were driving (Fischhoff et al. 1978).

Based on these conclusions, researchers hypothesized that psychological, social, or cultural factors affect people's judgments of the level of risk, and several lines of research emerged. This chapter examines the risk perception research field and the concept of social amplification of risk. Subsequently, the relations between these studies and systemic cyber risk are discussed.

4.1 Risk perception research

Concerning the study of risk perception, psychologists proposed the psychometric paradigm and used decision theory to explain the ways psychology and cognitive processes affect risk perception. Sociologists examined how social context and culture shape perceptions and cognition, and aspects such as the impact of social trust and cultural values were evaluated. Several studies focused on the portrayal of risk information by the media and how it affects the interpretation and response to risk by society. This session explores some of these risk perception studies.

The psychometric paradigm

The psychometric paradigm is a method to measure risks perceptions using numerical rating scales (Slovic 2016). Within the psychometric paradigm, people make quantitative judgments about the level of risk of various hazards. These judgments are compared with judgments about other properties of the risk, such as voluntariness, dread, controllability, benefits, and catastrophic potential (Slovic and Weber 2013).

Slovic and Weber (2002) indicate fifteen risk characteristics, condensed into two higher-order factors: the "dread risk" factor and the "unknown risk" factor.

The "dread risk" factor is related to the properties of risk events that may arouse fear in individuals and society. It is derived from ten risk characteristics:

- Catastrophic: Hazards that kill many people at once – such as terrorist attacks – are perceived as more dangerous than risks that kill one or few people at a time – like heart diseases or car accidents.
- Consequences fatal: When exposure to the risk causes a fatality, risk perception is higher.
- Dread: If the effects of the risk are more frightening, risk perception increases.

- Global catastrophic: A risk that affects several nations is perceived as higher than a local risk.
- High risk to future generations: If the risk has consequences to future generations, risk perception increases.
- Increasing over time: If the risk increases over time, perceived risk is higher.
- Involuntary: People usually underestimate risks if they are voluntary. Extreme sports like skiing and scuba diving are perceived as less risky since practising them is a choice and not an obligation.
- Not easily reduced: Risks that are difficult to mitigate are perceived as more dangerous.
- Not equitable: If risks and benefits are not equally distributed across society, perceived risk is higher.
- Uncontrollable: The risk is perceived as higher if the person has no control over it. That is why many people find it safer to travel by car than by aeroplane, even with the mortality numbers saying otherwise.

The “unknown risk” factor relates to characteristics that indicate uncertainty, and is composed of five risk properties:

- Has a delayed effect: The delay effect refers to the latency between the event and its consequences. Risks with delay effect tend to be perceived as higher.
- New: Risks that are new to society are perceived as higher than known risks.
- Not observable: Risks whose effect of exposure cannot be observed are perceived as higher.
- Unknown to experts: If experts do not have sufficient knowledge about the risk, risk perception increases.
- Unknown to those exposed: If a person does not know if he or she has been exposed, the risk is considered more dangerous.

Risks with high “dread risk” and “unknown risk” factors hold a high “signal value”, which serves as a warning signal for society and might be linked to the potential for second-order effects (Slovic, Lichtenstein, and Fischhoff 1984). A third relevant factor that may increase the signal value of the risk and affect risk perception is the event’s extent of exposure. Renn et al. (1992) compared 128 hazard events and found that the extent of exposure to the direct consequences of a hazard has more effect on risk perceptions and social mobilization than do actual harm.

At least one study investigated the influence of psychological factors on a potential systemic crisis caused by bank runs. Jonsson and Söderberg (2016) concluded that the following psychometric variables explain the perceived risk of personal economic collapse during a bank crisis: new risk, global catastrophic, increasing over time, and uncontrollable.

Cyber risk was also investigated in relation to psychometric variables by Van Schaik et al. (2017), which states that voluntariness, immediacy, catastrophic potential, dread, the severity of consequences, and control are significant predictors of perceived risk related to 16 security hazards on the Internet - such as identity theft, keylogger, cyber-bullying, and social engineering.

Social trust

Social factors also contribute to perceived risk, and one relevant aspect is social trust. Trust can be strongly correlated with risk perception in certain situations, especially when the lay public has limited knowledge about the risk. In that case, trust may be used as a substitute for knowledge, i.e., lay people may trust the industry, governmental agencies, or other common people to perceive benefits and risks. Therefore, the influence of trust in risk perception depends on whether or not people are convinced they have sufficient knowledge to assess the risk (Siegrist 2021). For instance, Freudenburg (1993), as cited in Siegrist (2021), studied trust of institutions responsible for nuclear waste risk management and concluded that the trust variable explains public concern at a greater level than do sociodemographic and ideological variables.

Trust is many times considered as multidimensional. Renn and Levine (1991), as cited in Kasperson et al. (2003), list five attributes of trust: competence (technical expertise), objectivity (free from bias), fairness (acknowledgement of different points of view), consistency, and faith (good will). The social-psychological literature indicates two major dimensions as being important in determining trust: competence and honesty (Frewer 2003).

Some studies addressed the effect of social trust in triggering systemic crises. Jonsson and Söderberg (2016) concluded that a lower level of confidence in an individual's bank leads to a higher perception of the risk of personal economic collapse, which could be a trigger of bank runs. Kaszowska and Santos (2014) argue that a higher "systemic risk perception" – which relates to the confidence in financial institutions' solvency - increases the vulnerability of the financial system to external shocks.

Media research

The way media portrays risk events are also the subject of several studies in the risk perception research field. Combs and Slovic (1978), as cited in Kasperson et al. (2003), analysed two US newspapers for their reporting of causes of death, and concludes that some of them, such as homicides and accidents, received more media coverage than others, such as diseases. The authors also indicate some correlation between media exposure and lay public judgments concerning the frequency of these causes of death. Other studies also indicate that the extension of media exposure intrinsically influenced people perceptions of the seriousness of the events and the political agenda (Mazur 1984, as cited in Kasperson et al. 2003).

However, other studies indicate that volume of information is only one of many influences on public perceptions of risk, so heavy and sustained media coverage does not necessarily amplify risk perception or cause significant secondary effects, but other factors need to be present in combination (Renn 1991; Xu et al. 2021).

Media studies also investigate changes in the coverage of risk events over time. Kasperson and Kasperson (2012), for instance, analysed news articles related to a proposed nuclear waste repository at Yucca Mountain in the United States of America. They indicated that the amount, duration, and character of media coverage may influence public perceptions about the risk and that there was a shift in discourse over time, with a growing depiction of victimization, distrust, unfairness, and villainy.

Concerning cyber risk, Xu et al. (2021) examined Chinese media news related to cyber events from 2009 to 2018 and concluded that news sentiment – motivated through sensationalism, dramatization, or media framing -, instead of news amount, influences societal cyber risk perception.

The next session examines the concept of social amplification of risk, which seeks to unify studies from various risk perception research fields, including the psychometric paradigm, social trust, and media research.

4.2 Social amplification of risk

The social amplification of risk concept was introduced by researchers from Clark University and Decision Research (Kasperson et al. 1988). They proposed a framework (SARF) that serves to describe how minor risk events sometimes produce massive public reactions, with substantial social and economic impacts (risk amplification), and how hazards that experts judge as serious occasionally receive little attention from society (risk attenuation). SARF accounts for findings from various fields of risk perception and risk communication research, including media research, psychometric and cultural schools of risk perception research, and studies of organizational response to risk.

The starting point is the assumption that risk events will be irrelevant or localized in their impact unless human beings observe and communicate them to others (Luhmann 1979, as cited in Kasperson et al. 2003). SARF holds that, as part of this communication process, risk events are portrayed through risk signals (images, signs, and symbols) that are generated, transmitted, received, and interpreted by social agents. In that process, these risk signals are transformed by social or individual amplification stations, such as scientists, reporters, mass media, politicians, government agencies, or other social groups.

The amplification stations may increase or decrease the volume of information, highlight certain aspects of a message, or reinterpret the symbols and images, which leads to particular interpretations and responses by other participants in the social system. Cultural biases and values of an organization or group, and individual psychological factors – such as risk heuristics, qualitative aspects of risks, prior attitudes, blame, and trust – influence the amplification or attenuation of risk signals.

Moreover, Kasperson et al. (1988) argue that some events will produce ripple effects, i.e., secondary and tertiary consequences, spreading risk far beyond the initial impact. Some of the possible secondary impacts are regulatory constraints, litigation, loss of credibility and trust, and stigmatization of a product, technology, facility, or community. Also, the risk may spread from directly affected victims to other sectors, geographic locations, or even future generations. Traditional risk analyses are not able to estimate this kind of adverse effect and thereby underestimate the overall risk from the event. The concept of social amplification of risk provides a corrective mechanism.

The framework's components are presented in Figure 1. The first components are the risk events' characteristics and properties that may influence the perception of risk by society. The two following components are the major stages of risk amplification: the risk information flow and the interpretation and response to risk by society and individuals. Lastly, there are the secondary impacts and ripple effects that are consequences of the social amplification of risk.

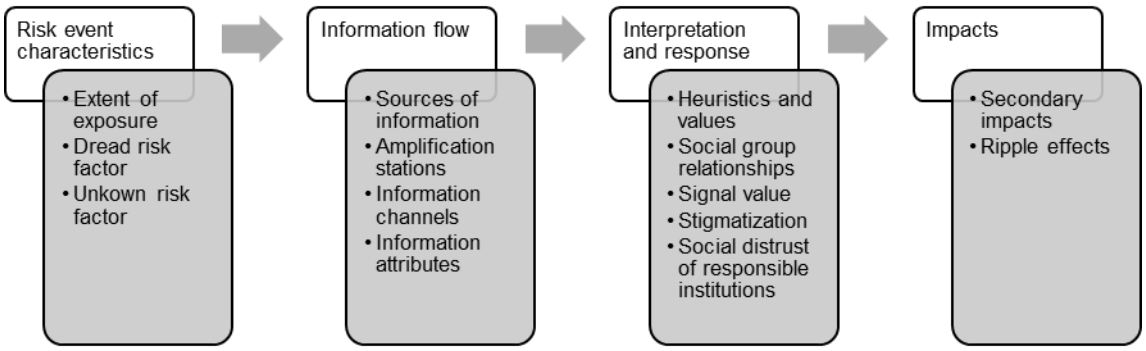


Figure 1 – SARF's components

Risk event characteristics

The risk event may be described by characteristics that may influence risk perception, including the extent of risk exposure – i.e., the number of people exposed to the direct consequences of the risk - and the qualitative properties of risk, which can be grouped into two main factors: the "dread risk" factor and the "unknown risk" factor, as explained in the psychometric paradigm research (see Session 4.1).

Information flow

Amplification and attenuation occur at different stages of the risk information flow. It begins with the portrayal of the event as a risk signal by a source of information, which could be communicated by a third-party or direct personal experience. The credibility of the communicating third-party affects risk perception, increasing or decreasing risk. If the risk signal arises through personal experience, previous knowledge, and familiarity of the individuals with the risk, among other factors, will shape how it is perceived.

After the initial risk communication, many social and individual amplification stations process the risk signals and communicate them to others. Examples of stations are the scientists or organizations who conduct and communicate the technical assessment of the risk, a risk-management institution, the news media, activist social organizations, opinion leaders within social groups, personal networks, politicians, and public agencies. Social stations are influenced by institutional structure, functions, and culture, while individual stations are affected by risk heuristics, qualitative aspects of risk, prior attitudes, blame, and trust.

Risk information is transferred through information channels, such as traditional media, social media, social groups, or direct conversations. Traditional media tend to give disproportionate coverage to rare or dramatic risks, which may affect the audience's risk perception. Social group interaction tends to integrate interpretations of risks into larger frames of values, producing resistance to new, conflicting information.

Finally, some of the information attributes that may amplify, or attenuate risk are:

- A large volume of information, such as massive media coverage.
- How controversial or disputed the information is.
- The dramatization of information, such as sensational headlines.
- The use of terms and concepts with symbolic connotations – e.g., the term “nuclear power” may entail past nuclear reactor accidents or even nuclear bombs.

Interpretation and response

Risk information is received by social agents, who interpret and respond to risk. Kasperson et al. (1988) hypothesize about the steps taken by risk message recipients. The process starts with filtering, decoding, and processing the information, possibly with the use of cognitive heuristics for drawing inferences. The following steps are attaching social values to information, interacting with one’s cultural and peer groups, formulating behavioural intentions to take actions against or tolerate the risk, and engaging in group or individual actions to accept, ignore, tolerate, or change the risk.

There are at least five major pathways to initiate response mechanisms (Kasperson et al. 1988, 2003):

- Heuristics and values, which refer to simplifying mechanisms to evaluate risk used by individuals, and to individual and group values that will determine which risks are important and what actions should be taken.
- Social group relationships, with groups influencing member responses and creating resistance to conflicting information.
- Signal value, which refers to properties of the risk event, such as dread and newness, that may influence risk perception.
- Stigmatization, referring to preconceived negative imagery of technology, environments, and companies, among others.
- Social distrust of responsible institutions and their managers caused, for example, by failures in risk management, lack of openness and transparency, failure to involve affected persons or lack of responsiveness to public concerns.

Impacts

The previous processes will then spawn institutional and social behaviour responses, such as political action, attitude changes, organizational responses, and social protest. These responses may result in secondary impacts and ripple effects.

Some of the possible secondary impacts are enduring mental perceptions, images, and attitudes, local impacts on economy, political and social pressure, changes in the physical nature of the risk, social disorder, regulation changes, increased liability and insurance costs, and repercussions on other technologies and social institutions.

These secondary impacts are perceived by social groups and individuals and may produce third-order ripple effects, which might be sectoral (the impact spreads from direct victims to companies, and then

to the whole industry), geographical (from a region to the whole country and then to other parts of the globe), and temporal (from present to future generations).

The next session relates risk perception and social amplification studies with systemic cyber risk.

4.3 Discussion

A systemic crisis caused by a reputational contagion event is a textbook case of the social amplification of risk concept. An event with a limited initial impact may turn into a serious crisis because participants of the financial system perceive the risk as greater than it is and start withdrawing funds from – or stop lending to – institutions that are not affected in the first place. This is true for any common-shock contagion scenario (see Session 2.3), but the cyber risk has specific characteristics that make crisis response even harder (see Session 3.1).

The main origin of a reputational contagion effect is the uncertainty caused by the lack of reliable information: participants of the financial system do not have enough data to estimate the likelihood of other institutions being affected by the same shock. In a serious cyber incident, it is usually not possible to immediately diagnose the real extension of the damage and to provide a good estimation of consequences, even for IT and cybersecurity experts working at the affected institutions.

Moreover, if it is believed that the initial incident was caused by a cyber-attack, participants may fear that other institutions have the same vulnerabilities and will soon be targeted by the attacker. The possibility of cyber warfare and the involvement of other nations add another layer of apprehension.

SARF's components are useful to understand how the initial event may become a systemic crisis (see Session 4.2). Characteristics of the risk event such as newness, dread, and extent of risk exposure may psychologically affect people's risk perception (see Session 4.1). A potential decrease of social trust of financial services institutions and public agencies is an additional challenge (see Session 4.1). The expected controversy among experts about risk consequences, the proliferation of rumours in personal networks, and the volume and dramatization of information in traditional and social media are other aspects worth considering (see Session 4.2).

It is possible to link some of the specific characteristics of cyber risk outlined in Session 3.1 with social amplification factors (Table 2). That is a plausible indication that major cyber incidents will be perceived as holding a high signal value risk by society.

Table 2 - Links between characteristics of cyber risk and social amplification factors

Cyber risk characteristic	**Social amplification factor**
Timing	Effect delayed
Complexity	Unknown to experts
Adversary intent	Not easily reduced
Persistent nature	Not observable
Speed of propagation	Increasing over time
Scale of propagation	Extent of risk exposure Global catastrophic

In short, financial stability risk managers should address risk perception factors to appropriately understand and analyse the risk of a reputational contagion event in the financial system caused by a cyber event, and this work argues that SARF may be a relevant tool to support risk analysts in accomplishing this task.

When considering systemic reputational risk treatment options, two important research fields are risk and crisis communication. The next chapter examines these topics.

