Reviewing Estimates of Cybercrime Victimisation and Cyber Risk Likelihood

Reviewing Estimates of Cybercrime Victimisation and Cyber Risk Likelihood

Daniel W. Woods
School of Informatics
University of Edinburgh
Edinburgh, UK
daniel.woods@ed.ac.uk

Lukas Walter
Department of Computer Science
University of Innsbruck
Innsbruck, Austria
csaw9252@student.uibk.ac.at

***Abstract*—Across both the public and private sector, cybersecurity decisions could be informed by estimates of the likelihood of different types of exploitation and the corresponding harms. Law enforcement should focus on investigating and disrupting those cybercrimes that are relatively more frequent, all else being equal. Similarly, firms should account for the likelihood of different forms of cyber incident when tailoring risk management policies. This paper reviews the quantitative evidence available for both cybercrime victimisation and cyber risk likelihood, providing a bridge between the academic fields of criminology and cybersecurity. We extract estimates from 48 studies conducted by a mix of academics, statistical institutes, and cybersecurity vendors using a range of data sources including victim surveys, case-control studies, and the insurance market. The victimisation estimates are categorised into: cyber attack; malware; ransomware; fraudulent email; online banking fraud; online sales fraud; unauthorised access; Denial of Service; and identity theft. For each category, we display all estimates in the years 2017–2021. Our review shows: (i) firms face higher victimisation rates than individuals, which increases in the number of employees; (ii) global surveys reveal a consistent relative ranking of countries in ransomware victimisation; (iii) although trends could be identified within studies that collect longitudinal data, these trends tended to contradict each other when compared across studies; and (iv) broad categories with unclear consequences (e.g. malware and fraudulent emails) displayed higher variance and average values than categories associated with specific outcomes (e.g. identity theft or online banking fraud). We discuss the outlook for cybercrime and cyber risk research.**

1. Introduction

Both individuals and firms are afflicted by cybercrime, but what is the victimisation rate? Figure 1 displays a diversity of estimates ranging from less than 1% to over 60%. Estimates are provided by a range of entities with differing approaches, data availability and incentives. For example, surveys have been commissioned by public agencies in the UK [1], EU [2], France [3], Netherlands [4], and Sweden [5], as well as private firms from insurance [6], [7] and computer security [8]–[11]. Within academia the topic is of interest to researchers from a range of disciplines including criminology [12], finance [13], and computer science [14].

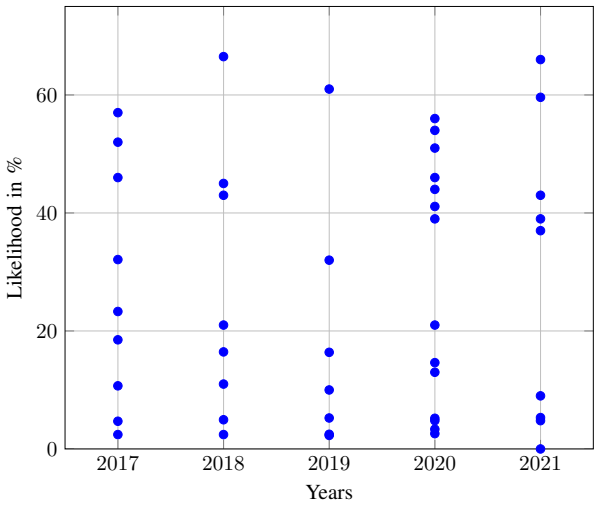

Figure 1. Five years of quantifying victimisation likelihood across cybercrime and cyber risk research leads to a range of estimates.

These entities have different incentives in estimating victimisation rates. Security vendors and insurers benefit when over-estimates create fear that can translate into demand for products and services [15]. In contrast, it was suggested that politicians and police chiefs happily claimed the credit for crime rates falling since the 1990s [15]. Official figures did not include online scams even though individuals were twice as likely to fall victim compared to traditional crimes [16].

Beyond the size of the estimates, the choice of which crimes to quantify can determine where law enforcement and wider society focuses its attention. For example, technology-enabled intimate partner violence lacks national and/or individual-level statistics [17, p. 664]. While we do not claim the following results from the lack of statistics, it is notable that security researchers do not consider domestic abusers when conducting security analyses of smart homes [18], instead focusing on external hackers who conduct malware and hacking crimes that are more commonly considered in cybercrime surveys [12].

Many estimates are not even based on survey data. Insurers estimate the probability of cyber incident, equivalent to victimisation rate, by dividing the number of claims by the number of policyholders who could have made a claim [6]. A similar approach (a case-control study) used by academics outside criminology is to collect publicly reported incidents and then normalise this by the number

of entities who could have suffered an incident, such as the firms in the S&P 500 [13] or all firms in the US in a given industry [19]. Even more exotic approaches exist [20].

One might argue these problems are caused by a lack of gate keeping and that law enforcement will look to official statistics. But even estimates produced by statistical institutes are problematic. A 2018 review that focused on surveys "judged to be very well conducted" [12, p. 11] concludes that "prevalence estimates between countries are incomparable due to, most of all, question wording" [12]. If even publicly funded institutes cannot agree upon standard questions, this creates space for security vendors to choose those questions that maximise fear and consequently sales [15]—they are unlikely to conduct such research if no-one consumes it.

Unreliable estimates of cybercrime victimisation matter because of how firms and governments use such figures to prioritise mitigation resources. Firms invest more in prevention if cybercrime is more likely to happen [21]. Law enforcement faces incentives to reduce the crime metrics used to evaluate the agency, possibly displacing resources away from crimes not tracked by the metric.

Together these concerns motivate a broad review that captures not only high-quality estimates, predominantly from statistical institutes, but also *grey literature*. Doing so allows us to examine how cybercrime victimisation rates are calculated and used by a range of actors—statistical institutes to inform policy, insurers to sell financial security, vendors to sell computer security, and academics from many disciplines to advance research agendas. We unashamedly build on the work of Reep-van den Bergh and Junger [12] by adding the years 2017–2021 (they consider 2009–2016) and by sampling much more grey literature. We also differentiate ourselves from surveys of cybercrime and cyber risk by extracting estimates for individuals and firms (not society [15], [22]) and by extracting actual likelihood estimates, which was not done in surveys of cyber risk [23]–[25].

Section 2 describes our search strategy and selection criteria. Section 3 presents the results. Section 4 discusses insights and limitations. Section 5 offers a conclusion.

2. Data Sources

Section 2.1 describes how we searched for studies and decided whether to include a study, as well as outlining the methodological details of each study. Section 2.2 identifies the crimes for which victimisation estimates are calculated, as well as identifying related work for each.

2.1. Sample of Studies

Search We used internet search engines to identify a broad range of studies. The website *google.com* indexes web-pages and documents allowing us to capture vendor surveys, and *scholar.google.com* indexes academic publications. We searched for combinations of the terms: *cybercrime*, *victimisation*, *cyber risk*, *likelihood*, and *quantify*. We also consulted surveys of cybercrime [12], [15], [22] and also cyber risk [23], [24]. We did not conduct a structured literature review because the topic is interdisciplinary and so we could not feasibly search all the relevant journals. For example, we found papers in criminology [12], [26], finance [13], and interdisciplinary cybersecurity [14], [19].

In choosing a broad search, we undoubtedly missed studies and so we cannot claim a comprehensive review, which is infeasible given the volume of studies. Sacrificing completeness allows for comparisons across diverse studies, which enables a critical perspective and for us to identify the strengths of different approaches. For example, the 2018 review [12] could not compare estimates across national institutes because of differences in survey design, which is solved by private firms who conduct global surveys with the same survey instrument.

Inclusion Our inclusion criteria is simply that a study reports a quantitative cybercrime victimisation estimate. We even include studies that do not self-identify as studying cybercrime, fostering the link between criminology and cybersecurity [27]. Most cyber risk outcomes have a corresponding crime, such as data breach–computer misuse or ransomware–extortion. Despite our broad inclusion criteria, we ignored cyber risk studies that only study losses without quantifying victimisation rates [28]–[34].

Types of Study Table 1 summarises the methodologies employed by the studies in our sample. The majority of studies use survey data, such that victimisation v is calculated as:

$$v = \frac{\text{Number of respondents who reported an attack}}{\text{Total number of survey respondents}}$$

Notably, the statistical institutes report how data is collected (e.g. telephone, face-to-face, postal or online) along with the response rates, whereas cybersecurity vendors often do not specify how responses were collected, let alone report the response rate. The sampled populations include a mixture of individuals and firms from many countries. We compare surveys of individuals with firms because a micro firm's computer network is closer to a household network than that of a multinational corporation.

