[9139] Reviewing Estimates of Cybercrime Victimisation and Cyber Risk Likelihood

PRELIMINARY DECISION: accept

Summary of Reviews

- Review 1: 1 (3)
- Review 2: 3 (4)
- Review 3: 2 (5)
- Review 4: -2 (4)

Reviews

Review 1

TOTAL SCORE: 1

Overall evaluation: 1 (weak accept)

Reviewer's confidence: 3 (medium)

This paper reviews the quantitative evidence available for both cybercrime victimisation for individuals and firms (not society) and cyber risk likelihood, aiming to identify insights on quantification.

The methodology is clearly described. The study is not a systematic review of relevant studies but followed a broad online search. Data were collected from 45 studies conducted by academics, statistical institutes, and cybersecurity vendors using a range of data sources including victim surveys, case-control studies, and the insurance market. Victimisation estimates are extracted from 2017–2021, across nine categories: cyber attack; malware; ransomware; fraudulent email, online banking fraud; online sales fraud; unauthorized access; Denial of Service; and identity theft.

The results are quite interesting, presenting the challenges faced with the use of non-systematic data collection, longitudinal trends seeming to contradict each other as well as different approaches followed in measuring crime prevalence for various types of attacks. A few notable findings are presented such as some studies reporting general banking fraud, in addition to online banking fraud. In addition, it is mostly the economic impact which is being measured not the societal impact of cyber-attacks.

The study summarises the findings clearly demonstrating the need for further efforts to develop better approaches around online victimisation quantification.

Similar challenges have been identified in relevant work such as by Button et al. (2020) looking specifically at victims of computer misuse. I would expect practical considerations and recommendations to be included on how we could solve these challenges. The suggestions provided seem high level.

It would be expected to also present existing data points (if any) for measuring more complex harms such as social or psychological impact of cyber-attacks.

Also, the paper needs a thorough spelling review as some errors are spotted. In page 2, please update this sentence: …and by sampling much more grey literature including grey literature (over 20 research studies versus 6 in their work).

Overall, this is a very interesting approach and it is expected to lead to interesting discussions during the workshop.

Review 2

TOTAL SCORE: 3

Overall evaluation: 3 (strong accept)

Reviewer's confidence: 4 (high)

This paper is a literature review of a sample of papers that examine the frequency of a set of cyber incidents. The paper flows well from one section to the next. However, it would benefit from editing by a native English speaker. There are a number of sentences which are grammatically incorrect. e.g. "they are unlikely to conduct such research if firms no-one consumers it."

The authors seek to derive useful estimates of cyber incident frequency, as defined by the number of incidents within a sample of entities, by the full population of entities. Computing this calculation across all papers provides, what the authors hope, is a reasonable approximation of the true likelihood of cyber attack. This approach is replicated for firm-based estimates, and consumer-based estimates. Certainly there are many limitations of, and caveats with, this approach, but the authors are clear to express those.

The authors write, "Unreliable estimates of cybercrime victimisation matter because of how firms and governments use such figures to prioritise mitigation resources" - this is a really important and useful observation and gets at the heart of much legal policy interventions. And yet reliable estimates remain very elusive.

The authors write, "Informal reasoning suggests firms invest more in prevention if cybercrime is more likely to happen." -- this is not informal reasoning, but classic economic cost minimization: investment in prevention controls is increasing with the benefit from doing so (ie. loss avoided).

Figure 3 is interesting. The authors suggest that incident rate is increasing in the number of employees a firm has. To my knowledge, that is a correlation that has not been estimated publicly before. And if nothing else, provides some evidence supporting the approach some insurance carriers take to pricing cyber risk -- that larger firms (as measure by assets or revenue) present a greater risk -- that is, if we assume asset/revenue is correlated with number of employees. That being said, Figure 3 still suffers from large confidence intervals, given that any inferences are identified with only a few data points.

Does table 3 represent the source data points for Figures 2 and 3? If so, it would be most helpful if it could include columns for Firms-based or Consumer-based (used in Fig 2), and size of employees (used in Fig 3).

In regard to crime prevalence for online sales fraud, the authors may be interested by annual data collected by the US Federal Trade Commission (FTC)' Sentinel database, which records consumer complaints for similar offenses, publicly available since 2006, https://www.ftc.gov/enforcement/consumer-sentinel-network/reports. Further, the US's Bureau of Justice Statistics (BJS), provides some annual reports of consumer identity theft, based on family household surveys. These are quite well done. See https://bjs.ojp.gov/topics/crime/identity-theft/

In regard to the scales used in the figures. While generally appropriate, I would actually like to see them all plotted on a scale from 0-100. Yes, it is generally good practice to keep the scale as focused as possible. However, this also has the effect of visually inflating the differences between estimates. And in this case, it may, actually, be more informative (useful) to see the plots scaled fully - then we may find that, in fact, the differences are not as pronounced as they appear.

The finding of no effect of COVID on the incident rates was also an interesting insight.

Overall, despite the data limitations, this was a wonderful paper to read. Well done.

