End User Cybercrime Reporting: What We Know and What We Can Do to Improve It

Morvareed Bidgoli
College of Information Sciences and Technology
The Pennsylvania State University
University Park, PA, USA
mbidgoli@psu.edu

Jens Grossklags
College of Information Sciences and Technology
The Pennsylvania State University
University Park, PA, USA
jensg@ist.psu.edu

***Abstract*—After a physical crime occurs an important action typically takes place: the reporting of the crime to the police. However, this action becomes more complex for a victim to properly execute when a cybercrime is experienced, which can be partly explained for instance by a lack of knowledge about cybercrimes and computer security. Cybercrime reporting is crucial because it can provide a multitude of data such as the prevalence of cybercrimes, the types and nature of the cybercrimes present, and the various resulting types of loss or harm (e.g., financial, psychological, emotional). Moreover, cybercrime reporting data is also actionable for two reasons: (1) prevention tips can be produced to educate users of how they can mitigate commonly occurring cybercrimes they may be faced with, and (2) the information provided can be useful for the appropriate law enforcement agencies to potentially reach a proper resolution for the cybercrime victim (i.e., the cybercriminal being caught, the recovery of stolen property). However, comparatively few academic works have focused on better understanding computer users' cybercrime reporting behaviors. In this paper, we first review the relevant literature, which predominantly focuses on the reasons that contribute to the underreporting of cybercrimes. Next, we highlight four particular challenges of cybercrime reporting. These challenges include the issue of computer users potentially having difficulty in properly identifying cybercrimes they may experience, fostering knowledge of how to report cybercrimes to the appropriate channels, providing incentives for cybercrime reporting, and the extent of feedback victims receive after filing a cybercrime report. Grounded in the surveyed literature and our previous work, we also provide a set of recommendations on how to approach these challenges in order to improve currently existing cybercrime reporting processes.**

Keywords*—*cybercrimes, cybercrime reporting, behavioral research, information policy

I. Introduction

The nature and future of crime has expanded over the last few decades – crime has increasingly infiltrated the online space. Computer users are susceptible to becoming victims of a wide range of cybercrimes ranging from socially engineered cybercrimes (e.g., phishing) to more technically oriented cybercrimes (e.g., malware). Today, we see large-impact cybercrime incidents such as consumer data breaches on the rise where companies like Target, Home Depot, and T.J. Maxx have proven vulnerable to hackers resulting in millions of American consumers' credit and debit card numbers being compromised. In 2014, the Internet Crime Complaint Center (IC3) received 269,422 complaints resulting in a total loss of $800,492,073; 45.9% of the complaints received reported financial loss [1]. According to Reuters, cybercrimes are estimated to cost $445 billion annually worldwide [2]. It is evident that cybercrimes are an imperative issue worth addressing and effectively tackling.

After a crime occurs an important action typically takes place, which is the reporting of the crime to the appropriate law enforcement authorities. It is practically instinctive for citizens to know to immediately dial 9-1-1 to reach their local law enforcement agency after a physical crime takes place, but what happens in the event that a cybercrime occurs? It is not clear to what entity a citizen should report their cybercrime victimization. This by itself is a noteworthy problem worth addressing since the reporting of a crime is the first step taken towards a potential resolution of a crime. Furthermore, cybercrime reporting is crucial because it can provide a multitude of information such as the prevalence of cybercrimes, the types and nature of the cybercrimes present, and the various resulting types of loss or harm (e.g., financial, psychological, emotional). Therefore, it is

vital to understand computer users' reporting behaviors so that we can find effective means to not only encourage more cybercrime reporting to take place, but also to raise more awareness of the extent to which virtually any computer user is susceptible to cybercrimes.

This paper is structured as follows: We will begin by presenting relevant literature with regards to the issue of cybercrime reporting (Section II) and continue with a set of challenges and recommendations for how the process of cybercrime reporting can be better addressed and promoted to the computer user population at large (Section III). Finally, we offer concluding remarks (Section IV).

