Corporate under-reporting of cybercrime: An investigation into its extent and consequences

Laure Lydon

Technical Report

RHUL–ISG–2022–7

11 April 2022

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Candidate Number: 1919577

Corporate under-reporting of cybercrime: An investigation into its extent and consequences

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway University of London.

Information Security Group
Royal Holloway, University of London
August 2021

Table of Contents

Executive Summary

Reporting crimes to law enforcement agencies is the starting point for any crime response or criminal investigation process. Without reporting crimes cannot be investigated and prosecutions cannot be pursued, furthermore effective response strategies cannot be developed. Despite the importance of cybercrime reporting, many evidential sources suggest a prevalence of corporate under-reporting of cybercrime. Exploration of corporate under-reporting of cybercrime is an area of academic scholarship within which there is a current lack of coverage. This study investigates the extent and consequences of corporate under-reporting, pursues greater understanding of potential barriers to reporting and considers potential strategies to improve reporting cultures.

Under-reporting of cybercrime is a difficult topic to investigate, with corporates unlikely to publicly discuss issues relating to cybercrime victimisation or reporting positions. This qualitative research study was undertaken by , anonymously interviewing 12 seasoned information security professionals, including Chief Information Security Officers, threat intelligence experts, and senior executives of security service providers and consultancies, to explore a cross section of information security industry views on corporate under-reporting of cybercrime, analysed using Braun and Clarke's (2008) thematic analysis method.

This study finds growing trends of general accessibility to cybercrime tools and services, with a rising tide of cyber-attack sophistication, identifying links between organised crime and the cyber-attacks routinely affecting corporates. Interview participants identify that most corporates do not report cybercrimes to law enforcement agencies. I argue that these trends in combination make corporate under-reporting an important and timely issue to examine.

1. Introduction

Despite the catalytic role of crime reporting in law enforcement and crime prevention, there are several different evidential sources that suggest a vast gap exists in external corporate [1] reporting of cybercrime. These include remarkably few cybercrime prosecutions[2] as compared with both official and commercial cyber incident or breach statistics [3], a gap identified and characterised by an established academic on cybercrime, David Wall (2007, 2008) over a decade ago. This gap remains, with potentially severe and wide-reaching societal consequences.

Academic scholarship specifically relating to corporate under-reporting of cybercrime is limited, as this study reveals through rigorous academic literature searches and review. With narrow academic topic coverage, it is difficult to objectively qualify or quantify any reporting gap that exists. Current understanding of corporate under-reporting of cybercrime is largely shaped by statistics and biased security industry and commercial coverage and media reporting of cybercrime and data breaches.

Since the early 2000's (Glaessner et al., 2004) there has been commercial recognition of a gap in corporates reporting cybercrimes to authorities. The

---

1 For the purposes of this study, the term 'corporates' is taken to mean businesses and other non-government, or not for profit organisations of all sizes, including Small / Medium Enterprises (SMEs) and large, global organisations.

2 Database of proceedings under the (UK) Computer Misuse Act 1990 (Turner, 2021)

3 Statistical data sources analysed within this study include, UK 2018 Commercial Victimisation Survey, (Home Office, 2019), UK Office for National Statistics Number of recorded incidents of hacking and cybercrime (Office for National Statistics, 2019), UK Department for Digital, Culture, Media, and Sport Cyber Security Breaches Survey 2019 (Department for Digital, Culture, Media, and Sport, 2019), Verizon 2020 Data Breach Investigations Report (Verizon, 2020), 2020 Crowd Strike Global Threat Report (Crowdstrike, 2020).

2004 World Bank Report Working Paper 'Electronic Safety and Soundness: Securing Finance in a New Age', states; 'There is a classic market failure whereby there is a natural lack of incentives for "truthful disclosure" of e-security problems precisely due to possible reputation damage' (Glaessner et al., 2004, p.22). Two decades on, coverage of cyber incidents and breaches within mainstream media suggests a continuing trend of corporate under-reporting of cybercrime, with frequent reports on the proliferation of ransomware attacks and clandestine corporate ransom payments, often strenuously denied by corporates, as seen in a 2020 article in The Times, reporting British companies discretely paying out millions of pounds in ransoms (Knowles, 2020).

Even though in recent years, following Target[4], Talk Talk[5] and Equifax[6] breaches, large corporate media management strategies have matured, typically becoming more structured components of cyber incident response plans, with minimum facts, conciliatory tone and 'responsibly under control' messaging now common formulae, any such public disclosures must be tightly and carefully managed to protect corporate reputation. Corporates have learned lessons from catastrophically mismanaged public relations, epitomised by the Equifax breach in 2017[7] that remained unreported for several months, and once disclosed, the magnitude of compromised records continually increased, and so too did media coverage, attracting widespread public criticism over inaccurate detection, delays in notifying customers and authorities (Berry, 2018). Often however, this proven need for careful media

[4] December 2013 malware-attack on US retail giant Target Corp's point of sale terminals comprising the accounts and personal data of circa.70 million Target customers (Osbourne, 2014)

[5] Cyber attacks announced in October 2015 that breached a Talk Talk Telecom Group PLC customer records database compromising the personal data of 15,656 of its customers (Porcedda and Wall 2019, Information Commissioner's Office, 2021)

[6] Equifax, a credit referencing and fraud prevention agency, experienced cyber-attacks between May and July 2017, exploiting an unpatched Apache Struts vulnerability, exposing records of 147.9 million Americans (Hay Newman, 2017, Wang and Johnson, 2018, Fruhlinger, 2020)

[7] See supra note 6

management now also implies corporates withholding essential reporting information, that could enable more effective law enforcement response.

In contrast to this common media disclosure approach, whilst many corporates the world over were compromised because of the Solarwinds breach in 2020[8], (in a breach that was announced as an 'unprecedented attack' demonstrating an entirely new level of sophistication), affecting both the private sector and US government systems, media channels around the world covered the breach airing an unprecedented corporate response. FireEye's CEO, Kevin Mandia, proactively and transparently publicly disclosed the breach upon discovery, telling the world what FireEye had found, how they had found it, sharing indicators of compromise. Despite the attack remaining unknown for months, the disclosures and approach taken by Fireye, working in collaboration with Big Tech companies, including Microsoft, to combat the SolarWinds compromise threats, have been heralded in media coverage. On 3 February 2021, CNBC covered a Congressional hearing on the attack, reporting Microsoft President, Brad Smith's testimony:

> *'The fact that we are here today, discussing this attack, dissecting what went wrong, and identifying ways to mitigate future risk, is only occurring because my fellow witness, Kevin Mandia, and his colleagues at FireEye, chose to be open and transparent about what they had found in their own systems, and to invite us at Microsoft to work with them to investigate the attack'* (Feiner, 2021).

Media interest in cybercrimes against corporates has grown and has additively seizing upon the suggestion of nation state involvement in high profile cyber-attacks[9], with cyber-politics now too enveloped. In March 2021, Sky News broadcast a series of special reports entitled 'Into the Grey Zone' including interviews with former senior intelligence officials, revealing covert attacks

[8] Also dubbed the Sunburst attack, advanced threat actors utilised SolarWinds' own security tools to hack its and that of its partner's [FireEye's] customers.

[9] Such as BBC news coverage of REvil cybercriminal group website takedown, following FBI accusations of REvil's responsibility for the high-profile US ransomware attacks (Tidy, 2021).

including cyber-crimes ‘conducted in a grey zone between war and peace’ (Haynes, 2021) highlighting a changing cyber landscape that potentially affects us all.

This study argues that corporate under-reporting of cybercrime is a topical issue, worthy of further academic scholarship, important to the future of information security management and effective law enforcement, that demands greater focus and understanding. This study intends to contribute to academic literature, aiming to answer the following core research questions:

1. What does the corporate cybercrime landscape look like?
2. What is the extent of corporate under-reporting?
3. What reasons are there for corporate under-reporting?
4. What are the consequences of under-reporting?
5. What potential strategies could improve reporting cultures?

