MEDIA FRAMING OF CYBERCRIME: IMPROVING VICTIMS’ REPORTING RATES

Lena Yuryna Connolly  
*Zayed University, lena.connolly@gmail.com*

Danica Čigoja Piper  
*Zayed University, danica.piper@zu.ac.ae*

Follow this and additional works at: [https://aisel.aisnet.org/ecis2022_rip](https://aisel.aisnet.org/ecis2022_rip)

**Recommended Citation**

[https://aisel.aisnet.org/ecis2022_rip/35](https://aisel.aisnet.org/ecis2022_rip/35)

This material is brought to you by the ECIS 2022 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2022 Research-in-Progress Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
MEDIA FRAMING OF CYBERCRIME: IMPROVING VICTIMS’ REPORTING RATES

Research in Progress

Lena Yuryna Connolly, Zayed University, Abu Dhabi, UAE, alena.connolly@zu.ac.ae
Danica Ćigoja Piper, Zayed University, Abu Dhabi, UAE, danica.paper@zu.ac.ae

Abstract

This research aims to explore news media reporting practices of cybercrime, specifically focusing on victim organizations. Drawing on the media framing theory, the intention of this study is to investigate frames that news media employs when reporting cybercrime. A basic premise of this work is that victims of cybercrime, organizations in particular, are reluctant to share information about cyber-attacks due to fear of being negatively represented by news media. This, in turn, discourages victims to be forthcoming with the information about attacks, weakening our defences against cybercrime. The ultimate purpose of this two-phased research is to develop a model for accurate cybercrime reporting for news media. In the first phase, victims of cybercrime (organizations) were interviewed to examine their perceptions about news media reporting of cyber incidents. The second phase will focus on examining frames that media outlets use to depict organizations that became victims of cybercrime.

Keywords: Cybercrime, News Media Reporting, Victim Organizations, Media Framing Theory.

1 Introduction

Cybercrime is on the rise (Bandler and Merzon, 2020). FBI (2020) reported 69% increase in cybercrime reporting in 2020 compared to 2019, estimating victims’ losses to $4.1 billion. Interpol (2020) further noted a substantial increase in criminal activities in cyberspace in 2020. Research on cybercrime, on the other hand, is still in a developing phase (Maimon and Louderback, 2019). In order to enhance our knowledge on the topic and develop measures to combat it, scholars argue that it is important to understand cybercrime victimisation (Connolly et al., 2020; Louderback and Antonaccio, 2017; Leukfeldt and Yar, 2016). Although new security breaches are reported on a daily basis and the excess of victims is overwhelming, research on cybercrime victimisation (where data is collected from actual, not hypothetical victims) is scarce (Connolly et al., 2020; Maimon and Louderback, 2019). This is in part due to cybercrime underreporting, a long-standing issue that has been widely addressed by researchers (Cheng et al., 2018; McMurdie, 2016) and professional bodies (ONS, 2020; ISACA, 2019), even though in some instances victims are required to report by law.

Organizations that become victims of cybercrime tend to conceal security incidents; and even if the breach becomes public knowledge, important details are not revealed (De Kimpe, 2020). The fear of negative publicity (Basuchoudhary and Searle, 2019; Fafinski et al., 2010) and subsequent adverse consequences for businesses (e.g., financial and reputational losses) remains a major barrier to information sharing (Connolly et al., 2021; Connolly and Lang, 2012; Cavusoglu et al., 2004). However, as cybercrime continues to hurt organizations and individuals around the globe, the need to converse with its victims is greater than ever before.

Skopik et al. (2016) highlighted the importance of platforms for cybersecurity information sharing, so relevant parties can acquire a thorough understanding of cyber-attack situations (e.g., discover covert cyber-attacks, issue early warnings, distribute threat intelligence data etc.) and protect their networks. Taking into consideration organizations’ reluctance to share information about cyber-attacks (Tounsi and Rais, 2018) and the harmful consequences of cybercrime underreporting (ONS, 2020; ISACA,
Media Framing of Cybercrime