5 Risk and crisis communication

Risk and crisis communication are two processes that comprise the exchange of messages with stakeholders to prevent or mitigate negative consequences from risks and crises. Considering public health as an example, campaigns to reduce smoking or increase road safety behaviours are considered risk communication, while the exchange of information about a current pandemic is crisis communication.

Risk and crisis communication processes intersect at a variety of points, but there are some fundamental differences (Reynolds and Seeger 2005). Risk communication is usually based on messages that seek behavioural change from the audience through the sending of frequent or routine information about a threat based on what is currently known. Messages are usually prepared long-term by technical experts or scientists, in a controlled and structured way, and are mainly persuasive.

In contrast, crisis communication seeks to explain a specific event with information about its current state, magnitude, remediation actions, cause, blame, and consequences. Messages are mainly informative, based on what is known and what is not known, spontaneous and reactive. The message preparation is short-termed and prepared not only by experts but also by authority figures.

This chapter examines the concepts of risk and crisis communication and presents some of the communication models and frameworks proposed in this research field. Finally, this topic is discussed in relation to systemic cyber risk.

5.1 Risk communication

Risk communication may be defined as the exchange of information about risks among risk assessors, risk managers, news media, interested groups, and the public (Muralikrishna and Manickam 2017, as cited in ScienceDirect 2021).

The way risk events are communicated affects the perception of risk by individuals and society and therefore is critical to the consequences of risk itself. In that matter, media outlets play an essential role, since they may shape the discourse of other actors - such as responsible institutions, public authorities, and experts - and many individuals will interpret and respond to the risk considering the information published on media channels.

Therefore, the risk communication research field has been largely influenced by risk perception studies, through the evolving understanding of risk from an “objective” and “determined by experts” perspective to a “subjective” and “perceived by laypeople” viewpoint (Balog-Way, McComas, and Besley 2020).

Financial authorities address systemic risk communication with ongoing financial stability-related messages, such as the publication of Financial Stability Reports and related speeches and interviews (Born, Ehrmann, and Fratzscher 2014). Meanwhile, cybersecurity authorities communicate cyber risk with the release of regular reports to inform the public and the companies about the most prominent cyber threats (Cybersecurity and Infrastructure Security Agency 2021; European Union Agency for Cybersecurity 2020; National Cyber Security Centre 2021).

Notably, these two types of risk communication use opposite strategies since financial authorities usually seek to reassure the financial system participants (“the system is secure”), while cybersecurity authorities aim to increase public awareness (“the threats have to be taken seriously”).

Crisis communication is also based on distinct strategies depending on the type of the crisis and who is responsible to manage it. The next session addresses this topic.

5.2 Crisis communication

There are at least two important research fields concerning crisis communication. One is crisis communication related to public hazards – such as natural disasters, public health emergencies, and financial systemic crises – which is mainly executed by public agencies and the government. The other is related to crisis management in individual organizations when response strategies are usually focused on reducing reputational damage.

Public hazards communication models

Public hazards crisis communication aims to inform the lay public about the risk and convince them to take action when appropriate. Depending on the level of the risk, communicators may seek to amplify risk perception of the public – e.g., when a natural disaster imposes evacuation of an area -, or, in contrast, to reduce anxiety, if the consequences of the risk are controlled and people’s actions might worsen the crisis.

Two main types of models for public hazards communication are found in the literature. The first type focuses on risk messages development. The Hazards Risk Communication Framework (Blanchard-Boehm 1998), for instance, defines a sequential process in which individuals that receive a risk message go through five stages: hearing, understanding, believing, confirming, and responding. These behavioural variables depend on characteristics of the message – content, style, channels, frequency, and traits of the source – and the receiver – physical and social environment, social attributes, and individual attributes.

Smillie and Blissett (2010) propose a model that consists of three main stages: (i) risk appraisal; (ii) situational analysis; and (iii) source analysis. Risk appraisal is an objective overview of the risk and its characteristics, including scientific facts about the risk, affected individuals and companies, perception attributes such as voluntariness and stigma, and social amplification factors based on SARF. Situation analysis is the definition of the likely perceived risk based on history, political and media environments, and characteristics of the public. Finally, source analysis refers to the self-analysis of the communicator, including trust issues, available tools, among others.

The IDEA model (Sellnow et al. 2017) consists of four elements - Internalization, Distribution, Explanation, and Action – and argues that risk messages are more effective if they include not only information about the risk, but also elements of personal relevance and actionable directions, appealing to affective and cognitive learning as a way to achieve desired behaviours.

The other type of public hazards communication model targets the communication process and stages. For instance, the CERC model (Reynolds and Seeger 2005) is a five-stage model, beginning with a pre-crisis stage – the risk communication phase –, followed by four stages related to a specific crisis event: initial event, maintenance, resolution, and evaluation. The ICC framework (Slabbert and Barker 2012) has three stages: proactive, reactive, and post-evaluative. The proactive stage implies two-way communication with stakeholders to build sustainable relationships and resolve issues to avoid crises. The reactive stage concerns communication activities aimed at mitigating the crisis and ensuring accurate media reporting. The post-evaluative stage involves the evaluation of interaction with the media and repairing misperceptions.

Concerning financial systemic crises, Maurer and Nelson (2020) recommend some actions directed to social media platforms. Systemic risk managers should seek quick coordination with social media companies to organize content takedowns, limit the number of people required to review and approve crisis responses, and work together with social media platforms to amplify corrective statements that debunk fake information and calm the markets down.

Organizational crisis communication models

Organizational crisis communication focuses on the mitigation of reputational damage to the organization after a major incident. Two prominent models stand out in the literature: the Image Restoration Theory (IRT) (Benoit 1997) and the Situational Crisis Communication Theory (SCCT) (Coombs and Holladay 2002). Since the latter was chosen as one of the foundations of this research, it will be detailed in the next session.

IRT focuses on message options, offering five categories of image repair strategies: denial, evasion of responsibility, reducing offensiveness, corrective action, and mortification. Benoit (1997) applied the theory to several case studies and indicates some recommendations for crisis communication concerning preparation before the crisis, identification of the nature of the crisis, and crisis handling. Examples of the suggestions are avoiding making false claims or arguments that may backfire, providing adequate support for claims, and reporting plans to correct and prevent recurrence of the problem.

Some models were proposed based on case studies from the financial sector or cyber breaches. Macliam (2007) used case studies within the South African financial sector to propose a model that focuses on communication with the media, consisting of three sectors: (i) the foundation, (ii) an analysis of a crisis situation, and (iii) content of communications. The foundation section comprises the structure necessary for effective crisis communication with the media, including a multidisciplinary crisis communication team, customer-friendly attitude, an open-door policy with the media, consistent messages, and a flexible strategy. The analysis section includes factors such as the context of the organization and its sector regarding past crises, the severity of the damage, and whether the organization is perceived as responsible for the event. Finally, the content of the message section has different recommendations depending on the responsibility perception of the public.

Knight and Nurse (2020) propose a framework that was based on data breaches selected from threat reports published by the United Kingdom's National Cyber Security Centre. For each selected event,

the authors analysed commentaries from security specialists about the appropriateness of the affected company's crisis communication. Then, the framework was refined after interviews with senior professionals. The resulting proposal includes two main stages – pre-event and cyber crisis response – and contains guidelines regarding, for example, the decision-making of disclosure, message framing, the timing of disclosure, and the channels for disclosure.

The next session details the SCCT framework, proposed by Coombs and Holladay (2002).

5.3 Situational Crisis Communication Theory

SCCT indicates how to manage organizational reputation during a crisis and is premised on matching the crisis response to the level of responsibility attributed. According to SCCT, crisis managers should begin by identifying the crisis type, estimating severity and the organization's performance history, and assessing the level of crisis responsibility based on these three variables. Then, the matching crisis response strategy would be selected.

Coombs and Holladay (2002) suggest a list of crisis types classified in three clusters, in order of attribution of crisis responsibility:

- Victim: the organization is a victim along with the stakeholders (natural disasters, rumours, workplace violence, or product tampering).
- Accidental: the crisis represents unintentional actions by the organization (challenges or technical breakdown).
- Preventable: the organization purposefully places stakeholders at risk, knowingly takes inappropriate actions, or there is avoidable human error (human breakdown or organizational misdeeds).

After determining the crisis type, the company should adjust its level of responsibility based on the severity of the incident and the organization's performance history. Greater severity means the public will attribute greater crisis responsibility to the company, while a good performance history – few past crises and a good relationship history with stakeholders – will decrease responsibility attribution.

Finally, the organization should choose the appropriate response strategy matching the estimated level of crisis responsibility. Coombs and Holladay (2002) propose eight response strategies in order from defensive to accommodative:

- An attack on the accuser: the organization confronts the group or person that claims a crisis exists.
- Denial: the organization states that there is no crisis.
- Excuse: the organization minimizes its responsibility for the crisis.
- Victimization: the organization portrays itself as a victim.
- Justification: the organization minimizes the impact of the crisis.
- Ingratiation: the organization praises stakeholders and reminds them of the past good deeds of the company.

- Corrective action: the organization tries to repair the damage and prevent a repeat of the crisis.
- Full apology: the organization publicly accepts responsibility and requests forgiveness for the crisis.

Defensive strategies should be used when the company has a low level of responsibility, and accommodative strategies should be used when the attribution of crisis responsibility is higher.

Coombs (2007) adds three response strategies: scapegoat (the company blames some person or group outside of the organization for the crisis), compensation (the company offers money or gifts to victims), and reminder (a subset of ingratiation). Furthermore, the author groups the strategies into three primary groups – deny, diminish, and rebuild – and one supplemental group – bolstering:

- Deny: attack the accuser, denial, scapegoat
- Diminish: excuse, justification
- Rebuild: compensation, apology, corrective action
- Bolstering: reminder, ingratiation, victimization

The next session discusses the presented risk and crisis communication concepts and relates them to systemic cyber risk.

5.4 Discussion

A financial crisis may be considered a public hazard, and so existing public hazards communication models may be used and adapted to address systemic risk. To avoid unnecessary worry and confusion, risk messages should be carefully designed and evaluated considering the attributes of the audience, the risk event characteristics, and situational analysis. The crisis communication process should be planned in advance and comprise a pre-crisis stage to build credibility with media and other stakeholders, and include specific actions directed to social media platforms such as those recommended by Maurer and Nelson (2020) (see Session 5.2).

Furthermore, systemic risk managers should consider the divergences among the risk and crisis communication strategies of the various interested parties, such as the conflict between financial stability risk communication and cyber risk communication (see Session 5.1).

In the cyber security community, it has been a best practice to be as transparent as possible during a cyber breach. Since the same tactics, techniques and procedures may be used by the attacker to compromise other institutions, the affected companies should reveal as much information as possible to help the community in containing the incident, with cybersecurity agencies also publishing actionable information about the threat. Additionally, many countries have specific regulations where the detailed disclosure of cyber breaches to the public is mandatory, such as the EU General Data Protection Regulation (the European Parliament and the Council 2016b).

In contrast, financial authorities may use less transparent crisis communication strategies, avoiding commenting, and downplaying the impacts. This strategy may be justifiable if their objective is to calm people down to avoid excessive actions such as bank runs. However, these contradictory response

strategies by different organizations concerning the same threat may amplify the perception of risk of society and individuals overall.

Furthermore, financial national authorities like central banks usually have some level of control in the narrative of traditional financial crises. Banks and other financial institutions will generally follow the instructions and recommendations of the financial authority concerning crisis communication.

Nevertheless, in a potential cyber breach, crisis communication might not be centralized in the financial authority, and strategies used by cybersecurity authorities and individual companies might be conflicting with the strategy the central bank would use to maintain confidence in the financial system. Affected companies will usually focus on mitigating the impact on their reputation, using frameworks such as IRT and SCCT (see Sessions 5.2 and 5.3). These response strategies, in some cases, might be counterproductive to the financial authority's efforts to mitigate a systemic crisis.

Finally, communication from opinion leaders, politicians, experts, and journalists during a crisis may also affect the overall perception of risk and should also be considered by financial crisis managers.

In short, systemic cyber risk communication planning should consider not only crisis communication from financial authorities, but also from the affected companies, engaged cybersecurity firms, cybersecurity agencies, and other relevant communicators.

Based on the theoretical concepts and the discussion presented to this point, this work analysed two case studies with the methodology described in the next chapter.

6 Data analysis method

To answer the research questions proposed in Session 1.3, this work used a directed content analysis approach (Hsieh and Shannon 2005) to examine two cyber risk events that affected financial services institutions. Equifax is one of the three major credit bureaus and Capital One is one of the largest banks in the US (Consumer Financial Protection Bureau 2021; Federal Financial Institutions Examination Council 2021).

These case studies were chosen since they had similarities in the type, magnitude, and root cause of the incident, while at the same time had very different consequences. Furthermore, the study selected a single source of information for content analysis – the CNBC website. Although this approach has some limitations (see Chapter 10), it allows a coherent comparison between these two events concerning media coverage.

SARF and SCCT are the frameworks that were used to develop the codebook for the directed content analysis. SARF was chosen since it is considered one of the most comprehensive tools for the study of risk (Rosa 2003), its concept of rippling effects is consistent with the notion of systemic risk, and its communication model is adequate to analyse the one-way information flow that is used in this study. Moreover, SARF is a widely used research tool. The paper that proposed the framework (Kasperson et al. 1988) was cited by 4,013 studies, including 499 studies since 2020[3]. Its foundations inspired previous systemic risk research (Kaszowska and Santos 2014) and cyber risk research (Jackson, Allum, and Gaskell 2004; Saridakis et al. 2016; Xu et al. 2021).

Concerning crisis communication frameworks, SCCT and IRT are the prominent models in this field, according to a quantitative review of crisis communication studies in public relations from 1991 to 2009 (Avery et al. 2010). SCCT was chosen because it defines a broader range of crisis response strategies.

The next sessions detail the data collection techniques, present the codebook that was used for the content analysis, and explain the coding and analysis procedures.

6.1 Data collection

The data corpus consists of two data sets. The first data set contains 131 news articles about the Equifax data breach downloaded from the CNBC website. The second one includes 17 news articles about the Capital One hack collected from the same media outlet.

Initially, ten US news media websites were selected because of their popularity and relevance: CNBC, CNN, USA Today, The Wall Street Journal, CBS News, NBC News, PBS, ABC News, NPR, and Fox

[3] According to Google Scholar in 11 Aug. 21: https://scholar.google.com/

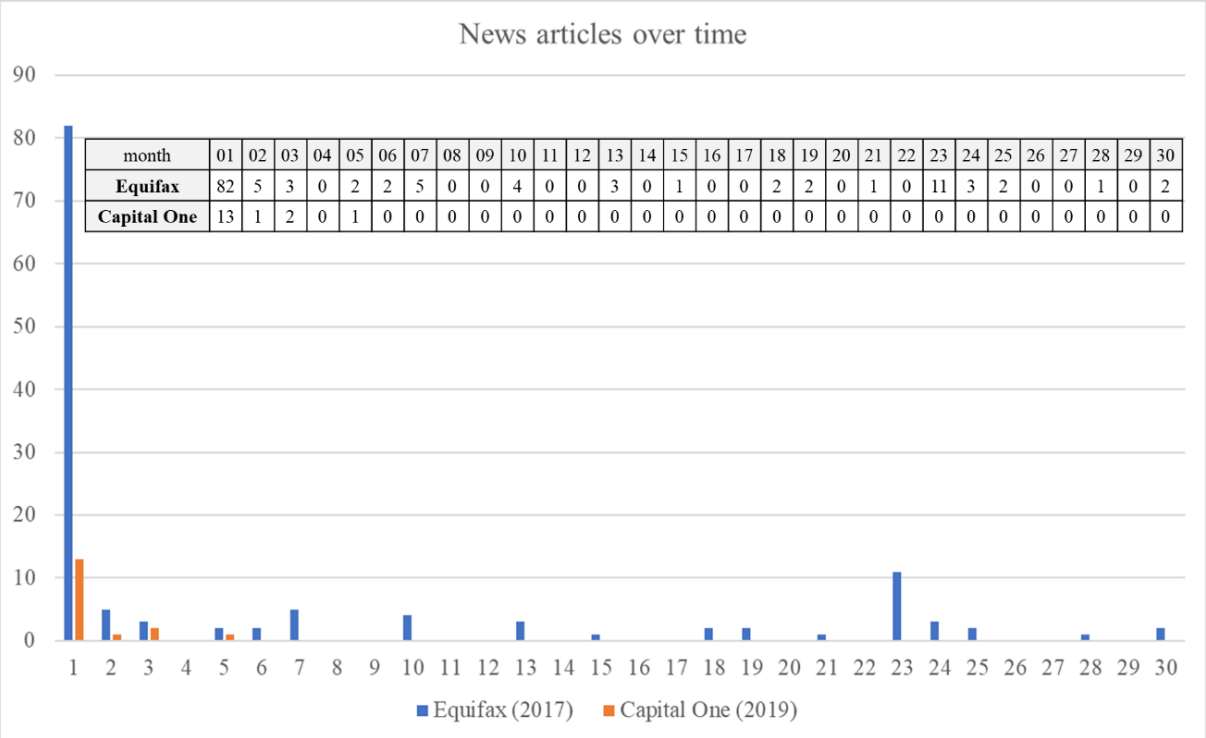
News. Then, keyword searching with the *googlesearch-python*[4] library was executed for the ten selected websites using the following search string: *"equifax data breach" OR "equifax breach"*.