Qualitative research techniques are used within this study to discover the views of experienced information security professionals across these five core research topics; providing realist insights into the current corporate cybercrime landscape, investigating the extent of corporate under-reporting, understanding the barriers that might exist to corporate reporting of cybercrime, considering the consequences of under-reporting, and exploring potential strategies to improve corporate reporting cultures.

1.1. Structure of the Report

The opening chapters of the report set out theories underpinning the core research questions, the research approach and methodology adopted for the study.

- Chapter 2, Project Literature Review
  Discusses academic coverage of related subject areas, introducing compass points to navigate issues associated with corporate under-reporting of cybercrime, which underpin the core research questions.

- Chapter 3, Methods
  Provides an overview of literature searches undertaken and outlines the qualitative research approach, including the semi-structured interview process and thematic analysis deployed.

Subsequent chapters form the main body of the report, consolidate interview findings through thematic analysis, with the treatment of key themes serving to answer the study's core research questions in relation to each of the five core topics covered:

- Chapter 4, The Cybercrime Landscape
  Aims to provide context, capturing participants' views on the types of cybercrimes affecting corporates, establishing an overarching picture of the current cybercrime landscape, with the aim of answering core research question 1 (as set out within the introduction above).

- Chapter 5, Corporate Under-Reporting of Cybercrime
  Seeks to establish the extent of corporate under reporting, based on the experiences of interviewees and drawing on comparisons with relevant cybercrime reporting statistics. This chapter aims to answer core research question 2.

- Chapter 6, Barriers to Reporting
  Exposes attitudes towards, and barriers to reporting, providing answers to core research question 3.

- Chapter 7, Under-Reporting Consequences
  Sets out the effects understood by participants of corporate under-reporting of cybercrime, answering core research question 4.

- Chapter 8, Potential Strategies to Improve Reporting Cultures
  Offers potential strategies to improve reporting cultures proposed by both interview participants directly and other potential improvement

strategies proposed by the researcher, shared with participants to solicit opinions on relative advantages and disadvantages of the potential implementation of such strategies, to answer core research question 5.

Within the final chapter conclusions are drawn on the extent of corporate underreporting, comparing theories explored through literature review with interview analysis findings, highlighting why corporate under-reporting matters and acting is vital to address the increasing problem of cybercrime proliferation.

.

2. Project Literature Review

As discussed within Chapter 1, broad-reaching literature searches have revealed limited academic authorship specifically relating to the topic of corporate under-reporting of cybercrime. The core research questions within this study are largely derived from gaps identified in academic literature.

The following chapter summarises the review of relevant literature sources that were found in support of this study. Additionally, relevant statistics are identified, against which qualitative interview findings are compared.

2.1. Literature Searches

Combinations of interchangeable terms were used to search a variety of databases, full results of which can be seen within Appendix 1 – Literature Search Results. Table 1 below shows search terms used:

Table 1 - Literature Search Terms

	Keyword 1	**Keyword 2**	**Keyword 3**
Synonyms	Organisation Organisation Corporate Business Private Sector	Reporting Under-reporting Enforcement Prosecution	Internet Crime Internet Enabled Crime Cyber Crime Cyber Data Breach Offenses

The Royal Holloway University of London's (RHUL) Library Search returned no direct 'hits', results were however returned through automated expanded search functionality. The keyword combination generating the most relevant results was: Corporate AND Under-Reporting AND Cybercrime, yielding 3248 expanded search results. Analysis of the first 1000 results produced 15 literature sources of direct relevance to this investigation, specifically referring

or alluding to corporate under-reporting of cybercrime, with diminishing returns beyond the first 500 results.

Through abstract analysis (with self-determination of relevance, currency, purpose, and authority), approximately 16% of the first 1000 results presented literature sources from subject categories supporting exploration of wider issues associated with under reporting, details of subject categories both included and excluded from this analysis are provided within Appendix 2 – Literature Review, Subject Categories.

2.2. Cybercrime and Corporate Reporting

As discussed within Chapter 1, shortfalls in corporate reporting of cybercrime have been observed for nearly two decades (Glaessnar et al., 2004), yet under-reporting appears to remain a concern. Neither cybercrime nor corporate reporting conditions exist in a vacuum, therefore understanding the nature of the current cybercrime landscape is an important precursor to the investigation of corporate under-reporting.

2.2.1. The Cybercrime Landscape

Literature searches in relation to the topic of corporate under-reporting of cybercrime are somewhat complicated, mainly due to ambiguity in defining:

- Cybercrimes,
- Cybercrimes that affect corporates,
- Reporting scope and criteria,
- Applicable jurisdictions or geographical reach.

Although cybercrime is now a commonly used term, there are many different definitions (Gordon and Ford, 2006, Wall, 2007), with no agreed definition of cybercrime (Anderson et al., 2013). Cybercrimes can encompass a broad range of activities, with differentiation often made between cyber-enabled

crimes[10] and cyber-dependent crimes[11] (although the lines between them are sometimes blurred) as described by (Wall, 2007). Generally, though, the term cybercrime is accepted to relate to malicious or nefarious activities carried out over the internet, or computer networks.

Establishing a baseline understanding of the volume and nature of cybercrimes affecting corporates assists in addressing the core research questions. Establishing such a view is complicated not only through a lack of common definition of cybercrime but also in the way that instances of cybercrimes are classified and treated as legal offences, as seen within UK examples below:

- The UK Office for National Statistics website states" Cybercrime is not a specific legal offence and thus does not form part of the offence list that is reported within the Official Statistics. However, there is some information on cybercrime available from these sources. The Crime Survey for England and Wales (CSEW) provides the best indication of the volume of computer misuse offences. This is because only a small proportion of all incidents are reported and recorded". (Office for National Statistics, 2021).
- The UK 2018 Commercial Victimisation Survey asks respondents who use computers at their premises about their experience of online crime, findings from the survey are reported within Crime Against Businesses: Findings from the 2018 Commercial Victimisation Survey Report (Home Office, 2019a). The report states that although described as crimes, not all incidents are recorded as a crime under the Home Office Counting Rules (e.g., phishing is treated as an enabler to computer misuse, no separate crime would be recorded in relation to the phishing, only the misuse crime would be recorded (Home Office, 2019a).

[10] Cyber enabled crimes seen essentially extensions of 'traditional' or 'terrestrial' crimes, facilitated or augmented using computing technologies and internet communications.

[11] Cyber-dependent crimes target internet connected devices with computing capability, without which the crime would not exist.

Based on the inconsistencies in cybercrime classification, lack of consistent definition and context presented within the statistics above, significant challenges exist in relying on official statistics alone to form a baseline view.

On the extent of cybercrime, of the industries included in the UK 2018 Commercial Victimisation Survey (Home Office, 2019a), on average, the number of incidents of online crime experienced by each (business) victim was 10 in the last 12 months (Home Office, 2019b). Some argue that commercially reported statistics can provide useful context, however, examination of relevant examples present even greater challenges:

- The Verizon 2020 Data Breach Investigations Report analyses 157,525 incidents from 81 contributors across 81 countries (Verizon, 2020), There is no information provided about contributors, the figures however suggest the volume of incidents affecting contributors differs significantly from the 1:10 ratio seen within the UK Crime Victimisation Survey (Home Office, 2019).
- The 2020 Crowd Strike Global Threat Report identifies some 35,000 breach attempts prevented within 2019 (Crowdstrike, 2020) upon which its report is based, but again provides no definition of breach attempts (that could range from reconnaissance activities to data exfiltration attempts) or number of affected entities (customers) to allow any comparison or analysis.

These examples show commercial statistics to be highly problematic in terms of consistency and they are produced to support sales agendas. Commercial statistics are not therefore considered to provide a firm basis for analysis within this study, but sometimes provide otherwise uncaptured contextual insights.