2019; Cheng et al., 2018; McMurdie, 2016), there is a need to search for alternative platforms that have the ability to share cyber intelligence. Since news media has a social responsibility to bring attention to the issues that are important to the public (cybercrime being one such issue), it can be viewed as one such information sharing platform. In this sense, media outlets may partly address the underreporting conundrum. The messages though must be properly framed in order to achieve the desired outcome (Romero-Masters, 2021; De Brujin and Janssen, 2017). More specifically, De Brujin and Janssen (2017) emphasised the complexity of issues related to cybersecurity and argued that the public messages about cybersecurity should be considered with caution. They found that cybersecurity issues are commonly over-dramatised or over-simplified, which does not result in the anticipated effect, but rather leads to further neglect of cybersecurity by organizations and therefore increased cybercrime activities. In similar vain, Romero-Masters (2021) called for more studies on media framing of cybersecurity as the next viable step to address cybercrime.

Research demonstrates that media has the ability to restrict readers to either ‘opposing’ or ‘favouring’ views about the subject of the news (Afzal and Harun, 2020). One way the media may shape a public opinion is by framing issues in a distinct way. Framing, as a theory of mass communication, refers to how the media packages and presents information, shaping public opinion. To date, scholars investigated the media framing of various important issues, ranging from environmental like climate change (Barlie and Kimpatsiaris, 2020) to political like Ukrainian crisis of 2000-2001 (Baysha and Hallahan, 2004). Barlie and Kimpatsiaris (2020), for instance, reported on how environmental activists made use of the COVID-19 pandemic by employing frames like ‘humans are the biggest virus’ to bring public’s attention to the urgencies of climate change. Furthermore, Baysha and Hallahan (2004) found out that no Ukrainian media organization covered the country’s political crisis in an objective way. The study revealed that the two main patterns of framing were overt propaganda and hidden manipulation. Media used frames in a form of metaphors and depictions that exploited cultural values and previous political events to manipulate public. Arguably, media has the ability to form a public opinion about victims of cybercrime, portraying victims with either positive or negative frames.

A comprehensive literature review demonstrated that only a handful of research was conducted to investigate the news framing of cybercrime. Demata (2017), for instance, examined articles printed in 2011-2016 by two major British tabloids, namely Daily Mirror and The Sun, and found that cybercrime was framed as a source of social danger and fear. The discourse strategies in representing cybercrime were very similar to those employed in the representations of such ‘outgroups’ as immigrants and terrorists. Moreover, Imangaiazovaya (2020) studied cybercrime framing in Russian and English media texts and found that cyber-attacks are represented via frames of war, game, pandemic and crime. Furthermore, Guanah et al. (2020) investigated media framing of cybercrime in Nigeria and found framing tactics to be useful in eradicating it. Using a sample of university students, Ko and Won (2016) discovered that media framing has a direct impact on risk perceptions of cybercrime. Wall (2008) argued that while distortions of cybercrime by media reporting lead the public’s lust for sensation and shocking information, they also lead to unnecessary cyber fears. Syed (2019) investigated data breach frames used on Twitter platform in the aftermath of the incident on Home Depot and concluded that certain negative frames had an adverse impact on company’s reputation. Recognising that in some instances ineffective post-breach communication by victim organizations may lead to negative media coverage, Knight and Nurse (2020) developed a framework for effective corporate communication after cybersecurity incidents. Although the aforementioned works are important contributions to the pool of knowledge in the realm of cybercrime framing, no studies were found that suggested practices to improve cybercrime reporting by news media. This is important because victims’ unwillingness to share vital data hurts our ability to fight cybercrime.

The intention of this two-phased study is to investigate the issue of news media reporting of cybercrime incidents. In the first instance, nine victims of cybercrime (totalling to fourteen attacks) that made news headlines were interviewed. Results, presented later in this paper, demonstrated that most of victims associated their experience with media as negative and decided to be less forthcoming with details on cyber-attacks in the future. The aim of the next phase, which is currently ongoing, is to validate victims’ statements regarding the negative media coverage by examining articles from two most popular media
outlets in the UK, that is BBC online portal and The Guardian (Statista, 2020). Frames used to represent cybercrime victim organizations will be sought after. The fundamental purpose of this research is to develop a model that will educate news media on accurate reporting of cybercrime (GoWA, 2022; Čigoja Piper, 2018; Goering, 2015; Haller, 1995). Ultimately, this study is a step forward in encouraging victims to be more forthcoming with the information about attacks. Such information will help reduce cybercrime.

