Lessons from the Equifax and Capital One Data Breaches on Social Amplification of Risk

Review of Integrative Business & Economics Research

Danilo Dias*
INESC-ID (PT)

José Borbinha
INESC-ID (PT), IST, Universidade de Lisboa (PT)

Pedro Mendonça
Centro Nacional de Cibersegurança (PT), Escola Superior de Comunicação Social (PT), UNIDCOM-IADE (PT)

ABSTRACT

Cyber incidents can halt critical economic functions or cause an extreme loss of confidence in the financial system. The prospect of reputational contagion events should be particularly considered by financial authorities 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: Cyber risk; systemic risk; social amplification of risk; crisis communication.

Received 22 October 2021 | Revised 18 January 2022 | Accepted 13 February 2022.

1 INTRODUCTION

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 profound consequences to the real economy. Therefore, financial authorities pursue the conservation of financial stability and the mitigation of systemic risk.

Traditional threats to financial institutions include market, credit, and operational risks (Siahaan & Anantadjaya, 2013). 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

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

financial stability, also known as transmission channels (European Systemic Risk Board, 2020; Healey et al., 2021; Office of Financial Research, 2017). 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).

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.

1.1 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 significant 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 & 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.

1.2 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.

First, it is important to consider 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.

A second key point is to understand what the relevant social amplification factors are 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, a fourth 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.

Therefore, this work proposes the following research questions, in relation to when a major data breach affects a financial services institution:

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

- **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?

1.3 RESEARCH APPROACH

The Equifax data breach announced in September 2017 and the Capital One data breach announced in July 2019 were chosen as case studies.

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 & 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.

1.4 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.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

1.5 DOCUMENT STRUCTURE

This document follows with the examination of research dedicated to risk perception and the concept of social amplification of risk (Section 2) and discusses studies about risk and crisis communication (Section 3).

Section 4 describes the data analysis method used in this research, including the data collection, the codebook development, and the coding and analysis procedures. Sections 5 and 6 report the analysis results of the two selected cases studies. In Section 7, this work discusses the results and answers the research questions.

Finally, Section 8 presents the conclusions, limitations, and suggestions for future work.

2 RISK PERCEPTION AND SOCIAL AMPLIFICATION OF RISK

Earlier studies on risk perception found that there were significant biases in people's perceptions of risks (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, such as the psychometric paradigm (Slovic and Weber 2002), which indicates fifteen risk characteristics, condensed into two higher-order factors: the "dread risk" factor is related to the properties of risk events that may arouse fear in individuals and society, while the "unknown risk" factor relates to characteristics that indicate uncertainty.

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 factors also contribute to perceived risk, and one relevant aspect is social trust. 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.

The way media portrays risk events are also the subject of several studies in the risk perception research field. 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 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).

The framework's components are presented in Figure 1.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

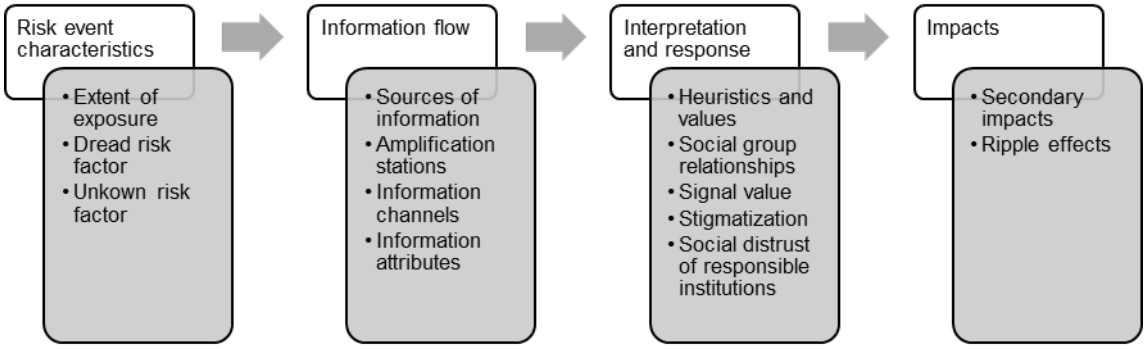


Figure 1 – SARF's components

SARF's components are useful to understand how an event with a limited initial impact may become a systemic crisis. Characteristics of the risk event such as newness, dread, and extent of risk exposure may psychologically affect people's risk perception. A potential decrease of social trust of financial services institutions and public agencies is an additional challenge. 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.