This study considers all types of cybercrimes that affect corporate organisations, to avoid taking a restricted view and potentially excluding certain types of crimes that may otherwise be overlooked. Cybercrimes considered include hacking, Denial of Service attacks, relevant content crime activities, and insider threats, the importance of which is seen within Williams et al. (2019).

In terms of geographical scope, considering global interconnectivity, remote execution, and the frequent trans-border nature of cybercrimes, this study remains non-geographic, drawing on examples from different jurisdictions.

2.2.2. Corporate Under-Reporting of Cybercrime

Limited academic sources are found to quantify the extent of corporate under-reporting. Of the 15 literature sources identified as directly relevant to this investigation, six sources relate to shortcomings relating to the (US) Securities and Exchange Commission (SEC) disclosure requirements for publicly traded companies to report material risks associated with cybersecurity and cybersecurity incidents (Higgins and Zatylny, 2018).

Whilst the emphasis of this investigation is to address under-reporting to authorities for the purposes of crime prevention and/or law enforcement; studies examining external reporting to regulatory authorities such as SEC corporate disclosure failings provide valuable insight into corporate reporting cultures. Aside from inadequacy findings concerning the SEC requirements themselves, a range of reporting issues are found, including companies providing generic information relating to cybersecurity or lacking meaningful detail with respect to their reporting of incidents, inconsistent determination of materiality (the threshold for SEC reporting), disclosure delay or withholding information to either protect shareholders, avoiding media coverage or to preserve brand value and reputation (Etzioni, 2011, Trope, 2012, Ferraro, 2013, Young, 2013, Amir et al., 2018). Etzioni (2011) claims that corporations are only concerned with the interests their own shareholders, preferring to counteract breach losses internally than expose weaknesses publicly to protect reputation.

Following the 2017 Equifax breach[12], the Securities and Exchange Commission set out new disclosure guidance in February 2018, emphasising Board

[12] See *supra note 6*

responsibilities for the oversight of cybersecurity and to better consider materiality in filings (Higgins and Zatylny, 2018). Despite the issuance of this additional guidance, Amir et al. (2018) continue to find evidence of management disclosure failures, estimating that disclosures are only made when investors already highly suspect an attack (with over 40% likelihood). Although their finding does not serve exactly to quantify the extent of under-reporting, it is a useful indicator as to the general balance of decision making and the point at which corporations bound by SEC requirements judge their responsibility to disclose must be fulfilled.

Statistics may also assist in determining the extent of corporate under-reporting. The UK Government (Department for Digital, Culture, Media, and Sport, 2020) Cyber Security Breaches asks respondents who say they suffered such an event, whether they reported their most disruptive breach internally and externally. The findings suggest that less than 10% of corporates report to law enforcement. Relevant statistics from the survey were shared with interview participants to initiate conversations, further discussed within Chapter 5.

2.2.3. Barriers to Reporting

Despite a lack of specific academic focus on corporate under-reporting of cybercrime as a standalone topic, there are some reasons suggested by academics for it.

- **Unaware**

  Within Ferraro's (2013) analysis of the US Securities and Exchange Commission's cyber security disclosure guidance, he notes that victims may remain unaware that they have suffered any form of attack.

- **Unwillingness**

  Wall (2007) discusses the potential unwillingness of organisations to identify themselves as cybercrime victims, citing Levi in highlighting practices of banks writing off or failing to declare losses to avoid reporting

(Levi, 2001, cited in Wall, 2007) and further identifies victims' disincentives to report, particularly when under threat (Wall, 2007).

The lack of willingness of companies to report cybercrime, as identified by Wall (2007), is further echoed in a more recent study by (Graham et al., 2019) focusing on the relevance of procedural justice to cybercrime, with the purpose of understanding the reporting intentions of both terrestrial crime and cybercrime victims, recognising in conclusion, significant under-reporting of cybercrimes to law enforcement agencies.

- **Impacts on Stock and Share Price**

Examining the impacts on stock and share price, Cavusoglu et al. (2004) analyse the impacts of security incident dis-closures on trading performance and value post breach, concluding, on average a loss of 2.1% of market value seen within two days of disclosure. A later study by Juma'h and Alnsour (2020) confirms that losses are generally short lived, with no substantial quarterly post breach changes. Researchers Laube and Böhme (2016), investigating the effectiveness of breach notification laws, acknowledge not only the costs incurred by breached organisations, but also those of dependent organisations, concluding that breach notification laws with significant penalties incentivise notification (where penalties far outweigh the costs of reporting). Despite this correlation, not all studies in this field arrive at the same, unanimous conclusion; in their study, Klaus and Elzweig (2020) suggest that use of different methods and measurements may produce inconsistent results, therefore denying a definitive theoretical position. Generally, however, these studies may assist in gauging the perceived importance of stock and share price as a factor in the determination of reporting decisions.

- **Brand and Reputation**

Corporates are, irrespective of direct financial costs are also concerned with brand reputation, Wang et al.(2013) study the language used in security breach reporting and the effect that this can have on public perception. A study of the 2014 Sony breach also explores public

perception immediately following disclosure, observing that instead of being perceived as a victim, the public's focus was on Sony's inaction (Krishna and Vibber 2017).

- **Reporting Thresholds**

As previously discussed, SEC cyber incident disclosures are required based on a threshold of materiality. Whilst this is not a distinction of the materiality of the type of cyber incident (or crime) but moreover, a determination of financial risk materiality (Higgins and Zatylny 2018)[13] the concept of determining financial materiality may still be useful as a point of comparison, also as a factor in reporting decisions.

- **Law Enforcement Challenges**

Additive potential reasons for under-reporting are suggested by Wall in relation to cybercrime policing and law enforcement challenges. These range from 'de minimism' (where crimes are not considered serious enough to be effectively addressed), coupled with legal characterisation of the seriousness of crime, to the lack of faith in constructive or successful law enforcement outcomes (Wall, 2007).

- **Reporting Processes**

Academic attention has more recently turned to addressing reporting processes, indicating that reporting mechanisms are at fault, Bidgoli et al. (2019) call out under-reporting and propose an interface to enable more effective reporting. Whereas Jhaveri et al. (2017) provide a reporting model to enable learning from voluntary reporting, this study will consider whether changes to reporting processes are needed.

[13] Whereas the materiality determination within the context of the EU General Data Protection Regulation is based on the materiality of the impact of the breach on data subjects.

2.2.4. Under-Reporting Consequences

Understanding the tapestry of effects and consequences of cybercrime is vital to unblock barriers to better reporting. In the following section a range of effects are reviewed.

- **Cybercrime Proliferation**

The fundamental concern with under-reporting is that it allows cyber criminals to stay in the shadows without being apprehended (Wall, 2008). When lucrative criminal behaviour goes unchecked, it proliferates, as seen with the increasing rise in ransomware attacks (Crowdstrike, 2020). The 'to pay or not to pay' ransom debate is well covered in literature, including (Morse and Ramsey, 2017, Newman, 2017).

- **Links to Organised Crime**

The potential connection between cybercrime and organised crime and associated implications are explored by Leukfeldt et al. (2017). The researchers study some 40 cybercrime investigations into criminal networks that conducted very specific types of cybercrime. These included phishing and malware attacks, in the Netherlands, Germany, UK and US, between 2004 and 2014. All 40 investigations resulted in the generation of sufficient evidence to prosecute. The study includes the examination of relationships between the members of the criminal networks (that vary in size), their physical and/or virtual world connections, their roles, skill levels, offending history, and connections with other criminal networks. It aims to determine the extent to which these networks commit-ting cybercrimes could be conceived as 'organised crime'. Despite its findings demonstrating that the majority of networks co-opt members to perform different roles, based on their level of skill, and in addition, finding five of the networks to have links to traditional organised crime groups; the study concludes that if only 'structure and composition' were considered, these networks would largely fail to meet existing definitions of organised crime and, furthermore highlights the challenges with transferring the concept of organised crime, legally signifying increased danger, to 'cyber-crime that is organised'

(Leukfeldt et al.,2017). The conclusions of the 2017 study did however find links to organised crime in low-level cyber-attacks on corporates (despite potential legal challenges in recognition). Understanding the potential wider consequences of cybercrime another potential factor in reporting decisions.