The CNBC website was chosen since its query had the greatest number of results: 280. The next step was selecting, among the search results, relevant news articles for the Equifax case study analysis. The following criteria were used for inclusion/exclusion:

- Video news articles without transcription were excluded. Only written text articles were considered.
- Written text news articles about the Equifax breach or its consequences were included.
- News articles about other cyber incidents that just mentioned the Equifax breach as an example were excluded.

After applying the inclusion/exclusion criteria, 131 news articles were included in the Equifax breach data set.

Then, for consistency, the same media outlet (CNBC) was used to search for news articles concerning the Capital One data breach. The following search string was used: *"capital one data breach" OR "capital one breach" OR "capital one hack" (site:cnbc.com)*. 46 news articles were found, and after applying equivalent criteria for inclusion/exclusion, 17 articles were selected.



month	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Equifax	82	5	3	0	2	2	5	0	0	4	0	0	3	0	1	0	0	2	2	0	1	0	11	3	2	0	0	1	0	2
Capital One	13	1	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 2 – Equifax and Capital One breaches news articles over time

[4] https://pypi.org/project/googlesearch-python/

The distribution of the news articles from both data sets over time is depicted in Figure 2. The month variable is relative to the day of the breach announcement – 7 September 2017 for the Equifax breach and 29 July 2019 for the Capital One breach. For example, for the Equifax breach, the first month is the interval from 7 September to 6 October 2017, the second month is from 7 October to 6 November 2017, and so on.

The next session details the codebook development.

6.2 Codebook

This work used a directed approach for content analysis, i.e., the study was guided by an existing framework (SARF) and theory (SCCT). Therefore, a structured codebook was developed before the start of coding.

Three main themes were used as the coding system's high-level categories:

1. **Social amplification factors:** risk properties, informational attributes, and response mechanisms that may cause amplification of risk perception from individuals and society.
2. **Impacts:** the secondary and third-order consequences of the risk event to the affected company and other organizations.
3. **Crisis communication strategies:** response strategies used by organizations to mitigate the effects of a crisis on their reputation.

The social amplification factors are selected from those described by SARF (Figure 1). The three factors from the risk event characteristics are considered – the extent of risk exposure, the "dread risk" factor, and the "unknown risk" factor. From the "information flow" factors, the information attributes – dramatization, controversy, and symbolic connotations – are used as codes ("volume of information" is also used in the analysis, but not for coding). From the "interpretation and response" factors, "stigmatization" and "social distrust of responsible institutions" are used for coding ("signal value" is implicitly used since it is closely related to the risk event characteristics). The remaining social amplification factors are not used in the analysis due to limitations of the methodology – for instance, only one information channel is used, and so it is not possible to verify the influence of this attribute in risk amplification.

Each theme is partitioned into several codes or subcategories. The next tables describe each code and display some data extract examples:

- Table 3 presents the codebook for the social amplification factors
- Table 4 presents the codes related to the impacts.
- Table 5 indicates the codes related to crisis communication strategies.

Table 3 - Codebook for social amplification factors

Social amplification factor	**Definition**	**Example**
Extent of risk exposure	The extent of risk exposure indicates the number of individuals directly affected by the risk event, even if its consequences are not yet known.	“That's significantly **over half of the US adult population** that probably had their information taken”
Dread risk factor: Increasing over time	This property indicates the risk level is going to rise before it declines.	“Just yesterday, the **number of consumers potentially affected in the breach was revised upward**.”
Dread risk factor: Involuntary	This property indicates the affected individuals did not choose to accept the risk.	“American consumers have **no choice**. Our information is included **whether we want it or not**.”
Dread risk factor: Not easily reduced	This property indicates that the mitigation of the risk is difficult.	“People need to understand that this is a forever problem,**"** Schulz said. "**Once your information is out there, you can't put the toothpaste back in the tube**”
Dread risk factor: Not equitable	This property indicates that the benefits and risks are not equally distributed across society.	“**Consumers are at the losing end** given the way the US credit reporting system is structured”
Dread risk factor: Uncontrollable	This property indicates a lack of control by the affected individuals in treating the risk.	“They questioned how private companies could amass so much personal data, **setting off efforts to bolster consumers' ability to protect and control their information**.”
Unknown risk factor: Has a delayed effect	This property indicates that there is a latency between the event and its consequences.	“Even if you did check, **thieves could save your info for years and use it down the road when you think the Equifax hack is old news**.”
Unknown risk factor: New	This property indicates that the risk is unprecedented in at least some of its aspects.	“**We have not been through the equivalent of this one**,**"** Fairbank said. "A lot of people are going to have to live the pain of this.”
Unknown risk factor: Not observable	This property indicates that the effect of the exposure on individuals cannot be observed.	“**Just because nothing looks amiss on your bank statements or your credit report now, that doesn't mean you haven't been compromised**.”
Unknown risk factor: Unknown to experts	This property indicates that experts do not have sufficient knowledge about the risk.	**“The great Equifax mystery: 17 months later, the stolen data has never been found**, and experts are starting to suspect a spy scheme”
Unknown risk factor: Unknown to those exposed	This property indicates that individuals do not know if they are exposed to the risk.	“For starters, an Equifax webpage dedicated to alerting consumers if they are among the 143 million potentially affected by the breach is causing **a great deal of confusion among people hoping for a definitive answer**.”
Controversy of information	This category includes facts that indicate differences of opinion or dispute of information among involved parties.	“**Bloomberg said the two attacks "involve the same intruders," citing an unnamed source, but the Equifax spokeswoman wrote that Mandiant has not come across evidence that would indicate the two hacks are related**.”
Dramatization of information	This category includes expressions that indicate dramatization and sensationalism of the risk event and its consequences.	"**It's a disaster. This breach has put almost every adult American in jeopardy**.”
Symbolic connotations	This category includes the use of terms and concepts with symbolic connotations.	(No examples were found in the data corpus)
Social distrust of responsible institutions	This category includes facts or opinions that indicate a reduction of trust in the companies affected by the risk event, or in public agencies responsible for managing the risk, caused by dishonesty or incompetence.	“**Management selling a few days after the discovery looks bad**, though extent of breach likely not known at that time.” “Sen. Mark Warner, D-Va., criticized Equifax's response to the breach, saying it seemed **the company was "not on guard," "very slow" and "very, very sloppy.**”
Stigmatization	This category includes facts or opinions that indicate stigmatization of technology or the companies involved in the risk event.	“Avoiding another **Equifax-like breach** is not something corporations can do alone”

Table 4 - Codebook for impacts

Impact	Definition	Example
Secondary impacts	This category includes information about secondary consequences that follow the original impact of the risk event. Some of the potential impacts are market losses, lawsuits, the retirement of executives, compensation to victims, and costs related to the incident response.	"We've seen a **$6 billion loss in market cap**, estimated losses from these breaches in excess of $20 billion." "Equifax said Friday **that its top information and security executives were retiring**, effective immediately as the company reels from its disclosure last week that it suffered a massive data breach potentially affecting 143 million people in the US"
Ripple effects	This category refers to information about impacts that affected other companies of the sector or even other sectors. New laws or regulations affecting different companies are examples of ripple effects.	"**New York Representative Carolyn Maloney asked the CEOs of TransUnion and Experian as to how each company is addressing its information security program in light of the Equifax data breach**." "Last September, **a federal law went into effect that prohibits credit-reporting firms from charging consumers for a credit freeze** (or to lift a freeze)."

Table 5 - Codebook for crisis communication strategies

Crisis communication strategy	Definition	Example
Deny	This communication strategy is used when the company denies the incident has happened, blames a third party or one specific employee, or accuses the person that revealed the incident.	**"AWS was not compromised in any way and functioned as designed,"** Amazon said in a statement to CNBC. " (denial) "An Amazon spokesperson criticized Warren's letter, written with Sen. Ron Wyden, D-Ore., for conflating the client and host in this way, saying via email: "**The letter's claim is baseless and a publicity attempt from opportunistic politicians**." (attack the accuser) "As Capital One has explained, the perpetrator attacked a **misconfiguration at the application layer of a Capital One firewall**." (scapegoat)
Diminish	This communication strategy is used when the company indicates the incident was not their fault nor critical.	"Begor said that in 2018, the **more than 1,200 data breaches against US corporations showed that companies of all types were falling victim to these crimes**." (excuse) "Begor, who became CEO after the scandal, said **there's no proof the data breach has had a negative impact on the impacted consumers**." (justification)
Rebuild	This communication strategy is used when the company apologizes for the incident, compensates the victims, or takes action so the incident does not happen again.	"**The CEO apologized** in an op-ed published Tuesday in USA Today and vowed **the company would "make changes" to ensure it wouldn't happen again**." (apology, corrective action) "Equifax has reached out to consumers, **offering a year's worth of free credit monitoring**, and waiving the usual fees charged for those who opt to place a freeze on their credit records." (compensation)
Bolstering	This communication strategy is used when the company reminds the audience of good past deeds or portraits itself as a victim.	"Equifax's CEO called the incident "**an attack on consumers and an attack on America**" on the conference call. The breach affected 147 million consumers, most in the US, but also in Europe and Canada." (victimization)

The next session describes the coding and analysis procedures.

6.3 Coding and analysis procedures

Each news article was manually examined, and relevant data were extracted and classified in the appropriate categories and codes. Then, a chronological analysis was performed. The chain of events was split into several periods, and for each term, the most relevant episodes were presented along with their classification according to the codebook.

Subsequently, social amplification factors were quantified by the number of news articles in which they were mentioned. The quantification considered three periods:

- Short-term: up to 30 days after the incident was revealed.
- Medium-term: from 31 days to 1 year after the incident was revealed.
- Long-term: more than 1 year after the incident was revealed.

Afterwards, a cross-case analysis was performed to indicate the significant differences between the two case studies and the results were discussed. Finally, the answers to the research questions were proposed.

The next two chapters present the results of the case studies analyses.

7 Equifax breach analysis

This chapter presents the results of the Equifax breach news articles analysis, including the codes found according to the chain of events, and the quantification of social amplification factors. During the presentation of the analysis results, the CNBC news articles are referenced by their Article ID indicated in the Appendix.

7.1 Chronological analysis

The day of the announcement – 07 September 2017

The Equifax breach was revealed on 07 September 2017, when the company issued a statement about the subject, apologizing to customers (1). The company said that the breach could potentially affect 143 million consumers in the US (1). The potential reduction of trust in Equifax was triggered not only by the breach itself but also by the fact that three of the company's executives had sold US$ 2 million in Equifax shares days after the attack was discovered (1). The company's shares fell more than 12 per cent on the day the breach was revealed (1).

Table 6 portrays the chain of events and corresponding categories and codes.

Table 6 - Chain of events on the day of the Equifax breach announcement (07 September 2017)

Category	Episode	Code
Crisis communication strategy	Equifax apologizes to customers.	Rebuild strategy (apology)
Social amplification factor	The announced breach may affect 143 million consumers. Equifax executives sold US$ 2 million in shares days after the attack.	Extent of risk exposure Social distrust (dishonesty)
Impact	Equifax shares fell more than 12%.	Secondary impact

The first week after the announcement – 08 - 14 September 2017

During the week after the breach was disclosed, the incident continued to be depicted as having a great extent of risk exposure. It was described as massive (10), colossal (24), and one of the largest data breaches of US history (3). Some dramatization of information was also observed, with the use of words such as "horror" (24) and "disaster" (21). Stigmatization of the company was seen in two headlines that used the expressions "Equifax-type data theft" (17) and "Equifax-like breach" (19).

Equifax maintained the rebuild response strategy, announcing several actions to investigate the incident and to ensure it would not happen again (18), and compensating victims with free credit monitoring and identity theft protection (23).

Nevertheless, experts indicated that the risk was not easily reduced, since the free credit monitoring offered by Equifax was not fully effective, and consumers should consider paying for better monitoring

services and credit freezes (9). Moreover, the risk was depicted as inequitable, with consumers and shareholders being financially affected, while executives would escape accountability (26).

Equifax published a website to help consumers know if they were affected, but the answers were not reliable (17), and experts advised US citizens to assume they were compromised (33) since information about how the breach occurred was not available (24).

Some episodes contributed to reducing the credibility of the affected company. Equifax's monitoring service terms banned users from participating in class-action lawsuits (9), indicating the potential dishonesty of the company. Also, suspect trading in Equifax options indicated, once more, the possibility of insider trading (12). A senator described Equifax's response to the breach as "very slow" and "very sloppy" (3), contributing to the perception of the company's incompetence, which was further enhanced by the disclosure of a vulnerability in Equifax's website in Argentina (30).

Several secondary impacts followed. Investment firms published reports indicating potential consequences to Equifax concerning credibility and material costs, and at least one firm removed Equifax from its recommended list (4). Moreover, a civil class-action lawsuit was filed (4), the US Congress announced a hearing about the case (11), and several investigations were launched by attorney generals from nearly 40 states (28) and the Federal Trade Commission (FTC) (29). At the end of the week, Equifax shares had fallen more than 30 per cent (30).

During the week, a congress representative called for a complete overhaul of the US credit reporting system and new legislation to protect consumers' identities, while a senator asked for more regulatory scrutiny of cybersecurity breach reporting (3), indicating potential ripple effects, i.e., the spreading of the consequences to other companies of the sector and even to other sectors. Moreover, a congress representative requested information about the security program of TransUnion and Experian – Equifax main competitors – and shares of TransUnion fell 8.5 per cent in a single day (21).

Table 7 portrays the chain of events on the first week after the breach announcement.

The second week after the announcement – 15 - 21 September 2017

In the following week, the hack was depicted as the fifth largest in history (44). Some dramatization followed. A technology attorney pointed to the possibility of bankruptcy of Equifax (31), and an opinion leader indicated that the leaked data was "the holy grail" for criminals (34).

Equifax added more compensation to victims, waiving the usual fees for credit freezes (40). However, the company continued to be criticized. An opinion leader said the company seemed to not know about what was happening (46), and an attorney said that US consumers were at the losing end of the credit reporting system and their information was handled by credit reporting companies without their consent (51).

Some details about the root cause of the breach surfaced, contributing to the image of the incompetence of Equifax. The flaw used by the attacker had been corrected by the software developer months earlier, but Equifax failed to install the security update (45).

