Help, I need somebody : examining the antecedents of social support seeking among cybercrime victims

Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims

Abstract

An important portion of internet users have faced cybercrime in recent years. One successful strategy for dealing with cybercrime victimization is to seek social support. However, previous studies showed that only a limited number of victims reaches out to family or friends to ask for help after a cybercrime incident. The current study sought to gain a better understanding of victims' social support seeking by exploring its antecedents. Specifically, the study took into account the role of (1) perception (i.e., perceived severity and perceived control), (2) primary responses (i.e., self-blame and denial), and (3) social capital (i.e., available [trusted] connections). Moreover, we explored the link between fear of cybercrime and these antecedents. Data collected from 334 cybercrime victims were analyzed using structural equation modeling. The findings indicated that victims with high perceived control and who ignore the incident, are less inclined to ask for help. Surprisingly, victims with high levels of self-blame are more likely to seek support. Moreover, we found that fear of crime is significantly related with perception and self-blame. Future awareness campaigns should stress that support seeking is part of the solution and should avoid placing the responsibility of victimization completely on the victim.

Keywords: social coping, social support, cybercrime, victimization, fear of cybercrime

1. Introduction

In recent decades, the role technology plays in people's lives has changed considerably. This evolution has provided society with a wide range of opportunities in terms of, for example, communication, entertainment, and learning (De Kimpe et al., 2019*)*, but also has facilitated the increase of a diversity of cybercrimes (Pupillo, 2018). Today, both policymakers (Europol, 2019) and scholars (e.g., Holt & Bossler, 2016) consider cybercrime to be an important topic of interest, and at least 71% of European internet users state to be concerned about one or more cybercrimes (European Commission, 2019). Moreover, in 2018, 8.5% of the Dutch citizens claimed they were a cybercrime victim (of crimes such as hacking, online fraud, identity theft, ransomware, and interpersonal incidents) (Statistics Netherlands, 2019). In that same year, the 2018 Safety Monitor of the Belgian Federal Police (2019) found that 8.14% of the sample was the victim of internet fraud, and 7.82% were victims of hacking of their computers or smartphones. Even though it can be questioned whether these data are accurate, since for example the Belgian survey did not provide clear definitions of the cybercrimes in question, and it is assumed that a considerable number of cybercrimes are never detected by the victims at all (Kabay, 2009; Wall, 2001), the numbers still indicate that cybercrime is an important topic to focus on.

Studies that have aimed to improve the safety of the online environment have applied several approaches. Some researchers have focused on understanding and increasing users' protection motivation (e.g., Ifinedo, 2012; Martens et al., 2019; Shillair et al., 2015; Tsai et al., 2016), and have aimed to identify which people are most likely to become a cybercrime victim (e.g., Bergmann et al., 2018; Kaakinen et al., 2018). Others have worked on technical improvements to limit online threats (e.g., Qabajeh et al., 2018; Tyugu, 2011). What these studies have in common is that they apply a situational preventive perspective and aim to reduce the amount of future cybercrime victims. However, it is likely that progress made in the cybersecurity field will always be paralleled by cybercriminals' increasing professionalism and sophistication (Millman, 2016). It can thus be expected that internet users will continue to be confronted with cybercrime victimization and its negative consequences in the future. These consequences can range

from financial or social problems to psychological and emotional disturbance (Jansen & Leukfeldt, 2018). So far, research has only paid limited attention to the way we can limit the negative experiences of cybercrime victims.

Qualitative research exploring the impact on and needs of cybercrime victims found that a considerable number of cybercrime victims does not share their victimization experience with family or friends (Cross et al., 2016b; Jansen & Leukfeldt, 2018). A possible explanation for this finding is that it is not unusual for victims of certain types of cybercrime, such as online fraud, to be blamed for their victimization (Conway & Hadlington, 2018; Cross, 2015; Cross et al., 2016a). This might affect their willingness to share their experiences with others. Nevertheless, in an offline context, seeking support has been found to be one of the most effective ways of successfully dealing with victimization, since it can also help to offset possible negative emotional and psychological effects and can provide victims with useful information to prevent future incidents (Cullen, 1994; Frieze et al., 1987; Littleton, 2010; Stadler et al., 2010). The same has been suggested regarding online victimization (Jansen & Leukfeldt, 2018). Consequently, it is imperative to further explore what deters cybercrime victims from seeking support and how we can encourage this behavior in the future. The current study will examine the antecedents of social support seeking, using representative survey data collected from 1753 respondents. Within this sample, 334 recent cybercrime victims (i.e., victimized in the last twelve months) were identified. This study will focus on the latter group. The results will provide us with useful insights that will allow us to limit the negative consequences experienced after a cybercrime incident (Green et al., 2010).

2. Consequences of cybercrime victimization

Given that a substantial number of internet users experience cybercrime incidents (Belgian Federal Police, 2019; European Commission, 2019; IC3, 2018; Statistics Netherlands, 2019), it is vital to take into account the consequences of these events. Victimization is a potentially traumatizing experience (Richards & Cross, 2018), which can be linked to a myriad of negative effects.

First, cybercrime can result in financial consequences (e.g., Hunton, 2012). A distinction can be made between direct and indirect costs or losses (Anderson et al., 2013). Direct losses are losses or damage experienced by the victim due to a cybercrime incident (e.g., money stolen by offenders, time lost, feelings of distress), while indirect losses are linked to the opportunity costs and losses for society as a whole as a result of cybercrime (e.g., loss of trust in online banking and other online services). Moreover, Anderson and colleagues (2013) also distinguish a third type of losses, namely defense costs, which relate to the preventive measures developed and deployed on a societal level (including the inconvenience caused by these measures).

Second, cybercrime victimization can result in several possible psychological and emotional effects. For example, cybercrime victims have reported reduced subjective well-being, feelings of depression, fear, shock, distress, sadness, anger and embarrassment (Cross et al., 2016b; Kaakinen et al., 2018). The emotional impact of certain types of cybercrime, such as online fraud, may be as severe as the financial consequences (Modic & Anderson, 2015). Victimization can also change the way victims perceive themselves and the world around them (DeValve, 2005). For example, some online fraud victims have claimed feeling stupid or cheated afterwards, and have reported decreased levels of trust in themselves and in others (Jansen & Leukfeldt, 2018), which can further develop into physical effects, such as sleeplessness or insomnia, nausea or weight loss (Cross et al., 2016a). These emotional and physical reactions are similar to the effects experienced by victims of traditional crimes (Lamet & Wittebrood, 2009).

This variety of negative consequences is linked to a specific set of victims' needs. One important factor in the way the incident is processed by the victim, is the support victims receive from their social environment (Lamet & Wittebrood, 2009; Wright, 2015). However, only a small number of cybercrime victims actually display help-seeking behaviors, such as talking about the incident with family and friends (Cross et al., 2016b; Maskall, 2017).

3. Social support seeking after (cyber)crime victimization

Crime victims will make an attempt to deal with the stress that is caused by a victimization experience. According to Frieze and colleagues (1987), there are two broad categories of coping strategies: actions that people take alone, and actions that involve receiving help from others. Seeking support falls into the second category. It is assumed that victims complete three steps before they decide whether or not to disclose the incident to a third party (van de Weijer et al., 2018). First, victims need to identify themselves as victims. Next, they assess the seriousness of the crime. Based on these two steps, they can make a final decision about whether to report the incident or not.

Victims can report a crime in a formal way (e.g., to authorities like the police) or can discuss the incident in a more informal manner (e.g., with people within their social support network) (Cross et al., 2016a). Research has considered approaching one's social support system to be a successful way of coping with the events (Cullen, 1994; Frieze et al., 1987; Jansen & Leukfeldt, 2018; Lamet & Wittebrood, 2009). Given that knowledge about cybercrime is changing rapidly (Chen & Zahedi, 2016), it might be especially useful for cybercrime victims to reach out to others for help or support. A victim's social support system can include family, friends, but also acquaintances such as neighbors or colleagues. These individuals can help the victim to deal with the incident by offering instrumental and/or expressive support (Cullen, 1994). The former type of support involves family and peers offering material aid, behavioral assistance or information, while the latter type involves offering emotional support and comfort (Barrera Jr & Ainlay, 1983; Cullen, 1994; Frieze et al., 1987).