- **Cyber Crime and Cyber Politics**

Dunn Cavelty and Wenger (2020) discuss the intersection of cyber security and politics, they argue that secret state sponsored cyber operations have become routine and offer observations that may prove useful in shaping strategies to improve corporate reporting culture, including the roles of governments, rules, and boundaries. Cybercrime takes on many different dimensions; with significant challenges to cybercrime attribution, (Hakimi, 2019, Finnemore and Hollis, 2020). The lines between the actions of nation state actors and cyber criminals working under the instruction of organised criminal groups can become blurred, Sailio et al. (2020) contests that differentiation between threat actors is not always possible. These issues raise new questions. Do corporates adequately understand the types of threats they face? Is understanding the threat important if the consequence to the corporate is the same?

2.2.5. Strategies to Improve Corporate Reporting

Four areas are explored in seeking to identify potential strategies to drive change and improvement to corporate cybercrime reporting cultures.

- **Public/Private Sector Partnership and Intelligence Sharing**

Laube and Böhme (2016) argue that there is a conflict of interests between corporates and authorities, with the need to incentivise information sharing between government agencies and private organisations. They stipulate that there needs to either be a strong regulatory incentive mechanism that includes security audits, or that at the opposite end of the spectrum, voluntary information sharing may be cultivated, with incentivisation created through improved investment decisions and prioritisation. Dutta

and McCrohan (2002) also advocate such public-private sector collaboration.

Intelligence sharing is predicated on trust (Wagner et al., 2019), Lewis and Weigert's (1985) consideration of the sociological concept of trust can be applied to explore trust implications that are intrinsic to effective intelligence sharing strategies.

- **A Role for Bystanders**

A complimentary approach to intelligence sharing for stronger defence may rest in Rowe's (2018) **'**bystander' theory. Rowe argues that bystanders are routinely 'a missing link in conflict systems' (Rowe, 2018). Through the juxtaposition of a conflict system with a cyber-crime environment, using Rowe's theory, bystanders (such as security technology providers) could be used to greater effect share information they gather and strengthen both defence and deterrence. Taking this approach could be explored to build on Perset's (2010) "Economic and Social Role of Internet Intermediaries", suggesting internet intermediaries are in a unique 'middleman' position to secure and protect individuals.

- **Safety Culture**

Syed's popular book, Black Box Thinking, takes cultural safety learnings from the aviation industry and looks at how they might be applied to improve performance. Demonstrated throughout the book in relation to the healthcare industry, Syed argues there is a culture of negativity towards failure and of 'cognitive dissonance' [14](Syed, 2015). A different approach to the application of safety culture is taken by Dekker and Breakey (2014) balancing a 'no-blame' culture against a culture where management intervention to get back on track is required. it may be beneficial to create a 'safe' or safety culture-oriented environment for confidential reporting to enable investigation and learning.

[14] Festinger's term describing 'the tension we feel when, among other things, our beliefs are challenged by evidence (Festinger,1957, Syed, 2015).

According to Ashford (2018), this is type of approach is one of the key aims of the UK's National Cyber Security Centre (NCSC) and reporting body Action Fraud's objectives for reporting channels, whether implemented effectively or not.

- **Norms, Law and Regulation**

The cyber security posture of many organisations operating in jurisdictions with mandatory reporting requirements is seen to increase, as shown in (Tang and Whinston, 2020), engendering an argument for mandatory cybercrime reporting and strong sanctions, whereas a more cautious approach to the introduction of cyber legislation is taken by Holt, discussing the implementation of Australian laws (Holt, 2018).

A proposed alternative or compliment to legislation (whether over or under sanctioned, that encourages reporting decisions to be made based on materiality thresholds), Finnemore and Hollis' work, 'Constructing Norms for Global Cybersecurity' sets a path or basis for voluntary agreement, for improved cyber behaviours based on 'group identity' that is to say those who identify with the identity of the target group (Finnemore and Hollis, 2016).

The above theories and readings serve to underpin interview questions and drive discussion with interviewees. Theories are compared with interview findings within the conclusion section of this study, Chapter 9.

3. Methods

This study utilises qualitative research techniques, employing semi-structured interviews to explore the core research questions outlined within Chapter 1.

3.1. Qualitative Research Interviews

Interviews were conducted with twelve seasoned information security professionals, drawing on the real-world experiences to probe topics that are not generally discussed publicly.

Interviews were conducted anonymously in accordance with the Royal Holloway University of London's ethics rules and procedures following a research ethics submission, resulting in review and ethics approval from the University's Information Security Group Ethics Panel.

Detailed information on the study was provided to all participants within a Participant Information Sheet and written consent obtained prior to participation.

High level participant profiles are provided below, with care taken to preserve participant anonymity. Industry descriptions and/or geographical details are omitted for participants whose roles are of high sensitivity:

- Participant 1 – Executive Director, UK based security consultancy
- Participant 2 – Senior Leader, international security organisation
- Participant 3 – Chief Information Security Officer (CISO) regulated industry
- Participant 4 – Senior Leader, international security organisation
- Participant 5 – Threat Intelligence Expert
- Participant 6 – CISO, regulated industry
- Participant 7 – Threat Intelligence Expert
- Participant 8 – Commercial Executive, international security organisation
- Participant 9 – Senior Director, UK based security consultancy

- Participant 10 – Information Security Officer, international organisation
- Participant 11 – CISO, international security organisation
- Participant 12 – CISO, international organisation, regulated industry.

Interview participation was voluntary, with no inducement, reward or recompense offered.

The duration of each interview was approximately 1 hour, with notes taken or full transcriptions produced from interview recordings (with participant consent). Interviews were both semi-structured and non-linear, topics covered were participant led as far as possible, remaining consistent with the realist theoretical approach.

Care was taken by the researcher not to express any personal opinions during the interviews, the use of theory and statistics was kept to the minimum necessary to instigate discussion, in order not to prime participants or influence their responses. Interview questions and discussion starters can be found within Appendix 3.

All interview data has been fully anonymised so that participants and the organisations by which they are employed cannot be identified.

3.2. Thematic Analysis Process

Analysis of the interview data follows the thematic analysis method, as described by Braun and Clarke (2008) following the six-phase process to conduct thematic analysis, exactly as they set out:

Table 2 - Phases of thematic analysis (Braun and Clarke, 2008)

Phase	Description of the process
1. Familiarising yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data to each potential theme.
4. Reviewing themes:	Checking if the themes work in relation to the coded extracts (level 1) and the entire data set (Level 2), generating a 'thematic map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

3.2.1. Analysis Approach

Interviews are discretely divided into two parts, the first part focusing on participants' views and experiences in relation to the study's core research questions; the second part, soliciting the opinions of participants regarding the feasibility of suggested strategies to improve reporting cultures.

Analysis of the data is consistent with the possible approaches set out by Braun and Clarke (2008). Analysis of the first part of the interviews follows a realist, semantic approach, where analysis is data-driven and meaning is derived directly from reality of the experiences shared by participants across each individual data point. The meaning of each data point is used to generate initial

codes, with the natural language used by participants mirrored as closely possible within these initial 'in vivo' codes. A second round of coding follows refining 'in vivo' codes[15] to produce summative or 'axio' codes[16].

The development of themes involves the analysis of axio codes, grouping codes based on their semantic or explicit meaning, to bring together related codes into themes (high-level groupings) and subthemes (more granular, specific issue groupings that directly cascade from the higher-level theme).