The paper is structured as follows:
Section 2 presents a theoretical framework that underpins this research study. Section 3 describes the research method employed in the first phase (including a sampling strategy and a data collection technique) and analysis of findings. This is followed by section 4 that focuses on the evaluation of trustworthiness of this study’s results. Section 5 outlines plans for the second phase of this study and completes this paper.

2 Theoretical Framework

Originated in 1950’s with the work of anthropologist Gregory Bateson, framing theory emerged with the notion of ‘framework’ “as a tool of the psyche that explains why people focus their attention of some stylized aspects of reality and not others” (Aruguete, 2020, p.1). Since then, the framing perspective has become a multi-disciplinary paradigm (Ardèvol-Abreu, 2015), receiving most attention in communication disciplines. In communication research, framing theory (i.e., commonly referred to as ‘news framing theory’ or ‘media framing theory’) posits that people’s perceptions are likely to be influenced when media messages are presented within certain frames (Senocak, 2017). In Entman’s (1993, p.52) words, “to frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described”. Similarly, D’Angelo (2019 p. 1) described “frame” as “individuals’ attempts to influence one other through linguistic and paralinguistic messages that define a situation, describe its attributes, and interpret its structures and rules”. Remarking on the variety of definitions of news frames in both theoretical and empirical contributions, De Vreese (2005, p. 53) simply defined ‘frame’ as “an emphasis in salience of different aspects of a topic”.

Framing theory is commonly used in the communication disciplines for two purposes: 1) to examine a media content (referred as ‘frame building’) and 2) to understand the interplay between media messages and public opinion (referred as ‘frame setting’) (De Vreese, 2005). Drawing on the notion that framing is a process, frame setting follows the frame building in this process (Scheufele, 1999). Frame building focuses on “how frames get established in societal discourse and how different frames compete for adoption by societal elites and journalists” (Scheufele, 1999, p. 55). The outcomes of the frame building process are the frames manifest in the text. Retorting to conundrum of frames’ origins, De Vreese (2005) argued that factors internal (e.g., editorial policies, news values) and external (e.g., elites and social movements) to journalism influence the structural qualities of news frames.

On the other hand, frame setting deals with the effects frames exert on audiences, which depends on individuals’ prior knowledge and predispositions (De Vreese, 2005). Although frames do not reach all people equally, their impact could be very powerful and somewhat universal (Tewksbury et al., 2000). As Tewksbury and Scheufele (2009, p. 53) noted, “news frames can exert a relatively substantial influence on citizens’ beliefs, attitudes, and behaviours”. Frame setting studies mainly divided into two dominant research streams, such as (1) an exploratory analysis of frames in media texts (e.g., Wessler and Rinke, 2014; Hardin and Simpson, 2007; Baysha and Hallahan, 2004), including critical discourse analysis (Budd et al., 2019; Čigoja Piper, 2018; Demata, 2017), and (2) the explanatory inquiries of the relationships between frames and audiences (e.g., Schemer, 2012; Igartua and Cheng, 2009; Tewksbury et al., 2000).

Scholars further suggested that framing involves an interplay between various types of frames in a text. Scheufele (1999), for instance, proposed to discern between ‘media’ frames and ‘individual’ frames.
The former is used by journalists to describe a particular issue, while the latter is “the set of knowledge a person (i.e., audience) has acquired about the issue, and it is used by him or her to evaluate and understand new information” (Tewksbury et al., 2000, p. 806). Scheufele (1999) argued that media frames can shape individual frames. Building on the notion that media frames alone may not be powerful enough to influence audience, Tewksbury et al. (2000, p. 806) introduced the concept of ‘advocate’ frames, which are “specific, careful constructed ways of interpreting the issue”. Therefore, media frames are defined as “news story telling formats”, while advocate frames – as “explanations and arguments intended to persuade”. Media frames, in turn, are influenced by journalist frames, which are shaped according to journalistic beliefs about the topics audiences prefer to read. Tewksbury et al. (2000, p. 806) further noted that “journalist frames may become problematic when they are highly stereotyped and uniform throughout news discourse”, corrupting the principle of objectivity. The event-centred stories (e.g., cybercrime incidents) are particularly susceptible to this bias.