Table 7 - Chain of events on the first week after the Equifax breach announcement (08 - 14 September 2017)

Category	Episode	Code
Crisis communication strategy	Equifax announces actions taken to investigate the incident and to ensure it will not happen again.	Rebuild strategy (corrective actions)
	Equifax compensates victims with free credit monitoring and identity theft protection.	Rebuild strategy (compensation)
Social amplification factor	The event is described as massive, colossal, and one of the largest breaches in history.	Extent of risk exposure
	Use of words “horror” and “disaster”.	Dramatization of information
	Use of expressions “Equifax-type data theft” and “Equifax-like breach”.	Stigmatization of the company
	Expert says Equifax credit monitoring offer is not effective.	The risk is not easily reduced
	Equifax executives would escape financial accountability.	The risk is not equitable
	Equifax website that indicates who was affected is not reliable.	The risk is unknown to those exposed
	Experts do not know how the breach occurred.	The risk is unknown to experts
	Equifax’s monitoring service terms bans users from participating in class-action lawsuits.	Social distrust (dishonesty)
	Suspect trading in Equifax options indicates the possibility of insider trading.	Social distrust (dishonesty)
	A senator describes Equifax’s response to the breach as “very slow” and “very sloppy”.	Social distrust (incompetence)
	Equifax used the word 'admin' for the login and password of a database.	Social distrust (incompetence)
Impact	Investment firm removes Equifax from its recommended list.	Secondary impact
	A civil class-action lawsuit is filed.	Secondary impact
	The US Congress announces a hearing about the case.	Secondary impact
	Several investigations are launched by attorney generals from nearly 40 states and the FTC.	Secondary impact
	Equifax shares fall more than 30 per cent.	Secondary impact
	A congressman calls for a complete overhaul of the US credit reporting system and new legislation to protect consumers’ identities.	Ripple effect
	A senator calls for more regulatory scrutiny of cybersecurity breach reporting.	Ripple effect
	A congressman requests information about the security program of TransUnion and Experian and shares of TransUnion falls 8.5 per cent in a single day.	Ripple effect

Bad news for Equifax followed, with the suspect trading by Equifax executives and others being investigated by federal prosecutors and Congress (50). Moreover, a second security incident that had happened some months earlier was revealed, and one controversy emerged when Bloomberg said the two attacks were performed by the same intruders, which was denied by Equifax (38). Adding up to the

loss of credibility of the company, the Equifax official account on Twitter misdirected users to a phishing website (49).

Meanwhile, the top information and security executives of Equifax retired (35), and a lawsuit was filed by the state of Massachusetts (45). Impacts continued to ripple with three bills introduced in Congress in response to the hack, including one that would prohibit credit reporting companies to charge for credit freezes (37).

Table 8 portrays the chain of events on the second week after the breach announcement.

Table 8 - Chain of events on the second week after the Equifax breach announcement (15 - 21 September 2017)

Category	**Episode**	**Code**
Crisis communication strategy	Equifax waives the usual fees for credit freezes.	Rebuild strategy (compensation)
Social amplification factor	The event is depicted as the fifth largest in history.	Extent of risk exposure
	A technology attorney points to the possibility of bankruptcy of Equifax.	Dramatization of information
	An opinion leader indicates that the leaked data is “the holy grail” for criminals.	Dramatization of information
	An opinion leader says the company seems to not know about what is happening.	Social distrust (incompetence)
	An attorney says that US consumers are at the losing end of the credit reporting system.	The risk is not equitable
	Consumers’ information is handled by credit reporting companies without their consent.	The risk is involuntary
	The flaw used by the attacker had been corrected by the software developer months earlier, but Equifax failed to install the security update.	Social distrust (incompetence)
	Suspect trading by Equifax executives and others are investigated by federal prosecutors and Congress.	Social distrust (dishonesty)
	A second security incident that happened some months earlier is revealed.	Social distrust (incompetence)
	A media outlet says the two attacks were performed by the same intruders, which is denied by Equifax.	Controversy of information
	Equifax official account on Twitter misdirects users to a phishing website.	Social distrust (incompetence)
Impact	The top information and security executives of Equifax retire.	Secondary impact
	A lawsuit is filed by the state of Massachusetts.	Secondary impact
	Three bills are introduced in Congress in response to the hack.	Ripple effect

Third and fourth weeks after the announcement – 22 September – 05 October 2017

During the next weeks, Equifax reinforced the rebuild strategy, hiring a law firm to do an independent review (67) and announcing a new service that would allow consumers to control access to their data (63).

News articles continued to depict the difficulties in reducing the risk. The president of an investment firm warned about how hard it is to change the Social Security number (55), which was one of the leaked personal data. As the investigations continued, the possibility of the involvement of a nation-state emerged (69), indicating it would not be easy to recover the data. Moreover, investigators found that 2.5 million more US customers were potentially affected than originally estimated (70).

Furthermore, the risk was portrayed as vague and indefinite for affected individuals (52), and as having a delayed effect, since the stolen information might be used by the attackers many years later (55).

The dramatization was observed in the headline of a news article that said that consumers "face a US$ 4.1 billion tab to freeze credit reports after Equifax breach", although this amount is just an estimation of how much would be paid if every US adult citizen used this service (75). Stigmatization of the affected company was seen when a senator advised people to not respond to emails that reference Equifax (60).

New episodes contributed to the social distrust of Equifax. Investigation showed the hackers were inside the company's network for two months without being noticed (52), and a former employee said that almost all employees had access to personal data (69). A lack of transparency was also observed since Equifax waited 40 days to reveal the cyber breach (57).

More secondary impacts were revealed. Equifax CEO retired (56) and had to testify in Congress (57), and more than 70 class-action lawsuits were filed against Equifax (52). Rippling effects include a public agency calling for sooner disclosure of cyber breaches (54), an opinion leader calling for changes in the whole credit model (64), a public agency director revealing changes in credit firms' oversight – including embedded regulators and a heightened level of scrutiny (61) -, and the White House cybersecurity coordinator announcing a review of the use of Social Security numbers by federal departments or agencies (77). Moreover, a poll showed three-quarters of the public favoured new laws or regulations to deal with credit bureaus (66).

Table 9 portrays the chain of events on the third and fourth weeks after the breach announcement.

One month to one year after the announcement – 06 October 2017 – 06 September 2018

After one month, articles about the breach became less frequent, but new stories continued to be published. Two episodes showed that the risk might be worse than previously reported: a document submitted by Equifax to the Senate indicated other types of personal information were also stolen (93), and a new investigation increased the number of affected individuals by 2.4 million (94).

The loss of credibility of Equifax went on, with the announcement of an investigation of another possible cyber breach (84), the sending of erroneous notification letters to customers (98), and with two ex-employees charged with insider trading related to the breach (102). Social distrust of the Consumer Financial Protection Bureau (CFPB) was also observed when the head of the agency was accused of stopping a probe of the breach (92).

Table 9 - Chain of events on the third and fourth weeks after the Equifax breach announcement (22 September 2017 - 05 October 2017)

Category	Episode	Code
Crisis communication strategy	Equifax hires a law firm to do an independent review.	Rebuild strategy (corrective action)
	The new Equifax CEO announces a new service to allow customers to control access to their data.	Rebuild strategy (corrective action)
Social amplification factor	Equifax CEO leaves the company with US$18.4 million in pension benefits.	The risk is not equitable
	An investment firm president warns about the difficulties of changing one person's Social Security number.	The risk is not easily reduced
	Investigators suspect a nation-state might be involved with the incident.	The risk is not easily reduced
	Investigators find that 2.5 million more US customers were potentially affected than originally estimated.	The risk is increasing over time
	A law professor says the injury is vague and very indefinite for affected individuals.	The risk is not observable
	A state attorney says that affected individuals have been put at risk of identity theft for years to come.	The risk has a delayed effect
	An investment firm president warns that the attackers may save the stolen information for years and use it in the future.	The risk has a delayed effect
	News article headline says that consumers face a US$ 4.1 billion tab to freeze credit reports after the breach.	Dramatization of information
	A senator advises not to respond to emails that reference Equifax.	Stigmatization of the company
	Hackers worked inside Equifax's computer network for two months without being noticed.	Social distrust (incompetence)
	Equifax waited 40 days to reveal the cyber breach.	Social distrust (dishonesty)
	A former Equifax employee says that almost all employees had access to personal data.	Social distrust (incompetence)
Impact	Equifax CEO retires.	Secondary impact
	More than 70 class-action lawsuits are filed against Equifax.	Secondary impact
	Equifax ex-CEO testifies in Congress.	Secondary impact
	A public agency calls for sooner disclosure of cyber breaches.	Ripple effect
	A public agency director says there will be changes in credit firms' oversight, including embedded regulators and a heightened level of scrutiny.	Ripple effect
	An opinion leader calls for changes in the whole credit model.	Ripple effect
	The White House cybersecurity coordinator announces a review of the use of Social Security numbers by federal departments or agencies.	Ripple effect
	Three-quarters of the public tell pollsters that they favour new laws or regulations to deal with credit bureaus.	Ripple effect

New consequences of the breach impacted Equifax. A United Kingdom public agency started an investigation on the breach (86), and a group of state regulatory agencies released a consent order

enforcing new governance requirements to Equifax (101). Moreover, the company announced it expected costs related to the breach to surge by US$ 275 million in 2018 (99).

Notable ripple effects were observed when a congressman introduced a bill to ban the use of Social Security numbers by credit bureaus (85), and senators called for laws concerning breach notification and the ability of consumers to opt-out of using credit-checking services (88). A positive ripple effect was observed for cybersecurity companies, with a cybersecurity fund returning more than 30 per cent since the Equifax breach (103).

Table 10 describes the chain of events from one month to one year after the breach announcement.

Table 10 - Chain of events from one month to one year after the Equifax breach announcement (06 October 2017 – 06 September 2018)

Category	**Episode**	**Code**
Crisis communication strategy	Equifax executives say they were victims of the hack attack.	Bolstering strategy (victimization)
Social amplification factor	Equifax submits a document to the Senate saying the attackers accessed personal information not previously reported.	The risk is increasing over time
	An additional 2.4 million individuals were affected.	The risk is increasing over time
	No fines or penalties are imposed on Equifax by state regulatory agencies.	The risk is not equitable
	Equifax investigates another possible cyber breach.	Social distrust (incompetence)
	The head of a public agency is accused of stopping a probe of the breach.	Social distrust (dishonesty)
	A former Equifax executive and an ex-employee are charged with insider trading related to the breach.	Social distrust (dishonesty)
	Equifax sends some affected consumers erroneous notification letters.	Social distrust (incompetence)
Impact	United Kingdom public agency investigates Equifax breach.	Secondary impact
	Equifax says it expects costs related to the breach to surge by US$ 275 million in 2018.	Secondary impact
	A group of state regulatory agencies release a consent order that enforces new requirements to Equifax.	Secondary impact
	Congressman introduces a bill to ban the use of Social Security numbers by credit bureaus.	Ripple effect
	Senators call for new laws concerning breach notification and the ability to opt-out of using credit-checking services.	Ripple effect
	A cybersecurity fund returns more than 30 per cent since the Equifax breach.	Ripple effect

One year to over two years after the announcement – 07 September 2018 – 10 February 2020

After one year, a change in crisis communication strategy by Equifax was observed. While it continued to announce corrective actions (109), the use of the diminish and bolstering strategies was also seen when Equifax claimed consumers had not suffered any harm (109) (diminish/justification), said there were more than 1,200 data breaches against US corporations in 2018 (110) (diminish/excuse), and called the incident an attack on consumers and America (116) (bolstering/victimization).

Social amplification factors continued to be depicted in the news articles. 17 months after the breach, the stolen data had not been found (108) and the attackers had not been identified by authorities (117), with experts believing it was probably held by a foreign intelligence agency (116). Some months later, four members of China's military were indicted (131).

Meanwhile, a Senate subcommittee released a report criticizing Equifax's handling of the data (111), and a state attorney said Equifax "put profits over privacy and greed over people" (116). The breach was called "the consumer scandal of the decade" (108).

More impacts followed, with new hearings in Congress, one of them including other credit reporting agencies (109). A rating agency downgraded its outlook on Equifax, which was the first time this happened for cybersecurity reasons (112).

A major settlement was finally announced, with Equifax having to pay up to US$ 700 million to settle US federal and state probes (117). However, it was still hard for consumers to prove their data was misused as a result of the breach (116), and a law institute director said the real beneficiaries of the Equifax settlement were the attorneys (129).

The settlement yielded a ripple effect that affected the FTC, a public agency responsible for the investigation of unfair or deceptive acts or practices by private organizations. A senator asked FTC's inspector general to open an investigation into the agency itself since it announced inaccurate compensation to victims of the breach (124).

Other relevant ripple effects were reported. A bill prohibiting credit-reporting firms to charge consumers for credit freezes took effect (104), meaning a loss of revenue for all companies of the sector, and a senator called for structural reforms and increased oversight of credit reporting agencies (117), indicating new laws or regulations might still be approved in the future.

Table 11 describes the chain of events from one year to over two years after the breach announcement.

In the next session, each one of the social amplification factor codes is quantified according to the number of news articles where they were found.

Table 11 - Chain of events from one year to over two years after the Equifax breach announcement (07 September 2018 – 10 February 2020)

Category	Episode	Code
Crisis communication strategy	Equifax claims consumers have not suffered any harm.	Diminish strategy (justification)
	Equifax says it hired 1,000 full-time employees and plans to spend US$ 1 billion on technology and security through 2020.	Rebuild strategy (corrective action)
	Equifax CEO says that in 2018 there were more than 1,200 data breaches against US corporations.	Diminish strategy (excuse)
	Equifax CEO calls the incident an attack on consumers and America.	Bolstering strategy (victimization)
Social amplification factor	Consumers advocates argue that Equifax has not been held accountable.	The risk is not equitable
	The stolen data has not been found 17 months after the breach.	The risk is unknown to experts
	Experts believe the stolen data is held by a foreign intelligence agency.	The risk is not easily reduced
	Two years after the disclosure, the hackers behind the incident had not been identified by authorities.	The risk is unknown to experts
	It will be difficult for consumers to prove their data was misused as a result of the Equifax breach.	The risk is not observable
	A law institute director says the real beneficiaries of the Equifax settlement are the attorneys.	The risk is not equitable
	Four members of China's military are indicted, indicating the data may be held by the China government.	The risk is not easily reduced
	A cyber-security expert says the Chinese might use the data a decade from now.	The risk has a delayed effect
	The breach is called the consumer scandal of the decade.	Dramatization of information
	A Senate subcommittee releases a report that criticizes Equifax's handling of data.	Social distrust (incompetence)
	A state attorney says Equifax put profits over privacy and greed over people.	Social distrust (dishonesty)
Impact	The Congress calls a hearing with executives from Equifax and Marriott.	Secondary impact
	A rating agency downgrades its outlook on Equifax.	Secondary impact
	Public authorities announce Equifax will pay up to US$ 700 million to settle US federal and state probes.	Secondary impact
	A bill prohibiting credit-reporting firms to charge consumers for credit freezes takes effect.	Ripple effect
	Congress calls a hearing with the CEOs of the three major US credit bureaus to discuss changes in legislation.	Ripple effect
	A senator calls for structural reforms and increased oversight of credit reporting agencies.	Ripple effect
	A senator calls for investigation into the FTC for misleading victims over compensation.	Ripple effect

7.2 Quantification of social amplification factors

The following event characteristics were found on the analysed CNBC news articles related to the Equifax breach:

- Extent of risk exposure
- Dread risk factor
    - Increasing over time
    - Involuntary
    - Not easily reduced
    - Not equitable
    - Uncontrollable
- Unknown risk factor
    - Has a delayed effect
    - Not observable
    - Unknown to experts
    - Unknown to those exposed

Table 12 shows the number of news articles that mention each factor distributed by when they were published.

Table 12 - Event characteristics: number of articles from Equifax breach

Days after the breach announcement	Extent of risk exposure	Dread risk factor	Unknown risk factor
<= 30 days	77	25	12
>30 days & <= 1 year	21	10	3
> 1 year	26	16	8
Total	124	51	23

8 news articles also portrayed the incident as new and unprecedented. However, the “newness” property was not considered in the “unknown risk” factor since the data breach was also described as not new by 9 articles (5 of them published in the short term).

Concerning the information flow from the Equifax data breach, the following attributes were found and measured (Table 13):

- Controversy
- Dramatization
- Volume

Messages with symbolic connotations about the Equifax data breach were not found during the content analysis of the CNBC news articles.

Table 13 – Information flow: number of articles from Equifax breach

Days after the breach announcement	Volume	Dramatization	Controversy
<= 30 days	82	6	1
>30 days & <= 1 year	21	1	0
> 1 year	28	2	0
Total	131	9	1

Regarding the interpretation and response to risk by society, the following mechanisms were found on the Equifax data breach analysis (Table 14):

- Social distrust of responsible institutions
- Stigmatization of the company

Table 14 – Interpretation and response: number of articles from Equifax breach

Days after the breach announcement	Social distrust	Stigmatization
<= 30 days	56	3
>30 days & <= 1 year	11	0
> 1 year	12	0
Total	79	3

The next chapter presents the Capital One data breach results.