Analysis of data from the second part of the interviews, utilises a combination of approaches. Analysis of the potential strategies to improve reporting cultures offered by participants directly follow the same realist approach, consistent with the first part of the interviews. Where other potential improvement strategies subsequently proposed to and socialised with interview participants are explored, a contextualist approach is taken. This is necessary where theories are shared with participants, analysis is theory-driven, searching for latent or underlying themes through more interpretive analysis of the data, as described within Braun and Clarke's (2008) proposed methods for thematic analysis.

3.2.2. Prevalent Themes and Subthemes

From 176 candidate themes generated through grouping coded data points, further analysis resulted in the focused thematic analysis of 72 statistically prevalent themes and subthemes (see Table 3 below), determined using two following criteria in combination, either through single occurrence or through recurrence across the data corpus:

[15] In vivo codes place emphasis on spoken word

[16] Axio codes conceptualise data analysed

- **Data point frequency**
  Where the number of data points generated in relation to each potential theme or subtheme is greater than or equal to the mean (mean = 4.3, rounded down to 4).

- **Relative frequency of participants**
  In order that themes are not derived from any individual perspective, the relative frequency of participants in relation to data points generated per potential theme or subtheme must be greater than or equal to 2.

3.2.3. Relationships Between Themes and Key Themes

Relationships and points of intersection between the 72 prevalent themes identified were mapped within the thematic map included within Appendix 4 and further examined. Through this process of further inductive analysis, 12 key themes were established, connections between themes shown within the thematic map. Key themes act as compass points across the data corpus, connecting prevalent data themes at an abstract level and charting the thematic analysis narrative. Key and prevalent themes discussed throughout the analysis chapters are listed within Appendix 5 - Key and Prevalent Themes and Subthemes.

The 12 key themes are used to structure the discussion across findings chapters within this report (Chapters 4 - 7) and to answer the study's core research questions. Some key themes span multiple research questions and are discussed more than once across chapters.

Although consensus and prevalence are the primary factors that shape the thematic analysis, idiosyncratic responses, outliers and tensions within themes are not ignored; these are instead singled out and highlighted where they are deemed noteworthy departures from the mainstream, offering a unique perspective not otherwise seen or considered.

4. The Cybercrime Landscape

This chapter addresses two key themes. The changing cybercrime landscape and blurred lines surrounding cybercrime. The first captures changes observed by interview participants in relation to cybercrime trends and environmental conditions. The second key theme demonstrates changes relating to increasing obscurity in presentation of attacks and attribution of cybercrimes, with links with organised crime and potential state sponsored activities described by participants, which introduce complications in determining the true nature of cybercrime threats.

4.1. Changing Cybercrime Landscape

Interview participants overwhelmingly pronounced ransomware, phishing, malware, and Denial of Service (DOS) attacks as primary threat concerns in terms of volume of attacks. The descriptions of these threats were multifaceted, presented in the context of a changing cybercrime landscape; Ransomware-as-a-Service, DOS as a precursory attack enabler and specific purpose malware all featured in conversation in evolutionary terms:

> *"Ransomware-as-a-Service (RaaS) is becoming the new hit man. You don't have to have high end hacking skills (anymore), you can buy the skills, like you can hire a car, that you drive into the event".*
> (Participant 5)

Participants used language such as "turning-point", "new era" and "varied" to describe increasing and shifting threat vectors and attack techniques, which many participants related to increasing accessibility to cybercrime capabilities:

> *"There's been an advancement of capability. There are capabilities now that are freely available online that were once the purview of Nation states in terms of being able to deploy that capability, and so having the knowledge and the mechanisms to do so, that's now freely available, you can do that from any laptop with any internet connection".*
> (Participant 8)

With readily available advanced cyber-attack tools, the differentiation between the spectrum of threat actors from novices to advanced persistent threat actors has become increasingly more challenging:

> *"People are looking at different things for different reasons, there isn't really a pattern at the moment".*
> (Participant 9)

Changes in the cybercrime landscape owing to access to more and more advanced capabilities are of particular significance in the context of understanding the cyber-crime threats corporates face, these issues are further discussed within the blurred lines key theme (within Sections 4.2 and 7.3 of this report).

Participants also talked of the improving effectiveness of cyber-criminals, improved performance of malware payloads and monetisation of attacks, and the development and enhancement of malware:

> *"X[17] organized crime groups are also looking at tactics; they tend to buy the tools, strip the tools down, see how they work, see if they can actually make them better as well, and then launch attacks with them".*
> (Participant 2)

Selling access to systems and data was highlighted by some participants as a growing, almost stand-alone cybercrime service offering. Cybercriminals no longer need their own capabilities to carry out end-to-end attacks and are increasingly seen to outsource or delegate roles based on different capability or assignment requirements, with the ability to simply reach out to others to obtain access to systems or data as needed.

The relevance of such a cellular or devolved organisational structure also featured heavily in relation to discussions on the sophistication of cybercrime.

[17] Some participants made references to specific advanced persistent threat groups and Nation states, treatment of which fall outside the scope of this study.

Links to organised crime and potential involvement of nation states are themes also analysed in the treatment of the blurred lines key theme.

Concerns of ungoverned cryptocurrencies enabling cybercrime activities were mentioned by some participants, suggesting an entire (cybercrime) ecosystem enabled by cryptocurrencies, allowing criminal activities to generally remain obscure; from transactions made within online criminal marketplaces to underground ransomware payments. This theme showed divergent views amongst participants, defined by tensions in ideology. In the main, participants agreed that paying ransoms serves only to propagate ransomware attacks. Whilst some participants took the view that ransom payments should be outlawed, others were more focused on the business reasons for making ransom payments, putting forward the argument that legislation would fail to prevent businesses paying ransoms, if paying a ransom served to achieve a business objective. Instead, they suggested that authorities should be engaged to provide advice and support corporates in making such decisions:

> *"People will very quickly look to pay whatever ransom is being asked for, to try and avoid those third-party impacts and keep it internal".*
> (Participant 8)

Changes in the cybercrime landscape were additionally highlighted by several participants as having noticeably manifested over the period of the COVID 19 pandemic; potentially equating changes with time spent at home allowing people greater free time to upskill:

> *"When you look at cybercriminals, because everybody is at home now as well, so you'll see the noise, the noise everywhere, because people that didn't have time to upskill themselves have now honed it".*
> (Participant 7)

This was seen to relate to the cyber-criminals more recently seen improvements in operational effectiveness.

Some participants were conscious of criminals exploiting pandemic circumstances, highlighting the recruitment of potentially vulnerable individuals into cyber-crime:

> *"Desperate people will do desperate things".*
> (Participant 3)

Some participants additively highlighted exploitation of victims affected by the pandemic :

> *“We continue to see a rise in invoice re-direct, with increasing companies taking loans, romance fraud, with bereaved victims being targeted, with criminals joining up the dots from different sources”.*
> (Participant 3)

Others were more concerned with criminals more generally exploiting hyper-connectivity and increasing internet dependency [7]:

> *“The Internet is more and more critical than it's ever been. More and more organisations are shifting towards digital, especially in the wake of COVID. And anything that can be put online, is being put online and as much as can be automated from a people perspective is”.*
> (Participant 4)

The changing cybercrime landscape key theme depicts a context of shifting sands; with increased cybercrime motivation, wider accessibility to the non-technical criminal of advanced cyber-attack tools, skills and services and the quick adaption of cybercriminals to exploit opportunities accentuated by environmental conditions, suggesting the pervasive cybercrime problem is set only to continue to grow.

4.2. Blurred Lines

This second key theme builds on the changing cybercrime landscape, recognising its altering characteristics. The blurred lines key theme embodies ambiguity of presentation of some cyber-attacks and attribution challenges, in part due to the increasing accessibility of cyber-attack resources and

commercialised services. This topic led some participants to directly debate the spectrum of threat actors and levels of sophistication behind the attacks experienced by corporates, both most commonly and less frequently. Whilst a wide spectrum of potential threat actors has long been recognised and explained within cybercriminal taxonomies[18] , new complications were raised by participants as the lines between typified threat actors and their motivations blur.