II. Related Work

The following section discusses related work focused on understanding the reasoning behind cybercrime reporting behaviors. Better understanding computer users' cybercrime reporting behaviors is crucial for two reasons. First, the reporting of cybercrimes serves an educational function for the general public by providing a statistical illustration of how severe of a social problem cybercrimes are (e.g., prevalence of cybercrimes, types of cybercrimes, and the harm that results from cybercrimes). Secondly, cybercrime reporting provides a window into better knowing what online practices or tools can be employed to mitigate cybercrime risk and hopefully even come to a proper resolution where the cybercrime can be mitigated and the cybercriminal can be apprehended. We observe that the most work has focused on identifying reasons for the underreporting of both physical crimes and cybercrimes. We review relevant literature in the following order: cybercrime reporting entities, reasons for the reporting of crimes, reasons for the underreporting of crimes, crime measurement issues and consequences of underreporting crimes, and end user proficiency in governmental agency reporting.

A. Cybercrime Reporting Entities

Before trying to understand what factors contribute to the reporting or underreporting of cybercrimes, it is worth noting where cybercrimes are reported in the United States. Fariborzi and Hajibaba [3] provide a systematic review of what entities oversee Internet crime complaints in a number of countries including the United States. In the United States, FBI local offices, the U.S. Secret Service, and the IC3 handle the reporting of cybercrimes such as hacking, Internet fraud, and cyberharassment [3]. There are also a number of useful online resources that U.S. computer users can consult on how to report cybercrimes such as the Law Enforcement Cyber Incident Reporting document provided by the Department of Homeland Security (DHS) (see [4]) and a description of the various steps it takes to report an identity theft provided by the Federal Trade Commission (FTC) (see [5]). In this paper, we specifically focus on the IC3 for our analysis and recommendations of how currently existing cybercrime reporting mechanisms can be improved.

B. Reasons for the Reporting of Crimes

When discussing cybercrime reporting, initial questions to ask are what triggers cybercrime reporting behaviors and how the process of cybercrime reporting can be better motivated. Skogan [6] states that the reporting of crimes takes place because people want to have the self-perception of being a "good citizen" aiming to help mitigate crime from occurring (pp. 121-122). Additionally, a victim's perception of a resolution being reached (i.e., the criminal being caught by the police and convicted by the courts) also encourages reporting [6, p. 121] [7].

C. Reasons for the Underreporting of Crimes

A number of reasons have been found that contribute to the underreporting of crimes both offline and online. One reason both Yar [8] and Wall [9] highlight is that a victim may consider the cybercrime they experienced to lack enough seriousness to warrant contacting the authorities. However, it is worth noting that as Skogan [6] points out the perceived severity of a crime such as an item of value being stolen in a burglary can increase the likelihood of reporting. Moreover, Schneider et al. [7] found that for both property and personal crimes with high severity (e.g., the amount of monetary loss for property crimes), there was a higher likelihood of reporting than for crimes with low to moderate severity. Goucher [10] provides other reasons for why cybercrimes go underreported such as a victim's perception that the process of reporting is "a waste of time and effort," that there is a low likelihood the cybercriminal will get caught, that the victim blames themselves for falling for a cybercrime, and that the victim does not want to be labeled as a "victim" (p. 17). To shed some light on the magnitude of one of the previously mentioned reasons, Goucher [10] cites a Symantec survey that found that "80% of responders said that they did not expect a cybercriminal to get caught" (p. 17).

Yar [8], Wall [9], and Goodman and Brenner [11] state that a cybercrime victim may be unaware that they experienced a cybercrime. Fafinski et al. [12] further add that the lack of knowledge that a cybercrime occurred is due in part to the lack of expertise computer users have in understanding the nature of existing cybercrimes (p. 14). Al- Nemrat et al. [13] further elaborate on this point by stating that cybercrime is a term people are familiar with, but that there are many interpretations as to what a cybercrime constitutes and not a specific definition that has been adopted for cybercrime (p. 56). They explain that this "definitional" issue can greatly affect the process of investigating and reporting [13, p. 56]. Both Wall [9] and Goodman and Brenner [11] suggest that a feeling of embarrassment over being a cybercrime victim can also be a contributing factor to a cybercrime going unreported. Lastly, Wall [14] makes the point that with the onset of new reporting mechanisms in countries like the United States (i.e., the IC3), it will take some time for such mechanisms to be adopted by the public (p. 194).

