RISCS

RISCS Briefing

Online Victimisation

Dr Maria Bada, RISCS Fellow • May 2021

Summary

This briefing describes interim findings of work which aims to 1) explore the impact of online crime in the UK from the victims' perspective and 2) understand the role, challenges, and capacity of the police, the judiciary and other authorities in dealing with such crimes. This has been achieved through a literature review, interviews with representatives from academia, the private sector, law enforcement, Government and prosecution and also by analysing statements by victims of a data breach.

This document details the psychological, emotional and physical harms which can be experienced by victims of cybercrime and highlights the challenges facing those trying to tackle this problem, whether working in law enforcement, Government and academia, including data gaps and barriers to data reporting.

Introduction

Cybercrime can affect everyone, for example at the individual level it can result to fraud incidents, or at the national level targeting critical infrastructure. A key aspect of understanding the public response to malicious cyber-attacks centers upon the fact that members of the public do not appear to perceive such attacks as a threat to themselves and, if they do, they believe that there is very little that they can do to prevent such an attack (Bada and Nurse, 2019). Something like this can be a problem because it can lead to individuals not taking the necessary measures to protect themselves online.

Victims of cyber-attacks and cybercrime can suffer emotional trauma which can often lead to depression (Kaakinen, et al., 2018). Similar findings with victims of computer misuse report psychological impacts such as anger, anxiety, fear, isolation and embarrassment (Button, et al., 2020). For example, a victim of identity theft after a data breach, might be left feeling violated, betrayed, vulnerable, angry and powerless (Kirwan and Power, 2011). Depending on the type of victimisation, the victim can go into stages of grief, suffer from anger or rage. In some cases, victims may even blame themselves and develop a sense of shame. The emotional impact can of course lead to trauma and consequently to physical symptoms such as difficulty sleeping (Dallaway, 2016).

Such impact can also be caused by a data breach. The personal data of an individual is sold off and they could be used later on at an unknown time. Harm may occur immediately after an incident or may be obvious in the long term. Therefore, the timing of the harm might be different for each victim. To the individuals whose personal data is leaked into the hands of someone unknown to them, the risk of harm is continuing. In the meanwhile, the individuals worry that their information will be misused and spend time and resources to protect themselves from this possibility (Solove, 2018).

The reactions to such an incident may differ according to the disclosed identity of a given attacker or the person who caused the data breach. Additionally, the scale of an attack will influence its impact. We have seen often the full extent of an attack not becoming apparent immediately (Agrafiotis, et al., 2016). For example, personal information stolen from a data breach, might be used years later for another attack. Overall, the severity of the impact of a cyber-attack, will also depend on the actual victim, their sense of self-efficacy and control of the situation. For example, the vast majority of victims of fraud and computer misuse have only been victimised once, with only a small proportion saying they have suffered two or more times.

Just as in other types of victimisation, victims of cybercrime can experience serious consequences, emotional or not. First of all, a repeat victim of a cyber-attack might face serious financial or emotional hardship which can lead to health problems. These victims are also more likely to require medical attention as a consequence of online fraud victimisation. This means repeat victims have a unique set of support needs, including the need for counselling, and support from the criminal justice system.

Methods and Victim Profile

In this study, the methods for data collection used are:

a. Literature review.
b. Interviews with stakeholders from academia, private sector, government, law enforcement and prosecution.
c. Victim impact statements by victims of data breach.

Data Collection

Interviews

The interviews aimed to understand:

d. The landscape of reporting, support and investigation of online crime.
a. Current policies/practises.
b. Victim understanding of online crime.
c. Skills and capacity of authorities to prevent and respond to victimisation.

Victim Impact Statements

The researcher gained access to anonymised data from victim impact statements from a court case concerning victims of a data breach. The purpose of the victim impact statement (VIS) is to inform judges of victims' crime-related physical, psychological, and financial harms (Miller, 2013). The statements include

Research Aim

The aim of this study is to: 1) explore the impact of online crime in the UK from the victims' perspective and 2) understand the role, challenges, and capacity of the police, the judiciary and other authorities in dealing with such crimes and providing support for victims.