Generally, participants' views agreed that the most frequent attacks experienced by corporates are low-level, opportunistic, unsophisticated attacks; however, many participants also referred to an, albeit lower, volume of attacks that *"push the envelope"* or present as being more sophisticated in nature.

Participants introduced three main challenges to determining the level of sophistication of attacks because of the changing landscape. Firstly, the potential involvement of some nation states in organised cybercrime activities:

> *"There's a degree of debate as to how involved some governments actually are, where online criminal forums are expanding exponentially".*
> *"The collusion of some governments with flat out criminal corporations, where the criminal corporations have an economic goal and the governments have a strategic nation state level goal and they just happen to overlap for certain scenarios…when X government needs to launch a deniable cyberattack, these channels will make themselves available and launch that deniable attack, that X government can, with a degree of plausibility, deny any involvement in".*
> (Participant 2)

Secondly, several participants discussed typical organisation structures seen within cybercrime operations and links to organised crime, in connection to this challenge:

[18] Such as Rogers (2006) and Seebruck (2015)

"So structurally, one of the reasons why organised crime is broken up into sort of specific task or specific mission groups, is essentially in order to isolate the various parts of the organisation and to make it difficult for law enforcement to understand who's in charge when there is a cellular type of structure and you know payments going back and forth between both organisations".

(Participant 10)

Thirdly, building on discussion relating to relative ease of access to cybercrime capabilities, some participants articulated the growing difficulties behind gaining a true understanding of the threats faced by corporates:

"The level of sophistication keeps getting pushed upwards, and that's mostly because of the commoditisation of cyberweapons".

(Participant 12)

Some participants were particularly concerned with issues of presentation of cyber-attacks:

"Anyone can look like an organised group; a ghost can look like a 1000 people. What could smell like organised crime, could just be very good marketing and tools. Organised activity could be one or two people that orchestrate with clever tech".

(Participant 5)

These three factors in combination, potential sponsorship of cybercrime groups by nation states, organised crime groups deliberately structuring operations to evade detection, co-opting or outsourcing cybercrime activities to other criminals, and novice criminals now obtaining access to sophisticated cyberattack resources opening opportunities previously beyond their reach were said to increase difficulty for corporates to really know what type of threat actors they are dealing with.

> *“If you leave the front door open, expect that the kid in the bedroom could cause a catastrophic impact, when the kid in the bedroom sells access to information or there is a technical hand off, or is it connected to X state? It becomes hard to tell, and you have to consider all possibilities”.* (Participant 5)

It is suggested that corporates defending against cyber-attacks need to be prepared for increasing ambiguity and associated potential impacts. Novice, non-technical cyber-criminals may present as more sophisticated threat actors. Conversely what presents as innocuous reconnaissance activity or a low-level phishing campaign could potentially be related to organised crime or even nation state sponsored activity.

5. Corporate Under-Reporting of Cybercrime

This chapter seeks to answer the research question: 'What is the extent of corporate under-reporting? Canvassing the views of participants on the scale and nature of cybercrime events affecting corporates to provide useful context upon which to further relate the experiences of participants on the extent of corporate under-reporting.

Two key themes provide an abstraction of prevalent themes arising from participants views on cyber-attack or breach statistics and on reporting; lack of data fidelity summarises the challenges raised by participants relating to collection of data and it's (un)reliability (also later discussed in Chapter 7). Within the second key theme, participants expressed a wide-held view that the majority of corporates under-report (cybercrime).

5.1. Lack of Data Fidelity

In the main, participants challenged official statistics relating to the percentage of organisations that reported having suffered an attack or breach in last 12 months. Some raised scope challenges with respect to survey coverage, suggesting that respondents were unlikely to be representative of all corporates:

> *"How representative does one feel that is genuinely of the corporate community? If you've had a breach of some description and it's been managed internally, maybe it's been reported in the right way, but it's not in the public domain, are you actually going to complete that survey? When you've successfully managed to maintain your brand and reputation as an organisation?"*
> (Participant 1)

Difficulty with definitions due to the absence of commonly applied definitions of cybercrime and distinctions between impactful and non-impactful unsuccessful attacks were also thought to affect classification of what constitutes a reportable attack or breach:

"It depends on what you define as a breach or attack. But that's why it's such a difficult subject to approach and it's such a difficult subject to get accurate numbers on, because what is one man's cyberattack, is the next man's malicious reconnaissance".

(Participant 2)

The overwhelming majority of participants stated in some form that no corporate remains untouched by cyber-attacks, captured within the prevalent theme 100%[19] of corporates suffer some form of breach:

"I would completely challenge the statistics by the fact that 100% of businesses that have an online presence have received some sort of malicious activity over the last 12 months. It's just the prevalence of it, you're not going to miss it."

(Participant 2)

"So, if you have malware now on a corporate device, you've been breached. Now, that breach might have been contained very quickly, very efficiently within that laptop and nothing has moved on, but I think 100% of businesses honestly are breached".

(Participant 12)

Other participants also raised issue with data integrity, and particularly the validity of commercial statistics:

"I think there may be some fake news out there where cyber is inundated with marketing and sales. Commercial statistics - 'lies, damn lies', the fact that there's order of magnitudes of difference between what a commercial organisation is saying versus government, it says to me that there's an issue"[20].

(Participant 4)

[19] (100% corporates with an internet presence)

There was general agreement that neither official nor commercial breach statistics can be relied upon. Many participants went on to make the make an association with external under-reporting, the impacts of which are also discussed within Chapter 7.

5.2. Majority of Corporates Under-Report

Reporting statistics from the UK Government's Department for Digital, Culture, Media, and Sport's (2020) Cyber Security Breaches Survey were shared with participants to solicit opinions and personal experiences. The survey suggests a significant gap between internal and external reporting with less than 10% of UK businesses reporting cybercrimes to law enforcement, the survey found :

- 91% of businesses and 59% charities reported their most disruptive breach to senior management / directors / trustees.
- Only 27% of businesses and 38% charities reported their most disruptive breach outside their organisation.
- Only 9% of most disruptive breaches were reported to the police and 6% to Action Fraud (Department for Digital, Culture, Media, and Sport, 2020).

Almost unanimously unsurprised by the statistics, participants also agreed that external under-reporting is in the majority, and reporting statistics presented are typically more reflective than they are reliable:

> "I think that the statistics are a reflection, rather than accurate".
> (Participant 5)

> *"That actually makes sense to me, I'm not surprised at all by the gap in external reporting. I can't say with certainty whether or not the numbers themselves sound right, but it does absolutely resonate".*
> (Participant 4)

> *"I am 100% confident that the vast majority of businesses are not reporting".*

(Participant 2)

The common lack of surprise in the prevalence of external under-reporting strongly characterises an underlying prevalent theme of avoidance and negativity towards external reporting, with many participants continuing to describe corporate fear of external reporting consequences, discussed within Chapter 6. One participant was however surprised by the significant gap in internal and external reporting numbers, describing the *"sub 10%"* of corporates reporting to law enforcement as:

"…quite worrying…"

(Participant 8).

A small number of participants made direct connections between the majority of corporates under-reporting (and the associated lack of data fidelity), with the absence of a legal requirement to report cybercrimes in the UK and other jurisdictions [21] , suggesting that such legislative requirements would be beneficial and should be adopted more widely:

"UK corporates are under no obligation to report the cyber incident in a timely manner".