Receiving appropriate social support can improve the way individuals process the effects of victimization (DeValve, 2005). With regard to victimization resulting from traditional crime, Mason and Benson (1996) stressed that family and friends can help victims to interpret the incident (e.g., by highlighting that the offender is to blame, not the victim). Moreover, receiving social support can help to maintain or enhance victims' self-esteem, speed up the processing of stress caused by the incident (Frieze et al., 1987), and stabilize emotional functioning (DeValve, 2005). These positive effects were established

in traditional crime research, but positive outcomes have also been found in cybercrime contexts. For example, victims of online fraud who reached out to professional support workers claimed that it was helpful for them to receive reassurance and advice (Cross et al., 2016b). Phishing and malware victims also experienced talking about the incident as healing and helpful (Jansen & Leukfeldt, 2018), just as young victims of cyberbullying and online harassment (Pereira et al., 2016), whose support seeking behavior was found to be related to reduced depressive feelings (Machmutow et al., 2012).

Although seeking support is associated with positive outcomes for the victims of both traditional crimes and online crimes, studies have found that victims often prefer to keep the incident to themselves (Cross et al., 2016b; Taylor, 2002). Only a minority of cybercrime victims report their experience in an official way. A study of Australian internet users indicated that, depending on the type of crime, cybercrime victims report the incident to the police in only 4% (i.e., attacks on computer systems) to 23% (i.e., online fraud or scams) of the cases (Morgan et al., 2016). A Belgian study that also took into account other reporting channels (e.g., banks and internet providers) found that between 15.4% (for viruses) and 58,0% (for scams) of the victimized households reported the incident (Verdegem et al., 2015). Van de Weijer and colleagues (2018) found similar police reporting rates (between 7.1% for hacking and 26.3% for identity theft) in the Netherlands. They concluded that, when compared to traditional crimes, cybercrimes are among the least-reported types of crime.

Less is known about informal support seeking behaviors. Jansen and Leukfeldt (2018) conducted an exploratory study in this field of thirty phishing and malware victims, which suggested that the proportion of cybercrime victims reaching out to their social support system is relatively small. Less than half of them (n = 13) reached out to people within their own social sphere. Even though we cannot generalize these results due to the small sample size, they indicate that an important part of cybercrime victims find it difficult or unnecessary to talk about the cybercrime incident with the people around them. To gain a better understanding of the social support seeking behavior of cybercrime victims, a larger-scale

approach is required. This will allow us to draw more reliable conclusions about social support seeking and enable us to make suggestions that could optimize cybercrime victims' ability to deal with incidents.

The current study will therefore aim to gain greater insight into support seeking behavior by relying on data collected from 334 cybercrime victims of the past twelve months. More specifically, this study will determine how (1) perception of the cybercrime event, (2) primary responses to the event and (3) a person's social capital are related to social support seeking. We will focus on these three factors because they play an important role in shaping the "state of balance" in stressful situations (Green et al., 2010). Moreover, given the importance of fear in helping us understand victims' perceptions and emotions (Meško, 2018), the current study will explore the relationship between these three factors and the fear of cybercrime. Figure 1 presents the conceptual model that is tested in the current study. In the next section, we will discuss the expected relationships between the study variables in further detail.

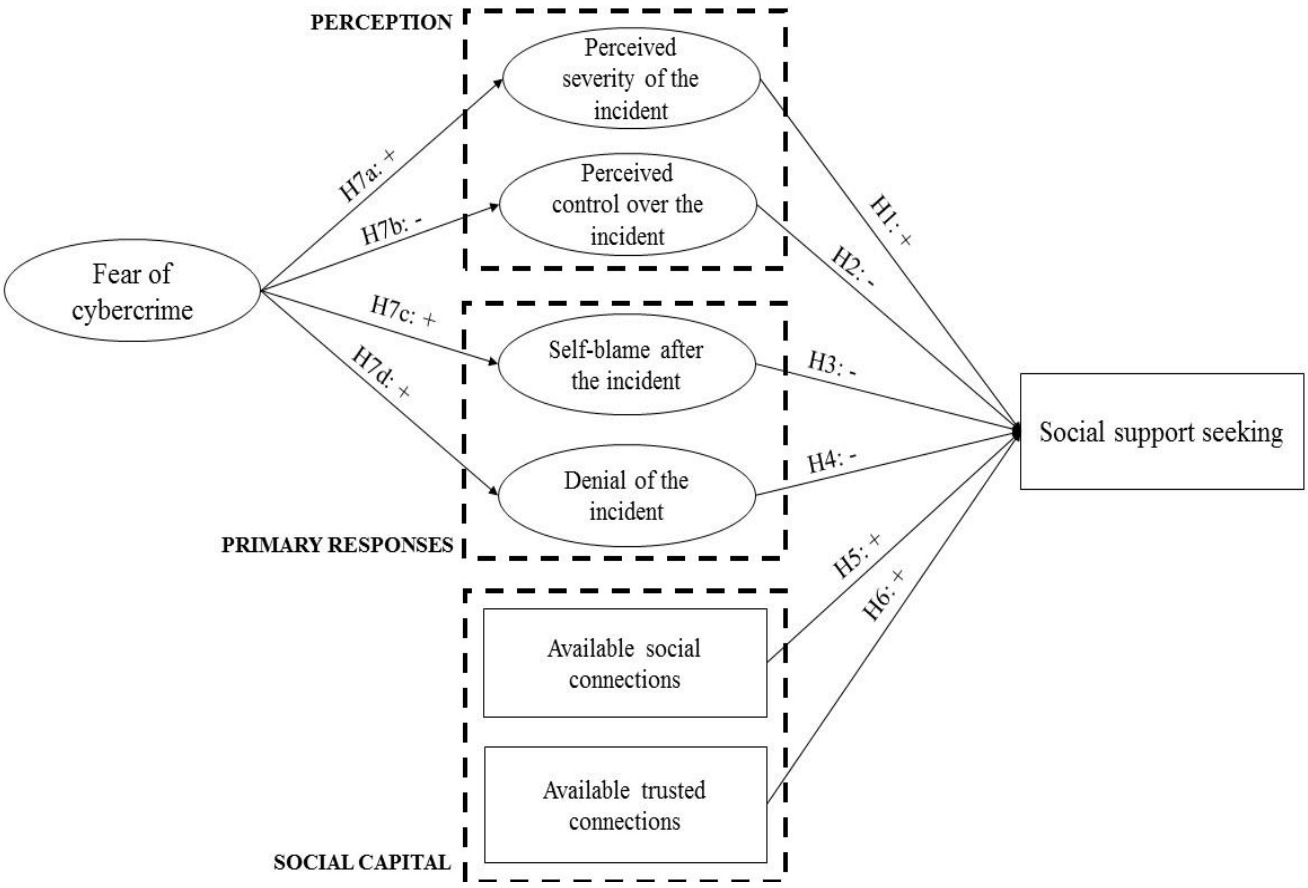

Figure 1 - Conceptual model of the antecedents of social support seeking by cybercrime victims

3.1. Perception of the event

The first factor that this study will consider, is the perception of the event. Based on the literature (e.g., Black & Hendy, 2018; Cross et al., 2016a; Goudriaan, 2006; van de Weijer et al., 2018), two important components will be taken into account: (1) the *perceived severity* of the incident, and (2) the *perceived control* over the incident.