D. Crime Measurement Issues and Consequences of Underreporting Crimes

There is also a set of less conventional explanations as to why both physical crimes and cybercrimes go unreported. Both Yar [8] and Wall [9] suggest that a cybercrime can go unreported due to how cybercrimes are recorded by the police. Yar [8] suggests that the police's perception of the severity of a cybercrime under consideration can impact whether or not they deem it worthy of being addressed; additionally, if a cybercrime is believed to have a low probability of being properly resolved it is unlikely to be recorded in the first place in order to maintain the public's perception of the police's overall effectiveness (p. 12). On the other hand, Wall [9] gives a different explanation for the issue by stating that a cybercrime victimization may not be officially recorded by a law enforcement agency as an incident of cybercrime if it was handled by another entity; for example, credit card fraud is typically an issue handled by banks or credit card companies (pp. 53-54).

Based on National Crime Panel victimization data, Singer [15] found that in certain instances of crime victimization, the fear of reprisal (i.e., a future attack) can lead to crimes going unreported. More specifically, this becomes evident in crimes involving females who were victims of domestic violence or rape and knew their attackers (i.e., a family member or spouse) [15]. Additionally, the severity of the crime also impacts the likelihood of reprisal, which others have shown can actually motivate the reporting of crimes to the police [15, pp. 289-290]. While it is recognized that the findings presented by Singer [15] are generalizable to certain instances of physical crimes, it can be argued that the fear of reprisal may also be a potential reason for cybercrimes going unreported in situations where a cybercrime victim may indeed know their attacker such as in cases of cyberstalking or cyberharassment.

Skogan [6] points to the importance of crime reporting by stating that a consequence of the non-reporting of crimes can lead to a misallocation of police resources leaving areas in need of attention underprotected (p. 115). Goodman [16] seconds this point by stating, "law enforcement resources are allocated based upon the number of reported crimes" (p. 484). Similarly, Swire [17] mentions that due to the small number of complaints that are received from each jurisdiction, it becomes difficult for law enforcement to effectively identify and target the "bad guys" (p. 108).

E. End Users' Proficiency in Governmental Agency Reporting

In non-cybercrime contexts, Bridges et al. [18] experimentally studied the behaviors of a small sample of undergraduate participants from a U.S. public research university to test their aptitude in correctly identifying the appropriate government agencies' websites in order to contact them. The researchers developed four different policy scenarios, which included a diabetes prescription recall, airport traffic, green house gas emissions, and health care (pp. 167-168). They found that only 50% of the study participants were able to complete the appropriate search tasks for each of the given scenarios illustrating that the participants did not know how to contact the appropriate government agencies to help resolve the policy issue in question [18, p. 170]. Additionally, participants shared thoughts of skepticism in contacting various government departments and agencies via social media by stating that such a process lacks "authenticity regarding what is done with the information once it is conveyed" and that an inundation of messages sent to the government would lead to a lower likelihood of a response being received from a government official [18, p. 172]. Although this study does not specifically entail testing the proficiency of undergraduate students reporting cybercrimes, it does shed light on how there is a lack of knowledge about the structure of government and who to contact when an issue concerning a private

citizen arises whether it be public policy or crime related. Additionally, it points to the general pessimism felt towards reporting issues to government agencies in not reaching an effective resolution. Thus, Skogan [6] states that citizen involvement in crime prevention along with an understanding of local government can help promote the likelihood of contacting the police (p. 132).

III. Recommendations on How to Better Address the Process of Cybercrime Reporting

Before providing our recommendations, we would like to mention previously discussed proposals provided by the literature on how to specifically address the underreporting of cybercrimes. Brenner [19] suggests having a civilian network that will be trained with "a set of operating standards and cyber event identification criteria" (p. 472). Brenner makes this recommendation based on the role of civilians in the Civil Air Patrol during World War II where civilians were "trained to recognize enemy aircraft, so as to report if any were seen" by further adding that such a network will be able to provide law enforcement agencies with information they may or may not have received [19, p. 473]. Moitra [20] highlights that better methods must be adopted to help mitigate the issue of the underreporting of cybercrimes. In particular, Moitra [20] suggests that this can be achieved by raising more public awareness about cybercrime reporting, bringing more attention to law enforcement agencies that receive reporting data, and developing a "well-understood, uniform taxonomy for cybercrime" (p. 451).