Reporting on the devices that are used to create frames, Gamson and Lasch (1980) identified (1) framing devices (e.g., metaphors, catchphrases, exemplars, depictions, and visual images) that suggest a framework within which to view the issue; and (2) reasoning devices (e.g., roots, consequences, and appeal to principle) that provide justifications or reasons for general positions. Stone (2002) added to the list of devices synecdoche (i.e., a figure of speech in which a whole is represented by one of its parts and vice versa like ‘new wheels’ refers to a new car or ‘ask for her hand’ refers to asking a woman to marry) and numbers as a method of describing events by means of measurements, typically using either extremely large or small numbers to exaggerate the theme.

3 Research Method and Analysis of Findings

This study consists of two phases, and both are exploratory in nature. The first phase, in which data was collected as part of a bigger study on ransomware (Connolly et al., 2020; Connolly and Borrion, 2020; Connolly and Wall, 2019) has been already conducted. This can be considered as a preliminary investigation into cybercrime victims’ experiences with media. Most of victims described their interactions with media as negative and decided to be less forthcoming with information about cyber-attacks in the future. These preliminary results served as compelling grounds for the next phase (currently ongoing), where news media reporting practices on cybercrime are being investigated.

3.1 Phase 1: Sampling Strategy, Data Collection and Data Analysis

A purposeful sampling approach was employed to collect data in Phase 1. Cybercrime incidents (ransomware attacks) that were broadcasted by media were selected. Dozens of victim organizations were contacted via email or phone, but only ten public organizations replied and agreed to be interviewed in-person or via Skype (i.e., oversees respondents). One of the victims, however, had a very busy work schedule and was only able to communicate via email. Since questions about experiences with journalists and media required some probing, this organization was excluded from the sample. Nine interviewees shared data on fourteen cyber-attacks (some organizations were attacked more than once). Participants, IT/Security Managers and Executive Managers with an average professional experience of 17 years, were directly involved in responding to ransomware attacks. Table 1 outlines relevant information on victim organizations and interviewees. Participants were asked questions about their experiences with media.

<table>
<thead>
<tr>
<th>Organization alias</th>
<th>Industry; size; sector</th>
<th>Number of attacks</th>
<th>Interviewee position; experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>LawEnfJ</td>
<td>Law enforcement; small; public</td>
<td>1</td>
<td>IT/Security Manager; 13 years</td>
</tr>
<tr>
<td>GovSecJN</td>
<td>Government; large; public</td>
<td>1</td>
<td>IT/Security Manager; 9 years</td>
</tr>
<tr>
<td>GovSecJ</td>
<td>Government; large; public</td>
<td>4</td>
<td>IT/Security Manager; 9 years</td>
</tr>
<tr>
<td>EducInstF</td>
<td>Education; large; public</td>
<td>1</td>
<td>IT/Security Manager; 18 years</td>
</tr>
</tbody>
</table>
An inductive content analysis was used to analyze data (Bengtsson, 2016). Since data was not voluminous (due to the preliminary nature of this phase), the analysis was completed in three stages. First (decontextualization), the transcribed data was read several times to “obtain the sense of the whole, that is, to learn what is going on” (Bengtsson, 2016, p11) in order to break it into smaller meaning units. Further, codes were assigned to these units (Table 2). Second (categorization), categories were identified with aim to group the codes from the previous stage. Some data units fitted within the identified categories, others prompted the construction of additional categories. Some categories were deemed as irrelevant to the study objectives and subsequently were eliminated (Table 2). The final stage (compilation) involved data interpretation and write up, results of which are presented in the next several paragraphs.