Even though the collective impact of cybercrime on society is serious, its consequences on an individual level are not always perceived as such (Wall, 2008). Studies on (cyber)crime reporting to the police acknowledge that perceived severity plays a crucial role in victims' decision-making processes (Goudriaan, 2006; Ruback et al., 1984; Tarling & Morris, 2010). One reason for this is that, when a person believes an incident is serious, the need to be compensated or helped increases, and, thus, heavily outweighs

the cost of reporting (van de Weijer et al., 2018). When an internet user is convinced that a victimization experience is not serious enough, this deters him or her from reporting the incident (Cross et al., 2016a; Taylor, 2002; Wall, 2008). Given the link between the perceived severity of crime and its reporting, we expect that social support seeking and perceived severity are linked in a similar way. Consequently, we hypothesize (H):

H1: There is a positive relationship between perceived severity of cybercrime and social support seeking.

When people experience victimization, they can feel a loss of control (Taylor, 2002). This low perceived control indicates that the person does not know how to change the situation at hand (Black & Hendy, 2018). Perceived control, or the lack thereof, can influence the further steps internet users take after cybercrime victimization. For example, a study of online fraud victims found that when these victims felt like they had enough skills to deal with the incident on their own, and thus felt like they had control over the situation, they were less likely to seek formal support (Cross et al., 2016a). The same might hold true for seeking out informal social support. When perceived control is low, we expect that one will try to resolve this feeling by reaching out to a person who can help the victim to deal with the situation. This results in the following hypothesis:

H2: There is a negative relationship between perceived control and social support seeking.

3.2. Primary responses to the event

The second component that this study will take into account are the initial responses of a victim to a cybercrime event. Given that the current study wants to understand why a considerable number of cybercrime victims fail to seek social support, we will focus on two responses that are believed to play an important role (Green et al., 2010): (1) *self-blame* and (2) *denial*.

Some of the feelings most often associated with cybercrime victimization are shame and embarrassment. These feelings are believed to stem from self-blame (Cross et al., 2016b). Blaming themselves is a reaction that helps victims to control their emotional responses to the events (Green et al.,

2010; Jansen & Leukfeldt, 2018). Even though self-blame is traditionally considered to be a negative reaction, it is also recognized as beneficial to some extent. By perceiving their own actions and behaviors as part of the reason why the incident occurred, victims may feel more confident about avoiding future incidents, allowing them to regain control over the situation (Frieze et al., 1987). However, self-blame also has some negative consequences, because it is seen as a reason for victims not wanting to report incidents (Bidgoli & Grossklags, 2016; Goucher, 2010; Wall, 2008). Feelings of embarrassment can make it difficult for people to talk with others about the crime (van de Weijer et al., 2018). This reluctance to share one's experiences might also be associated with the victim-blaming discourse that exists with regard to specific types of cybercrime, such as online fraud (Cross et al., 2016a). If cybercrime victims internalize this victim-blaming perspective, they may end up feeling too embarrassed to talk about the incident with friends and family. This leads us to formulate the following hypothesis:

H3: There is a negative relationship between self-blame and social support seeking.

Apart from blaming him-/herself for the victimization, another response a victim might initially have is to ignore or deny the incident. Through these actions, victims distance themselves from the victimization incident and its potentially harmful consequences (Green et al., 2010). Research has suggested a negative relationship between avoidance of situations and people's behavioral intention (Rippetoe & Rogers, 1987). Therefore, we can assume that victims in a cybercrime context who ignore or deny the incident and its consequences will be less likely to mention the incident to the people they trust. We hypothesize:

H4: There is a negative relationship between denial and social support seeking.

3.3. Social capital

A third aspect that this study on social support seeking needs to consider, is victims' *social capital*. Research on traditional types of fraud, pointed out that a person's social network (i.e., consisting of family and friends) is an important factor to take into account in understanding victims' reactions (Mason &

Benson, 1996). Informal support is not necessarily accessible to every (cybercrime) victim. Moreover, even when potential social support is available, an additional requirement is that the victim believes they can trust and will not be judged by the available individuals (Cross et al., 2016a). This leads us to assume that not only the number of social connections a person has (i.e., the size of the network), but that also the level of confidentiality existing between the victim and the available support (i.e., the strength of the existing ties) plays an important role in social support seeking. Consequently, we suggest the following two hypotheses:

H5: A positive relationship exists between the number of available social connections and social support seeking.

H6: A positive relationship exists between the number of trusted connections and social support seeking.

3.4. Fear of cybercrime

Apart from examining the role of perceived severity and control, self-blame, denial and social capital in social support seeking, the current study will include another crucial factor. More specifically, it will explore how the emotion *fear of cybercrime* is related to the antecedents.

Fear of crime is a well-established concept in the criminology and victimology literature. The broad conceptualization of fear of crime distinguishes a cognitive dimension, an emotional-affective dimension, and a behavioral dimension (Fattah & Sacco, 1989; Ferraro & Grange, 1987; Gabriel & Greve, 2003; Greve, 1998). The cognitive dimension refers to a process of converting signals and stimuli concerning threat and danger into a risk assessment of personally becoming a victim of crime (Ferraro & Grange, 1987; Gabriel & Greve, 2003). Ferraro (1995) describes the emotional-affective component as "an emotional response of dread or anxiety to crime or symbols that a person associates with crime" (p. 4). The resulting behavioral component is considered to be a defensive reaction to an emotional state of mind when experiencing fear. This concerns the overt effect of fear of crime in an individual's everyday life (Franklin et al., 2008). In

this study we will take into account the emotional component of fear, rather than the cognitive dimension of risk perception.

Meško (2018) points out that fear can help us to understand people's perception of events, as well as their reactions to those events. Therefore, we will examine the link between fear of cybercrime, (1) perception and (2) primary responses to the event. In the conceptual model, available social connections and available trusted connections serve as independent variables, since we do not expect fear of cybercrime to have a direct influence on the size of a person's network or the udy strength of his/her available ties.

Theoretical models that are based on fear appeals (e.g., Rogers, 1975; Witte, 1992), consider inducing fear as a way to convey the perception that a threat or incident is severe. Findings in a cybercrime context confirm the importance of fear appeals in the way a threat is perceived (Johnston & Warkentin, 2010). Hence, when people experience fear of cybercrime, we assume they will believe it to be more severe. This study therefore hypothesizes that:

H7a: A positive relationship exists between fear of cybercrime and perceived severity of cybercrime.

Traditional crime research assumes a close link between fear of crime and perceived control (e.g., Jackson, 2009; Sacco & Glackman, 2009). Studies have not only established that perceived control over crime is linked to a higher frequency of worry about crime (Jackson, 2004), but also have examined the influence of fear of crime on perceived control. In a longitudinal study by Shippee (2012) regarding the sense of personal control, fear of crime proved to have a negative relationship with perceived control at baseline, even though this effect did not persist over time. Based on these findings, in this study we assume that a similar negative relationship exists between fear of cybercrime and perceived control over the incident, especially among recent cybercrime victims. We hypothesize:

H7b: A negative relationship exists between fear of cybercrime and perceived control.

Research has pointed out that, while dealing with feelings of stress and fear, it can be questioned whether crime victims can make rational decisions following the victimization experience (Goudriaan,

2006). More specifically, fear is believed to be an emotion that triggers fight-or-flight responses in individuals. Even in cases where people feel able to deal with a threat or incident, fear can evoke a strong flight impulse (Chen, 2017). Theoretical models, such as the Extended Parallel Process Model (Witte, 1992), pose that, when people experience high levels of fear, emotional processes are elicited that aim to diminish this fear (Witte, 1996). In the context of technology threats, these responses include (among others) fatalism, denial, and internalization of blame (Liang & Xue, 2010). However, so far little empirical research has focused on fear of cybercrime and its relationship to these responses. One recent study by Brands and van Wilsem (2019) indicated that there is a strong link between online fear and avoidance behavior (i.e., avoiding performing specific online behaviors, such as online purchasing). Similarly, we assume that cybercrime victims with high levels of fear of cybercrime will be more likely to react to an incident by ignoring the incident or by blaming themselves for the incidents. We hypothesize:

H7c: A positive relationship exists between fear of cybercrime and self-blame.