It is possible to link some of the specific characteristics of cyber risk identified by Bank for International Settlements and International Organization of Securities Commissions (2016), European Systemic Risk Board (2020), and Healey et al. (2018), with social amplification factors (Table 1). That is a plausible indication that major cyber incidents will be perceived as holding a high signal value risk by society.

Table 1 - 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

3 RISK AND CRISIS COMMUNICATION

When considering systemic reputational risk treatment options, two important research fields are risk communication and crisis 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).

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 et al., 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

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

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").

On the other hand, 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 & Holladay, 2002). These response strategies, in some cases, might be counterproductive to the financial authority's efforts to mitigate a systemic crisis.

Therefore, 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.

4 DATA ANALYSIS METHOD

To answer the research questions proposed in Subsection 1.2, this work used a directed content analysis approach (Hsieh & 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 having quite different consequences. Furthermore, the study selected a sole source of information for content analysis – the CNBC website. Although this approach has some limitations (see Section 9), it allows a coherent comparison between these two events concerning media coverage.

4.1 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 News. Then, keyword searching with the *googlesearch-python*[1] 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.

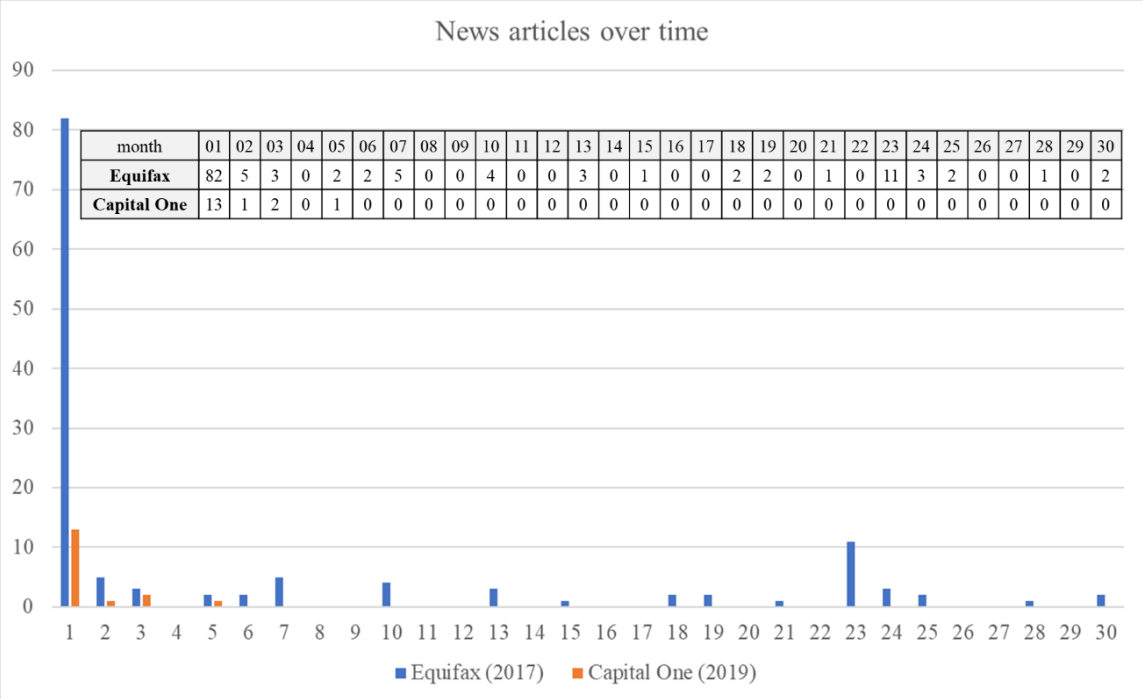
[1] https://pypi.org/project/googlesearch-python/

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

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

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.