3.2 Phase 1: Results

Several participants shared information about their negative experiences with media. IT/Security Managers from LawEnfJ and LocGovJN, for instance, acknowledged a harmful effect of media coverage on their reputation:

“The media gruesomely exaggerated the ransom amount [from three-digit figure to seven-digit figure; in fact, the ransom for the victim was around £300 per machine and only a handful of machines were infected]... This damaged our reputation because of adverse local and international coverage”. [LocGovJN, IT/Security Manager]

“Our reputation was affected to a degree. It is not fun waking up and reading about yourself in Ars Technica in this context [negative], especially if facts are not accurate... The attack was not as bad as it was presented in the article... So, yes, to some degree there was a hit to our reputation”. [LawEnfJ, IT/Security Manager]

IT/Security Manager from LocGovJN argued that exaggerated facts by media had a knock-on effect on their recovery process. Subsequently, the decision was made to vigorously filter all calls to the IT Department during future ongoing incidents and establish communication only with organizations that are trying to help (e.g., law enforcement):

“...And within half an hour [of media exposure], I had five police officers on the doorstep because they thought we were subject to an ongoing live fraud or bribery. And also, vendors, Security vendors then followed suit and printed information which was wrong and damaging to us. And that was disappointing actually because we expect security vendors to try and establish fact. And it just did not help because what the effect was – we were overloaded with different parties contacting us... Vendors and media, trying to get a hold of us, creating ‘communication Wild West’...They created almost their own denial-of-service... We were in the middle of a difficult recovery and this situation did not help us at all...We will have to rethink our communication strategy with the media in the future...At the least we will need to implement some switchboard to filter calls to our department and communicate only with organizations that are trying to help like law enforcement”. [LocGovJN, IT/Security Manager]

IT/Security Manager from LawEnfJ shared similar experience, which prompted them to make a decision to be less forthcoming with details on cyber-attacks with the media in the future:

“Excessive media attention hampered our recovery process because we were busy being pulled off to answer questions when we were actively trying to deal with the issue that was going on. It changed our attitude of how we would approach this in the future. I do not think we would be as forthcoming with that information, at least not directly to the press as we do right now”. [LawEnfJ, IT/Security Manager]
Furthermore, IT/Security Manager from EducInstF shared that media’s description of the incident was somewhat inaccurate, which led to the interest from UK’s crime agencies, wasting already limited resources:

“We contained it fairly quickly. But we had a lot of press about it. The incident got picked up quite heavily within the media and around the world, and the media made it sound an awful lot worse than it actually was. This led to interest from NCA, NCSC and lots of other agencies.” [EducInstF, IT/Security Manager]

IT/Security Managers from LawEnfJU and HealthSerJU were surprised by the lack of criticism in news articles and suggested that this is due to too many attacks happening at the same time:

“We were very surprised and to this day I am still very surprised that we were not hammered by the media. We were one of a number of agencies in the area that got infected at the same time. I think that at the time it was going on so much, that we probably got lost in the background”. [LawEnfJU, IT/Security Manager]

“We did not get criticised because it was a global issue. When you are part of the gang, then you are tarred with the same brush.” [HealthSerJU, IT/Security Manager]

There were also two positive comments about the value of journalism and its social responsibility to broadcast important issues. An IT/Security Manager from LawEnfJ, for instance, argued that when victims share information about security incidents, they ultimately help others:

“I think we have been able to help other organizations by being open about it. I hear stories from other sectors and other businesses where they have been affected, and it has never made public, and no one ever knows about it. They are handling all that internally. To some degree it is nice to be open and to be able to talk about that particular incident”. [LawEnfJ, IT/Security Manager]

An Executive Manager from EducInstF noted that victims give advantage to criminals when concealing the facts:

“And I can tell you that one of the things that really bothers me about security incidents is that organizations hide this information. But the more people keep this behind closed doors, the less we know. We are giving the advantage to the bad guys by not sharing this information. This is why we were so open about our breach”. [EducInstF, Executive Manager]

It is clear that media has an important task of bringing awareness about cybercrime issues, but how these incidents are reported is a different matter. Some study participants noted that media representation was negative in nature, which had additional adverse knock-on consequences on victim organizations. The fact that in some instances media reports were inaccurate, further exacerbated these negative consequences. As a consequence, and unsurprisingly, some victim organizations decided to be less forthcoming with the details about cyber-attacks. But others emphasized the importance of sharing this information. It is, therefore, critically important to investigate cybercrime reporting practices by news media and develop a model to improve such practices. Phase 2 of this study will address these objectives.