H7d: A positive relationship exists between fear of cybercrime and denial.

4. Method

4.1. Data collection and participants

To test the proposed conceptual model, we collected data during the Social Capital in Neighborhoods (SCAN) study in October and November of 2018. The SCAN study is a yearly large-scale survey study among the citizens of Ghent (Flanders, Belgium). By means of computer-assisted personal interviewing during home visits using a structured questionnaire, respondents were questioned face-to-face about the characteristics of their neighborhood and their social capital. Respondents then privately answered more personal questions (e.g., concerning online and offline risk behaviors and victimization experiences) on the interviewers' devices. Interviewers stayed in the room to be able to provide assistance and clarifications if necessary. A forced choice method was used (i.e., it was mandatory to provide an answer to the questions). Hence, there were no missing data. The interviewers explicitly stressed, before the start of the survey, that

participants could withdraw from participation at any given time, and that they could contact the researchers to request the removal of their case from the dataset after the data collection had taken place.

From each neighborhood, we selected a stratified sample of 40 inhabitants based on gender (male or female), age (16–24, 25–34, 35–44, 45–54, 55–64, 65+) and nationality (Belgian or non-Belgian), which was representative of the composition of that specific neighborhood. By selecting 40 respondents in 50 neighborhoods, the study aimed to obtain a representative sample of 2,000 citizens of Ghent. We obtained contact information for each of the selected respondents through the 2018 municipal registry, including five substitutes with the same characteristics for each original respondent. The interviewers contacted these substitutes if the selected respondents could not be reached after three home visits, declined to participate or did not fit the inclusion criteria (i.e., sufficient knowledge of Dutch, minimum age of 16, and not residing in an institutional setting, such as a retirement home). The ethics committee of [DEPARTMENT, UNIVERSITY] provided ethical approval for the study.

Ultimately, 1,949 citizens of Ghent participated in the study. After data cleaning, 1,753 questionnaires were found to be valid. This sample comprised 1,601 internet users (91.3%). A total of 630 (39.4%) of the internet users had been victims of cybercrime during the past five years. Focusing on the past 12 months, we found 334 cybercrime victims (20.9% of internet users). Given the focus of the current study, the latter subsample was used for further analyses. A total of 54.5% (n = 182) of the victims were male, while 45.5% (n = 152) were female. Participating victims were between 16 and 87 years of age (M = 43.47, SD = 16.22). In addition, 90.7% (n = 303) had the Belgian nationality. Regarding education, 56.6% (n = 189) of the victims had a university or college degree, 32.0% (n = 107) graduated from high school and 11.4% (n = 38) had a lower level of education.

4.2. Measures

The items included in the questionnaire were based on validated measures and adapted to the cybercrime context when necessary (cf. infra). The content of the items was discussed among experts and among the

authors of this paper. Moreover, a panel of non-experts provided feedback on the clarity of the items for a non-academic population, identified errors in the text, gave us greater insight into the length of the questionnaire (i.e., we aimed for an average of twenty minutes for completion), and assisted with the correct and logical routing of the online questionnaire.

4.2.1. Cybercrime victimization

As part of this large-scale survey, we asked respondents whether they were ever a victim of six types of cybercrime: phishing, online identity theft, consumer fraud, hacking, ransomware, or other types of malware. As a starting point, this *selection* of cybercrimes was inspired by the special Eurobarometer on cybersecurity, which is a recent European study that takes into account a wide diversity of cybercrimes at the same time (Eurobarometer, 2017). However, we then focused specifically on *computer-based offenses*, which are cybercrimes where, usually, not a specific individual (e.g., cyberstalking), but anyone with a device can be targeted (Bossler & Holt, 2010). This category of cybercrimes is similar to what Gordon and Ford (2006) describe as *Type I cybercrimes*. Moreover, we selected cybercrimes in which offenders usually have a *socio-economic motive*, rather than a psychological (e.g., cyberstalking) and/or geopolitical (e.g., cyber terrorism) motive (i.e., categorization as proposed by Ibrahim, 2016). We also left out the more content-related cybercrimes (e.g., encountering hate speech or pornography) in which victimization could be considered to be more passive. We are convinced that applying this narrower focus to the six cybercrimes will yield the most useful results. Nevertheless, our selection ensured sufficient diversity of cybercrime types, which leaves room for comparison. For example, we included both social (i.e., *online consumer fraud, identity theft, phishing*) and more technical forms (i.e., *hacking, ransomware, other malware*) of cybercrime (Martens et al., 2019). A definition accompanied the six selected cybercrimes to make sure that all users had the same interpretation of these terms.

For each cybercrime type, respondents were asked if they had ever been victimized, at work or at home, on a computer, laptop, tablet or smartphone. Five options were provided: (1) “I have been a victim in the past 12 months”; (2) “I have been a victim more than a year ago, but less than five years ago”; (3) “I

have been a victim more than five years ago"; (4) "I have never been a victim of this crime"; (5) "I don't know". For each cybercrime, only one answer could be provided. Between 6.8% (i.e., for consumer fraud) and 11.6% (i.e., for identity theft) of the internet users selected the final option "I don't know".

To examine *phishing* victimization, respondents were asked: "Did you ever share sensitive information (e.g., passwords, credit card details) after you received a fraudulent message by e-mail, phone, text message and/or social media?" It was explained further: "In this message the phisher usually pretends to be a company or person you know (e.g., your bank, your boss)". This description was based on the most recent Eurobarometer (2017) and on a study by Reyns (2015). To determine whether respondents ever encountered *online identity theft*, they were asked: "Did anyone ever steal your personal details (e.g., password, credit card details) online and then pretend to be you?" (Eurobarometer, 2017). *Consumer fraud* victimization was measured by asking: "Did you ever (partially) pay for something online without receiving the promised goods, services and/or prices in return?" This question was based on a study by Leukfeldt and Yar (2016). To describe *hacking*, respondents were asked: "Were you ever inconvenienced by someone accessing your e-mail, social media accounts or the data on your computer, laptop, tablet or smartphone without your permission?" The studies by Reyns (2015) and van Wilsem (2013) were consulted to construct this definition. To determine whether respondents ever were ever victims of *malware*, they were asked: "Were you ever inconvenienced by an infection of your computer, laptop, tablet or smartphone by a malicious type of software (e.g., virus, Trojan horse, spyware)?" (Bergmann et al., 2018; Bossler & Holt, 2009). Last, we included a separate category for *ransomware*, given its topical character. Respondents were asked: "Were the data on your computer, laptop, tablet or smartphone ever blocked, accompanied by the message that your data would only be unlocked if you paid a sum of money?". This definition was based on a study by Bergmann and colleagues (2018).

The questionnaire only provided more detailed questions on the experience of cybercrime victimization to those who indicated they were a victim of one or more cybercrimes during the past 12 months. If respondents experienced victimization by different crimes during the past 12 months, they were

asked which was the most recent. All further questions on victims' perceptions, emotions, reactions, and social support seeking focused on this most recent victimization experience.

4.2.2 Perceived severity

Three items from Witte (1996) were adapted to the current study's focus. More specifically, we adapted the original items to measure perceived severity (e.g., "I believe that [health threat] is serious") by replacing their focus on health threats to a focus on the most recent experience with cybercrime (e.g., "I believe that [most recent incident] is serious"). Each item was scored on a five-point Likert scale ranging from *disagree* (= 1) to *agree* (= 5). The internal reliability proved to be good (α = .86).

4.2.3 Perceived control

To operationalize perceived control, we adapted three items that were originally used to measure overall security behavior self-efficacy (Anderson & Agarwal, 2010). Since we apply a reactive perspective in this study, we were not interested in whether victims believed that taking preventive security measures was entirely under their control, but wanted to identify how they felt specifically after the most recent incident they experienced (e.g., "I had the skills that were necessary to solve [the most recent incident] on my own"). A five-point Likert scale (*disagree* (= 1) to *agree* (= 5)) was used. This scale has a strong internal reliability (α = .93).