We will now address four challenges we believe are worth addressing in order to improve the process of end user cybercrime reporting. These challenges are as follows:

- defining a cybercrime victimization,
- fostering knowledge of how to report cybercrimes,
- incentivizing the cybercrime reporting process, and
- providing feedback during the cybercrime reporting process.

A. Challenge #1: Defining a Cybercrime Victimization

Cybercrime is a term that many computer users may believe they seem to understand, but do not necessarily understand within the legal context. The extent to which computer users have knowledge of cybercrimes is crucial when it comes to the cybercrime reporting process. Without proper knowledge of the cybercrimes that exist today, we are more likely left with the significant consequences of cybercriminals being successful and cybercrimes being left unreported. Given the complexities of legally defining various cybercrimes and the continued evolution and emergence of new cybercrimes, it becomes a great challenge to the reporting process as pointed out by Al-Nemrat et al. [13]. Thus, it becomes evident that the extent of a computer user's cybercrime knowledge is an important factor that influences the cybercrime reporting process for them to first be able to identify that a cybercrime occurred. Secondly, we believe the label of "victim" or "victimization" becomes yet another challenging aspect to tackle from a potential victim's vantage point in that they may have varying definitions regarding when they have crossed the "victim line." For example, if a computer user is a victim of credit card fraud it is customary to report the fraudulent charges to an individual's respective bank; however, as Wall [9] points out when banks are notified of credit card fraud the police are typically not notified of the victimization leaving the cybercrime unreported. Moreover, such an example also prompts the question: if a cybercrime is "solved" (e.g., property is returned or malware is removed from a personal computer) does a computer user still consider themselves a victim? Should they still feel obligated to report their cybercrime experience to the appropriate law enforcement agencies? These are questions we believe are worthwhile to unpack since such negotiations made on behalf of a cybercrime victim can greatly impact the cybercrime reporting process.

In order to address this problem space, we would have to find ways to properly educate society at-large about the cybercrimes that exist. One way of achieving this could be by providing specific and clear delineations as to what constitutes a cybercrime and what does not via current reporting mechanisms such as the IC3 to help mitigate potential confusion that can significantly impact the likelihood that cybercrimes will go reported.

B. Challenge #2: Fostering Knowledge of How to Report Cybercrimes

While there have been a number of reasons provided by the literature as to why cybercrimes go underreported, there is only limited research exploring what role knowledge of cybercrime reporting plays during the reporting process. In a previous study we conducted, we found

that undergraduate students did not feel knowledgeable enough to report cybercrimes [21]. In fact, out of 10 individuals interviewed, there was not a single interviewee who knew how to officially report a cybercrime [21]. Additionally, out of 222 survey participants only 4.5% had heard of the IC3 [21]. What makes these results even more troubling is the fact that despite not feeling confident in their abilities to report cybercrimes, a majority of the study's participants expressed that they believed having knowledge in how to report cybercrimes and having access to cybercrime victimization statistics were important [21]. It is evident from these findings alone that a lack of knowledge about how to report a cybercrime to the appropriate entities can greatly impact the likelihood that a cybercrime will be reported. Therefore, we consider it crucial that more awareness needs to be brought to society at-large about the resources that are at an individual's disposal when they find themselves victimized by a cybercrime (e.g., contacting the IC3).

Furthermore, the process of reporting cybercrimes is rather complex and is not as straightforward as the simple dialing of 9-1-1 in the event of a physical crime. In order to help illustrate this, consider a cybercrime victim was interested in reporting identity theft; a cybercrime that according to the U.S. Bureau of Justice Statistics affected 17.6 million Americans in 2014 [22]. According to the Federal Trade Commission's (FTC) website, an identity theft should be reported to the following entities: the companies where the fraud occurred, the FTC, and the victim's local police department [5].

With our research we aim to bridge the gap between computer users' desire to report cybercrimes and the knowledge they need in order to do so.

C. Challenge #3: Incentivizing the Cybercrime Reporting Process

A common sentiment among computer users is that reporting cybercrimes will not lead to satisfactory results being reached such as the cybercriminal getting caught, which can negatively impact a willingness to engage in the reporting effort [10]. However, there may be ways to help alleviate such concerns to help encourage the reporting of cybercrimes. Fafinski et al. [12] highlight that the specific issue of incentivizing the cybercrime reporting process should be addressed. For instance, they propose reasoning about potential outcomes that can be produced post-reporting such as providing advice to computer users to ensure online protection or instituting effective policing procedures to tackle cybercrimes [12, p. 17].