Review 3

TOTAL SCORE: 2

Overall evaluation: 2 (accept)

Reviewer's confidence: 5 (expert)

To my knowledge, this is the first study of its kind that expands on the work of Reep-van den Bergh and Junger and uses a broader sample of surveys, both methodologically (incorporating vendors' data) and geographically (going beyond European data). This is a much-needed approach because these statistics play a disproportionate role in driving cybersecurity spending and policies. The commonalities that are identified can help us better grasp the real nature of the prevalence of cyber-attacks and cybercrime in Western countries, while the strong variations can also indicate what biases the methodologies used by vendors can introduce to their results and reporting.

I would suggest the authors add a few more surveys, such as Canada's Cyber Security and Cybercrime Survey, which is probably one of the largest in the world (12k businesses) with very high response rate (more than 70% I believe) and has been conducted twice already: https://www.serene-risc.ca/en/statistics-canada. Statistics Canada has also a couple of interesting national surveys that deal with individual cybercrime victimization.

I think the discussion section might also need a few more sentences on the differences found in vendor studies (especially in terms of over-reporting), and that the sociology of quantification can provide some useful insights to contextualize all of this).

On p. 9, it is stated that estimates derived from insurance data tend to be lower: this may be due to the fact that almost half of victim firms do not make insurance claims, even if they have purchased coverage, as shown in the Statistics Canada Cybersecurity survey. This is hard to explain but may be the source of the difference, if the pattern holds in the US.

Finally, just before the conclusion, the authors suggest developing an alternative model of science in which meta-reviews are collaboratively updated. I would argue this is the way forward and would challenge the authors to sketch what such a model would look like, for example by just developing a centralized repository of all the studies that get published and their results...

Overall, I don't understand why such useful work has not been done before and I find this paper an interesting contribution to the literature, even if the findings might not be as crunchy as they hoped.

Review 4

TOTAL SCORE: -2

Overall evaluation: -2 (reject)

Reviewer's confidence: 4 (high)

The author(s) conducted a search on current reports of cybercrime victimization and prevalence, with the aim to provide a benchmark for stakeholders. To do so, the author(s) used a combination of keywords (cybercrime, victimisation, cyber risk, likelihood, quantify) using Google and Google Scholars. The author(s) calculated likelihood of victimisation for each included article, study or survey and compared them across types of victims (individuals versus firms) and countries. In addition, the author(s) conducted a linear regression correlating the number of employees with likelihood. Findings show contradiction in victimization likelihood across reports and surveys, except for ransomware victimization where the global ranking is relatively consistent. In addition, result show that larger firms have a higher likelihood of being victimized.

1) In Section I:

a. The inclusion of Figure 1 in the first paragraph may lead to confusion for readers as there was no context provided. For example, it was unclear how the percentages were calculated, or which data sources were included for analysis. The author(s) should consider moving this figure towards the end of Section 1 or Section 3.

b. The third paragraph on the lack of statistics on technology-enabled intimate partner violence seems irrelevant to the current study. In addition, there are statistics on specific acts technology-enabled intimate partner violence such as cyberstalking. For example, the Center for Disease Control in the US conducts the National Intimate Partner and Sexual Violence Survey where technology-enabled stalking (e.g., use of technology to spy on the victim from a distance) is included. Here is the link to the most recent report: https://www.cdc.gov/violenceprevention/pdf/nisvs/NISVS-Stalking-Report_508.pdf

c. The author(s) should define what is meant by the following statement: “We also differentiate ourselves from surveys of cybercrime and cyber risk by extracting estimates for individuals and firms (not society) …”. It is unclear how these populations are defined or different from one another.

2) In Section II

a. In Section II-A, the use of “cybercrime” as a keyword might be problematic as there is a lack of consistent definition in the term across countries. In addition, it is unclear how the keyword “cybercrime” led to the datasets included in the current study. For example, in the study by Reep-van den Bergh and Junger, cyberbullying/threats/sexual offence was identified whereas that category is missing despite overlap in reviewed surveys. In addition, it is unclear how the author(s) of the current study treated studies using a general measurement of cybercrime without explicitly measuring specific types of cybercrime.

b. In Section II-A, it would be helpful for the author(s) to state the total number of studies identified by the keyword searches and how many studies were excluded.

c. In Table I, the author(s) should avoid using “?” in the table. In addition, it is unclear how firms and organizations are defined.

d. It is unsure how some research and/or surveys were excluded from the sample. For example, when conducting a keyword search using “cybercrime” and “victimisation” on Google Scholar, the following study using an Australian sample appeared in the search result, but it was not included in the current study:

- Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. Journal of Criminological Research, Policy and Practice.

The author(s) should elaborate on their inclusion criteria. This would allow readers to better contextualize the findings in the current study.

3) In Section III

a. Instead of Table III, the author(s) should consider using other forms of data presentation (e.g., graphs like Figure 1).

b. The alignments of Figure 6-9 need to be consistent.

4) In Section V, the author(s) should consider replicating the same design but focusing on specific type of cybercrime (e.g., ransomware).