4.2.4 *Self-blame*

Two items to measure self-blame were derived from study by Wang and colleagues (2017), which specifically focused on phishing email detection. This is one of the few studies in the cybercrime context that does not only take into account adaptive, but also maladaptive, behaviors of internet users. We selected two of Wang and colleagues' (2017) three items on emotion-focused processing of a threat, since the third item did not involve self-blame, but worry (i.e. "I worried about my inadequacies"). The items were adapted in our study to focus specifically on victims' most recent victimization experience (e.g., "I blamed myself for [the most recent incident] because I didn't know what to do"). Answers were indicated on a five-point

Likert scale ranging from *disagree* (= 1) to *agree* (= 5). Using the Spearman-Brown coefficient to calculate the reliability of this two-item scale (Eisinga et al., 2013), indicated an internal reliability of .74.

4.2.5 Denial

Three items from Wang and colleagues' (2017) study, which we described in section 4.2.4, were used to operationalize denial (e.g., "I didn't take [the recent incident] too seriously"). The original study focused on dealing with a phishing detection task, while we focused the three items on dealing with the most recent incident. Answers were given on a 5-point Likert scale (*disagree* (= 1) to *agree* (= 5)). The scale can be considered reliable ($\alpha = .72$).

4.2.6 Available social connections

Social capital was measured in two ways: the availability of social connections and of trusted connections. First, respondents were asked to estimate how many people they had contact with on an average day. It was specified that this included face-to-face interaction, but also interactions by phone, letters or through the internet, for personal reasons and/or professional reasons. This could also include interactions with people they did not know well (Fu, 2005). An open field was provided that required a numerical answer.

4.2.7 Available trusted connections

Consistent with the measure used to assess available social connections, a single item was used to measure available trusted connections. Respondents were asked to estimate how many people in their environment (friends, family, and acquaintances) they could discuss personal issues with. This question could be answered in an open field that required a numerical answer.

4.2.8 Fear of cybercrime

To measure the emotion fear of cybercrime, rather than the cognitive assessment of perceived risk, the approach of Virtanen (2017) was applied: for each of the six cybercrimes that were covered in this study, respondents were asked to what degree they were afraid of becoming a victim of this cybercrime type. A

five-point Likert scale ranging from *disagree* (= 1) to *agree* (= 5) was provided. The scores for each cybercrime were combined into a single fear of cybercrime scale. The internal reliability of this scale proved to be good (α = .90).

4.2.9 Social support seeking

The outcome variable social support seeking was measured by using a single dichotomous item (*false* (= 0) and *true* (= 1)). Specifically, it was questioned whether the victim asked someone they trusted (e.g., a friend, a parent, or a colleague) for help and/or advice after the incident. This item was based on the social coping subscale from the Cyberbullying Coping Questionnaire (Jacobs et al., 2015). For example, in the current study, we left out a coping item that was specifically interesting in the context of cyberbullying, but less relevant in the cybercrime context (i.e., saving messages as evidence)."

4.2.10 Control variables

We included gender (*male* (= 0) and *female* (= 1)), age, educational attainment, past online victimization and type of cybercrime as control variables in our model. Age was calculated based on the respondent's birth year, and, for educational attainment three categories were provided (*university or college degree* (= 3), *high school degree* (= 2) or *lower education level* (= 1)). Previous victimization was measured by adding up the different cybercrimes respondents were confronted with one to five years ago. Scores could range between 0 and 5. Lastly, type of cybercrime was included as a control variable, making a distinction between *technical* (= 1) and *social* (= 2) types of cybercrime. Technical cybercrimes refer to hacking and malware (including ransomware), social cybercrimes include phishing, online identity theft, and consumer fraud.

4.3. Data analysis

The data were analyzed using structural equation Modeling in Mplus 7.4 (Muthén & Muthén, 2012). Given the dichotomous outcome variable, a probit regression was estimated using weighted least squares estimation. The fit of both the measurement and structural model was estimated by using several goodness-

of-fit indices. More specifically, the Root Mean Square Error of Approximation (RMSEA), the Comparative Fit Index (CFI), the Standardized Root Mean Squared Residual (SRMR, for the measurement model) and the Weighted Root-Mean-Square Residual (WRMR, for the structural model) were taken into account. Ideally, RMSEA has a value of .05 or lower, CFI has a value of .96 or higher for binary outcomes, WRMR has a value below 1.0 (Yu, 2002), and SMSR is smaller than .08 (Hu & Bentler, 1999).

Table 1
Descriptive statistics (n = 334)

Variable	Items	M	SD
Perceived severity			
(α = .86)	I am convinced that [experienced cybercrime] is a severe phenomenon.	4.13	1.01
	I am convinced that [experienced cybercrime] is a serious problem.	4.16	1.04
	I am convinced that [experienced cybercrime] is a considerable problem.	4.15	.94
Perceived control			
(α = .93)	I felt capable of solving [the incident] on my own.	3.05	1.57
	I felt like I had the knowledge that was necessary to solve [the incident] on my own.	2.98	1.52
	I felt like I had the skills that were necessary to solve [the incident] on my own.	3.00	1.55
Self-blame			
(ρ = .74)	I blamed myself for [the incident] because I didn't act better.	2.33	1.41
	I blamed myself for [the incident] because I didn't know what to do.	2.17	1.35
Denial			
(α = .72)	I ignored [the incident].	2.14	1.43
	I didn't take [the incident] too seriously.	2.53	1.47
	I decided that there was no reason to try to solve [the incident].	2.08	1.34
Available social connections	With how many people in your personal environment (friends, family, or acquaintances) can you discuss important personal issues?	10.78	36.18
Available trusted connections	How many people do you have contact with on an average day?	36.05	65.66
Fear of cybercrime			
(α = .90)	I am afraid to become a victim of malware.	3.41	1.40
	I am afraid to become a victim of ransomware.	3.17	1.46
	I am afraid to become a victim of hacking.	3.43	1.43
	I am afraid to become a victim of phishing.	3.05	1.56
	I am afraid to become a victim of identity theft.	3.10	1.49
	I am afraid to become a victim of consumer fraud.	3.28	1.44
Social support seeking	After [the incident], I asked someone that I trust (e.g., a friend, a parent, a colleague) for help and/or advice.	.46	.50

5. Results

5.1. Preliminary analyses

Preliminary analyses indicate that, of all the recent cybercrime victims (n = 334) in the overall sample, 35.6% (n = 119) has most recently been inconvenienced by malware (ransomware excluded). For 22.8% of the victims, the most recent incident they encountered was consumer fraud (n = 76); for 20.1% of the sample it was phishing (n = 67). The prevalence of hacking (11.1%; n = 37), identity theft (6.6%, n = 22), and ransomware (3.9%, n = 13) was lower. Of all these recent victims, 46.4% (n = 155) decided to ask someone they trusted (e.g., a friend, parent, or colleague) for help or advice. This implies that more than half the victims did not reach out to seek social support.

Table 2 displays the correlations that were found between the constructs in the model. Significant relationships were found between the outcome variable and most of the other variables included in this study. No correlation was found between the social capital variables and social support seeking. Moreover, the correlation between social support seeking and perceived severity was insignificant ($p = .057$). Furthermore, fear of crime was positively correlated with perceived severity ($p < .001$) and self-blame ($p < .05$), and negatively correlated ($p < .001$) with perceived control and available social connections ($p < .01$).