8 Capital One breach analysis

This chapter presents the results of the Capital One breach news articles analysis, including the codes found according to the chain of events, and the quantification of social amplification factors. During the presentation of the analysis results, the CNBC news articles are referenced by their Article ID indicated in the Appendix.

8.1 Chronological analysis

The day of the announcement – 29 July 2019

When revealing the breach, Capital One used the rebuild strategy, apologizing to customers (132).

The breach was characterized by a great extent of risk exposure, with more than 100 million affected individuals (132). The fact that the Federal Bureau of Investigation (FBI) had already arrested the individual allegedly responsible for the breach (132) contributed to attenuate the "unknown risk" factor.

Capital One estimated costs to the company of up to US$ 150 million in 2019 (132).

Table 15 portrays the chain of events and corresponding categories and codes.

Table 15 - Chain of events on the day of the Capital One breach announcement (29 July 2019)

Category	Episode	Code
Crisis communication strategy	Capital One CEO apologizes to customers.	Rebuild strategy (apology)
Social amplification factor	The announced breach affected 100 million individuals in the United States and approximately 6 million in Canada. The FBI arrested an individual that allegedly was responsible for the breach.	Extent of risk exposure The risk is known to experts (risk attenuation)
Impact	Capital One estimates the hack will cost the company approximately $100 million to $150 million in 2019.	Secondary impact

The first week after the announcement – 30 July 2019 - 5 August 2019

In the following week, Capital One used the rebuild and diminish strategies, announcing compensation, and saying it was not likely the stolen information would be used for fraud or disseminated (133). Amazon.com also had to respond to the breach, since the data was stored in Amazon Web Services (AWS). The cloud provider used the deny strategy, stating that AWS was not compromised (134).

The risk was portrayed as not easily reduced by cybersecurity experts (133) and a bank CEO (138), which may have amplified risk perception. Capital One's credibility was possibly affected by the fact that a single individual was able to penetrate its defences (147), and the flaw was a misconfiguration of an application firewall by the bank's technicians (134).

Some secondary impacts were observed, with Capital One's stocks closing down 5.89 per cent on the day after the announcement (134), a state attorney general stating her office would investigate the breach (147), a credit card customer suing Capital One (147), and Congress opening an inquiry into the breach (141).

Ripple effects were also seen when Amazon.com founder Jeff Bezos was included in the congressional inquiry (141), and the relationship between big technology companies, cloud providers, and banks was questioned (134).

Table 16 portrays the chain of events on the first week after the breach announcement.

Table 16 - Chain of events on the first week after the Capital One breach announcement (30 July 2019 - 5 August 2019)

Category	**Episode**	**Code**
Crisis communication strategy	Capital One says it plans to offer free credit monitoring and identity protection to affected customers.	Rebuild strategy (compensation)
	Capital One says it is unlikely that the information was used for fraud or disseminated.	Diminish strategy (justification)
	Amazon.com says AWS was not compromised and functioned as designed.	Deny strategy (denial)
Social amplification factor	A cybersecurity expert says that a credit freeze is not an effective solution to mitigate identity theft.	The risk is not easily reduced
	The reason for the breach was a misconfiguration of an application firewall.	Social distrust (incompetence)
	A single individual was able to penetrate Capital One's defences and gain access to the accounts.	Social distrust (incompetence)
	A cybersecurity expert says that protecting against a single individual with access to the company can be difficult.	The risk is not easily reduced
	A bank CEO said the threat of cybersecurity might be the biggest threat to the US financial system since adversaries are smart and relentless.	The risk is not easily reduced
Impact	Capital One's stock closes down 5.89%.	Secondary impact
	A state attorney general states her office will investigate the breach.	Secondary impact
	A credit card consumer sues Capital One in a proposed class action.	Secondary impact
	Congress opens an inquiry into the Capital One breach.	Secondary impact
	The incident is said to bring up major issues facing the biggest tech companies, cloud firms, and banks.	Ripple effect
	Amazon.com is included in Congress inquiry into the breach.	Ripple effect

The second week after the announcement – 6 – 12 August 2019

There were no published news articles by CNBC during the second week after the breach announcement.

Third and fourth weeks after the announcement – 13 – 26 August 2019

In the next weeks, Capital One employees contributed to increasing the lack of trust when they raised concerns about the bank's cybersecurity unit, including high turnover among senior leaders and staff, and failure to install software to detect and prevent hacking (142). No new significant impacts were revealed.

Table 17 portrays the chain of events on the third and fourth weeks after the breach announcement.

Table 17 - Chain of events on the third and fourth weeks after the Capital One breach announcement (13 – 26 August 2019)

Category	Episode	Code
Crisis communication strategy	No relevant episode.	
Social amplification factor	Capital One employees raise concerns about the bank's cybersecurity unit, including high turnover among senior leaders and staff, and failure to install software to detect and prevent hacking.	Social distrust (incompetence)
Impact	No relevant episode.	

More than four weeks after the announcement – 27 August 2019 – 17 December 2019

After four weeks, the debate shifted to Amazon.com and other cloud service providers. Congress representatives called on the Financial Stability Oversight Council to consider designating Amazon Web Services, Microsoft Azure, and Google Cloud as systemically important financial market utilities, which would subject the tech firms to enhanced oversight by the Federal Reserve (144).

Furthermore, senators asked the FTC to explore Amazon.com's role in the breach, stating that the cloud provider failed to add software protection against the attack that caused the breach. The senators' request was considered a step toward a public discussion of cloud providers' regulatory oversight (144).

Amazon.com responded with the "denial" and "attack the accuser" strategies, saying the senators' claim was baseless and a publicity attempt from opportunistic politicians (144).

Table 18 portrays the chain of events occurring more than four weeks after the breach announcement.

In the next session, each one of the social amplification factor codes is quantified according to the number of news articles where they were found.

Table 18 - Chain of events occurring more than four weeks after the Capital One breach announcement (27 August 2019 – 17 December 2019)

Category	Episode	Code
Crisis communication strategy	Amazon.com responds to a senator's letter saying its claim is baseless and a publicity attempt from opportunistic politicians.	Deny strategy (attack the accuser)
Social amplification factor	Senators write in a letter to the Federal Trade Commission that Amazon.com failed to add software protection against the attack that caused the breach. The Capital One breach is listed on the 5 biggest data hacks of 2019.	Social distrust (incompetence) Extent of risk exposure
Impact	Congress representatives call on the Financial Stability Oversight Council to consider designating Amazon Web Services, Microsoft Azure, and Google Cloud as systemically important financial market utilities, which would subject the tech firms to enhanced oversight by the Federal Reserve. Senators ask the FTC to explore Amazon.com's role in the breach. The senators' request is a step toward a public discussion of cloud providers regulatory oversight.	Ripple effect Ripple effect Ripple effect

8.2 Quantification of social amplification factors

The following event characteristics were found on the analysed CNBC news articles related to the Capital One breach:

- Extent of risk exposure
- Dread risk factor
- Not easily reduced

Table 19 shows the number of news articles that mention each factor distributed by the day of publishing.

Table 19 – Event characteristics: number of articles from Capital One breach

Days after the breach announcement	Extent of risk exposure	Dread risk factor
<= 30 days	12	4
>30 days & <= 1 year	3	1
> 1 year	0	0
Total	15	5

The “unknown risk” factor was not significant in the portrayal of the Capital One breach.

Concerning the information flow from the Capital One data breach, the following attributes were found and measured (Table 20):

- Dramatization
- Volume

Indications of “controversy of information” or “symbolic connotations” about the Capital One data breach were not found during the content analysis of the CNBC news articles.

Table 20 – Information flow: number of articles from Capital One breach

Days after the breach announcement	Volume	Dramatization
<= 30 days	13	2
>30 days & <= 1 year	4	0
> 1 year	0	0
Total	17	2

Regarding the interpretation and response to the risk by society, the following mechanisms were found on the Capital One data breach analysis (Table 21):

- Social distrust of responsible institutions

Stigmatization was not displayed in the analysed articles.

Table 21 – Interpretation and response: number of articles from Capital One breach

Days after the breach announcement	Social distrust
<= 30 days	5
>30 days & <= 1 year	2
> 1 year	0
Total	7

In the next chapter, this work interprets the results aiming to answer the research questions stated in Session 1.3.

9 Discussion of results

This chapter presents a discussion of the results. It initiates with the analysis of the main differences between the two case studies and concludes with answers to the research questions.

9.1 Cross-case analysis

Both cases have extents of data exposure with the same order of magnitude, a similar root cause – a lack of basic cybersecurity hygiene - and similar crisis communication strategies used by the companies. Nevertheless, the consequences were very different (Table 22).

Table 22 - Consequences of Equifax and Capital One data breaches

Equifax data breach	**Capital One data breach**
148 million affected individuals	100 million affected individuals
Root cause: vulnerable application	Root cause: misconfigured application
Response strategy: rebuild (short-term), diminish and bolstering (longer-term)	Response strategy: rebuild and diminish
131 news articles on the CNBC website	17 news articles on the CNBC website
There was high media coverage during the following weeks after the incident, and new facts continued to be published for more than two years	The media coverage was concentrated on the week of the announcement, with few articles being published later
More than 70 class-action lawsuits were filed against Equifax	A customer sued Capital One, and a state attorney general announced an investigation
Three executives retired, including the CEO	No retirement of executives
Congress representative asks for a complete overhaul of the credit reporting system	Congress representatives ask for changes in cloud service providers oversight
Public agency announces a stricter regulation on credit agencies	No changes in regulation
Rating agency Moody's lowered its rating outlook on Equifax from stable to negative	Rating outlook not affected
A new law affecting all credit agencies was approved	No relevant laws changed
A judicial agreement was announced where Equifax would pay 700 million dollars to settle federal and state investigations	Capital One has agreed to pay 80 million dollars to settle federal charges (this information was collected from other media outlets since it was not found in the CNBC news articles)

This work argues that the discrepancy of the impacts may be explained by the distinct degrees of social amplification factors, which are explored for the remainder of this session.

Frequency of the social amplification factors

The Equifax data breach had a greater relative frequency of social amplification factors for all attributes but one. The extent of risk exposure, the "dread risk" and "unknown risk" factors, the controversy of information, and stigmatization had a higher relative frequency in the Equifax breach depiction, while dramatization of information had a higher rate in the Capital One breach representation (Table 23).

Table 23 – Absolute and relative frequency of social amplification factors from each case study

Social amplification factor	Equifax breach	Capital One breach
Extent of risk exposure	124 (95%)	15 (88%)
Dread risk factor	51 (39%)	5 (29%)
Unknown risk factor	23 (18%)	-
Volume of information	131	17
Dramatization of information	9 (07%)	2 (12%)
Controversy of information	1 (01%)	-
Social distrust of responsible institutions	79 (60%)	7 (41%)
Stigmatization	3 (02%)	-

However, the distinction between the two incidents is especially notable when the absolute frequency of the social amplification factors is considered. There was a significant disparity concerning the volume of information, with a difference of one order of magnitude in news articles published by CNBC. This aspect may be at the same time cause and consequence of a higher perceived risk, i.e., the Equifax data breach was perceived as a higher risk than the Capital One hack, resulting in broader media coverage. And this increase in media exposure brings to the public new aspects of the risk event that amplify risk perception even further.

As a result, the absolute frequency of all social amplification factors is considerably greater in the Equifax breach depiction. The “dread risk” and “social distrust” factors, for instance, are exhibited approximately ten times more in the Equifax breach articles than in the Capital One breach (Table 23).

Qualitative differences of the social amplification factors

Other relevant disparities appear when a qualitative analysis of the social amplification factors is performed. While the “dread risk” factor in the Capital One breach is limited to the risk being not easily reduced, the Equifax breach comprises many other “dread” properties. Firstly, affected individuals willingly shared their information with Capital One, while Equifax used the information without their consent (risk is involuntary). Also, the Equifax risk was portrayed as not equitable - with executives escaping financial accountability - and increasing over time, with the number of affected individuals growing as the investigations continued. These characteristics were not found in news articles concerning the Capital One breach. Finally, both events were depicted as “not easily reduced” since mitigating actions were not fully effective, but while the Capital One breach was perpetrated by an insider, Equifax attackers could be intelligence officers working for a foreign nation-state, making the recovery of the data harder.

The “unknown risk” factor was also very dissimilar between the two case studies. Capital One breach was portrayed as not significantly different from previous incidents, and since the breach was announced simultaneously with the arresting of a suspect, affected individuals and experts knew with reasonable

confidence where was the data and probably believed it would not be used. On the contrary, several months after the Equifax breach was announced, the public did not know how the breach had occurred, the stolen data had not been found, and the hackers had not been identified by authorities. Therefore, individuals were not sure if they were affected and how their data would be used.

Qualitative analysis also shows significant differences in social distrust. While the loss of credibility of Capital One is limited to a failure in maintaining a secure configuration of an internal application, the Equifax case study was characterized by several distinct episodes that suggested incompetence or dishonesty by the technicians, managers, and executives of the company.

Evolution of the social amplification factors over time

Another relevant aspect to be considered is the evolution of the frequency of social amplification factors over time. As expected, the absolute frequency of all social amplification factors was higher in the short term for both incidents. However, the Equifax breach coverage showed an increase in the absolute frequency of several social amplification factors in the long term when compared to the medium-term (Table 24).

The analysis of the relative frequency of social amplification factors over time also brings some relevant information. In the Capital One breach news articles, all but one of the social amplification factors decreased over time. The exception was “social distrust of responsible institutions”, and its increase was related to the loss of credibility of Amazon.com, not Capital One. In contrast, the Equifax breach portrayal was characterized by an increase in the relative frequency of the “dread risk” and “unknown risk” factors, which possibly contributed to maintaining a high perception of the risk and the interest of the audience in the subject (Table 24).

Table 24 – Absolute and relative frequency of social amplification factors by the period the news articles were published

Social amplification factor	Equifax (short-term)	Equifax (medium-term)	Equifax (long-term)	Capital One (short-term)	Capital One (medium-term)
Extent of risk exposure	77 (94%)	21 (100%)	26 (93%)	12 (92%)	3 (75%)
Dread risk factor	25 (30%)	10 (48%)	16 (57%)	4 (31%)	1 (25%)
Unknown risk factor	12 (15%)	3 (14%)	8 (29%)	-	-
Volume of information	82	21	28	13	4
Dramatization of information	6 (07%)	1 (05%)	2 (07%)	2 (15%)	0 (00%)
Controversy of information	1 (01%)	0 (00%)	0 (00%)	-	-
Social distrust of responsible institutions	56 (68%)	11 (52%)	12 (43%)	5 (38%)	2 (50%)
Stigmatization	3 (04%)	0 (00%)	0 (00%)	-	-

Regarding sustained media exposure, while CNBC continued to broadcast several stories and opinions about the Equifax breach in the following weeks after its announcement, the same did not happen with

the Capital One hack, which was covered mainly on the week the breach was revealed. Moreover, news stories about the Equifax breach continued for more than two years, while the coverage of the Capital One incident lasted less than five months.

It is possible to link some of the episodes and corresponding social amplification factors with ripple effects, at least hypothetically. Table 25 and Table 26 show some of the potential relations between episodes, identified ripple effects, and amplification factors, for the Equifax and Capital One breaches.

Crisis communication strategies

Although it might be expected that the use of more accommodative crisis response strategies by the affected companies - such as the announcement of corrective actions, compensation to victims, and apologies - would attenuate the consequences of the incident, no relation was found comparing the two case studies.

Equifax focused initially on rebuilding its reputation, but it was not effective. In contrast, Capital One used the diminish strategy along with the rebuild strategy since the beginning. This was facilitated by the fact that Capital One was able to indicate that it was unlikely that the information had been used for fraud or disseminated, since a suspect of committing the crime had already been identified. Equifax only used the diminish strategy many months later, when experts signalled the stolen data had not been seen in criminal forums. Table 27 shows the crisis communication strategies used by both companies over time.

Other considerations

Another aspect worth noting is blame attribution. While Equifax was considered the sole responsible for its breach, Capital One ended up sharing the blame with Amazon.com, which shifted the debate to cloud service providers.