Case-control studies are common in the cyber risk literature [23]. This involves identifying a group of victims, commonly via databases of publicly reported incidents, and then identifying a control group who did not report such an incident, which leads to the calculation:

$$v = \frac{\text{Number of entities who publicly-reported an attack}}{\text{Total number of entities}}$$

Romanosky uses publicly reported incidents collected by a data broker normalised by the number of US firms in that industry [19]. Eling and Schnell [13] collect cyber incidents affecting firms in the S&P 500 from the SAS OpRisk database and normalise by the number of firms in the S&P 500 and the years in their sample window. An insurance firm makes in effect the same calculation, using their own claims data normalised by all the policyholders they insure [6], [56]. In addition, we conduct our own case-control using the Critical Infrastructure Ransomware Incident Data set [66], which contains 1,066 incidents between November 2013 and October 2021. We normalise by the number of firms in each EU member state [67], the UK [68] and worldwide [69].

2.2. Victim Classification

Different studies adopt different levels of granularity when it comes to victimisation. Table 2 shows which

Study	Country (ISO 3166)	Mode data collection	Year earliest data collection	Periodicity	Response Rate	Number of Respondents	Respondent
CSBS 2017 [35]	GB	Telephone	2016	Every year	27%	1,523	Firms
CSBS 2018 [36]	GB	Telephone	2017	Every year	25%	1,519	Firms
CSBS 2019 [37]	GB	Telephone	2018	Every year	23%	1,566	Firms
CSBS 2020 [38]	GB	Telephone	2019	Every year	27%	1,348	Firms
CSBS 2021 [1]	GB	Telephone	2020	Every year	19%	1,419	Firms
EC 2017 [39]	EU	Face-to-face & CAPI	2017	Every year[a]	?	28,093	15+
EC 2019 [40]	EU	Face-to-face & CAPI	2018	Every year[a]	?	27,339	15+
EC 2020 [2]	EU	Face-to-face & CAPI	2019	Every year[a]	?	27,607	15+
Dreiß 2020 [41]	DE	CATI	2018	Every year[b]	11.6%	4,981	Firms
Dreiß 2021 [42]	DE	Online	2020	Every year[b]	11.7%	687	Firms
NTU 2017 [5]	SE	Telephone/online/postal	2016	Every year	59%	11,600	16-84
NTU 2018 [43]	SE	Online/postal	2017	Every year	40.5%	74,032	16-84
NTU 2019 [44]	SE	Online/postal	2018	Every year	40.6%	73,461	16-84
NTU 2020 [45]	SE	Online/postal	2019	Every year	40.6%	73,813	16-84
NTU 2021 [46]	SE	Online/postal	2020	Every year	41%	74,351	16-84
VM 2016 [4]	NL	Online/postal	2016	Every year[a]	38.5%	81,000	15+
VM 2017 [47]	NL	Online/postal	2017	Every year[a]	39.3%	150,000	15+
VM 2020 [48]	NL	Online/postal	2019	Every year[a]	41.6%	135,000	15+
CVS 2016 [3]	FR	Face-to-face	2015	Every year[a]	?	20,000 - 25,000	15+
CVS 2017 [49]	FR	Face-to-face	2016	Every year[a]	?	20,000 - 25,000	15+
CVS 2018 [50]	FR	Face-to-face	2017	Every year[a]	?	20,000 - 25,000	15+
CVS 2019 [51]	FR	Face-to-face	2018	Every year[a]	?	20,000 - 25,000	15+
Biancotti [52]	IT	CATI	2016	One-off	?	3,854	Firms
Romanosky [19]	US	Advisen database	2004	One-off	N/A	12,603	Firms
Castro et al. [53]	GB	Online	2014	One-off	?	1,500	Firms
TAB [10]	?	Survey, not specified	2017	One-off	?	?	Firms
Riek et al. [14]	IT, NL, DE, GB, EE, PL	Telephone	2015	One-off	?	6,394	18+
Paoli et al. [26]	BE	Online	2016	One-off	4.9%	310	Firms
Woods et al. [20]	US	Insurance premiums	2003	One-off	N/A	6,828	Firms
Crowd 2020 [9]	Global	Telephone/online	2020	Every year	?	2,200	Firms
Crowd 2021 [54]	Global	Telephone/online	2021	Every year	?	2,200	Firms
Eling et al. [13]	US	S&P 500	2009	One-off	N/A	500	Firms
Proximus [11]	BE, NL	Survey, not specified	2020	One-off	?	87	Firms
Franke et al. [55]	SE	Survey, not specified	2019	One-off	17%	649	Firms
Coal 2020 [56]	US, CA	Insurance claims	2019	Every year[b]	N/A	25,000	Firms
Coal 2021 [6]	US, CA	Insurance claims	2020	Every year[b]	N/A	25,000	Firms
SOPH 2020 [57]	Global	Survey, not specified	2020	Every year[b]	?	5,000	Firms
SOPH 2021 [8]	Global	Survey, not specified	2021	Every year[b]	?	5,400	Firms
His 2017 [7]	DE, US, GB	Online	2016	Every year	?	3,036	Firms
His 2018 [58]	DE, US, GB	Online	2017	Every year	?	4,103	Firms
His 2019 [59]	DE, ES, GB, FR, BE, US, NL	Online	2018	Every year	?	5,392	Firms
His 2020 [60]	DE, ES, GB, FR, BE, US, NL, IE	Online	2019	Every year	?	5,569	Firms
His 2021 [61]	DE, ES, GB, FR, BE, US, NL, IE	Online	2020	Every year	?	6,042	Firms
CSCSC 2017 [62]	CA	Online	2017	Every two years	86%	12,597	Firms
CSCSC 2019 [62]	CA	Online	2019	Every two years	76%	12,274	Firms
Drew [63]	AU	Online	2019	One-off	?	595	18+
VOIT 16 [64]	US	CATI	2016	Every two years	77%	96,100	16+
VOIT 18 [65]	US	CATI	2018	Every two years	72%	102,400	16+
Own Approach	Global	Ransomware database	2013	One-off	N/A	1,066	Firms

TABLE 1. LITERATURE CHARACTERISTICS. [a] SOMETIMES A YEAR IS MISSING. [b] UNTIL NOW ONLY 2 PUBLICATIONS ARE PUBLISHED

categories are considered for each study in our sample. We identify related work for each category in the following.

Cyber attack There is no clear definition for a cyber attack, with some acknowledging it may even include legal activities [70]. An influential taxonomy from 1998 defines an attack as "a series of steps taken by an attacker to achieve an unauthorized result" [71], which confirms the broadness of this category. Turning to one of the studies in our sample, Biancotti [52] reports that 43% of firms suffered an incident in the last year, yet most of these incidents had a cost less than 10k euros (62%) or no costs at all (31%) with just 0.1% of the respondents reporting losses exceeding 200k euros. Table 2 shows this is the category of interest for cyber risk researchers [13], [19]. We included espionage estimates under cyber attack because the term is used in the context of international relations and law [72].

Malware Malware victimisation involves malicious software—for example a virus, worm, spyware, or Trojan [73]—infecting the victim's device. It is difficult to measure and different surveys collect related information "in very different ways" [12]. Much like the cyber attack

Source	Cyber attack	Ransom-ware	Fraudulent email/website	Malware	Online banking	Espionage	Unauthorised access	Online sales fraud	Denial of service	Identity theft
CSBS 2017 [35]	flt	l	l	l	l		l		l	
CSBS 2018 [36]	flt	l	l	l	l		l		l	
CSBS 2019 [37]	flt	l	l	l	l		l		l	
CSBS 2020 [38]	flt	l	l	l	l		l		l	
CSBS 2021 [1]	flt	l	l[b]	l	l		l		l	
EC 2017 [39]		l	l	l	l		l	l		l
EC 2019 [40]		l	l	l	l		l	l		l
EC 2020 [2]		l	l	l	l		l	l		l
Dreiß 2020 [41]	flt	flt	flt[b]	flt		flt			flt	
Dreiß 2021 [42]	flt	flt	flt[b]	flt		flt			flt	
NTU 2017 [5]					l[a]			l[a]		
NTU 2018 [43]					l[a]			l[a]		
NTU 2019 [44]					l[a]			l[a]		
NTU 2020 [45]					l[a]			l[a]		
NTU 2021 [46]					l[a]			l[a]		
VM 2016 [4]	l		l[b]		l[d]			l		l
VM 2017 [47]	l		l[b]		l[d]			l		l
VM 2020 [48]	l		l[b]		l[d]			l		l
CVS 2016 [3]					fl					
CVS 2017 [49]					fl					
CVS 2018 [50]					fl			fl		
CVS 2019 [51]					fl			fl		
Biancotti [52]	flt									
Romanosky [19]	fl		f							
Castro et al. [53]	fl									
TAB [10]	l									
Riek et al. [14]	l	flt	flt	l	flt			flt		
Paoli et al. [26]	l	flt				flt	flt	flt		
Woods et al. [20]	fl	f								
Crowd 2020 [9]	t	fl	l[b]	l						
Crowd 2021 [54]	t	fl								
Eling et al. [13]	fl									
Proximus [11]	flt		l[b]	l					l	
Franke et al. [55]						l			l	
Coal 2020 [56]	l	fl	l		fl					
Coal 2021 [6]	l	fl	l[c]		fl					
SOPH 2020 [57]		fl								
SOPH 2021 [8]		fl								
His 2017 [7]	flt									
His 2018 [58]	flt	fl		l					l	
His 2019 [59]	fl	l		l					l	
His 2020 [60]	fl	fl	l[c]	fl					l	
His 2021 [61]	fl	fl	l[c]	l					l	
CSCSC 2017 [62]	flt	l				l	l		l	
CSCSC 2019 [62]	flt	l				l	l		l	
Drew [63]	fl	fl	fl[b]	fl	fl			fl	fl	
VOIT 2016 [64]										flt
VOIT 2018 [65]										flt
Own Approach		l								