(Participant 10)

A few participants commented on US Securities and Exchange Commission (SEC) material cyber incident disclosure requirements and on the EU General Data Protection Regulation, suggesting that these requirements could go further than their current application:

"The problem with the SEC is that this is a 20% solution, because when you look at modern economies like the UK, the EU and the United States, I'm going to say 70 to 80% roughly, are small medium enterprises that

21 Beyond existing regulatory reporting provisions, such as those made within the European Union General Data Protection Regulation (GDPR), UK Data Protection Act (DPA) 2018, or in the US, the Securities and Exchange Commission (SEC) material security incident disclosure requirements for publicly listed corporations.

are powering those economies and the vast majority of them have some sort of digital footprint. So, if the mandatory requirement under the SEC is for publicly listed companies, we are getting basically 20% mandatory reporting requirements on the whole of the economy".
(Participant 10)

"I think there's some reform needed on the regulation which says, ideally, there's some type of motivation for the stick. Everybody freaked out about GDPR because they were worried they were going to lose money. Very few people talked about why GDPR had to exist in the first place and the history of how information can be abused".
(Participant 4)

In contrast, other participants were more critical of the EU GDPR and of taking a mandatory legislative approach to external reporting in general, with frequent use of language and references to 'penalties', 'fines' and 'fear', cross cutting a number of prevalent themes:

"I'm not sure that legal obligations have worked particularly well, at the moment, because of the fear factor".
(Participant 11)

Questions were raised over the effectiveness of punitive regulations:

"Does regulation force organisations to report? Or does that provide a range of penalties, be they financial or otherwise, if you are detected; does that address under-reporting? By bringing in regulation and threatening does that address under-reporting? Or does that not just penalise the reporters or those that are caught out?
(Participant 1)

The enforcement approach of some of the EU data protection regulators was condemned by some participants:

> *“The way the regulatory bodies pursue people after a breach, all that does is rub salt into the wounds and it means that the organisation that has a had a breach, they are in the press again and again, it's repeated”.* (Participant 11)

Participant responses indicate the extent of corporate under-reporting of cybercrime is predominant and far more widespread than official statistics suggest. Divisions of opinion were, however, seen to exist across the participant group regarding the necessity of legal or regulatory provisions to mandate and therefore force external reporting, in opposition to condemnation of punitive regulatory approaches taken, threatening weighty penalties. The latter approach was seen by some participants to inhibit rather than encourage reporting, with punitive regulation cited as the most significant barrier to external reporting. These split views were very similar in nature to participants’ polarised opinions regarding underground ransom payments, previously seen in Chapter 4; with resistance to control stemming from the central viewpoint of the business, describing mandatory disclosure provisions as running counter to business objectives. These and other potential barriers to reporting are discussed further within Chapter 6 below.

6. Barriers to Reporting

Key themes presented within this chapter expose participants' attitudes towards and potential barriers to reporting, to answer the core research question 'What reasons are there for corporate under-reporting?'

The key themes show an axis of three primary reporting positions; an inability to report; an intrinsic unwillingness to report; or an event-based position involving calculated risk-based reporting decisions. Three additional key themes address corporate disincentives to report externally; corporate fear of external reporting consequences, no benefit to report, and ineffective law enforcement. Each are discussed as additive barriers to reporting.

6.1. Inability to Report

Inability to report, the first reporting position identified, was commonly recognised amongst participants. Various corporates are at some point unaware of the cyber-attacks they have experienced:

> *"Either you're a business that knows you've had a breach or been hacked, or you're a business that isn't aware you've been breached. You're only one of the two".*
> (Participant 1)

Some participants gave specific examples of corporates who had failed to detect cyber-attacks. In the following example, a small corporate was assisted in detection and response by a more security mature corporate:

> *"We found, when we were looking into some traffic hitting us, that it was from a small business in another county, and we spoke to them, it was blatantly clear to us that they'd been compromised, and we helped them tidy it up, though they wouldn't have a clue, right? But there's small organisations like that all over the place".*
> (Participant 6)

The inability of many corporates to detect and report breaches was also discussed in relation to the interpretation the UK Government Department for Digital, Culture, Media, and Sport Cyber Security Breaches Survey 2020's statistics on reporting (Department for Digital, Culture, Media, and Sport, 2020), suggesting that these statistics may be more reflective of the percentage number of organisations able (or unable) to detect breaches:

> *"46% [of* businesses reporting in a survey having had a cyber breach or attack] *is not a bad percentage, if you say that nearly 50% can say that they've actually identified that they've had a breach, and that's the difference, because a lot of organisations aren't even aware that there's something there".*
>
> (Participant 7)

A few participants suggested that corporate ability to detect attacks or breaches is often linked to size and/or maturity of the corporation:

> *"It's only really organisations that are either publicly traded or regulated, or have got a big consumer base, or internet presence, where they've got to start taking it seriously (that can detect) and even then; that's the spectrum".*
>
> (Participant 6)

Even for larger, more mature corporations however, challenges of effective monitoring across the entire corporate technology footprint were identified, with too much to monitor. The suggestion that detection and awareness of attacks, often presents a non-trivial challenge to large corporates and remains an issue to some degree:

> *"For anyone to know the end to end, to fully monitor all the all endpoints, everything, is a task that I think is utopia".*
>
> (Participant 7)

Prior to discussing the two remaining reporting position related themes, it is essential to address an underlying key theme, corporate fear of external reporting consequences, that underpins both remaining reporting positions, unwillingness to report, and calculated risk-based reporting decisions.

6.2. Corporates Fear of External Reporting Consequences

Fearful attitudes towards external reporting of cybercrime came to the fore across the data corpus, through frequent use of language describing a fearful reporting atmosphere:

> *"…the perils of reporting".*
> (Participant 1)

> *"I think a lot of it stems from fear and uncertainty".*
> (Participant 6)

> *"Corporates are scared just now to report".*
> (Participant 2)

Corporate fear of external reporting was seen to stem from the consequences of reporting, accentuating the consequences of being the corporate victim of a cybercrime itself.

6.2.1. Consequences of External Reporting

In relation to the key theme above, consequences of reporting (described as feared by corporates) are grouped into six themes described below.

The first theme describing the consequences of under reporting is negative publicity. This centres on participants' deep seated concerns describing media over exposure of cyber-attacks and breaches, and the percolation of negative publicity:

> *"Bad publicity is probably the worst, because it filters down everywhere, to customers and recruitment, everywhere".*
> (Participant 11)

Within this theme corporate misrepresentation also featured as a subtheme:

“Businesses need to keep some level of confidentiality. A snapshot by itself, doesn't necessarily represent the bigger trends of what's happening within the business. If you have a big breach, it doesn't necessarily mean that your information security programme is not good.”
(Participant 12)

Another subtheme that emerged from negative publicity brought into focus a societal blame culture, with corporates developing effective media strategies to gain public acceptance as a victim and minimise corporate ‘blame’ and impact:

“I think there is a very focused blame culture within society in general that looks very negatively on cyber breaches, regardless of how well they managed”.
(Participant 9)

Careful management of media and messaging often produces unintended consequences, described by some as impeding incident management in the process:

“The idea of suffering an impactful data breach is to downplay it and minimise, which is of course, what you want to do, and to feed the media of various small pieces of the larger problem to minimise and desensitise and hope that the next spectacular data breach takes the public eye off of the organisation. This is a huge problem because the organisation is plunged into a crisis situation, where communications of clear and relevant information are being actively suppressed by the marketing team, the PR team, the even the investigators are limited in their scope of the investigation”.
(Participant 10)

The second theme relating to consequences of under reporting is impact to brand and reputation. Here, participants were principally concerned with the time and investment it takes to build a brand and how quickly its reputation can be knocked down, mainly by media coverage, sometimes with irreparable consequences:

“That stain doesn't go away sometimes”.
(Participant 11)

A third theme concerning consequences of reporting relates to stock or profit. Share price or bottom line is identified as a concern resultant only from reporting, not as a direct cost of the cybercrime itself.