Participants

Interviews were conducted with 11 representatives from Action Fraud, Police Constabulary, Regional Organised Crime Unit, a Large Organisation (with several thousand employees) and academics specializing in victimisation.

information such as demographics of victims, information about the incident and the impact on the victims.

Profile of Victims

In this study, a sample of 83 victim impact statements were analysed. The victims' personal details were breached between 2005 and 2019. The victims whose personal details were breached were women, UK residents, 27-52 years old.

- Victims had experienced some form of personal information data breach.
- The data breach was caused due to providing their personal details for commercial reasons to a company they trusted. The data were then sold to third companies without their consent.

Results

Impact of Data Breach

The data analysed from the victim impact statements illustrate the different types of impact of an incident such as a data breach. The specific profile of the victims does not allow for the findings to be generalised. The data revealed that:

- On most occasions, the victims of data breach experienced an extreme violation of their privacy and security of their data.
- Many of the victims of a data breach were also victims of fraud (hacked bank accounts).
- For the individuals whose personal data is leaked into the hands of someone unknown to them, the harm such as stress and anxiety is continuing.

Overall, the majority of victim impact statements state that stress was one of the symptoms caused by the data breach. Fear was also one of the emotions mentioned in most statements. A very common symptom in victims of online and offline crime is also feeling violated. Some of the psychological or emotional symptoms described in victim impact statements are presented below:

Psychological and Emotional Impact upon Victims of Data Breach

Impact on Victim	Symptoms
Psychological	Stress
	Anxiety
	Depression
Emotional	Panic
	Frustration
	Worry
	Angry
	Afraid
	Disappointed
	Upset
	Guilty
	Embarrassed
	Feeling violated
Health related Impact	Lack of Sleep
	Harassment

Data Breach resulting in Fraud

Also, 31.3% of the victims had experienced a fraud related incident as a result to the data breach. Some examples here are described as stated by the victims:

"I have also been the victim of numerous Frauds. For example, my Uber, PayPal and Spotify accounts have all been hacked and I have had to change the passwords for these" (Victim 1).

"I have also been the victim of Fraud as someone used by E-Bay account via Paypal to fraudulently purchase a video game" (Victim 2).

"My email account was hacked twice last year, as was my Netflix account and my Barclay Card Account was hacked two years ago" (Victim 3).

Current practises and capacity

The key issues identified from the interviews conducted with experts in the field are a lack of:

- Awareness around reporting
- Data around victimisation
- Training of law enforcement and judiciary
- Understanding of the barriers and facilitators for victims to report online crimes
- Support for victims

In terms of Police practises, currently data are collected around the vulnerability of online victims, the type of harm and impact caused by an incident, and reporting practises. However, this process is not structured. Therefore, the data are not comparable across forces.

Reporting online incidents

An interesting point that came after discussions with experts, is about reporting incidents from victims. As mentioned, "Victims will try to report to charities, on twitter, to the police… The police do not always have the resources or the capacity to handle such cases. It is not their fault…" (Academic).

Regarding the traits and characteristics of victims who would actually report an incident it is mentioned that "Victims are all interested about their data privacy. The under 35's are more aware of the value of their data" (Prosecutor).

Gaps and Challenges

1. Lack of data

One of the main challenges in conducting research in the field of cybercrime and victimisation is the lack of data. Identifying the best methods for collecting and sharing data for such research is necessary, as well as the use of a broad range of research methodologies and tools. Access to datasets collected by the police, such as Action Fraud, complaint records from Telecoms, or cases prosecuted under the Computer Misuse Act, could lead into more targeted research. Coordinated data collection from the authorities can also help researchers conduct research which can inform policy making at a faster pace.