TABLE 2. DIFFERENT TYPES OF CYBERCRIME COVERED. f INCLUDES QUESTIONS ABOUT FINANCIAL LOSS. l INCLUDES QUESTIONS ABOUT LIKELIHOOD. t INCLUDES QUESTIONS ABOUT TIME LOSS. [a] NOT NECESSARILY ONLY ONLINE. [b] ONLY CONSIDERS PHISHING ATTACKS. [c] ONLY CONSIDERS BUSINESS EMAIL COMPROMISE. [d] ONLY CONSIDERS WEB SKIMMING

category, there is a question of whether a malware infection victimises even when it is re-mediated before a loss. Academic research has uncovered the criminal business models supplying malware [74], [75], the techniques employed [76], [77] and potential mitigations [78]. Button et al. [79] interview 52 victims of the UK's Computer Misuse Act and find that a quarter were caused by malware including ransomware.

Ransomware Ransomware is a specific form of malware in which the victim's system is rendered inoperable via encryption, after which payment is demanded in exchange for the decryption key. Some ransomware actors threaten to publish the victim's data [80]. Research has explored ransomware samples [81], [82], payments on various blockchains [83]–[85], and the associated business models [86], [87].

Fraudulent email This category comes from the European Commission's survey, which asks:

> In the last three years, has anybody in your family, amongst your friends or acquaintances experienced or been a victim of any of these situations?
> Receiving fraudulent emails or phone calls asking for their personal details (including access to their computer, logins, banking or payment information)

We also classified phishing and business email compromise (BEC) crimes under this category, as well as generic

email scams leading to an admittedly bloated category. There is a rich body of research on many aspects of phishing [88], [89], BEC [90], [91], and email scams [92], [93].

Online Banking Fraud Many surveys include online banking fraud as a distinct category even though it could result from malware, fraudulent emails or another mode of attack. A malware infection leading to banking fraud could be counted under both categories, which illustrates the immature state of cybercrime classification and measurement [94]. Researchers have analysed banking fraud cases [95], causes [96] and mitigations [97], [98].

Unauthorised Access Much like the previous category, unauthorised access could be achieved by multiple means. The European Commission survey only considers access to social media or email accounts, whereas Paoli et al. [26] include any information system of a business:

> "By this we mean any malicious event or action that threatens the reliability, integrity and/or availability of the information systems of a business (the receipt of phishing e-mail, data breaches, unauthorized access, etc. with or without consequences or damage)."

There is a relevant body of research on account hijacking [99], [100], passwords [101] and authentication more generally [98].

Online Sales Fraud The European Commission includes a category:

> Online fraud where goods are not delivered, are counterfeit, or are not as advertised

The NTU survey [5] even includes non-online fraud. This category is unlike the others in that it is not caused by compromising the security of a victim's device or access credentials, but simply the seller's dishonesty. To the extent such a thing is possible, it is an 'old' cybercrime, comprising 44.6% of the reports to the FBI's Internet Crime Complaint Center in 2006 [102].

Denial of Service This category was taken from the CSBS survey [35], which asks:

> Have any of the following happened to your organisation in the last 12 months, or not? Denial-of-service attacks that take down your website

Again, this could plausibly be caused by malware or a phishing attack. However, denial of service (DoS) is most commonly understood to occur when an adversary sends large volumes of internet traffic that compromise the availability of a computer system. Research has covered business down-times [103], the criminal market for booter services [104], and measuring distributed DoS attacks [105]. Highlighting the diverse motivations for cybercrime, DoS attacks are often used to disrupt competing online gamers [106].

Study	Year	Respondent	Publisher	Likelihood
Castro et al. [53]	2014	Firms	A	18.3%
Romanosky [19]	2016	Firms	A	0.21%
CVS [3]	2016	Individuals	G	2.26%[a]
CSBS [35]	2017	Firms	G	46%
EC [39]	2017	Individuals	G	18.5%
CVS [49]	2017	Individuals	G	2.44%[a]
VM [4]	2017	Individuals	G	10.7%
NTU [5]	2017	Individuals	G	4.7%
Hiscox [7]	2017	Firms	I	57%
Biancotti [52] Firms	2017	Firms	A	23.3%
Biancotti [52] Employees	2017	Firms	A	32.1%
TAB [10]	2017	Firms	I	52%
NTU [43]	2018	Individuals	G	4.95%
VM [47]	2018	Individuals	G	11%
Hiscox [58]	2018	Firms	I	45%
CVS [50]	2018	Individuals	G	2.44%[a]
CSBS [36]	2018	Firms	G	43%
Riek et al. [14]	2018	Individuals	A	16.45%
Paoli et al. [26]	2018	Firms	A	66.5%
CSCSC [62]	2018	Firms	G	21%
CSBS [37]	2019	Firms	G	32%
EC [40]	2019	Individuals	G	16.38%
CVS [51]	2019	Individuals	G	2.49%[a]
NTU [44]	2019	Individuals	G	5.25%
Hiscox [59]	2019	Firms	I	61%
Woods et al. [20]	2019	Firms	A	2.3%
VOIT [64]	2019	Individuals	G	10%
Dreiß [41]	2020	Firms	G	41.1%
CrowdStrike [9]	2020	Firms	I	56%[b]
Eling et al. [13]	2020	Firms	A	2.6%
Proximus [11]	2020	Firms	I	54%
NTU [45]	2020	Individuals	G	5.2%
VM [48]	2020	Individuals	G	13%
Coalition [56]	2020	Firms	I	3.35%
SOPHOS [57]	2020	Firms	I	51%[b]
Hiscox [60]	2020	Firms	I	39%
CSBS [38]	2020	Firms	G	46%
EC [2]	2020	Individuals	G	14.63%
Franke et al. [55]	2020	Firms	A	4.8%
CSCSC [62]	2020	Firms	G	21%
Drew [63]	2020	Individuals	A	44%
Coalition [6]	2021	Firms	I	5.32%
CSBS [1]	2021	Firms	G	39%
SOPHOS [8]	2021	Firms	I	37%[b]
Own Approach	2021	Firms	N/A	0.0005%[b]
Dreiß [42]	2021	Firms	G	59.6%
NTU [46]	2021	Individuals	G	4.8%
CrowdStrike [54]	2021	Firms	I	66%[b]
Hiscox [61]	2021	Firms	I	43%
VOIT [65]	2021	Individuals	G	9%

TABLE 3. SUMMARY OF PUBLICATIONS UNDER CONSIDERATION. THE LIKELIHOOD COLUMN IS PURELY FOR COMPARATIVE PURPOSES AND INVOLVED SOME DISCRETION, BY WHICH WE SELECTED OR CALCULATED THE MOST GENERIC ESTIMATE FROM EACH PUBLICATION.
A = ACADEMIC, I = INDUSTRY WHITE PAPER, G = GOVERNMENT AGENCY OR STATISTICAL INSTITUTE
[a] ONLY ONLINE BANKING [b] ONLY RANSOMWARE

3. Results

Table 3 provides a coarse summary of the victimisation estimates. Here, we try to present the most generic estimate, in line with the broad category *Cyber Attack*, for each study. Throughout we report the year of publication for comprehensibility, as it would be difficult to visualise studies who collect data over multiple years (e.g. case control studies [13], [19]). This is not a problem for statistical institute and vendor surveys, which publish soon after data collection. However, some academic studies have a delay due to publishing procedures. Riek et al. [14] published a study in 2018 based on data collected in 2015.