Table 2
Correlations between components of the proposed model (n = 334); * p < .05; ** p < .01; *** p < .001

	Variable	1	2	3	4	5	6	7
1	Perceived severity	-						
2	Perceived control	-.04	-					
3	Self-blame	.07	-.11	-				
4	Denial	-.08	.03	.08	-			
5	Available social connections	.02	.04	-.01	-.07	-		
6	Available trusted connections	.05	-.04	.03	.05	.02	-	
7	Fear of cybercrime	.27***	-.21***	.11*	-.09	-.16**	.01	-
8	Social support seeking	.10	-.32***	.16**	-12*	-.02	.07	.21**

5.2. Measurement model

First, we estimated the measurement model, which included perceived severity, perceived control, self-blame, denial and fear of crime as the latent constructs. Based on the goodness-of-fit indices that were consulted, it could be concluded that the model had a good fit with the data: RMSEA = .04 (CI: .03 - .05); CFI = .98, and SRMR = .04. All factor loadings had a minimal value of .37.

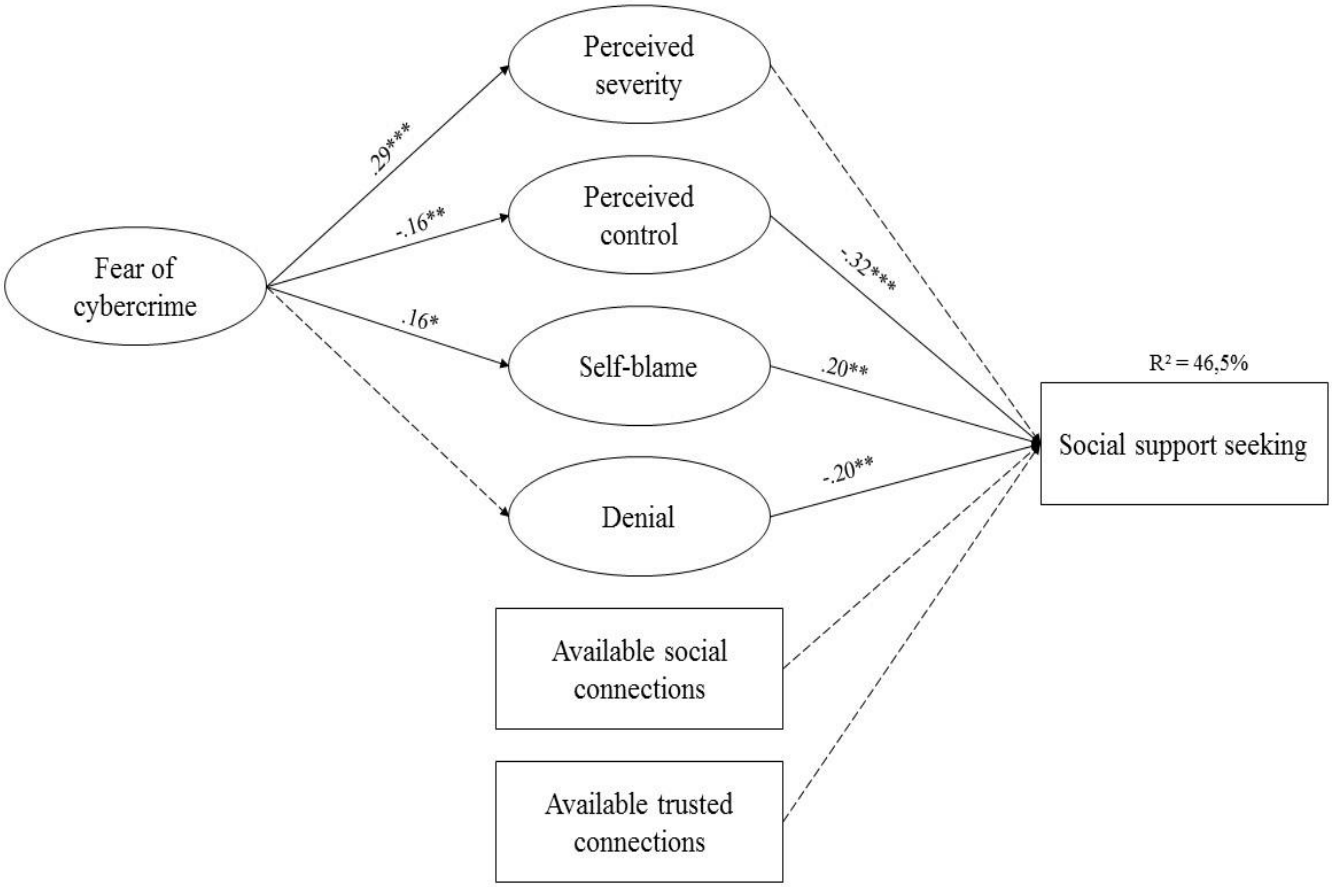

Figure 2 - Full model of the determinants of social support seeking. Note: all the reported coefficients are standardized values, controlled for age, gender, education, prior victimization and type of cybercrime. Dashed lines represent non-significant results. * p < .05; ** p < .01; *** p <.001

5.3. Structural model

Next, we assessed the structural model, including five covariates and social support seeking as the observed outcome variable. The model fit with the data proved to be good based on the fit indices: RMSEA = .02 (CI: .00 - .03); CFI = .96 and WRMR = .72. The final results are displayed in Figure 2.

The analyses showed that, as hypothesized, perceived control (β = -.32; p < .001) (H2) and denial (β = -.20; p < .01) (H4) had a negative significant relationship with social support seeking. Another significant relationship was found between self-blame and social support seeking (β = .20; p < .01), but this

relationship was positive instead of negative. H3 can thus only partly be confirmed. No significant association was found between perceived severity (β = .10; p = .13) (H1), available social connections (β = .42, p = .10) (H5), available trusted connections (β = .02, p = .82) (H6) and social support seeking.

Almost all the expected relationships including fear of cybercrime were significant. A positive association was found between fear on the one hand, and perceived severity (β = .29; p < .001) (H7a) and self-blame (β = .16; p < .05) (H7c) on the other hand. The association between fear of cybercrime and perceived control was found to be negative (β = - .16; p < .01) (H7b). The relationship between fear and denial was not significant (β = - .13; p = .07) (H7d).

The control variables included were age, gender, educational attainment, prior victimization (i.e., 1 to 5 years) and type of cybercrime victimization (i.e., technical or social). Taking these control variables into account, some additional relationships were found. Significant associations were identified between perceived control and gender (β = - .18; p < .01), education (β = .12; p < .05), age (β = -.21; p < .001) and type of cybercrime (β = .17; p < .01). This implies that perceived control was higher for men than women, that people with a higher degree and younger people perceive greater control and that victims of social types of cybercrime (e.g., phishing) perceive greater control over the situation than victims of a technical form of cybercrime (e.g., hacking). In addition, self-blame was negatively related to type of cybercrime (β = -.16; p < .05). Victims will blame themselves more when they were victims of a technical form of cybercrime. Moreover, positive relationships existed between fear of cybercrime and gender (β = .16; p < .01), and fear and age (β = .26; p < .001). Hence, women and older internet users tend to report higher levels of fear. No significant associations were found between the covariates and the outcome variable. Without the control variables, the model explained 36.5% of the variance in social support seeking. The final model, including control variables, explained 46.5% of the variance.

6. Discussion and conclusion

The current study aimed to gain a better understanding of the social support seeking behavior of cybercrime victims. By taking into account (1) perception of the event, (2) initial responses to the event and (3) social capital (Green et al., 2010), this study determined which components served as antecedents for social support seeking. Moreover, the link between the emotion fear of cybercrime and these antecedents was explored. The results provide useful insights that will help policymakers to convince victims to talk about their experiences and, in doing so, limit the negative consequences resulting from victimization.

First, the results showed that victims who feel that they can solve the issue on their own are less likely to ask for help from somebody else. However, feeling in control does not necessarily mean that internet users perform the correct actions to minimize harm. Therefore, it would be useful to emphasize to victims with high levels of perceived control (especially male, highly educated and young internet users) that talking about the issue and asking for a second opinion is a sensible thing to do, since this can improve the outcome. In traditional crime reporting, research also found that men, young people, and people with higher education were less likely to contact the police (Goudriaan, 2006). By pointing out to these groups of individuals, in particular, that seeking social support is considered to be part of the solution, these victims might include support seeking in their process of solving an online incident.