The IC3 provides helpful Internet crime prevention tips on their website (www.ic3.gov) and on another website they run (www.lookstogoodtobetrue.com) which provides a list of testimonials from people who either fell victim to a scam or experienced a scam and share how they avoided being a victim. However, it is apparent that such websites are not well publicized and known to computer users [21].

To better incentivize reporting, resources provided from currently existing cybercrime reporting mechanisms (e.g., the IC3 and FTC) need to be better publicized, so that the general public can utilize prevention tips to mitigate their cybercrime risk. Moreover, it is reasonable to expect that if computer users actually saw tangible output such as cybercrime victimization statistics, online prevention tips, or knowledge of a police presence making effective strides towards combatting cybercrimes then more computer users would feel compelled to report cybercrimes. In addition, given the fact that entities like the IC3 are run by federal law enforcement agencies (i.e., the FBI), it may make more sense to consider the creation of alternative reporting channels to handle cybercrime reports that are on a more localized level. Localization of reporting mechanisms (e.g., at the city or county level) may incur incremental costs, but the benefits are likely to outweigh the costs for two reasons. First, the report data received would appear more relevant to the population at hand. Second, the perceived line of communication between the victim and law enforcement would be less far removed.

D. Challenge #4: Providing Feedback During the Cybercrime Reporting Process

The final challenge ties in well with challenge #3 in terms of trying to understand ways in which we can better convey the benefits tied to reporting in order to encourage end user cybercrime reporting. Currently, there is not enough public knowledge about the extent to which a victim receives feedback about their reported case. We know with physical crimes that actual follow-ups do take place with victims to keep them informed about the status of their cases; however, there is not the same level of transparency when it comes to the cybercrime reporting process. A partial account of what happens with cybercrime reports is provided by the IC3's 2014 Internet Crime Report in which they state that

out of the 269,422 complaints they received over 1,500 referrals were relayed to the appropriate law enforcement agencies [1, p. 19]; however, we do not know the rate of success of those referrals or whether any feedback was provided to the victims about these referrals.

Due to the lack of transparency provided by the IC3 in their report regarding the matter of feedback, we suggest exploring the possibility of an entity such as the IC3 to produce case files that a user can access to see the current status of their filed report. The addition of such a feature can potentially boost the public's confidence in the reporting process to enhance the perception that positive outcomes can be achieved from filing a report or at the very least that a potentially effective feedback loop exists. However, we are also aware that the addition of such a feature may be a substantial burden for the back-end side of reporting (i.e., report responders such as information security companies and law enforcement); thus, a feasible middle-ground solution must ultimately be found for the issue of feedback.

Despite these inherent tradeoffs, if currently existing cybercrime reporting mechanisms (e.g., the IC3) provide at least incrementally more information regarding the potential feedback both victims and the public would receive (whether it is the creation of case files or anecdotal stories/clearance rates of closed reported cybercrime cases) then it could potentially encourage more cybercrime reporting to take place.

IV. Conclusion

In this paper, we discussed relevant literature that pertains to cybercrime reporting. To our knowledge, there have only been a few recommendations provided by the literature [19], [20] on how to begin effectively addressing the well-stated issue of the underreporting of cybercrimes; moreover, there is virtually no literature conducted on how current cybercrime reporting mechanisms can be better designed to help mitigate such an issue. We then provided a list of four important challenges within the context of the cybercrime reporting process along with initial recommendations on how such challenges can be overcome.

One main takeaway from the four challenges discussed is computer users' lack of knowledge of how to report cybercrimes. In particular, as shown by results from our previous work [21], an active segment of the computer user population (i.e., undergraduate students) do not have confidence in their ability to report cybercrimes. Thus, we need to find effective ways to promote public awareness about how to report cybercrimes as well as how to protect against and learn more about cybercrimes (i.e., access to cybercrime victimization statistics, prevention tips, etc.).