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.



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

4.2 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 were selected from those described by SARF (Figure 1). The three factors from the risk event characteristics were 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

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

connotations – were used as codes ("volume of information" was also used in the analysis, but not for coding). From the "interpretation and response" factors, "stigmatization" and "social distrust of responsible institutions" were used for coding ("signal value" is implicitly used since it is closely related to the risk event characteristics). The remaining social amplification factors were 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.

The crisis communication strategies were based on SCCT, which proposes eleven response strategies and groups them into four groups (Coombs, 2007; Coombs & Holladay, 2002):

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

4.3 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.

5 EQUIFAX BREACH ANALYSIS

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

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

Table 2 shows the number of news articles that mention each factor distributed by when they were published.

Table 2 - 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

We realize that 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 3):

- 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 3 – 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 4):

- Social distrust of responsible institutions
- Stigmatization of the company

Table 4 – 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

6 CAPITAL ONE BREACH ANALYSIS

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

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

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

Table 5 shows the number of news articles that mention each factor distributed by the day of publishing.

Table 5 – 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 6):

- 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 6 – 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 7):

- Social distrust of responsible institutions

Stigmatization was not displayed in the analysed articles.

Table 7 – 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

7 DISCUSSION OF RESULTS

This section 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.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

7.1 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 8).

Table 8 - 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, as follows.

7.1.1 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 9).

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 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 9).

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

Table 9 – 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%)	-

7.1.2 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 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.

7.1.3 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 10).

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

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

risk" factors, which possibly contributed to maintaining a high perception of the risk and the interest of the audience in the subject (Table 10).

Table 10 – 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 11 and Table 12 show some of the potential relations between episodes, identified ripple effects, and amplification factors, for the Equifax and Capital One breaches.

Table 11 - 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 congressperson 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 congressperson 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)

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

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 returned 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 12 - Links 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	(medium-term) Senators ask the Federal Trade Commission to explore the role of Amazon in the breach.	Social distrust (incompetence)

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

against the attack that caused the breach.		
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)

7.1.4 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 13 shows the crisis communication strategies used by both companies over time.

Table 13 - 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)	-

7.1.5 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.

7.2 ANSWERING THE RESEARCH QUESTIONS

Based on the presented findings of the cross-case analysis, we propose now the answers to the research questions listed in Subsection 1.2. They were examined in the analysis of the collected data, i.e., these answers are therefore valid for the two cases studied.

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 explain 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.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

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 attenuating 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 9):

- 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 10).

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 11), while the Capital One breach had few occurrences (Table 12). 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.

8 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,

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

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 along with the "rebuild" strategy may be important when dealing with a cyber crisis.

8.1 CONCLUSIONS

Concluding, when a major data breach affects a financial services institution:

- **RQ1: Which risk event characteristics relate to sustained media coverage?** 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?** 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?** 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?** The use of the diminish strategy along with the rebuild 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.

8.2 LIMITATIONS AND FUTURE WORK

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.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

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.

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.
The dataset collected for this work is freely available upon request to the first author.

ACKNOWLEDGEMENTS

This work was supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UIDB/50021/2020 and by the European Commission program H2020 under the grant agreement 822404 (project QualiChain).

This paper is a revised version of the communication, by the same authors, with the title "Cybersecurity and Social Amplification of Risk in Financial Systems: Lessons Learned from the Equifax and Capital One Data Breaches" published in the proceedings of the SIBR 2022 - Conference on Interdisciplinary Business Economics Research, January 6th - 7th, 2022, Tokyo, which communicates the results of the the MSc dissertation, by the first author, with the title "Cybersecurity and Social Amplification of Risk in Financial Systems", submitted in September 2021 to the Instituto Superior Técnico, Universidade de Lisboa, in the scope of the MSc program "Mestrado Bolonha em Segurança de Informação e Direito no Ciberespaço".