As expected, we found that people who ignore a cybercrime incident are less inclined to ask someone for help in order to find a solution. It might be interesting for future awareness campaigns to stress the benefits of confiding in someone, since this can encourage victims to solve potential problems, instead of ignoring incidents.

Our findings surprisingly indicate that victims who blame themselves for the incident are actually more likely to seek support. Blaming oneself is a strategy that allows victims to regain control over the situation (Frieze et al., 1987). Consequently, social support seeking might be closely related to taking back that control, since looking for help allows victims to learn from their mistakes. A genetic confounder

variable could also have played a role here (Barnes et al., 2014). This result places an important responsibility on the family members, friends or colleagues whose advice is sought by victims. People who are part of the victim's support system should therefore be guided to provide the best help possible, in order not to reinforce the victim-blaming perspective these victims have already internalized. Awareness campaigns for example, could stress the fact that victims are not alone and not to blame, simultaneously highlighting the best way for peers to help a victim. When victims reach out to professional counsellors after victimization, these professionals could also provide guidance to the family and peers of the victim.

With regard to fear of cybercrime, the tested relationships with perception and self-blame were found to be significant. This finding points out the importance of emotions when studying cybercrime. For a long time, cybersecurity research has approached internet users as rational individuals who base their decisions on the result of cognitive processes (e.g., Chou & Chou, 2016; Crossler & Bélanger, 2014). Our results stress the importance of emotions, since they do have an important influence on the perceptions that are held and the initial responses to incidents.

Interestingly, not all the hypotheses could be confirmed. For example, the results indicated that there is no significant relationship between perceived severity and social support seeking. When victims reach out to their peers for support, they apparently do so regardless of the perceived severity of the incident. Since the importance of perceived severity has mostly been suggested in the context of formal reporting (Taylor, 2002; van de Weijer et al., 2018; Wall, 2008), our results might indicate that other factors play a role in predicting social support seeking compared to formal support seeking. The (perceived) characteristics of the offence might be of less importance when victims reach out for social support, while the internal reactions do have an influence on social support seeking. This can be considered a hopeful finding, because in reality every cybercrime victim could benefit from receiving support, regardless of the characteristics of the crime.

We found no significant relationship between the availability of (trusted) connections and support seeking in our final model, which stresses that social capital and social support seeking are two distinct

concepts that are not necessarily related. However, existing research on violent and nonviolent crime victims did find that social support, consisting of both perceived and received support, was positively related to dealing with the problem (Green et al., 2010). Why this was not confirmed in the cybercrime context is unclear. It might be interesting for future studies to take into account whether the victim believes that he or she has connections with the necessary technical or digital skills to deal with a cybercrime incident.

In conclusion, future awareness campaigns should avoid placing the responsibility for victimization completely on the victim. Stressing that everybody can potentially become a cybercrime victim, and that disclosing victimization is part of the solution, might lower the threshold for talking about victimization for those who believe they can deal with the incident on their own, or who would rather ignore the incident altogether. Moreover, tackling the victim-blaming perspective in communication *with* potential victims and *about* victims might ensure that family and peers who offer support do not cause more damage (i.e., secondary victimization). In addition to increasing awareness, it could also be helpful to implement evidence-based guidelines for professional counselors on how to deal specifically with cybercrime victims and their environment.

7. Limitations and future research

Even though the current study makes a valuable contribution to the field of cybercrime research, it should be stressed that the research design has its limitations. First, a cross-sectional design was applied, so we could not determine causal effects. The results should therefore be interpreted with caution. For example, the positive relationship found between self-blame and social support seeking might also indicate that the support that was offered induced feelings of self-blame. Longitudinal studies are required in order to obtain more conclusive findings on this matter.

We should also acknowledge the limitations of using self-reported victimization data. Even though the current study provided definitions for every type of cybercrime that was included in the questionnaire,

and the interviewer was present to clarify these questions further when required, it is still possible that respondents did not fully understand what these cybercrimes entailed. We encourage future researchers to include manipulation checks to explicitly test people's understanding of the definitions.

It should be noted that based on the current data collection, repeated victimization by the same cybercrime type could not be determined. A victim who experienced three phishing incidents in the past twelve months could not be distinguished from a victim who experienced only one phishing incident in the past twelve months. Future studies should therefore measure prior victimization in a more detailed way, since this could provide additional insights.

It would be interesting for future research to explore additional antecedents of social support seeking. For instance, an interesting factor that could explain another part of the variance in social support seeking, is social norm. More specifically, it would be interesting to take into account what the assumed attitude of peers and family is towards cybercrime victimization. If they are assumed to have a negative attitude regarding online victimization (e.g., something that only happens to careless internet users), it is likely that victims will not talk about what happened to them. Also, personal characteristics like extraversion or egocentrism could directly or indirectly contribute to the willingness to ask for help. Likewise, it would be valuable to include additional questions about the way social support seeking is experienced (e.g., as a negative or positive experience) and about the identity of those providing support (e.g., their gender or relationship with the victim).

Last, it is important to stress that, to date, no general agreement about the definition of cybercrime exists (Donalds & Osei-Bryson, 2019; Holt & Bossler, 2014; Putnik & Boskovic, 2015; Tsakalidis & Vergidis, 2017). This situation can generate confusion for both end users (Conway & Hadlington, 2018) and researchers, which could have problematic consequences for intervention and prevention (Jahankhani et al., 2014). Also victimization by specific types of cybercrime is measured in different ways. For example, in the special Eurobarometer on cyber security (Eurobarometer, 2017) malware victimization was defined as *detecting* malware on one's device, while other studies have focused on *data loss or data damage* caused

by malware infection (Bergmann et al., 2018; Bossler & Holt, 2009). In the current study, we opted to focus more broadly on *inconvenience* caused by malware infection. The lack of established guidelines on how cybercrime victimization should be measured is a limitation that should be taken into account when interpreting the results of the current study and when comparing victimization rates between studies.

8. Bibliography

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Springer.

Barnes, J. C., Boutwell, B. B., Beaver, K. M., Gibson, C. L., & Wright, J. P. (2014). On the consequences of ignoring genetic influences in criminological research. *Journal of Criminal Justice*, *42*(6), 471–482.

Barrera Jr, M., & Ainlay, S. L. (1983). The structure of social support: A conceptual and empirical analysis. *Journal of Community Psychology*, *11*(2), 133–143.

Belgian Federal Police. (2019). *Veiligheidsmonitor 2018.* Federale Politie DGR - Informatie en ICT.

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 84–90.

Bidgoli, M., & Grossklags, J. (2016). End user cybercrime reporting: What we know and what we can do to improve it. *Cybercrime and Computer Forensic (ICCCF), IEEE International Conference On*, 1–6.

Black, P., & Hendy, H. M. (2018). Perceived powerlessness as a mediator between life stressors and deviant behaviors. *Deviant Behavior*, 1–10.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227–236.

Brands, J., & van Wilsem, J. (2019). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*, 1–22.

Chen, Y. (2017). Examining internet users' adaptive and maladaptive security behaviors using the extended parallel process model. *ICIS 2017 Proceedings*. Thirty Eighth International Conference of Information Systems, South Korea. http://aisel.aisnet.org/icis2017/Security/Presentations/3

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *Mis Quarterly*, *40*(1), 205–222.

Chou, H.-L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, *65*, 334–345.

Conway, G., & Hadlington, L. (2018). How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. *Policing*, 1–11.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187–204.

Cross, C., Richards, K., & Smith, R. G. (2016a). *Improving responses to online fraud victims: An examination of reporting and support*. Criminology Research Grant Scheme, Australian Institute of Criminology. http://crg.aic.gov.au/reports/1617/29-1314-FinalReport.pdf

Cross, C., Richards, K., & Smith, R. G. (2016b). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, *518*, 1–14.

Crossler, R. E., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, *45*(4), 51–71.