Additionally, we believe that there are opportunities for research to be done in order to improve currently existing cybercrime reporting mechanisms (i.e., the IC3) and in the process to incentivize cybercrime reporting to take place. Therefore, we also observe that there is a need for design improvements to be made to both the user interface as well as the back-end side of cybercrime reporting websites (i.e., providing suitable data to increase incentives to report such as feedback during the reporting process). Tackling the issues underlying cybercrime reporting is a crucial step towards fighting the war on cybercrime.

References

[1] "2014 Internet Crime Report [Online]," 2014, available at: https://www.fbi.gov/news/news_blog/2014-ic3-annual-report.

[2] P. Sandle, "Cyber crime costs global economy $445 billion a year: Report," *Reuters*, 2014.

[3] E. Fariborzi and M. Hajibaba, "Computer crimes, problems, law enforcement for solving complaints and education," in *International Proceedings of Computer Science & Information Technology*, vol. 43, 2012, pp. 19–23.

[4] "Law Enforcement Cyber Incident Reporting [Online]," available at: https://www.dhs.gov/sites/default/files/publications/LawEnforcementCyberIncidentReporting.pdf.

[5] "Federal Trade Commission IdentityTheft.gov [Online]," available at: https://identitytheft.gov/Steps.

[6] W. G. Skogan, "Reporting crimes to the police: The status of world research," *Journal of Research in Crime and Delinquency*, vol. 21, no. 2, pp. 113–137, 1984.

[7] A. L. Schneider, J. Burcart, and L. A. Wilson, "The role of attitudes in decisions to report crimes to the police," *Criminal Justice and the Victim*, 1976.

[8] M. Yar, *Cybercrime and the Internet*, 2nd ed. SAGE, 2013.

[9] D. S. Wall, "Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime," *International Review of Law, Computers & Technology*, vol. 22, no. 1–2, pp. 45–63, 2008.

[10] W. Goucher, "Being a cybercrime victim," *Computer Fraud & Security*, vol. 2010, no. 10, pp. 16–18, 2010.

[11] M. D. Goodman and S. W. Brenner, "Emerging consensus on criminal conduct in cyberspace," *International Journal of Law and Information Technology*, vol. 10, no. 2, pp. 139—-223, 2010.

[12] S. Fafinski, W. H. Dutton, and H. Z. Margetts, "Mapping and measuring cybercrime," *Oxford Internet Institute Working Paper No. 18*, 2010.

[13] A. Al-Nemrat, H. Jahankhani, and D. S. Preston, "Cybercrime victimisations/criminalisation and punishment," *Global Security, Safety, and Sustainability*, pp. 55–62, 2010.

[14] D. S. Wall, "Policing cybercrimes: Situating the public police in networks of security within cyberspace," *Police Practice and Research*, vol. 8, no. 2, pp. 183—-205, 2007.

[15] S. I. Singer, "The fear of reprisal and the failure of victims to report a personal crime," *Journal of Quantitative Criminology*, vol. 4, no. 3, pp. 289—-302, 1988.

[16] M. D. Goodman, "Why the police don't care about computer crime," *Harvard Journal of Law & Technology*, vol. 10, no. 3, pp. 465–494, 1997.

[17] P. Swire, "No cop on the beat: Underenforcement in e-commerce and cybercrime," *Journal on Telecommunications and High Technology Law*, vol. 7, no. 107, pp. 107—-126, 2009.

[18] F. Bridges, L. Appel, and J. Grossklags, "Young adults' online participation behaviors: An exploratory study of web 2.0 use for political engagement," *Information Polity*, vol. 17, no. 2, pp. 163–176, 2012.

[19] S. W. Brenner, "'At light speed': Attribution and response to cybercrime/terrorism/warfare," *The Journal of Criminal Law and Criminology*, vol. 97, no. 2, pp. 379–475, 2007.

[20] S. Moitra, "Developing policies for cybercrime," *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 13, no. 3, pp. 435–464, 2005.

[21] M. Bidgoli, B. P. Knijnenburg, and J. Grossklags, "When cybercrimes strike undergraduates," *Eleventh Symposium on Electronic Crime Research (eCrime)*, 2016.

[22] E. Harrell, "Victims of identity theft, 2014 [online]," 2015, U.S. Department of Justice, available at: http://www.bjs.gov/content/pub/pdf/vit12.pdf.