REFERENCES

[1] Bank for International Settlements, & International Organization of Securities Commissions. (2016). *CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures*. https://www.bis.org/cpmi/publ/d146.pdf

[2] Benoit, W. L. (1997). Image Repair Discourse and Crisis Communication. *Public Relations Review*, *23*(2), 177–186.

[3] Born, B., Ehrmann, M., & Fratzscher, M. (2014). Central bank communication on financial stability. *Economic Journal*, *124*(577), 701–734. https://doi.org/10.1111/ecoj.12039

[4] Consumer Financial Protection Bureau. (2021). *List of Consumer Reporting Companies*. https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2021-06.pdf

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

[5] Consumer News and Business Channel. (2021). *International Business, World News & Global Stock Market Analysis*. https://www.cnbc.com/world/?region=world
[6] Coombs, W. T. (2007). Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory. *Corporate Reputation Review*, *10*(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049
[7] Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets: Initial Tests of the Situational Crisis Communication Theory. *Management Communication Quarterly*, *16*(2), 165–186. https://doi.org/10.1177/089331802237233
[8] Cybersecurity and Infrastructure Security Agency. (2021). *Analysis Reports*. https://us-cert.cisa.gov/ncas/analysis-reports
[9] European Systemic Risk Board. (2020). *Systemic Cyber Risk*. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf
[10] European Union Agency for Cybersecurity. (2020). *ENISA Threat Landscape - 2020*. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
[11] Federal Financial Institutions Examination Council. (2021). *Large Holding Companies*. https://www.ffiec.gov/npw/Institution/TopHoldings
[12] Fischhoff, B., Hohenemser, C., Kasperson, R. E., & Kates, R. W. (1978). Handling hazards can hazard management be improved? *Environment*, *20*(7), 16–37. https://doi.org/10.1080/00139157.1978.9928700
[13] Healey, J., Mosser, P., Rosen, K., & Tache, A. (2018). *The Future of Financial Stability and Cyber Risk*. Brookings Institution. https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/
[14] Healey, J., Mosser, P., Rosen, K., & Wortman, A. (2021). The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability. *Journal of Financial Transformation*, *53*, 94–107. https://ideas.repec.org/a/ris/jofitr/1670.html
[15] Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687
[16] Jonsson, S., & Söderberg, I.-L. (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), 763–779. https://doi.org/10.1080/13669877.2016.1247375
[17] Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. X., & Ratick, S. (1988). The Social Amplification of Risk: A Conceptual Framework. *Risk Analysis*, *8*(2), 177–187. https://doi.org/10.1111/J.1539-6924.1988.TB01168.X
[18] Kaszowska, J., & Santos, J. L. (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), 146–170.
[19] National Cyber Security Centre. (2021). *Weekly threat reports*. https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)

[20] Office of Financial Research. (2017). *Cybersecurity and Financial Stability: Risks and Resilience*. OFR Viewpoint Papers. https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf
[21] Siahaan, P. L. E., & Anantadjaya, S. P. (2013). Measuring Risk: Is It Necessary? An Empirical Study in Indonesian Banks. *Review of Integrative Business and Economics Research*, *2*(2), 8–21.
[22] Slovic, P., & Weber, E. U. (2013). Perception of Risk Posed by Extreme Events. In Applegate, Gabba, & LaitosSachs (Eds.), *Regulation of Toxic Substances and Hazardous Waste* (2nd ed.). Foundation Press.
[23] van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038
[24] Xu, W., Murphy, F., Xu, X., & Xing, W. (2021). Dynamic communication and perception of cyber risk: Evidence from big data in media. *Computers in Human Behavior*, *122*, 106851. https://doi.org/10.1016/j.chb.2021.106851

ISSN: 2304-1013 (Online); 2304-1269 (CDROM); 2414-6722 (Print)