Other factors may have contributed to the disparities in the breaches' consequences but could not be analysed within the available data corpus. Among these factors are the previous reputation and credibility of the companies, the political context and agenda-setting of the moment, and the fact that Capital One may have learned from Equifax's errors and benefited from the potential exhaustion of the topic's coverage caused by the previous breach.

Based on the presented cross-case analysis, the next session indicates the answers to the research questions listed in Session 1.3.

Table 25 - Potential links between ripple effects and social amplification factors in Equifax breach

Episode	Ripple effect	Social amplification factor
The announced breach may affect 143 million consumers.	(short-term) A congressman calls for a complete overhaul of the nation's credit reporting system.	Extent of risk exposure
A senator describes Equifax's response to the breach as "very slow" and "very sloppy".	(short-term) A senator calls for more regulatory scrutiny of cybersecurity breach reporting.	Social distrust (incompetence)
The flaw used by the attacker had been corrected by the software developer months earlier, but Equifax failed to install the security update.	(short-term) A congressman requests information about the security program of TransUnion and Experian.	Social distrust (incompetence)
An attorney says that US consumers are at the losing end of the credit reporting system.	(short-term) Three bills are introduced in Congress in response to the hack.	The risk is not equitable
Equifax waited 40 days to reveal the cyber breach.	(short-term) A public agency calls for sooner disclosure of cyber breaches.	Social distrust (dishonesty)
A former Equifax employee says that almost all employees had access to personal data.	(short-term) A public agency director says there will be changes in credit firms' oversight, including embedded regulators and a heightened level of scrutiny.	Social distrust (incompetence)
Consumers' information is handled by credit reporting companies without their consent.	(short-term) An opinion leader calls for changes in the whole credit model.	The risk is involuntary
An investment firm president warns about the difficulties of changing one person's Social Security number.	(short-term) The White House cybersecurity coordinator announces a review of the use of Social Security numbers by federal departments or agencies.	The risk is not easily reduced
An attorney says that US consumers are at the losing end of the credit reporting system.	(short-term) Three-quarters of the public tell pollsters that they favour new laws or regulations to deal with credit bureaus.	The risk is not equitable
An investment firm president warns about the difficulties of changing one person's Social Security number.	(medium-term) Congressman introduces a bill to ban the use of Social Security numbers by credit bureaus.	The risk is not easily reduced
Hackers worked inside Equifax's computer network for two months without being noticed.	(medium-term) A cybersecurity fund returns more than 30 per cent since the Equifax breach.	Social distrust (incompetence)
Consumers' information is handled by credit reporting companies without their consent.	(medium-term) Senators call for new laws concerning the ability to opt-out of using credit-checking services.	The risk is involuntary
News article headline says that consumers face a US$ 4.1 billion tab to freeze credit reports after the breach.	(long-term) A bill prohibiting credit-reporting firms to charge consumers for credit freezes takes effect.	Dramatization of information
Consumers advocates argue that Equifax has not been held accountable.	(long-term) Congress calls a hearing with the CEOs of the three major US credit bureaus to discuss changes in legislation.	The risk is not equitable
A Senate subcommittee releases a report that criticizes Equifax's handling of data.	(long-term) A senator calls for structural reforms and increased oversight of credit reporting agencies.	Social distrust (incompetence)
A law institute director says the real beneficiaries of the Equifax settlement are the attorneys.	(long-term) A senator calls for investigation into the Federal Trade Commission for misleading victims over compensation.	The risk is not equitable

Table 26 - Potential link between ripple effect and social amplification factors in Capital One breach

Event	Ripple effect	Social amplification factor
The reason for the breach was a misconfiguration of an application firewall.	(short-term) The incident will bring up major issues facing the biggest tech companies, cloud firms, and banks.	Social distrust (incompetence)
Protecting against a single individual with access to the company can be difficult.	(short-term) Amazon.com is included in Congress inquiry into the breach.	The risk is not easily reduced
A single individual was able to penetrate Capital One's defences and gain access to the accounts.	(medium-term) Congress representatives call on the Financial Stability Oversight Council to consider designating Amazon Web Services, Microsoft Azure, and Google Cloud as SIFMUs, which would subject the tech firms to enhanced oversight by the Federal Reserve.	Social distrust (incompetence)
Senators write in a letter to the Federal Trade Commission that Amazon.com failed to add software protection against the attack that caused the breach.	(medium-term) Senators ask the Federal Trade Commission to explore Amazon.com's role in the breach.	Social distrust (incompetence)
Senators write in a letter to the Federal Trade Commission that Amazon.com failed to add software protection against the attack that caused the breach.	(medium-term) The senators' request is a step toward a public discussion of cloud providers regulatory oversight.	Social distrust (incompetence)

Table 27 - Crisis communication strategies from Equifax and Capital One over time

Term	Equifax	Capital One
Short-term	Rebuild strategy (apology, compensation, corrective actions)	Rebuild strategy (apology, compensation) Diminish (justification)
Medium-term	Bolstering (victimization)	-
Long-term	Diminish (excuse, justification)	-

9.2 Answering the research questions

RQ1: Which risk event characteristics relate to sustained media coverage?

The Equifax data breach was characterized by sustained media coverage, while the Capital One breach was not. Since both incidents had extents of risk exposure with the same order of magnitude, this event characteristic by itself does not explains media coverage. The fact that many data breaches affecting millions of individuals were disclosed in the last years may justify why this property, in isolation, is not decisive.

On the other hand, the discrepancy in media coverage might be explained by the "dread risk" and "unknown risk" factors, since the risk events had significant differences concerning those properties. So, there is an indication that data breaches with higher "dread risk" and "unknown risk" factors tend to be marked by sustained media coverage. The fact that Capital One may have learned from the experience

from the Equifax case and the possibility of exhaustion of the topic's media coverage may have contributed to attenuate these social amplification factors.

RQ2: What social amplification factors may be relevant concerning those risk events?

The analysis of the relative frequency of the social amplification factors in the news articles shows that the following factors may be relevant concerning data breaches affecting financial services institutions (Table 23):

- Extent of risk exposure
- Dread risk factor
- Unknown risk factor
- Volume of information
- Social distrust of responsible institutions

In contrast, dramatization and controversy of information, symbolic connotations, and stigmatization were not significantly present on the analysed data corpus.

RQ3: How does the relevance of these social amplification factors and the incidence of ripple effects change over time?

Considering the absolute frequency of the social amplification factors over time, a strong reduction was observed after 30 days (Table 24).

The relative frequency, in contrast, was not characterized by a general rule. Some of the social amplification factors became relatively more frequent over time, while others had decreasing rates. Differences were also observed between the two cyber incidents. For instance, while in the Equifax breach the "dread risk" factor went up, in the Capital One incident the "dread risk" factor incidence reduced over time.

Regarding the manifestation of ripple effects, the Equifax data breach was characterized by several episodes over short, medium, and long terms (Table 25), while the Capital One breach had few occurrences (Table 26). This may be related to the continued depiction of social amplification factors in the Equifax breach as a consequence of sustained media exposure.

RQ4: How do crisis communication strategies used by the affected institutions relate to the attenuation of perceived risk?

Both companies used the rebuild strategy initially, but it was not effective for Equifax. One significant difference was the use of the diminish strategy by Capital One since the beginning, which may have attenuated the perception of risk by society. Therefore, the use of the diminish strategy along with the rebuild strategy may be related to the attenuation of social amplification factors, such as the "dread risk" and "unknown risk" factors, decreasing perceived risk and reducing the consequences of the incident.

Summary

This work suggests the following answers to the research questions, which were examined in the analysis of the collected data, i.e., these answers are therefore valid for the two cases studied.

When a major data breach affects a financial services institution:

RQ1: Which risk event characteristics relate to sustained media coverage?

A1: The “dread risk” factor and the “unknown risk” factors seem to be related to sustained media coverage.

RQ2: What social amplification factors may be relevant concerning those risk events?

A2: The extent of risk exposure, the “dread risk” factor, the “unknown risk” factor, the volume of information, and “social distrust of responsible institutions” may be relevant social amplification factors concerning those risk events.

RQ3: How does the relevance of these social amplification factors and the incidence of ripple effects change over time?

A3: The absolute frequency of social amplification factors greatly reduces after 30 days. Concerning relative frequency, there is no general rule, with some of the amplification factors increasing over time, while others reduce. Ripple effects continue to be generated in the medium and long term if new episodes and social amplification factors are persistently portrayed by media outlets.

RQ4: How do crisis communication strategies used by the affected institutions relate to the attenuation of perceived risk?

A4: The use of the diminish strategy since the beginning seems to be related to the attenuation of perceived risk while using the rebuild strategy in isolation seems to be ineffective.

10 Conclusions and future work

A cyber incident targeting financial institutions might provoke a systemic crisis through a severe operational disruption or a reputational contagion event. Public and private entities from the financial sector have been made efforts to improve their cyber resilience, but that might not be enough to mitigate the risk of a widespread loss of confidence in the financial system provoked by a cyber threat.

This work investigated whether the SARF and SCCT frameworks may be valuable tools to analyse a potential reputational contagion event caused by a cyber source. For that, directed content analysis was performed in a data corpus consisting of 148 news articles from CNBC regarding the Equifax and Capital One data breaches from 2017 and 2019, respectively.

Based on the analysed data, this work found relevant social amplification factors - the extent of risk exposure, the “dread risk” factor, the “unknown risk” factor, the volume of information, and social distrust of responsible institutions – that may be responsible for sustained media coverage, amplification of perceived risk, and the generation of secondary impacts and ripple effects after a data breach affecting financial companies. Moreover, it indicated that the “diminish” crisis communication strategy may be important when dealing with a cyber crisis.

One of the limitations of the methodology is the use of only one source of information – the CNBC website. So, the analysed data may be biased by the editorial policy of this media outlet. Moreover, although traditional media outlets continue to be a relevant source, individuals receive information from many other channels, including specialized media, alternative media, social networks, and direct conversations. So, the way the risk events are portrayed by a media outlet is just one component of how individuals will perceive the risk, but the full-scale interpretation of the risk will depend on several other factors. Also, risk perception depends not only on the source and channels of information, but also on personal experience, group membership, and other social and cultural aspects.

Another limitation is the fact that the research was based on only two data breach risk events. To confirm the results, it would be important to expand the study to incorporate a greater number of risk events, including other types of cyber incidents such as ransomware and espionage.

Additionally, none of the analysed incidents brought broader implications to the financial stability, and so the links between social amplification factors and systemic effects - such as credit shortage, liquidity crunch, or bank runs – could not be examined.

Therefore, this analysis suggests the following topics for further research:

- The analysis of more types of cyber events, such as ransomware, espionage, phishing scams, denial-of-service, and attacks based on the spread of disinformation.
- The inclusion of more sources of information, such as social media, press releases, government documents, specialized media, and other media outlets, and the investigation of the implications of different editorial policies in the results (since this aspect was assumed as uniform in this work’s data corpus).

- The use of surveys with financial system's stakeholders to validate the conclusions and address the correlation with systemic effects, with questions directed to specific triggers such as the perception of personal economic collapse.

Other themes that may be explored in future research are the possibility of automating the proposed content analysis scheme with the use of artificial intelligence and machine learning, and the use of the suggested frameworks to enhance systemic cyber risk perception and communication inside organizations.

Despite all the pointed limitations, this study presents reasonable evidence that SARF and SCCT are relevant tools for constructing codebooks to analyse cyber events that may generate a loss of confidence in financial systems and trigger a systemic crisis.

Ultimately, this work contributes to the advance of the state of the art of systemic cyber risk research concerning reputational contagion events.

Bibliography

Avery, Elizabeth Johnson, Ruthann Weaver Lariscy, Sora Kim, and Tatjana Hocke. 2010. “A Quantitative Review of Crisis Communication Research in Public Relations from 1991 to 2009.” *Public Relations Review* 36(2):190–92. doi: 10.1016/J.PUBREV.2010.01.001.

Balog-Way, Dominic, Katherine McComas, and John Besley. 2020. “The Evolving Field of Risk Communication.” *Risk Analysis* 40(S1):2240–62. doi: 10.1111/risa.13615.

Bank for International Settlements. 1994. “64th Annual Report.” Retrieved August 20, 2021 (https://www.bis.org/publ/arpdf/archive/ar1994_en.pdf).

Bank for International Settlements, and International Organization of Securities Commissions. 2016. “CPMI-IOSCO – Guidance on Cyber Resilience for Financial Market Infrastructures.” (June):32. Retrieved August 13, 2021 (https://www.bis.org/cpmi/publ/d146.pdf).

Bartholomew, Philip F., and Gary W. Whalen. 1995. “Fundamentals of Systemic Risk.” in *Banking, Financial Markets and Systemic Risk*.

Benoit, William L. 1997. “Image Repair Discourse and Crisis Communication.” *Public Relations Review* 23(2):177–86.

Blanchard-Boehm, RD. 1998. “Understanding Public Response to Increased Risk from Natural Hazards: Application of the Hazards Risk Communication Framework.” *International Journal of Mass Emergencies and Disasters* 16(3):247–78.

Boer, Martin, and Jaime Vazquez. 2017. “Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System.” *Institute of International Finance*. Retrieved August 13, 2021 (https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767).

Born, Benjamin, Michael Ehrmann, and Marcel Fratzscher. 2014. “Central Bank Communication on Financial Stability.” *Economic Journal* 124(577):701–34. doi: 10.1111/ecoj.12039.

Bouveret, Antoine. 2018. “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.” *IMF Working Papers*. Retrieved August 13, 2021 (https://www.imf.org/-/media/Files/Publications/WP/2018/wp18143.ashx).

Combs, Barbara, and Paul Slovic. 1978. “Newspaper Coverage of Causes of Death:” *Journalism Quarterly* 56(4):837–43. doi: 10.1177/107769907905600420.

Consumer Financial Protection Bureau. 2021. “List of Consumer Reporting Companies.” Retrieved August 10, 2021 (https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2021-06.pdf).

Consumer News and Business Channel. 2021. “International Business, World News & Global Stock Market Analysis.” Retrieved August 17, 2021 (https://www.cnbc.com/world/?region=world).

Coombs, W. Timothy. 2007. “Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory.” *Corporate Reputation Review* 10(3):163–76. doi: 10.1057/palgrave.crr.1550049.

Coombs, W. Timothy, and Sherry J. Holladay. 2002. “Helping Crisis Managers Protect Reputational Assets: Initial Tests of the Situational Crisis Communication Theory.” *Management Communication Quarterly* 16(2):165–86. doi: 10.1177/089331802237233.

Cyber Risk Institute. 2020. “The Profile – Cyber Risk Institute.” Retrieved August 8, 2021 (https://cyberriskinstitute.org/the-profile/).

Cybersecurity and Infrastructure Security Agency. 2021. “Analysis Reports.” Retrieved August 9, 2021 (https://us-cert.cisa.gov/ncas/analysis-reports).

European Banking Authority. 2019. “EBA Guidelines on ICT and Security Risk Management.” Retrieved August 8, 2021 (https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf).

European Central Bank. 2018a. “Cyber Resilience Oversight Expectations for Financial Market Infrastructures Cyber Resilience Oversight Expectations for Financial Market Infrastructures-Contents.”

European Central Bank. 2018b. “TIBER-EU Framework.” Retrieved August 9, 2021 (https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf).

European Central Bank. 2020. “Combating Cybercrime: Sharing Information and Intelligence as the First Line of Defence.” Retrieved August 16, 2021 (https://www.ecb.europa.eu/paym/intro/mip-online/2020/html/2009_mip_online.en.html).

European Central Bank. 2021. “Financial Stability.” Retrieved September 8, 2021 (https://www.ecb.europa.eu/pub/financial-stability/html/index.en.html).

European Commission. 2020a. “Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector.” Retrieved August 9, 2021 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0595).

European Commission. 2020b. “Proposed Directive on Measures for a High Common Level of Cybersecurity across the Union.” Retrieved August 9, 2021 (https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union).

European Systemic Risk Board. 2020. “Systemic Cyber Risk.” Retrieved July 24, 2021 (https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf).

European Union Agency for Cybersecurity. 2020. “ENISA Threat Landscape - 2020.” Retrieved August 9, 2021 (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends).