Cullen, F. T. (1994). Social support as an organizing concept for criminology: Presidential address to the Academy of Criminal Justice Sciences. *Justice Quarterly*, *11*(4), 527–559.

De Kimpe, L., Walrave, M., Ponnet, K., & Van Ouytsel, J. (2019). Internet safety. In R. Hobbs & P. Mihailidis (Red.), *The International Encyclopedia of Media Literacy* (pp. 1–11).

DeValve, E. Q. (2005). A qualitative exploration of the effects of crime victimization for victims of personal crime. *Applied Psychology in Criminal Justice*, *1*(2), 71–89.

Eisinga, R., Grotenhuis, M. te, & Pelzer, B. (2013). The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown? *International Journal of Public Health*, 1–6.

Eurobarometer. (2017). *Special Eurobarometer 464a: Europeans' attitude towards cyber security*. European Commission.

European Commission. (2019). *Special Eurobarometer 480: Europeans' attitude towards Internet security*. European Commission.

Europol. (2019). *Europol in brief 2018: Fighting crime across borders*. https://www.europol.europa.eu/activities-services/main-reports/europol-in-brief-2018

Fattah, E. A., & Sacco, V. F. (1989). *Crime and Victimization of the Elderly*. Springer Verlag.

Ferraro, K. F. (1995). *Fear of crime: Interpreting victimization risk*. State University of New York Press.

Ferraro, K. F., & Grange, R. L. (1987). The measurement of fear of crime. *Sociological Inquiry*, *57*(1), 70–97.

Franklin, T. W., Franklin, C. A., & Fearn, N. E. (2008). A multilevel analysis of the vulnerability, disorder, and social integration models of fear of crime. *Social Justice Research*, *21*(2), 204–227.

Frieze, I. H., Hymer, S., & Greenberg, M. S. (1987). Describing the crime victim: Psychological reactions to victimization. *Professional Psychology: Research and Practice*, *18*(4), 299.

Fu, Y. (2005). Measuring personal networks with daily contacts: A single-item survey question and the contact diary. *Social Networks*, *27*(3), 169–186.

Gabriel, U., & Greve, W. (2003). The psychology of fear of crime. Conceptual and methodological perspectives. *British Journal of Criminology*, *43*(3), 600–614.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security*, *2010*(10), 16–18.

Goudriaan, H. (2006). *Reporting crime: Effects of social context on the decision of victims to notify the police*.

Green, D. L., Choi, J. J., & Kane, M. N. (2010). Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. *Journal of Human Behavior in the Social Environment*, *20*(6), 732–743.

Greve, W. (1998). Fear of crime among the elderly: Foresight, not fright. *International Review of Victimology*, *5*(3–4), 277–309.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55.

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review*, *28*(2), 201–207.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57.

IC3. (2018). *2017 Internet Crime Report*. Federal Bureau of Investigation. https://pdf.ic3.gov/2017_IC3Report.pdf

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

Jackson, J. (2004). Experience and expression: Social and cultural significance in the fear of crime. *British Journal of Criminology*, *44*(6), 946–966.

Jackson, J. (2009). A psychological perspective on vulnerability in the fear of crime. *Psychology, Crime & Law*, *15*(4), 365–390.

Jacobs, N. C., Völlink, T., Dehue, F., & Lechner, L. (2015). The development of a self-report questionnaire on coping with cyberbullying: The Cyberbullying Coping Questionnaire. *Societies*, *5*(2), 460–491.

Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 205–228.

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

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 129–137.

Kabay, M. E. (2009). Understanding studies and surveys of computer crime. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (5th ed.). Wiley.

Lamet, W., & Wittebrood, K. A. (2009). *Nooit meer dezelfde: Gevolgen van misdrijven voor slachtoffers*. Sociaal en Cultureel Planbureau.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Littleton, H. L. (2010). The impact of social support and negative disclosure reactions on sexual assault victims: A cross-sectional and longitudinal investigation. *Journal of Trauma & Dissociation*, *11*(2), 210–227.

Machmutow, K., Perren, S., Sticca, F., & Alsaker, F. D. (2012). Peer victimisation and depressive symptoms: Can specific coping strategies buffer the negative impact of cybervictimisation? *Emotional and Behavioural Difficulties*, *17*(3–4), 403–420.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150.

Maskall, P. (2017). Risk and digital security: The perception versus reality and the cognitive biases of online protection. *4th International Conference on Economic Sciences and Business Administration*, 280–287.

Mason, K. A., & Benson, M. L. (1996). The effect of social support on fraud victims' reporting behavior: A research note. *Justice Quarterly*, *13*(3), 511–524.

Meško, G. (2018). On some aspects of cybercrime and cybervictimization. *European Journal of Crime, Criminal Law and Criminal Justice*, *26*(3), 189–199.

Millman, R. (2016). Cyber-criminals becoming increasingly professional. *SC Media UK*. https://www.scmagazineuk.com/cyber-criminals-becoming-increasingly-professional/article/1477487

Modic, C., & Anderson, R. (2015). It's all over but the crying: The emotional and financial impact of internet fraud. *IEEE Security & Privacy*, *13*(5), 99–103.

Morgan, A., Dowling, C., Brown, R., Mann, M., Voce, I., & Smith, M. (2016). *Evaluation of the Australian cybercrime online reporting network*. Australian Institute of Criminology.

Muthén, L., K., & Muthén, B., O. (2012). *Mplus User's Guide. Seventh Edition.* Muthén & Muthén.

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior*, *62*, 136–146.

Pupillo, L. (2018). *EU cybersecurity and the paradox of progress* (pp. 1–6). https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. Automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*, 44–55.

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*, *22*(4), 396–411.

Richards, K., & Cross, C. (2018). Online fraud victims' experiences of participating in qualitative interviews. *Criminal Justice Studies*, *31*(1), 95–111.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, *52*(3), 596.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93–114.

Ruback, R. B., Greenberg, M. S., & Westcott, D. R. (1984). Social influence and crime-victim decision making. *Journal of Social Issues*, *40*(1), 51–76.

Sacco, V. F., & Glackman, W. (2009). Vulnerability, locus of control, and worry about crime. *Canadian Journal of Community Mental Health*, *6*(1), 99–111.

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207.

Shippee, N. D. (2012). Victimization, fear of crime, and perceived risk: Testing a vulnerability model of personal control. *Sociological Perspectives*, *55*(1), 117–140.

Stadler, C., Feifel, J., Rohrmann, S., Vermeiren, R., & Poustka, F. (2010). Peer-victimization and mental health problems in adolescents: Are parental and school support protective? *Child Psychiatry & Human Development*, *41*(4), 371–386.

Statistics Netherlands. (2019). *Digitale veiligheid & criminaliteit 2018*. https://www.cbs.nl/nl-nl/publicatie/2019/29/digitale-veiligheid-criminaliteit-2018

Tarling, R., & Morris, K. (2010). Reporting crime to the police. *The British Journal of Criminology*, *50*(3), 474–490.

Taylor, N. (2002). Reporting of crime against small retail businesses. *Trends & Issues in Crime and Criminal Justice*, *242*, 1.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150.

Tyugu, E. (2011). Artificial intelligence in cyber defense. *2011 3rd International Conference on Cyber Conflict*, 1–11.

van de Weijer, S. G., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, 1–23.

van Wilsem, J. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437–453.

Verdegem, P., Teerlinck, E., & Vermote, E. (2015). *Measuring cost and impact of cybercrime in Belgium (BCC): D.3.1.1. Risk perception report (1st wave, 2015).*

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law*, *24*(3), 323–338.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 1–17). Routledge.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1–2), 45–63.

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378–396.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329–349.

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), 317–342.

Wright, M. F. (2015). Cyber victimization and adjustment difficulties: The mediation of Chinese and American adolescents' digital technology usage. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *9*(1).

Yu, C.-Y. (2002). *Evaluating cutoff criteria of model fit indices for latent variable models with binary and continuous outcomes* (Vol. 30). University of California, Los Angeles Los Angeles.