<table>
<thead>
<tr>
<th>Categorization</th>
<th>Decontextualization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative consequence of media coverage</td>
<td>Hampered recovery&lt;br&gt;Damaged reputation&lt;br&gt;Communication ‘wild west’&lt;br&gt;Contacted by national crime agencies – waste of country’s resources&lt;br&gt;Leaked information&lt;br&gt;Invasive communication tactics&lt;br&gt;Being a high-profile organization is disadvantage</td>
</tr>
<tr>
<td>Positive consequence of media coverage</td>
<td>Helping others&lt;br&gt;Not giving advantage to bad guys</td>
</tr>
<tr>
<td>Surprisingly positive outcome</td>
<td>Got lost in the background&lt;br&gt;Global issue</td>
</tr>
<tr>
<td>Lessons learned</td>
<td>Less forthcoming with media in the future&lt;br&gt;Communicating only with helpful organizations&lt;br&gt;Tactical perspective</td>
</tr>
</tbody>
</table>

Table 2. Data Analysis Results: Phases 1 and 2.
4 Results Trustworthiness

Several tactics were used to ensure the trustworthiness of data analysis results. The Ethics Committee at the University of Leeds approved this research. All necessary procedures were followed to preserve participants’ anonymity and data confidentiality. Consent forms were signed by all study participants. Cyber-attacks can inflict a great deal of emotional pain on victims. Interviews, unfortunately, can force victims to relive these traumatic experiences. Bearing this in mind, the lead researcher demonstrated compassion and solidarity during interviews. Participants were also informed that they can stop interview at any time if it becomes hard to relive ransomware attacks. Finally, interviewees were notified that they can withdraw from the study at any time.

The first phase of this study was preliminary, hence, reaching theoretical saturation was deemed irrelevant. The aim was rather to explore if victims of cybercrime encounter any negative experiences with the media, and, if yes, what are victims’ reactions to these interactions. Nevertheless, fourteen cyber-attacks were explored, while “a point of sufficient theoretical saturation is normally reached after about a dozen or so observations” (Miles and Huberman, 1994, pp. 30-31).

5 Remaining Work

The aim of the second phase is to conduct critical discourse analysis of the cybercrime reporting by news media, with the specific focus on cyber-attacks in organizational settings. Data will be collected from two most popular media outlets in the UK, that is BBC online portal (as a referent media, which is a part of respectable public media service in UK) and The Guardian, as the second most popular news portal in the UK (Statista, 2020). A typical cluster sampling approach will be used in order to reduce a regular annual sample bias (e.g., expected reporting style and topics during holidays and expected usual yearly dynamics in reporting). Articles from 1st of June 2020 until 31st of May 2021, therefore, will be reviewed and analyzed.

The results of the second phase will serve as a basis for the development of a model for accurate reporting of cybercrime by news media (GoWA, 2022; Čigoja Piper, 2018; Goerig, 2015; Haller, 1995). The model will provide recommendations and precise instructions on how to deliver correct and truthful information about cyber-attacks and its victims (more precisely, organizations). It will offer an opportunity to change the current media framework in which the topic is placed (e.g., the view of the topic, the angle from which the topic is regarded, the selection of interlocutors, the choice of terminology, the reference to victims etc.). Furthermore, the model will be a step forward in changing attitudes of the media and the public about victims of cyber-attacks. Once completed, the results of this work (the model, in particular) will be shared with the UK media regulatory body Ofcom, the National Council for the Training of Journalists, and the BBC Media Action. In cooperation with these bodies, recommendations will reach all media outlets in the UK. Potentially, the model could become part of journalists’ training curriculum in the UK. An impartial media reporting of cybercrime is a step forward in encouraging victims to be more forthcoming with the information about cyber-attacks.

6 Acknowledgment

I would like to extend my sincere gratitude to all respondents for their invaluable contribution to this research. I greatly appreciate interviewees’ time and genuine effort. I am very grateful for additional inputs during and after data analysis.

This work was supported by Zayed University Start Up Grant [R21041] and the Engineering and Physical Sciences Research Council via grant scheme EMPHASIS [EconoMical, PsycHologicAl and Societal Impact of RanSomware] [EP/P011721/1].
References