European Union Agency for Cybersecurity. 2021. “European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership.” Retrieved August 16, 2021 (https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership).

Federal Financial Institutions Examination Council. 2021. “Large Holding Companies.” Retrieved August 10, 2021 (https://www.ffiec.gov/npw/Institution/TopHoldings).

Financial Services Information Sharing and Analysis Center. 2021. “Financial Services Information Sharing and Analysis Center.” Retrieved August 16, 2021 (https://www.fsisac.com/).

Financial Stability Board. 2017. “Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices.” Retrieved August 9, 2021 (https://www.fsb.org/wp-content/uploads/P131017-2.pdf).

Fischhoff, Baruch, Christoph Hohenemser, Roger E. Kasperson, and Robert W. Kates. 1978. “Handling Hazards Can Hazard Management Be Improved?” *Environment* 20(7):16–37. doi: 10.1080/00139157.1978.9928700.

Freudenburg, William R. 1993. “Risk and Recreancy: Weber, the Division of Labor, and the Rationality of Risk Perceptions.” *Social Forces* 71(4):909–32. doi: 10.1093/SF/71.4.909.

Frewer, Lynn J. 2003. “Trust, Transparency, and Social Context: Implications for Social Amplification of Risk.” Pp. 123–37 in *The Social Amplification of Risk*. Cambridge University Press.

Group of Seven. 2016. “G7 Fundamental Elements of Cybersecurity for the Financial Sector.” Retrieved August 8, 2021 (https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf).

Group of Seven. 2018. “G7 Fundamental Elements for Threat-Led Penetration Testing.” Retrieved August 16, 2021 (https://www.bancaditalia.it/media/notizie/2018/G7-FE-Threat-Led-Penetration-Testing.pdf?language_id=1).

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Adriana Tache. 2018. “The Future of Financial Stability and Cyber Risk.” *Brookings Institution*. Retrieved August 13, 2021 (https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/).

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Alexander Wortman. 2021. “The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability.” *Journal of Financial Transformation* 53:94–107.

Hsieh, Hsiu Fang, and Sarah E. Shannon. 2005. “Three Approaches to Qualitative Content Analysis.” *Qualitative Health Research* 15(9):1277–88. doi: 10.1177/1049732305276687.

International Organization for Standardization. 2009. “ISO/Guide 73:2009(En), Risk Management — Vocabulary.” Retrieved August 20, 2021 (https://www.iso.org/obp/ui/fr/#iso:std:iso:guide:73:ed-1:v1:en).

International Organization for Standardization. 2018. “ISO 31000:2018(En), Risk Management — Guidelines.” Retrieved August 20, 2021 (https://www.iso.org/obp/ui/fr/#iso:std:iso:31000:ed-2:v1:en).

Jackson, Jonathan, Nick Allum, and George Gaskell. 2004. “Perceptions of Risk in Cyberspace.” Retrieved July 5, 2021 (https://www.researchgate.net/publication/30528235_Perceptions_of_risk_in_cyberspace).

Jonsson, Sara, and Inga-Lill Söderberg. 2018. “Investigating Explanatory Theories on Laypeople’s Risk Perception of Personal Economic Collapse in a Bank Crisis-the Cyprus Case.” *Journal of Risk Research* 21(6):763–79. doi: 10.1080/13669877.2016.1247375.

Kaffenberger, Lincoln, and Emanuel Kopp. 2019. “Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment.” *Carnegie Endowment for International Peace*. Retrieved August 20, 2021 (https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911).

Kasperson, Jeanne X., Roger E. Kasperson, Nick Pidgeon, and Paul Slovic. 2003. “The Social Amplification of Risk: Assessing Fifteen Years of Research and Theory.” Pp. 13–46 in *The Social Amplification of Risk*. Cambridge University Press.

Kasperson, Roger E., and Jeanne Kasperson. 2012. “Media Risk Signals and the Proposed Yucca Mountain Nuclear Waste Repository, 1985–1989.” *Social Contours of Risk* 148–75. doi: 10.4324/9781849772549-18.

Kasperson, Roger E., Ortwin Renn, Paul Slovic, Halina S. Brown, Jacque Emel, Robert Goble, Jeanne X. Kasperson, and Samuel Ratick. 1988. “The Social Amplification of Risk: A Conceptual Framework.” *Risk Analysis* 8(2):177–87. doi: 10.1111/J.1539-6924.1988.TB01168.X.

Kaszowska, Jagoda, and Juan Luis Santos. 2014. “The Role of Risk Perception in the Systemic Risk Generation and Amplification: Agent-Based Approach.” *ACRN Journal of Finance and Risk Perspectives* 3(4):146–70.

Kaufman, George G., and Kenneth E. Scott. 2003. “What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?” *Independent Review* 7(3):371–91.

Knight, Richard, and Jason R. C. Nurse. 2020. “A Framework for Effective Corporate Communication after Cyber Security Incidents.” *Computers and Security* 99:102036. doi: 10.1016/j.cose.2020.102036.

Kopp, Emanuel, Lincoln Kaffenberger, and Christopher Wilson. 2017. “Cyber Risk, Market Failures, and Financial Stability.” *IMF Working Papers* 17(185). Retrieved August 13, 2021 (https://www.imf.org/-/media/Files/Publications/WP/2017/wp17185.ashx).

Luhmann, N. 1979. *Trust and Power. Wiley.*

MacLiam, Juliette Kathryn. 2007. “A Conceptual Model of Crisis Communication with the Media: A Case Study of the Financial Sector.” *Dissertation Abstracts International Section A: Humanities and Social Sciences* 68(5-A):1718.

Maurer, Tim, and Arthur Nelson. 2020. “International Strategy to Better Protect the Financial System Against Cyber Threats.” Retrieved August 9, 2021 (https://carnegieendowment.org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105).

Mazur, Allan. 1984. “The Journalists and Technology: Reporting about Love Canal and Three Mile Island.” *Minerva* 22:45–66.

Merton, Robert C., and Zvie Bodie. 1995. “A Conceptual Framework for Analyzing the Financial Environment.” in *In The Global Financial System: A Functional Perspective*.

Muralikrishna, Iyyanki v., and Valli Manickam. 2017. “Environmental Risk Assessment.” Pp. 135–52 in *Environmental Management: Science and Engineering for Industry*. Butterworth-Heinemann.

National Cyber Security Centre. 2021. “Weekly Threat Reports.” Retrieved August 9, 2021 (https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc).

National Institute of Standards and Technology. 2018. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.” Retrieved August 8, 2021 (http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

Office of Financial Research. 2017. “Cybersecurity and Financial Stability: Risks and Resilience.” *OFR Viewpoint Papers*. Retrieved July 24, 2021 (https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf).

Renn, Ortwin. 1991. *Risk Communication and the Social Amplification of Risk*. Dordrecht: Springer.

Renn, Ortwin, William J. Burns, Jeanne X. Kasperson, Roger E. Kasperson, and Paul Slovic. 1992. “The Social Amplification of Risk: Theoretical Foundations and Empirical Applications.” *Journal of Social Issues* 48(4):137–60.

Renn, Ortwin, and Debra Levine. 1991. “Credibility and Trust in Risk Communication.” Pp. 175–217 in *Communicating Risks to the Public*. Dordrecht: Springer.

Reuters. 2016. “SWIFT Says Commercial Bank Hit by Malware Attack like $81M Bangladesh Hack.” Retrieved August 8, 2021 (https://www.cnbc.com/2016/05/12/swift-says-commercial-bank-hit-by-malware-attack-like-81m-bangladesh-hack.html).

Reynolds, Barbara, and Matthew W. Seeger. 2005. “Crisis and Emergency Risk Communication as an Integrative Model.” *Journal of Health Communication* 10(1):43–55. doi: 10.1080/10810730590904571.

Rosa, Eugene A. 2003. “The Logical Structure of the Social Amplification of Risk Framework (SARF): Aferatheoretical Foundations and Policy Implications.” Pp. 47–79 in *The Social Amplification of Risk*. Cambridge University Press.

Saridakis, George, Vladlena Benson, Jean Noel Ezingeard, and Hemamali Tennakoon. 2016. “Individual Information Security, User Behaviour and Cyber Victimisation: An Empirical Study of Social Networking Users.” *Technological Forecasting and Social Change* 102:320–30. doi: 10.1016/j.techfore.2015.08.012.

van Schaik, Paul, Debora Jeske, Joseph Onibokun, Lynne Coventry, Jurjen Jansen, and Petko Kusev. 2017. “Risk Perceptions of Cyber-Security and Precautionary Behaviour.” *Computers in Human Behavior* 75:547–59. doi: 10.1016/j.chb.2017.05.038.

Schmidt, Reinhard H., and Marcel Tyrell. 2005. “What Constitutes a Financial System in General and the German Financial System in Particular?” in *The German Financial System*.

ScienceDirect. 2021. “Risk Communication - an Overview.” Retrieved August 18, 2021 (https://www.sciencedirect.com/topics/earth-and-planetary-sciences/risk-communication).

Sellnow, Deanna D., Derek R. Lane, Timothy L. Sellnow, and Robert S. Littlefield. 2017. “The IDEA Model as a Best Practice for Effective Instructional Risk and Crisis Communication.” *Communication Studies* 68(5):552–67. doi: 10.1080/10510974.2017.1375535.

Siegrist, Michael. 2021. “Trust and Risk Perception: A Critical Review of the Literature.” *Risk Analysis* 41(3):480–90. doi: 10.1111/risa.13325.

Slabbert, Yolandi, and Rachel Barker. 2012. “Beyond Reactive Crisis Communication with the Media. An Integrated Crisis Communication Framework.” P. 68 in *ICCMTD-2012*.

Slovic, Paul. 2016. “Understanding Perceived Risk.” *Environment* 58(1):25–29. doi: 10.1080/00139157.2016.1112169.

Slovic, Paul, Sarah Lichtenstein, and Baruch Fischhoff. 1984. “Modeling the Societal Impact of Fatal Accidents.” *Management Science* 30(4):464–74. doi: 10.1287/MNSC.30.4.464.

Slovic, Paul, and Elke U. Weber. 2013. “Perception of Risk Posed by Extreme Events.” in *Regulation of Toxic Substances and Hazardous Waste*, edited by Applegate, Gabba, and LaitosSachs. Foundation Press.

Smillie, L., and A. Blissett. 2010. “Viewpoint: A Model for Developing Risk Communication Strategy.” *Journal of Risk Research* 13(1):115–34. doi: 10.1080/13669870903503655.

The European Parliament and the Council. 2010. “Regulation (EU) No 1092/2010.” Retrieved September 8, 2021 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010R1092&from=EN).

The European Parliament and the Council. 2016a. “Directive (EU) 2016/1148.” Retrieved August 8, 2021 (https://eur-lex.europa.eu/eli/dir/2016/1148/oj).

The European Parliament and the Council. 2016b. “Regulation (EU) 2016/679.” Retrieved August 9, 2021 (https://eur-lex.europa.eu/eli/reg/2016/679/oj).

The White House. 2013. “Executive Order - Improving Critical Infrastructure Cybersecurity.” Retrieved August 8, 2021 (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity).

Vieira, Ricardo. 2016. “Risk Management : Principles for the Definition of Viewpoints and Views.” Lisboa.

World Bank Group. 2020. “Financial Sector’s Cybersecurity: A Regulatory Digest.” Retrieved August 9, 2021 (https://thedocs.worldbank.org/en/doc/361881595872293851-0130022020/original/CybersecDigestv5Jul2020FINAL.pdf).

Xu, Wei, Finbarr Murphy, Xian Xu, and Wenpeng Xing. 2021. “Dynamic Communication and Perception of Cyber Risk: Evidence from Big Data in Media.” *Computers in Human Behavior* 122:106851. doi: 10.1016/j.chb.2021.106851.

Appendix - List of the data corpus news articles

Table 28 comprises a list of all the analysed news articles and indicates which social amplification factors were found in each article. The following acronyms are used:

- **EE:** Extent of risk exposure
- **DR:** Dread risk factor
- **UR:** Unknown risk factor
- **DI:** Dramatization of information
- **CI:** Controversy of information
- **SD:** Social distrust of responsible institutions
- **St:** Stigmatization

Table 28 - News articles and corresponding social amplification factors

Article ID	URL	EE	DR	UR	DI	CI	SD	St
1	https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html	x					x	
2	https://www.cnbc.com/2017/09/07/equifax-cyberattack-three-executives-sold-shares-worth-nearly-2-million-days-after-data-breach.html	x					x	
3	https://www.cnbc.com/2017/09/08/equifax-breach-congresswoman-waters-calls-for-credit-reporting-reform.html	x					x	
4	https://www.cnbc.com/2017/09/08/equifax-plunges-as-breach-will-cost-company-hundreds-of-millions.html	x					x	
5	https://www.cnbc.com/2017/09/08/equifax-response-to-data-breach-leaves-many-consumers-confused.html	x	x	x			x	
6	https://www.cnbc.com/2017/09/08/equifax-security-exec-john-kelley-earned-2-point-8-million-in-2016.html	x						
7	https://www.cnbc.com/2017/09/08/equifax-tweets-happy-friday-after-security-breach.html	x					x	
8	https://www.cnbc.com/2017/09/08/house-panel-will-hold-hearing-on-huge-equifax-data-breach.html	x	x					
9	https://www.cnbc.com/2017/09/08/how-to-protect-yourself-after-the-equifax-data-breach.html	x	x	x			x	
10	https://www.cnbc.com/2017/09/08/massive-equifax-cyberattack-triggers-class-action-lawsuit.html	x					x	
11	https://www.cnbc.com/2017/09/08/new-york-attorney-general-launches-investigation-into-equifax-breach.html	x						
12	https://www.cnbc.com/2017/09/08/suspect-trading-in-equifax-options-before-breach-might-have-generated-millions-in-profit.html	x					x	
13	https://www.cnbc.com/2017/09/08/were-you-affected-by-the-equifax-data-breach-one-click-could-cost-you-your-rights-in-court.html	x	x				x	
14	https://www.cnbc.com/2017/09/11/equifax-tumbles-nearly-8-percent-after-data-breach.html	x					x	
15	https://www.cnbc.com/2017/09/11/senate-finance-committee-wants-to-know-who-knew-what-and-when-at-equifax.html	x					x	
16	https://www.cnbc.com/2017/09/12/equifax-breach-may-push-investors-to-ask-tough-cybersecurity-questions.html	x					x	
17	https://www.cnbc.com/2017/09/12/how-to-prepare-for-the-next-equifax-type-data-theft.html	x	x	x				x
18	https://www.cnbc.com/2017/09/12/in-usa-today-op-ed-equifax-ceo-richard-f-smith-says-we-will-make-changes.html	x					x	
19	https://www.cnbc.com/2017/09/12/mnuchin-avoiding-another-equifax-like-breach-is-not-something-corporations-can-do-alone.html	x	x				x	x
20	https://www.cnbc.com/2017/09/12/senators-seek-answers-on-equifax-breach-including-details-on-stock-sales.html	x					x	
21	https://www.cnbc.com/2017/09/13/equifax-ceo-richard-smith-to-testify-before-house.html	x			x		x	
22	https://www.cnbc.com/2017/09/13/equifax-shares-sink-9-percent-as-massachusetts-prepares-lawsuit-over-breach.html	x					x	