The diversity of values in Figure 1 make more sense when dis-aggregated by respondent. Figure 2 shows that firms report higher victimisation than individuals. Multiple surveys commissioned by cybersecurity firms and consul-

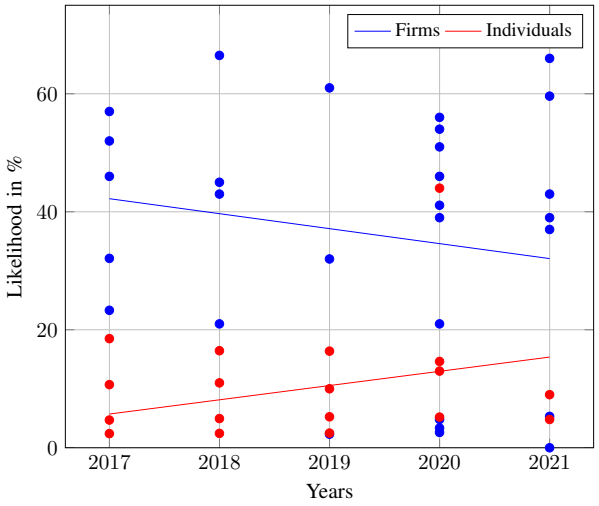

Figure 2. Linear Regression: Firms versus Individuals

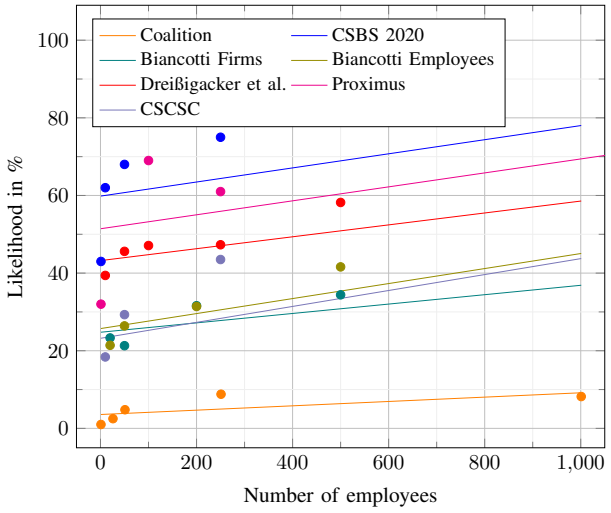

Figure 3. Linear Regression: Number of Employees

Study	Global	UK	Belgium	Germany	US
EC [2]	-	1	2	3	-
Sophos [8]	1	2	4	3	5
CrowdStrike [9]	2	1	-	4	3
Own Approach	1	2	3	3	5

TABLE 4. THE RANK ORDERING OF EACH ESTIMATE FROM LOWEST TO HIGHEST

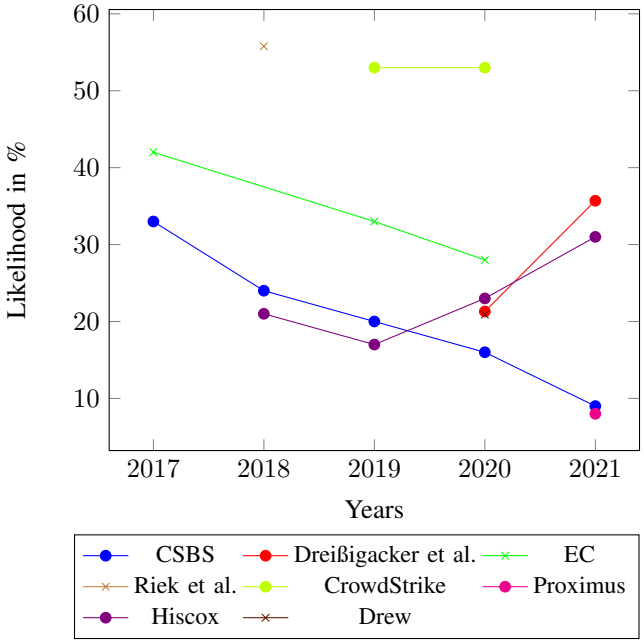

Figure 4. Crime prevalence for malware

tancies [8]–[11] find that firms are more likely than not to suffer an incident, whereas just one academic study does so [26]. All of the firm-level estimates lower than 20% in Figure 1 are produced using case-control studies [6], [13], [56]. For example, Eling et al. [13] find 130 incidents affecting firms in the S&P500 and normalise by years in which data was collected:

$$v = \frac{\text{Number of incidents reported by S\&P500}}{500 \times \text{Sample window in years}} = 0.026$$

This estimate is closer to those associated with estimates derived from insurance data (5.3% [6] and 2.3%[20]). This suggests the vendor surveys are over-reporting victimisation among firms [107].

However, case-control studies can also be distorted by reporting biases. To illustrate the danger with this methodology, our case-control uses all ransomware incidents collected by Rege [66] and divides this by the number of firms in the world. This figure drastically underestimates ransomware incidence. It is distorted by collection biases—ransomware incidents cannot be counted if the firm does not disclose, if the press do not report on the incident, or if the research team building the dataset do not find the press report [66]. In contrast, estimates of the number of global firms correct for under-reporting [69], which means this approach under-estimates the likelihood of cyber incident.

A number of studies further dis-aggregate by the size of the firm. Figure 3 shows that larger firms suffer higher rates of victimisation, a relationship that holds across all the studies who provide such dis-aggregation. We did not estimate a pooled regression line because of differences between research designs.

The global surveys also allow for cross-country comparisons as the ordering of the countries provide insights into the relative victimisation rates in each country. Table 4 shows UK firms face a lower likelihood of cyber incident than Germany, Belgium and the US in every study for which the comparison is possible. The studies conflict on whether the UK faces a lower incidence than the global average, and also whether the US or Germany faces the highest incidence.

The remaining figures display estimates for specific crimes. Throughout we use a circle for a firm-level estimate and cross for individuals. We caution readers that the axes are not aligned, which would have obscured nuances in those categories with lower absolute victimisation rates.

Figure 4 shows malware victimisation estimates range from 10–60%. Studies collecting data over multiple years display variation, such as the CSBS survey that progressively dropped from 33% to less than 10% in five years [1]. Although this downwards trend was confirmed by the European Commission's survey [2], other surveys

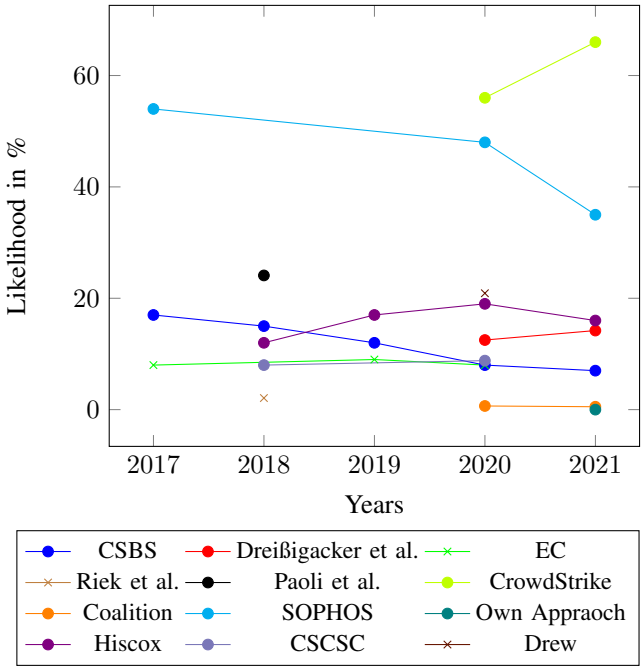

Figure 5. Crime prevalence for ransomware

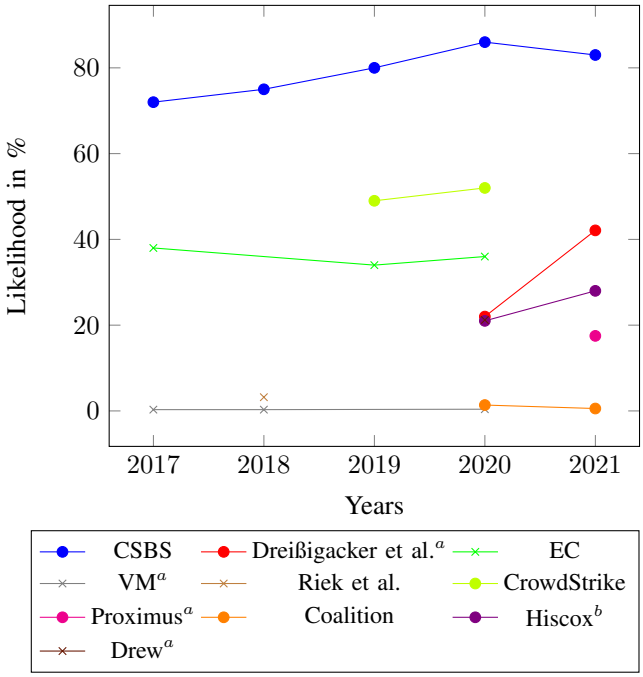

Figure 6. Crime prevalence for fraudulent emails or fraudulent websites
[a] only phishing attacks
[b] only business email compromise

found an upwards trend [41]. Conflicting temporal trends are common across all categories.

Figure 5 displays the victimisation rates for ransomware, which are mostly lower than malware victimisation as we would expect given ransomware is a subset of malware. We see a similar pattern to malware in which the highest estimates were conducted by security vendors [8], [9]. Estimates derived from studies that collect data across multiple years are more stable than for malware.It is worth noting that even though ransomware victimisation appears to be stable, the societal impact could be deteriorating if the ransom demands are increasing.

Figure 6 displays estimates for the fraudulent email category, which vary more than any other category. Across all five years of the CSBS survey, between 70 and 85% of respondents report "fraudulent emails or being directed to fraudulent websites has happened to [their] organisation in the last 12 months", which could even include simply receiving a phishing email without any further interaction. In contrast, Coalition only consider BEC victims who file an insurance claim, which requires proving a monetary loss has occurred, and unsurprisingly Coalition report a much lower victimisation rate [6], [56]. Despite the variance in the estimated value, studies that collect longitudinal data are relatively stable over time, at least compared to the malware estimates in Figure 4.

