Cybersecurity and Social Amplification of Risk in Financial Systems

Danilo Dias

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.

1 INTRODUCTION

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 (European Systemic Risk Board 2020).

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 (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 a reputational contagion event affecting 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 event in the financial system and cause a systemic crisis.

2 PROBLEM DEFINITION

Systemic cyber risk caused by a reputational contagion event brings new challenges to financial stability risk analysis, since:

- Typical risk analysis strategies, such as estimating the likelihood of events and the nature and magnitude of their consequences, are not suitable 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.
- 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).
- 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. For that, it is critical to understand the factors that may amplify risk perception during a cyber crisis, such as:

- The level of media coverage, since a high volume of news stories published by media outlets is correlated with the amplification of perceived risk.
- 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.
- 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.
- 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 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?

3 RESEARCH APPROACH

To support this investigation, two cyber events were chosen as case studies: the Equifax data breach announced in September 2017 and the Capital One data breach announced in July 2019. 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 news 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, with existing literature and theory used to create a structured codebook prior to the start of coding (Hsieh and Shannon 2005). 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 chapter discusses the analysis results of the two selected case studies.

4 DISCUSSION OF RESULTS

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 1). This work argues that the discrepancy of the impacts may be explained by the distinct degrees of social amplification factors.

Table 1 - 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)

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 2).

Table 2 – 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 2).

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 probably 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.

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 3).

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 3).

Table 3 – 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 4 and Table 5 show some of the potential relations between episodes, identified ripple effects, and amplification factors, for the Equifax and Capital One breaches.

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

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.

Table 4 - 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 5 - 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 6 - 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)	-

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 following answers to the research questions are indicated.

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 the 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.

5 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.

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, and denial-of-service attacks.
- 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.

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

BIBLIOGRAPHY

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).

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, 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.

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).

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/).

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.

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.