2. Barriers and facilitators in victim reporting

A better understanding of the barriers and factors that facilitate victims reporting an incident is needed. Setting clear guidelines and maintaining accessible communication channels for those affected to contact the authorities need to be further explored. A multi-sector approach needs to be followed with academics in collaboration with law enforcement, the private and public sector.

Prevention and training in victimisation: Setting guidelines for training law enforcement and the judiciary on basic cybercrime related aspects and on the victims' needs is imperative. In addition, shaping effective policy interventions in order to counter the psychological, emotional, behavioural, physical and financial impact of cybercrime on victims is necessary. Online victims will often avoid the Internet after their negative experience, therefore interventions to ensure victims are comfortable online again may be essential for their wellbeing.

Awareness and e-safety: Everyone should have the opportunity to use the internet safely and securely without being at risk of becoming a victim. Internet safety is important to secure online transactions for example or prevent children from online harms. However, it is difficult to eliminate cybercrime and there is lack of understating and research around the psychological impact of cybercrime for victims. At the moment research in this area is limited, therefore it is not clear what the best approach to supporting online victims would be.

Conclusion

Overall, this research has shown that online victimisation is a potentially traumatizing experience which can be linked to a myriad of negative effects. The impact of a data breach on an individual can cause different levels of psychological/emotional harm. In contrast to physical cyber harm, psychological/emotional cyber harm can be both the primary harm of an incident and have a long-term and indirect cascading effect, which either follows other types of harm or occurs in parallel. Psychological harm can be a secondary or subsequent type of harm for victims who have suffered another type of direct or primary harm, e.g. economic harm in the form of financial losses of fraud victims.

More detailed findings will be published later this year in the form of an academic paper. Findings will also be shared with practitioners and policy stakeholders.

Ethical considerations

Ethical issues throughout this research were particularly considered to protect personal information that could lead to identifying participants. There were also procedural concerns relating to data protection requirements. All anonymised data were collected and stored using encrypted methods.

Contacts

If you would like to discuss about this research or interested in further details, please contact: Maria Bada, maria.bada@cl.cam.ac.uk.

During her RISCS Fellowship on Cybercrime, Maria Bada has been exploring the impact of online crime of victims and how these might differ from the situation and needs of victims of traditional offline crimes. The RISCS Fellowship will deliver policy recommendations for training and risk assessment, a future research agenda, and practical options for supporting similar research going forward.

Many thanks to the NCSC and the Home Office for assisting in this research.

References

Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Roberts, T., & Upton, D.M., *Cyber Harm: Concepts, Taxonomy and Measurement (August 1, 2016), Saïd Business School WP 2016-23.* Retrieved from: https://ssrn.com/abstract=2828646 or http://dx.doi.org/10.2139/ssrn.2828646

Bada, M. and Nurse, J.R.C. (2019). The Social and Psychological Impact of Cyber-Attacks in *Emerging Cyber Threats and Cognitive Vulnerabilities.* Editors: Professor Vladlena Benson and Dr John McAlaney, Elsevier. https://arxiv.org/abs/1909.13256

Button, M., Sugiura, L., Blackbourn, D., Shepherd, D. W. J., Wang, V., & Kapend, R. (2020). *Victims of Computer Misuse: Main Findings.* University of Portsmouth. https://www.gov.uk/government/organisations/home-office

Dallaway, E (2016). #ISC2Congress: Cybercrime Victims Left Depressed and Traumatized. *Infosecurity Magazine.* Retrieved from https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/

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.*

Kirwan, G. & Power, A. (2011). *The Psychology of Cyber Crime: Concepts and Principles.* IGI Global.

Miller, K-L. (2013). Purposing and Repurposing Harms: The Victim Impact Statement and Sexual Assault. *Qualitative Health Research, 23(11):1445-1458.* doi:10.1177/1049732313507753

Solove, D.J. (2018). *Risk and Anxiety: A Theory of Data-Breach Harms.* 96 Tex. L. Rev. 737.