Figure 7 shows that estimates for online banking fraud are all within 1–11%, excluding the estimates for card skimming, which appears to be very rare. It is also worth noting some studies report general banking fraud, in addition to online banking fraud. The longitudinal studies are relatively stable over time and may even be trending downwards since 2019. The studies based on internal cyber insurance claims data represent an exception [6], [56].

Figure 8 shows the victimisation rate for online sales fraud. The VM and NTU rates are remarkably consistent

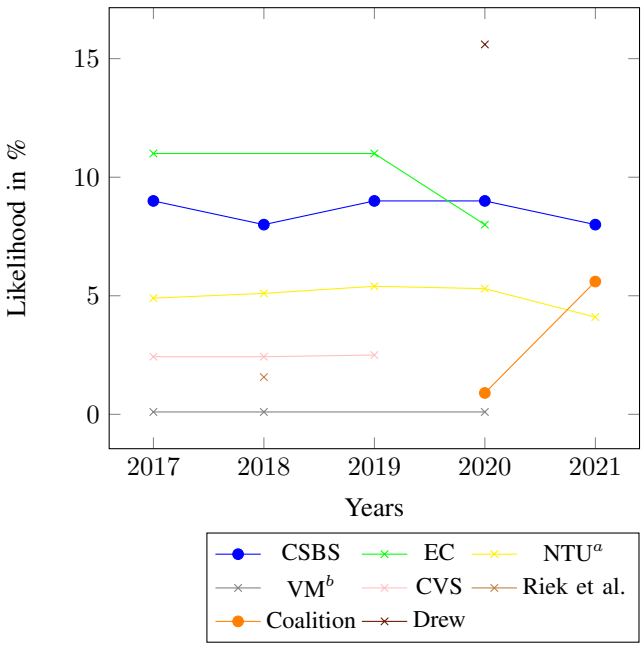

Figure 7. Crime prevalence for online banking fraud
[a] banking in general, not necessary online banking
[b] only web skimming

over time and in terms of absolute value. However, closer inspection reveals this is a coincidence as the NTU figure includes non-online fraud too. The other studies display a range of values, with the EC line trending downwards. Again, this highlights the problem of reading too much into an individual study.

The remaining categories are quantified relatively infrequently. Figure 9 displays the unauthorised access victimisation rates across three studies. The estimate from

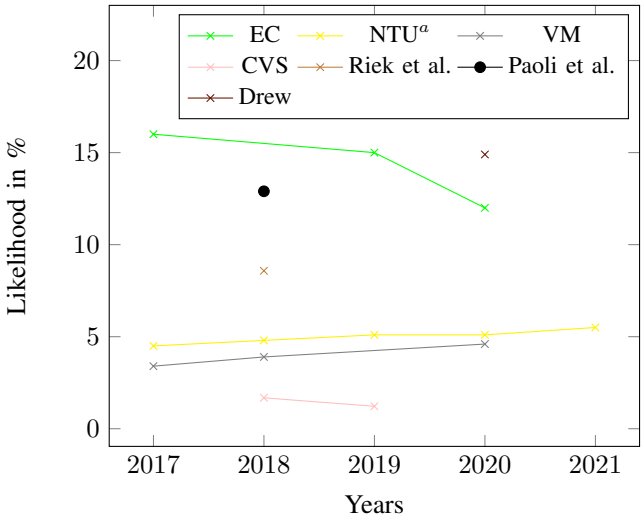

Figure 8. Crime prevalence for online sales fraud
[a] sales fraud in general, not necessary online

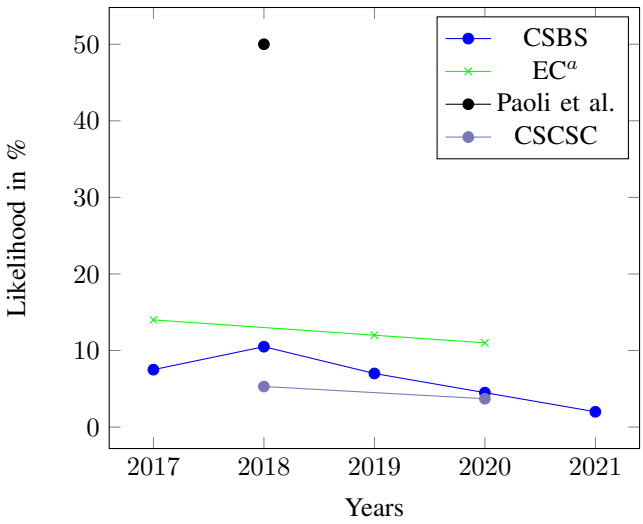

Figure 9. Crime prevalence for unauthorised access
[a] only social media or email

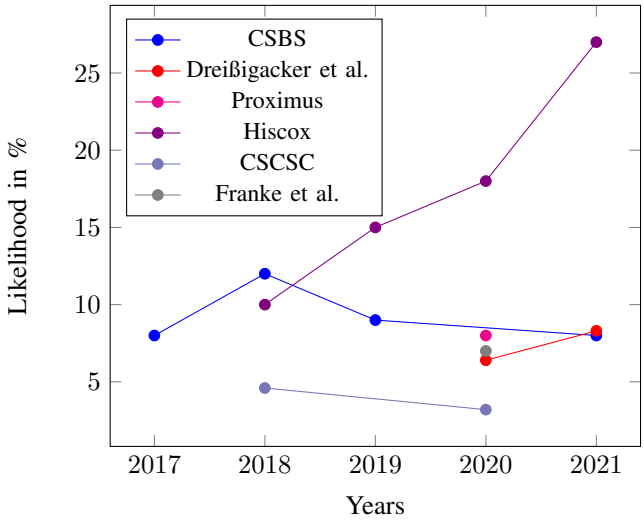

Figure 10. Crime prevalence for Denial of Service

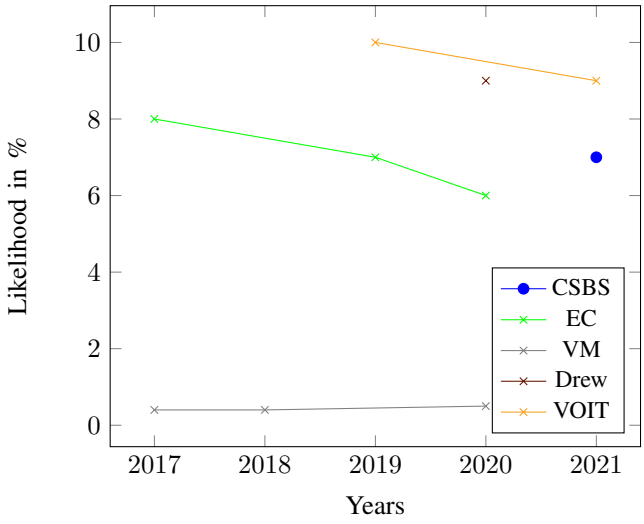

Figure 11. Crime prevalence for identity theft

Paoli et al. [26] is much higher because they include events with no consequences:

> "By this we mean any malicious event or action that threatens the reliability, integrity and/or availability of the information systems of a business (the receipt of phishing e-mail, data breaches, unauthorized access, etc. with or without consequences or damage)."

The two studies with longitudinal data report stable estimates over time, which may even be trending downwards. The European Commission survey only include events leading to unauthorised access to social media or email.

Figure 10 shows Denial of Service victimisation over time. The longitudinal development of the Hiscox estimate is perhaps most worrying, growing by 150% in four years. However, the other studies contradict this both in terms of trend (CSBS is stable) and absolute values. Ignoring the Hiscox estimates, the absolute values of the remaining studies are consistently around 6–12%, perhaps the most consistent category.

Finally, Figure 11 presents three estimates of identity theft victimisation. Again, the longitudinal trends seem to contradict each other—the European Commission survey suggests a downwards trend, whereas VM suggests more stability. The range of values is relatively small (just 8%) but still the VM estimates are an order of magnitude lower than the EC estimates. CSBS only started collecting this data in the 2021 study [1], which may in itself reflect rising prevalence.

4. Discussion

Aggregate Insights Although much remains uncertain, the following insights emerged:

- **I1** Firms face greater victimisation rates than individuals (Figure 2), which increases in the number of employees (see Figure 3).
- **I2** Longitudinal studies of ransomware victimisation were surprisingly stable across a number of studies, although the absolute values varied based on the research design.

I3 Global surveys also reveal a consistent relative ranking of countries in ransomware victimisation (see Table 4).

I4 Broad categories with unclear consequences (e.g. malware and fraudulent emails) displayed higher victimisation than categories associated with concrete losses (e.g. identity theft or online banking fraud).