Article ID	URL	EE	DR	UR	DI	CI	SD	St
23	https://www.cnbc.com/2017/09/13/equifax-waives-credit-lock-fees-for-consumers-amid-criticism.html	x	x					
24	https://www.cnbc.com/2017/09/13/heres-what-went-wrong-for-equifax-in-those-first-48-hours-commentary.html	x		x	x		x	
25	https://www.cnbc.com/2017/09/13/us-senator-on-equifax-hack-somebody-needs-to-go-to-jail.html	x					x	
26	https://www.cnbc.com/2017/09/14/consumers-but-not-executives-may-pay-for-equifax-failings.html	x	x				x	
27	https://www.cnbc.com/2017/09/14/cramer-equifax-ceo-should-be-fired-today-after-data-breach-fallout.html	x						
28	https://www.cnbc.com/2017/09/14/equifax-says-web-server-vulnerability-led-to-hack.html	x						
29	https://www.cnbc.com/2017/09/14/equifax-tumbles-as-ftc-confirms-investigation-into-breach.html	x					x	
30	https://www.cnbc.com/2017/09/14/equifax-used-admin-for-the-login-and-password-of-a-non-us-database.html	x		x			x	
31	https://www.cnbc.com/2017/09/14/equifax-will-not-survive-fallout-from-massive-breach-says-technology-attorney.html	x			x			
32	https://www.cnbc.com/2017/09/14/house-equifax-probe-may-result-in-more-regulation-congressman.html	x					x	
33	https://www.cnbc.com/2017/09/14/social-capital-ceo-equifax-data-breach-has-probably-happened-before.html	x						
34	https://www.cnbc.com/2017/09/15/cramer-says-equifax-data-is-the-holy-grail-of-what-bad-guys-want.html	x			x		x	
35	https://www.cnbc.com/2017/09/15/equifax-security-and-information-executives-to-retire-dj-reports.html	x						
36	https://www.cnbc.com/2017/09/15/heres-what-it-costs-to-freeze-your-credit-after-equifax-breach.html	x	x					
37	https://www.cnbc.com/2017/09/15/senator-warren-introduces-equifax-bill-launches-industry-probe.html	x					x	
38	https://www.cnbc.com/2017/09/18/equifax-acknowledges-second-security-incident-march.html	x				x	x	
39	https://www.cnbc.com/2017/09/18/equifax-aside-consumers-may-never-get-to-easily-sue-financial-firms.html	x					x	
40	https://www.cnbc.com/2017/09/18/equifax-should-stop-collecting-monitoring-fees-says-conn-ag.html	x	x				x	
41	https://www.cnbc.com/2017/09/18/questions-still-remain-about-equifaxs-actions-dc-attorney-general.html	x						
42	https://www.cnbc.com/2017/09/18/short-seller-carson-block-personally-sues-equifax-over-cyberbreach.html	x	x					
43	https://www.cnbc.com/2017/09/18/trading-by-equifax-execs-under-federal-scrutiny-report-says.html	x					x	
44	https://www.cnbc.com/2017/09/19/cramer-makes-a-new-addition-to-the-mad-money-wall-of-shame.html	x			x		x	
45	https://www.cnbc.com/2017/09/19/massachusetts-equifax-hack-exposed-more-than-half-state-to-risk.html	x					x	
46	https://www.cnbc.com/2017/09/20/cramer-sen-elizabeth-warren-is-right-on-equifax-data-breach.html	x	x				x	
47	https://www.cnbc.com/2017/09/20/cybersecurity-lessons-from-equifax-data-breach--commentary.html	x	x				x	
48	https://www.cnbc.com/2017/09/20/equifax-says-attacker-interacted-with-server-on-march-10.html	x						
49	https://www.cnbc.com/2017/09/20/equifax-tweets-sent-breach-victims-to-phishing-site.html	x		x			x	
50	https://www.cnbc.com/2017/09/20/house-finance-committee-seeks-information-on-equifax-options-activity.html	x					x	
51	https://www.cnbc.com/2017/09/21/equifax-data-breach-why-the-united-states-was-wide-open.html	x	x				x	
52	https://www.cnbc.com/2017/09/22/do-you-want-to-sue-equifax-over-the-cyberbreach-winning-a-lawsuit-may-not-be-so-easy.html	x		x			x	
53	https://www.cnbc.com/2017/09/25/credit-freeze-logjams-at-equifax-appear-to-be-easing.html	x	x	x				
54	https://www.cnbc.com/2017/09/26/after-equifax-hack-sec-jay-clatyon-we-are-constantly-under-attack.html	x					x	
55	https://www.cnbc.com/2017/09/26/equifax-ceo-easy-hacking-dump-changing-social-security-number-hard.html	x	x	x				
56	https://www.cnbc.com/2017/09/26/equifax-ceo-retires-following-an-epic-data-breach-affecting-143-million-people.html	x					x	
57	https://www.cnbc.com/2017/09/26/equifax-ceo-walks-away-with-18-million-pension-benefit.html	x	x				x	
58	https://www.cnbc.com/2017/09/26/equifax-dumped-ceo-to-get-ahead-of-brutal-grilling-from-sen-warren-next-week-analyst.html						x	

Article ID	URL	EE	DR	UR	DI	CI	SD	St
59	https://www.cnbc.com/2017/09/26/jim-cramer-likes-equifax-stock-more-now-that-ceo-richard-smith-is-gone.html	x					x	
60	https://www.cnbc.com/2017/09/26/sen-corker-ive-told-family-not-to-respond-to-equifax-emails.html	x						x
61	https://www.cnbc.com/2017/09/27/big-changes-coming-for-credit-firms-in-wake-of-equifax-hack-cfpb-director-says.html	x						
62	https://www.cnbc.com/2017/09/27/equifax-breach-san-francisco-city-attorney-dennis-herrera-lawsuit.html	x		x			x	
63	https://www.cnbc.com/2017/09/27/equifax-interim-ceo-paulino-do-rego-barros-jr-apologizes-on-hacking.html	x						
64	https://www.cnbc.com/2017/09/27/equifaxs-bad-methodology-is-worse-than-its-data-breach-commentary.html		x				x	
65	https://www.cnbc.com/2017/09/27/palo-alto-networks-ceo-talks-equifax-hack-dont-chase-the-ambulance.html	x						
66	https://www.cnbc.com/2017/09/27/the-real-problem-with-credit-reports-is-the-astounding-number-of-errors-equifax-commentary.html						x	
67	https://www.cnbc.com/2017/09/29/equifax-board-hired-law-firm-wilmerhale-to-review-early-august-stock-trades.html	x					x	
68	https://www.cnbc.com/2017/09/29/equifax-board-weighing-executive-pay-clawbacks-in-next-few-days-report.html							
69	https://www.cnbc.com/2017/09/29/equifax-investigators-looking-into-possible-insider-help-bloomberg-says.html	x	x				x	
70	https://www.cnbc.com/2017/10/02/equifax-2-point-5-million-more-consumers-may-be-affected-by-data-breach-than-originally-stated.html	x	x					
71	https://www.cnbc.com/2017/10/02/equifaxs-then-ceo-waited-three-weeks-to-inform-board-of-massive-data-breach-testimony-says.html	x					x	
72	https://www.cnbc.com/2017/10/03/equifax-ex-ceo-tells-congress-he-takes-full-responsibility-for-massive-data-hack.html	x	x				x	
73	https://www.cnbc.com/2017/10/03/former-equifax-ceo-to-testify-on-massive-data-breach.html	x					x	
74	https://www.cnbc.com/2017/10/03/former-equifax-chief-to-face-questions-from-us-congress-over-hack.html	x	x				x	
75	https://www.cnbc.com/2017/10/03/it-costs-consumers-4-point-1-billion-to-freeze-credit-reports.html	x	x	x	x			
76	https://www.cnbc.com/2017/10/04/cramer-3-equifax-executives-must-be-investigated-for-insider-trading.html	x	x				x	
77	https://www.cnbc.com/2017/10/04/equifax-breach-time-to-stop-using-social-security-numbers-commentary.html		x	x				
78	https://www.cnbc.com/2017/10/04/equifaxs-ex-ceo-faces-grilling-from-sen-elizabeth-warren.html	x					x	
79	https://www.cnbc.com/2017/10/04/equifaxs-smith-senate-hearing-on-breach.html	x					x	
80	https://www.cnbc.com/2017/10/04/someone-dressed-like-the-monopoly-guy-is-photobombing-the-senates-equifax-hearing.html	x					x	
81	https://www.cnbc.com/2017/10/05/equifax-calls-for-free-credit-locks-experians-reply-nope.html	x						
82	https://www.cnbc.com/2017/10/05/watch-former-equifax-ceo-richard-smith-face-congress.html	x						
83	https://www.cnbc.com/2017/10/11/despite-equifax-breach-consumers-doing-little-to-guard-against-fraud.html	x		x				
84	https://www.cnbc.com/2017/10/12/equifax-shares-drop-nearly-3-percent-after-new-cyber-breach.html	x	x				x	
85	https://www.cnbc.com/2017/10/13/rep-patrick-mchenry-wants-credit-bureaus-to-stop-using-social-security-numbers-by-2020.html	x	x				x	
86	https://www.cnbc.com/2017/10/24/uk-financial-watchdog-investigates-equifax-hacking.html	x						
87	https://www.cnbc.com/2017/11/03/equifax-special-committee-says-executive-stock-sales-were-in-the-clear.html	x					x	
88	https://www.cnbc.com/2017/11/08/marissa-mayer-equifax-ceo-testify-before-senate-commerce-committee.html	x	x				x	
89	https://www.cnbc.com/2017/11/08/watch-yahoos-marissa-mayer-equifax-ceo-testify-before-senators.html	x						
90	https://www.cnbc.com/2017/11/10/equifax-executives-forego-annual-bonuses.html	x						
91	https://www.cnbc.com/2018/01/29/equifax-extends-free-credit-freezes-to-june-30.html	x	x	x				
92	https://www.cnbc.com/2018/02/05/us-consumer-protection-official-puts-equifax-probe-on-ice-sources.html	x					x	
93	https://www.cnbc.com/2018/02/09/shares-of-equifax-dive-because-data-breach-was-reportedly-worst-than-everyone-thought.html	x	x				x	
94	https://www.cnbc.com/2018/02/26/half-of-adults-have-not-checked-their-credit-since-equifax-breach.html	x	x	x				

Article ID	URL	EE	DR	UR	DI	CI	SD	St
95	https://www.cnbc.com/2018/03/08/senate-banking-bill-would-make-credit-freezes-free.html	x	x					
96	https://www.cnbc.com/2018/03/10/in-the-wake-of-the-equifax-data-breach-consumers-more-at-risk.html	x	x		x			
97	https://www.cnbc.com/2018/03/14/former-equifax-executive-charged-with-insider-trading-ahead-of-data-breach.html	x					x	
98	https://www.cnbc.com/2018/04/02/equifax-sends-some-consumers-notification-letters-with-incorrect-data.html	x	x				x	
99	https://www.cnbc.com/2018/04/05/massachusetts-can-sue-equifax-over-data-breach-judge-rules.html	x					x	
100	https://www.cnbc.com/2018/06/08/these-five-states-have-the-worst-data-security-practices-in-the-country-.html	x						
101	https://www.cnbc.com/2018/06/27/equifax-breach-consent-order-issued.html	x	x				x	
102	https://www.cnbc.com/2018/06/28/former-equifax-software-development-manager-charged-with-insider-tradi.html	x					x	
103	https://www.cnbc.com/2018/07/03/since-the-equifax-hack-last-year-cyber-security-stocks-have-quietly-o.html	x						
104	https://www.cnbc.com/2018/09/07/equifax-anniverary.html	x	x	x	x		x	
105	https://www.cnbc.com/2018/09/20/free-credit-freezes-now-in-effect.html	x						
106	https://www.cnbc.com/2018/09/21/credit-freezes-are-now-free-theres-one-case-you-should-do-it.html	x						
107	https://www.cnbc.com/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html							
108	https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html	x	x	x	x			
109	https://www.cnbc.com/2019/02/27/american-consumer-credit-rating-system-is-broken.html	x	x	x			x	
110	https://www.cnbc.com/2019/03/07/equifax-marriott-ceos-testify-in-senate-over-data-breaches.html	x	x				x	
111	https://www.cnbc.com/2019/03/07/senators-will-grill-equifax-marriott-executives-on-data-breaches.html	x	x				x	
112	https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html	x	x					
113	https://www.cnbc.com/2019/07/20/equifax-reportedly-nears-700-million-settlement-of-data-breach-probes.html	x						
114	https://www.cnbc.com/2019/07/22/equifax-ceo-says-company-still-faces-cyberattacks-every-day.html	x		x			x	
115	https://www.cnbc.com/2019/07/22/equifax-deal-includes-free-credit-reports-but-that-wont-prevent-fraud.html	x	x	x				
116	https://www.cnbc.com/2019/07/22/equifax-reveals-details-of-671-million-settlement.html	x	x	x			x	
117	https://www.cnbc.com/2019/07/22/equifax-to-pay-up-to-650-million-in-data-breach-settlement.html	x	x	x			x	
118	https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html	x					x	
119	https://www.cnbc.com/2019/07/25/how-to-claim-your-compensation-from-the-equifax-data-breach-settlement.html	x	x					
120	https://www.cnbc.com/2019/07/26/you-could-make-125-by-filling-out-this-equifax-data-breach-claim-form.html	x						
121	https://www.cnbc.com/2019/07/29/is-it-better-to-get-125-or-free-credit-monitoring-from-equifax.html	x						
122	https://www.cnbc.com/2019/07/30/equifax-data-breach-step-by-step-guide-on-how-to-file-a-claim.html	x	x					
123	https://www.cnbc.com/2019/07/31/ftc-equifax-might-run-out-of-cash-so-please-take-monitoring.html	x						
124	https://www.cnbc.com/2019/08/14/elizabeth-warren-calls-for-inquiry-into-ftc-over-equifax-settlement.html	x					x	
125	https://www.cnbc.com/2019/09/03/half-of-hacked-companies-say-they-struggle-to-attract-new-customers.html							
126	https://www.cnbc.com/2019/09/06/two-years-after-equifax-breach-consumers-still-vulnerable-to-id-theft.html	x						
127	https://www.cnbc.com/2019/09/09/equifax-adds-extra-step-to-claim-125-damage-award.html	x	x					
128	https://www.cnbc.com/2019/09/09/equifax-settlement-you-need-to-update-your-claim-to-get-125.html	x	x					
129	https://www.cnbc.com/2019/12/19/court-awards-80-million-to-consumer-attorneys-in-equifax-case.html	x	x				x	
130	https://www.cnbc.com/2020/02/10/consumers-cant-be-complacent-even-if-hackers-didnt-use-equifax-data.html	x	x	x			x	

Article ID	URL	EE	DR	UR	DI	CI	SD	St
131	https://www.cnbc.com/2020/02/10/equifax-hack-justice-department-indicts-4-chinese-military-members.html	x	x				x	
132	https://www.cnbc.com/2019/07/30/capital-one-breach-customer-records-social-security-numbers.html	x						
133	https://www.cnbc.com/2019/07/30/capital-one-data-breach-5-things-to-do-if-you-were-affected.html	x	x					
134	https://www.cnbc.com/2019/07/30/capital-one-hack-allegations-describe-a-rare-insider-threat-case.html	x	x		x		x	
135	https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html	x						
136	https://www.cnbc.com/2019/07/30/how-to-protect-yourself-from-fraud-in-wake-of-capital-one-data-breach.html	x						
137	https://www.cnbc.com/2019/07/30/how-to-tell-if-you-were-affected-by-the-capital-one-breach.html	x						
138	https://www.cnbc.com/2019/07/30/jamie-dimons-worst-fears-for-banks-realized-with-capital-one-hack.html	x	x		x		x	
139	https://www.cnbc.com/2019/07/30/paige-thompson-alleged-capital-one-hacker-stole-100-million-peoples-data.html	x					x	
140	https://www.cnbc.com/2019/08/01/atm-hack-attacks-caught-on-video.html	x						
141	https://www.cnbc.com/2019/08/01/trump-allies-open-congressional-inquiry-into-capital-one.html	x						
142	https://www.cnbc.com/2019/08/16/stocks-making-the-biggest-moves-premarket-deere-nvidia-ge-facebook-capital-one-more.html						x	
143	https://www.cnbc.com/2019/09/26/heres-everything-cyber-criminals-can-do-if-they-steal-your-credit-card.html		x					
144	https://www.cnbc.com/2019/10/24/elizabeth-warrens-move-on-amazon-could-be-a-precursor-to-sifmu-status.html	x					x	
145	https://www.cnbc.com/2019/10/24/senators-urge-investigation-of-amazons-role-in-capital-one-hack.html	x					x	
146	https://www.cnbc.com/2019/12/17/the-5-biggest-data-hacks-of-2019.html	x						
147	https://www.cnbc.com/2019/07/30/capital-one-shares-dive-after-data-breach-affecting-100-million.html	x					x	
148	https://www.cnbc.com/2019/07/31/akamai-ceo-data-breaches-like-capital-one-show-need-for-zero-trust.html	x	x					