While none of these results are groundbreaking, our review at least outlines what is known and provides a benchmark for future research. For example, the ranking of countries for ransomware victimisation (**I2**) represent a small step towards global comparisons with the associated perils [108]–[110]. We also did not find any evidence that the Covid pandemic represented a structural break in the pattern of cybercrime. While we do not place high confidence in negative results given the amount of noise in our data, it does contribute to an emerging body of work on how the pandemic impacted cybercrime [111]–[114].

The estimates of cyber attack (Table 3), ransomware and others could potentially inform cyber insurance pricing, which was shown to be crude [115]. For example, the identity theft estimates we extracted are larger than those that insurers filed with regulators to justify identity theft insurance prices, which range from 0.01–3.8% [116]. More generally, the victimisation estimates derived from insurance data [6], [56] tended to be lower than comparable firm-level estimates from (admittedly shaky) survey data [9], [57], which could be explained by reporting biases in cybercrime surveys [107]. Benchmarking cybercrime estimates against insurance claims could be useful going forward because of the adversarial reporting dynamics—the client reports to receive claims, and the insurer investigates to prevent fraud. Admittedly, some firms may not report small incidents because of administrative overhead or the possibility doing so impacts future insurance prices. This requires insurance firms to actually release the data, which may undermine their competitive advantage [117], and so we should celebrate any insurer that does so.

Limitations Realistically, the insights we derived are weak given we reviewed over 40 studies. Originally, we set out to conduct a meta-analysis in which estimates are calculated from data pooled across all studies. Such meta analyses are widely used in medicine in which the cost of running trials means many studies lack statistical power individually, but pooling the results can lead to greater confidence in the estimated value. Doing so relies on studies adopting similar research designs. Unfortunately this is not yet common in cybercrime/cybersecurity research as shown by Table 1 and 2. As an earlier review noted [12], the lack of standardised questions make it difficult to compare across survey results. These problems are compounded in surveys conducted by cybersecurity vendors in which key research design considerations are not reported, such as the mode of data collection and response rate.

Overlooking whole classes of harm is a problem that runs deeper than poor research design, which is at least quantified if one accepts a sufficient tolerance for error. Some harms may be quantified but not under the banner of cybercrime/risk. For example, Thomas et al. [118] find evidence that 48% of respondents were victims of online abuse (25% to severe abuse) in 2018, an increase from 2016. Other categories may not yet be recognised because the 'cyber' aspect is a novel development, such as in technology-enabled intimate partner violence [17, p. 664]. Yet other crimes are ignored because of overly specific questions. For example, online banking and sales fraud were quantified (see Table 2) but not romance scams [119], eWhoring [120] and other niche scams. Keen readers will note that we criticised the category of *cyber attack* because it was so broad as to become meaningless, and just now we criticised granular victimisation estimates for overlooking other harms. Our contradiction belies a trade-off. Given finite resources, we can either collect high-level data that captures many crimes but abstracts away from the details that can actually be operationalised, or we collect granular data that blinds us to whole classes of harm.

At this point, we should reflect on the endeavour of quantification [121]. It is broadly agreed that measurement is important [12], [122], [123] and yet the state of measurement has been crticised in the context of both cybersecurity [23], [124], [125] and cybercrime [15], [126], [127]. That researchers, ourselves included, publish questionable measurements is reminiscent of the politician's syllogism—'we must do something, this is something, therefore we must do this'. Is there a threshold at which measurements are so misleading as to be better off left unpublished? How about when cyber attack likelihood varies from 0.21% [19] to 66% [26], [54] as in Table 3?

Clearly conducting this research demonstrates we do not endorse the nihilism that says we cannot measure cybercrime. At risk of lecturing from the ivory tower, we believe in incremental progress, transparency, and embracing criticism. Surveys published without methodological details like response rates or the mode of data collection (see many vendor studies in Table 1) should be discounted and possibly even ignored. Moving towards standard categories of cybercrime and the corresponding survey questions would aid comparison across surveys [12]. And then we need to regularly collate studies and critically review research design, as we have done in this paper. In doing so, we unashamedly extended the work of Reep-van den Bergh and Junger [12] by including low quality studies and adding the years 2017–2021. Is an alternative model of science in which meta-reviews are collaboratively updated as new studies are published possible?

5. Conclusion

Academics, security vendors, law enforcement, firms, and individuals are all interested in or affected by cybercrime victimisation rates. This leads to a contested space in which different entities publish estimates using various methodologies based on data collected about diverse populations. We reviewed 48 studies and discovered that the diversity of factors—the specific crime studied, methodology, and population of interest—lead to range of victimisation estimates (see Table 3). The value of our review comes in identifying how to account for these factors and adjust estimates accordingly.

The choice of which population to study helps to explain why the estimates differ. Firms face a higher

rate of victimisation than individuals (Figure 2) and firms with more employees face even higher rates (Figure 3). A limited number of studies allow us to compare across countries, we find that UK firms suffer comparatively lower likelihood of ransomware incident compared to Belgium, Germany and the US, and that this result holds across multiple datasets.

The method of study is another consideration. Estimates provided by statistical institutes are incomparable due to differences in survey instruments [12]. Turning to less rigorous studies, surveys commissioned by cybersecurity vendors, which tend to omit methodological details (see Table 1), report the highest rates of victimisation. Estimates provided by case-control studies are an order of magnitude lower, which suggests the vendor surveys over-estimate victimisation.

Finally, victimisation varies across different cybercrimes. Rates are much higher when unsuccessful attacks are also counted, such as when an entity receives a fraudulent email without responding or when a malware infection is re-mediated without any loss. Such events have been experienced by the majority of respondents in some surveys. Specific outcome based questions, such as whether identity theft or online banking fraud occurred, lead to smaller and more consistent estimates. In spite of this, Figure 4–11 did not identify any longitudinal trends that held across multiple studies of the same category of cybercrime, and there was no clear spike in cybercrime following the Covid pandemic.

Acknowledgements

We thank Rainer Böhme and the anonymous reviewers for the constructive feedback and comments, of which the most interesting could not be addressed due to space issues. As part of the open-report model followed by the Workshop on Attackers CyberCrime Operations (WACCO), all the reviews for this paper are publicly available at https://github.com/wacco-workshop/WACCO/tree/main/WACCO-2022. DW is funded by the European Commission's call H2020-MSCA-IF-2019 under grant number 894700.

References

[1] UK Department for Digital, Culture, Media & Sport, "Cyber security breaches survey 2021," 2021. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021

[2] European Commission and Directorate-General for Migration and Home Affairs, *Europeans' attitudes towards cyber security*. European Commission, 2020.

[3] Institut National de la Statistique et des Études Économiques (INSEE), "Cvs—cadre de vie et sécurité 2016," 2016. [Online]. Available: https://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-Cadre-de-vie-et-securite-2016

[4] Statistics Netherlands, "Veiligheidsmonitor 2016," 2017. [Online]. Available: https://www.cbs.nl/nl-nl/publicatie/2017/09/veiligheidsmonitor-2016

[5] The Swedish National Council for Crime Prevention (Brå), "Swedish crime survey 2017," 2018. [Online]. Available: https://bra.se/publikationer/arkiv/publikationer/2018-01-29-nationella-trygghetsundersokningen-2017.html

[6] Coalition Inc., "H1 2021 cyber insurance claims report," 2021. [Online]. Available: https://info.coalitioninc.com/download-2021-h1-cyber-claims-report.html

[7] Hiscox Inc., "The Hiscox cyber readiness report 2017," 2017. [Online]. Available: https://www.hiscox.co.uk/cyberreadiness

[8] Sophos Ltd., "The state of ransomware 2021," 2021. [Online]. Available: https://secure2.sophos.com/en-us/content/state-of-ransomware

[9] CrowdStrike Inc., "2020 CrowdStrike global security attitude survey," 2020. [Online]. Available: https://www.crowdstrike.com/resources/reports/global-attitude-survey-2020/

[10] The Alternative Board, "Pulse survey cybersecurity," 2017. [Online]. Available: https://www.thealternativeboard.com/pulse-survey-cybersecurity

[11] Proximus, "How companies manage cybersecurity," 2021. [Online]. Available: https://cybersecurity.proximus.be/survey2021/research-report-cybersecurity

[12] C. M. Reep-van den Bergh and M. Junger, "Victims of cybercrime in Europe: a review of victim surveys," *Crime Science*, vol. 7, no. 1, pp. 1–15, 2018.

[13] M. Eling and W. Schnell, "Capital requirements for cyber risk and cyber risk insurance: An analysis of Solvency II, the U.S. risk-based capital standards, and the Swiss solvency test," *North American Actuarial Journal*, vol. 24, no. 3, pp. 370–392, 2020.

[14] M. Riek and R. Böhme, "The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates," *Journal of Cybersecurity*, vol. 4, no. 1, 10 2018.

[15] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. Van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *The economics of information security and privacy*. Springer, 2013, pp. 265–300.

[16] M. Tcherni, A. Davies, G. Lopes, and A. Lizotte, "The dark figure of online property crime: Is cyberspace hiding a crime wave?" *Justice Quarterly*, vol. 33, no. 5, pp. 890–911, 2016.

[17] J. Slupska and L. M. Tanczer, "Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things," in *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Emerald Publishing Limited, 2021.

[18] J. Slupska, "Safe at home: Towards a feminist critique of cybersecurity," *St Antony's International Review*, vol. 15, no. 1, pp. 83–100, 2019.

[19] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135, 2016.

[20] D. W. Woods, T. Moore, and A. C. Simpson, "The county fair cyber loss distribution: Drawing inferences from insurance prices," vol. 2, no. 2. New York, NY, USA: Association for Computing Machinery, apr 2021. [Online]. Available: https://doi.org/10.1145/3434403

[21] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[22] R. Anderson, C. Barton, R. Böhme, R. Clayton, C. Ganán, T. Grasso, M. Levi, T. Moore, and M. Vasek, "Measuring the changing cost of cybercrime," in *18th Workshop on the Economics of Information Security (WEIS 2019)*, 2019.

[23] D. W. Woods and R. Böhme, "SoK: Quantifying cyber risk," in *IEEE Symposium on Security and Privacy*, Oakland, CA, May 2021, pp. 909–926.

[24] M. McShane, M. Eling, and T. Nguyen, "Cyber risk management: History and future research directions," *Risk Management and Insurance Review*, 2021.

[25] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy006, 2018.

[26] L. Paoli, J. Visschers, and C. Verstraete, "The impact of cybercrime on businesses: A novel conceptual framework and its application to belgium," *Crime Law Soc Change*, vol. 70, pp. 397–420, 2018.

[27] B. Dupont and C. Whelan, "Enhancing relationships between criminology and cybersecurity," *Journal of Criminology*, vol. 54, no. 1, pp. 76–92, 2021.

[28] B. Edwards, S. Hofmeyr, and S. Forrest, "Hype and heavy tails: A closer look at data breaches," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 3–14, 2016.

[29] Ponemon Institute, "Cost of a data breach study available at https://www.ibm.com/security/data-breach," 2018. [Online]. Available: https://www.ibm.com/security/data-breach

[30] Verizon LLC, "2021 data breach investigations report," 2021. [Online]. Available: https://enterprise.verizon.com/en-gb/resources/reports/dbir/

[31] L. Axon, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese, "Analysing cyber-insurance claims to design harm-propagation trees," in *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*. IEEE, 2019.

[32] M. Eling and N. Loperfido, "Data breaches: Goodness of fit, pricing, and risk measurement," *Insurance: Mathematics and Economics*, vol. 75, pp. 126–136, 2017.

[33] M. Eling and J. Wirfs, "What are the actual costs of cyber risk events?" *European Journal of Operational Research*, vol. 272, no. 3, pp. 1109–1119, 2019.

[34] A. Erola, I. Agrafiotis, J. R. Nurse, L. Axon, M. Goldsmith, and S. Creese, "A system to calculate cyber-value-at-risk," *Computers & Security*, vol. 113, p. 102545, 2022.

[35] UK Department for Digital, Culture, Media & Sport, "Cyber security breaches survey 2016," 2016. [Online]. Available: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016

[36] ——, "Cyber security breaches survey 2018," 2018. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

[37] ——, "Cyber security breaches survey 2019," 2019. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

[38] ——, "Cyber security breaches survey 2020," 2020. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020

[39] European Commission and Directorate-General for Migration and Home Affairs, *Europeans' attitudes towards cyber security*. European Commission, 2017.

[40] ——, *Europeans' attitudes towards cyber security*. European Commission, 2019.

[41] A. Dreißigacker, B. von Skarczinski, and G. Wollinger, *Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019*, 03 2020.

[42] ——, *Cyberangriffe gegen Unternehmen in Deutschland Ergebnisse einer Folgebefragung 2020*, 2021.

[43] The Swedish National Council for Crime Prevention (Brå), "Swedish crime survey 2018," 2019. [Online]. Available: https://bra.se/bra-in-english/home/publications/archive/publications/2019-03-08-swedish-crime-survey-2018.html

[44] ——, "Swedish crime survey 2019," 2019. [Online]. Available: https://bra.se/bra-in-english/home/publications/archive/publications/2019-11-12-swedish-crime-survey-2019.html

[45] ——, "Swedish crime survey 2020," 2020. [Online]. Available: https://bra.se/bra-in-english/home/publications/archive/publications/2020-10-15-swedish-crime-survey-2020.html

[46] ——, "Swedish crime survey 2021 available at https://bra.se/bra-in-english/home/publications/archive/publications/2021-10-12-swedish-crime-survey-2021.html," 2021. [Online]. Available: https://bra.se/bra-in-english/home/publications/archive/publications/2021-10-12-swedish-crime-survey-2021.html

[47] Statistics Netherlands, "Veiligheidsmonitor 2017," 2018. [Online]. Available: https://www.cbs.nl/nl-nl/publicatie/2018/09/veiligheidsmonitor-2017

[48] ——, "Veiligheidsmonitor 2019," 2020. [Online]. Available: https://www.cbs.nl/nl-nl/publicatie/2020/10/veiligheidsmonitor-2019

[49] Institut National de la Statistique et des Études Économiques (INSEE), "Cvs—cadre de vie et sécurité 2017," 2017. [Online]. Available: https://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-Cadre-de-vie-et-securite-2017

[50] ——, "Cvs—cadre de vie et sécurité 2018," 2018. [Online]. Available: https://www.interieur.gouv.fr/Interstats/L-enquete-Cadre-de-vie-et-securite-CVS/Rapport-d-enquete-Cadre-de-vie-et-securite-2018

[51] ——, "Cvs—cadre de vie et sécurité 2019," 2019. [Online]. Available: https://www.interieur.gouv.fr/Interstats/L-enquete-Cadre-de-vie-et-securite-CVS/Rapport-d-enquete-Cadre-de-vie-et-securite-2019

[52] C. Biancotti, "The price of cyber (in)security: evidence from the italian private sector," in *17th Workshop on the Economics of Information Security (WEIS 2018)*, 2018.

[53] J. Hernandez-Castro and E. Boiten, "Cybercrime prevalence and impact in the uk," *Computer Fraud and Security*, vol. 2014, p. 5–8, 02 2014.

[54] CrowdStrike Inc., "2021 CrowdStrike global security attitude survey," 2021. [Online]. Available: https://www.crowdstrike.com/resources/reports/global-security-attitude-survey-2021/

[55] U. Franke and J. Wernberg, "A survey of cyber security in the swedish manufacturing industry," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2020, pp. 1–8.

[56] Coalition Inc., "H1 2020 cyber insurance claims report," 2020. [Online]. Available: https://info.coalitioninc.com/download-2020-cyber-claims-report.html

[57] Sophos Ltd., "The state of ransomware 2020," 2020. [Online]. Available: https://news.sophos.com/en-us/2020/05/12/the-state-of-ransomware-2020/

[58] Hiscox Inc., "The Hiscox cyber readiness report 2018," 2018. [Online]. Available: https://www.hiscox.co.uk/cyberreadiness

[59] ——, "The Hiscox cyber readiness report 2019," 2019. [Online]. Available: https://www.hiscox.co.uk/cyberreadiness

[60] ——, "The Hiscox cyber readiness report 2020," 2020. [Online]. Available: https://www.hiscox.co.uk/cyberreadiness

[61] ——, "The hiscox cyber readiness report 2021," 2021. [Online]. Available: https://www.hiscox.co.uk/cyberreadiness

[62] Statistics Canada, "Canadian survey of cyber security and cybercrime 2019," 2020. [Online]. Available: https://www.serene-risc.ca/en/statistics-canada

[63] J. M. Drew, "A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies," *Journal of Criminological Research, Policy and Practice*, vol. 6, pp. 17–33, 2020.

[64] U.S. Department of Justice, "Victims of identity theft, 2016," 2019. [Online]. Available: https://bjs.ojp.gov/library/publications/victims-identity-theft-2016

[65] ——, "Victims of identity theft, 2018," 2021. [Online]. Available: https://bjs.ojp.gov/library/publications/victims-identity-theft-2018

[66] A. Rege, "Critical infrastructure ransomware incident dataset version 11.6 available at https://sites.temple.edu/care/ci-rw-attacks/," *Temple University*, 2020.

[67] European Commission, "SME fact sheet 2021," https://ec.europa.eu/growth/smes/sme-strategy/sme-performance-review.

[68] GOV.UK, "Companies register activities: 2018 to 2019," https://www.gov.uk/government/statistics/companies-register-activities-statistical-release-2018-to-2019.

[69] Statista, "Estimated number of companies worldwide from 2000 to 2020, by region."

[70] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[71] J. D. Howard and T. A. Longstaff, "A common language for computer security incidents," Sandia National Lab, Albuquerque, New Mexico, Tech. Rep., 1998.

[72] M. Dunn Cavelty, "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse," *International Studies Review*, vol. 15, no. 1, pp. 105–122, 2013.

[73] J. Aycock, *Computer viruses and malware*. Springer Science & Business Media, 2006, vol. 22.

[74] V. Valeros and S. Garcia, "Growth and commoditization of remote access trojans," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 454–462.

[75] G. Di Tizio and C. N. Ngo, "Are you a favorite target for cryptojacking? a case-control study on the cryptojacking ecosystem," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 515–520.

[76] V. Šembera, M. Paquet-Clouston, S. Garcia, and M. J. Erquiaga, "Cybercrime specialization: An exposé of a malicious android obfuscation-as-a-service," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2021, pp. 213–226.

[77] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in *2012 IEEE symposium on security and privacy*. IEEE, 2012, pp. 95–109.

[78] K. Rieck, T. Holz, C. Willems, P. Düssel, and P. Laskov, "Learning and classification of malware behavior," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2008, pp. 108–125.

[79] M. Button, D. Blackbourn, L. Sugiura, D. Shepherd, R. Kapend, and V. Wang, "From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the united kingdom," *Telematics and Informatics*, vol. 64, p. 101675, 2021.

[80] R. Richardson, M. M. North, and D. Garofalo, "Ransomware: The landscape is shifting-a concise report," *International Management Review*, vol. 17, no. 1, pp. 5–8, 2021.

[81] A. Gazet, "Comparative analysis of various ransomware virii," *Journal in computer virology*, vol. 6, no. 1, pp. 77–90, 2010.

[82] K. P. Subedi, D. R. Budhathoki, and D. Dasgupta, "Forensic analysis of ransomware families using static and dynamic analysis," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 180–185.

[83] K. Liao, Z. Zhao, A. Doupé, and G.-J. Ahn, "Behind closed doors: measurement and analysis of Cryptolocker ransoms in Bitcoin," in *2016 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2016, pp. 1–13.

[84] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz003, 2019.

[85] É. Leverett, E. Jardine, E. Burns, A. Gangwal, and D. Geer, "Averages don't characterise the heavy tails of ransoms," in *2020 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2020, pp. 1–12.

[86] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The ransomware-as-a-service economy within the darknet," *Computers & Security*, vol. 92, p. 101762, 2020.

[87] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, "Tracking ransomware end-to-end," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 618–631.

[88] P. Burda, L. Allodi, and N. Zannone, "Dissecting social engineering attacks through the lenses of cognition," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2021, pp. 149–160.

[89] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, and M. F. Costabile, "Human factors in phishing attacks: A systematic literature review," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–35, 2021.

[90] G. Simpson and T. Moore, "Empirical analysis of losses from business-email compromise," in *2020 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2020, pp. 1–7.

[91] A. Cidon, L. Gavish, I. Bleier, N. Korshun, M. Schweighauser, and A. Tsitkin, "High precision detection of business email compromise," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1291–1307.

[92] J. Isacenkova, O. Thonnard, A. Costin, A. Francillon, and D. Balzarotti, "Inside the scam jungle: A closer look at 419 scam email operations," *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1–18, 2014.

[93] M. Button and C. Cross, *Cyber frauds, scams and their victims*. Routledge, 2017.

[94] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *Journal in Computer Virology*, vol. 2, no. 1, pp. 13–20, 2006.

[95] J. Jansen and R. Leukfeldt, "How people help fraudsters steal their money: An analysis of 600 online banking fraud cases," in *Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, 2015, pp. 24–31.

[96] ——, "Phishing and malware attacks on online banking customers in the netherlands: A qualitative analysis of factors leading to victimization," *International Journal of Cyber Criminology*, vol. 10, no. 1, p. 79, 2016.

[97] S. Drimer, S. J. Murdoch, and R. Anderson, "Optimised to fail: Card readers for online banking," in *International Conference on Financial Cryptography and Data Security*. Springer, 2009, pp. 184–200.

[98] R. Anderson, *Security engineering*. John Wiley & Sons, 2008.

[99] K. Thomas, F. Li, C. Grier, and V. Paxson, "Consequences of connectivity: Characterizing account hijacking on Twitter," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 489–500.

[100] E. Bursztein, B. Benko, D. Margolis, T. Pietraszek, A. Archer, A. Aquino, A. Pitsillidis, and S. Savage, "Handcrafted fraud and extortion: Manual account hijacking in the wild," in *Proceedings of the Internet Measurement Conference*, 2014, pp. 347–358.

[101] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Communications of the ACM*, vol. 58, no. 7, pp. 78–87, 2015.

[102] D. G. Gregg and J. E. Scott, "A typology of complaints about ebay sellers," *Communications of the ACM*, vol. 51, no. 4, pp. 69–74, 2008.

[103] U. Franke, H. Holm, and J. König, "The distribution of time to recovery of enterprise IT services," *IEEE Transactions on Reliability*, vol. 63, no. 4, pp. 858–867, 2014.

[104] A. Hutchings and R. Clayton, "Exploring the provision of online booter services," *Deviant Behavior*, vol. 37, no. 10, pp. 1163–1178, 2016.

[105] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems (TOCS)*, vol. 24, no. 2, pp. 115–139, 2006.

[106] M. Karami and D. McCoy, "Rent to pwn: Analyzing commodity booter ddos services," *Usenix login*, vol. 38, no. 6, pp. 20–23, 2013.

[107] D. Florêncio and C. Herley, "Sex, lies and cyber-crime surveys," in *Economics of Information Security and Privacy III*. Springer, 2013, pp. 35–53.

[108] S. Karstedt, "Comparing cultures, comparing crime: Challenges, prospects and problems for a global criminology," *Crime, Law and Social Change*, vol. 36, no. 3, pp. 285–308, 2001.

[109] J. P. Lynch, "Problems and promise of victimization surveys for cross-national research," *Crime and justice*, vol. 34, no. 1, pp. 229–287, 2006.

[110] J. Lusthaus, M. Bruce, and N. Phair, "Mapping the geography of cybercrime: A review of indices of digital offending by country," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 448–453.

[111] A. V. Vu, J. Hughes, I. Pete, B. Collier, Y. T. Chua, I. Shumailov, and A. Hutchings, "Turning up the dial: the evolution of a cybercrime market through set-up, stable, and covid-19 eras," in *Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 551–566.

[112] D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, and N. Díaz-Castaño, "Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk," *European Societies*, vol. 23, no. sup1, pp. S47–S59, 2021.

[113] S. Kemp, D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño, "Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during covid-19," *Journal of Contemporary Criminal Justice*, vol. 37, no. 4, pp. 480–501, 2021.

[114] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, p. 102248, 2021.

[115] S. Romanosky, A. Kuehn, L. Ablon, and T. Jones, "Content analysis of cyber insurance policies: how do carriers price cyber risk?" *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz002, 2019. [Online]. Available: https://dx.doi.org/10.1093/cybsec/tyz002

[116] D. W. Woods, "Quantifying privacy harm via personal identity insurance," *Available at SSRN 3984005*, 2021.

[117] D. W. Woods and A. C. Simpson, "Policy measures and cyber insurance: a framework," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 209–226, 2017.

[118] K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. G. Kelley, D. Kumar *et al.*, "SoK: Hate, harassment, and the changing landscape of online abuse," in *IEEE Symposium on Security and Privacy*, Oakland, CA, May 2021, pp. 247–267.

[119] M. T. Whitty and T. Buchanan, "The online romance scam: A serious cybercrime," *CyberPsychology, Behavior, and Social Networking*, vol. 15, no. 3, pp. 181–183, 2012.

[120] S. Pastrana, A. Hutchings, D. Thomas, and J. Tapiador, "Measuring ewhoring," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 463–477.

[121] W. N. Espeland and M. L. Stevens, "A sociology of quantification," *European Journal of Sociology/Archives Européennes de Sociologie*, vol. 49, no. 3, pp. 401–436, 2008.

[122] D. Geer, K. S. Hoo, and A. Jaquith, "Information security: Why the future belongs to the quants," *IEEE Security & Privacy*, vol. 1, no. 4, pp. 24–32, 2003.

[123] D. W. Hubbard and R. Seiersen, *How to measure anything in cybersecurity risk*. John Wiley & Sons, 2016.

[124] V. Verendel, "Quantified security is a weak hypothesis: A critical survey of results and assumptions," in *Proceedings of the 2009 Workshop on New Security Paradigms (NSPW 2009)*. ACM, 2009, pp. 37–50.

[125] S. Romanosky and E. Petrun Sayers, "Enterprise risk management: Understanding the role of cyber risk," *Available at SSRN 3903305*, 2021.

[126] C. H. Gañán, M. Ciere, and M. van Eeten, "Beyond the pretty penny: The economic impact of cybercrime," in *Proceedings of the 2009 Workshop on New Security Paradigms (NSPW 2017)*, 2017, pp. 35–45.

[127] S. Tajalizadehkhoob, R. Böhme, C. Ganán, M. Korczyński, and M. V. Eeten, "Rotten apples or bad harvest? what we are measuring when we are measuring abuse," *ACM Transactions on Internet Technology (TOIT)*, vol. 18, no. 4, pp. 1–25, 2018.