“Certain corporations are going to have the impact contained very closely. The people who are responsible for cyber defence, senior management and Boards with the motivation is supposed to resolve any issues quickly before it becomes public and therefore protect the shareholders and the share price”.
(Participant 8)

The fourth theme concerning consequences of reporting relates to liabilities and fines. Many participants described a legal pre-occupation with both sizeable fines that could be levied by regulators, creating an image of an unwanted penalties culture:

“Right now, what the ICO is doing, is just waiting for the accidental train to happen and then weighing in with large and dissuasive fines”.
(Participant 10)

“There needs to be a different culture, different to penalties that affect brand reputation and organisational fines”.
(Participant 1)

Concerns were additionally expressed by a smaller number of participants relating to exposure of corporate weakness and potential tortious liability.

A clear relationship was seen to exist between restraint to report and the potential for fines to be incurred (this theme was also mirrored in participant’s suggestions of potential strategies to improve reporting cultures, detailed within Chapter 8).

The fifth reporting consequence theme considered operational costs. Although participants suggested that reporting externally may result in increases to the financial costs of incident response, this was not considered to be the most significant of operational consequences. Some participants called out the *"pain"* of managing external reporting, or of being:

> *"put through the wringer",*
>
> (Participant 5)

describing more of a human impact on responders and management overhead involved in crisis response.

The sixth and final consequence of external reporting identified by participants was fear of loss of corporate control of the incident. Reporting to authorities and bringing law enforcement into an investigation was described by a few participants as a last resort, with corporates *"scared"* of law enforcement agencies taking control of the investigation*, "almost coming to blows"* over handing over corporate data or apprehension over loss of control of the corporate operating environment:

> *"The game with authorities can sometimes be a bit problematic, because when you bring them in, of course, if there is something that is a clear blame crime, where they have to be involved because there is some sort of impact that is beyond just the realms of your business domain …If you bring the authorities in, they start managing the incident for you, to some extent, they take some of the control, depending on the level of ambiguity or clarity and what's at stake in that moment in time, and you start losing control of your own incident".*
>
> (Participant 12)

These external reporting consequences are considerations that can be seen to affect both corporate willingness (or unwillingness) to report a well as risk calculation-based reporting strategies, explored in the two remaining reporting positions.

6.3. Unwillingness to Report

Avoidance and negativity towards reporting was a theme signposted at various times through interview conversations. In many instances reporting externally was framed by participants as running counter to the mission of most businesses:

> *"The main reasons behind not disclosing are all business centric and business oriented".*
> (Participant 12)

External reporting was seen by many participants a process that requires a Board level decision. Discussing internal reporting to Boards, a few participants questioned whether Boards always want to know about incidents (officially or unofficially) :

> *"When you report you get one of two responses; either 'What do you need and how can we help'? or 'surprised, this has come up, or this came up before and was dealt with'… plausible deniability as soon as you raise something they don't want to hear, and make you question yourself".*
> (Participant 3)

Even when faced with regulatory requirements to report however, some participants indicated that some corporates would remain unwilling to report:

> *"For most corporates, sweeping it under the rug, if at all plausible, is more preferable than trying to disclose it, with the one exception of highly regulated organisations, where the less ethical ones will try to find a way around reporting if they can".*
> (Participant 4)

> *"Some don't report because they just don't want to do it".*
> (Participant 11)

This default unwillingness was described by participants as very deliberate, as opposed to more nuanced reporting considerations seen within the following section.

6.4. Calculated, Risk Based Reporting Decisions

Reporting externally, even where participants indicted corporates taking a compliant approach, was described as a matter for deliberation:

> *"There are ramifications for not reporting, but there are also ramifications for reporting".*
> (Participant 5)

> *"That middle pause has been introduced, maybe a sanity check, but maybe that's a poor word, but a point where people stop and think 'Hold on, what are the consequences? Either way, that has now been inserted into that decision making process".*
> (Participant 11)

Many participants talked openly about corporates making calculated risk-based external reporting decisions on when and whether appropriate to report:

> *"If it's significant enough that you need to externally report that, you likely will. But the risk of reporting an incident, the risk of the damage to brand and reputation, does a corporate organisation not need to weigh that up?"*
> (Participant 1)

Consideration of impact to the organisation was predominantly seen as the main factor driving internal reporting:

> *"When it's disruptive, now you know you have a problem - when business stops, the executives want to know why".*
> (Participant 1)

Whereas external reporting considerations were generally described as driven by regulatory reporting requirements and materiality of breaches, with explicit reference to the European Union General Data Protection Regulation (GDPR):

> *"If personal data is involved and it needs to be reported, via the regulatory agencies, under the GDPR and the mirror statute in the UK. The problem is that to meet the reporting statute, there has to be*

demonstratable harm from the data breach [to the individual], and so, that determination is made usually by corporate counsel or data protection".

(Participant 10)

The decision to report externally was widely, but not universally, positioned as a Board level decision, some participants described some Board members being more comfortable than others in reporting to agencies rather than taking internal containment decisions:

"What security leaders many times need to think about themselves is, when the is right time to bring the authorities in? It's not always so clear cut".

(Participant 12)

A number of participants equated the level of comfort or discomfort in making external reporting decisions with the level of cyber experience of Board members:

"Their [Board members] lack of cyber understanding makes it more difficult, their instant reaction is always, do not report this unless we absolutely have no other choice".

(Participant 2)

"It's a risk / benefit thing with people, there's fear and uncertainty and in their minds, if they don't have those kind of advisors, those people at board level that can steer it, they're probably just thinking I can see loads of downsides, can't see any upsides; there's no law that tells me I have to do this, so why would I?'"

(Participant 6)

Some participants acknowledged that even when faced with an absolute requirement to report to a regulator, some corporates may still consider the risks of non-reporting:

“If you've got lack of reporting to a regulator, where there’s a legal requirement, you are on the road to nowhere, aren't you? ...if you're found out, that's the thing, isn't it? ‘If’ you’re found out”.

(Participant 7)

Participants were consistent in identifying a set of circumstances under which corporates might be more inclined to report externally. generally, where control of media messaging or good public relations are seen to be important, if a breach is in the public domain, it has been leaked or posted on social media, or where the impact is likely to be reputational:

“You might consider reporting to law enforcement for things that are material because you are reporting them to the regulator and you are making a press statement about it. Everything else goes underneath the radar. It's massively time-consuming fuzz and you know nothing is going to happen anyway”.

(Participant 6)

Most participants discussed the role of cyber-insurance as a contributing factor in the reporting decision calculation:

“From a financial benefit standpoint, which is if you've been attacked, then you've suffered a loss, then you might have certain avenues where you can recover the costs through, for example insurance”.

(Participant 12)

Predominantly, the cyber-insurance market was described by participants as under-developed or immature, and seen to introduce variance to the corporate reporting position, described as *“muddying the waters*” both in terms of policy coverage and the level of ransoms demanded by cybercriminals:

“I think [the cyber-insurance market] hasn't developed enough, not least because people don't understand the threat particularly well, because people aren't always reporting on incidents where the threat is realised,

and therefore you have this problem where some insurance policies will pay out, some won't, and it creates that sort of mismatch on what is 10 GB of data worth, in the ransomware world?"
(Participant 8)

One participant held a somewhat outlying view, describing a corporate over-reliance on cyber-insurance, implying that a greater and more consistent level of cyber-insurance maturity has been reached:

"Organisations are using cyber insurance mechanisms to pay the various fines and ransoms for which is essentially an information security failure of the organisation. This has operationalised the expense of a data breach, to the point where some companies are far more comfortable in paying a cyber insurance premium than they are in actually taking effective steps to meet the requirements of something like a framework, like Cyber Essentials".
(Participant 10)

The calculated risk-based reporting decisions key theme defines a state that is neither determined by ability to report, nor by default corporate unwillingness; but is largely driven by both internal, business centric factors and external issues including public-opinion and insurance.

However, unlike the inability to report, both unwillingness and calculated, risk-based reporting positions both demonstrate a reluctance to report underpinned by corporate fear of external reporting, only the latter has a somewhat less predetermined outcome.

6.5. Ineffective Law Enforcement

This key theme draws together a collection of themes relating to reporting arrangements and law enforcement that together present significant disincentives and contribute to corporate reluctance to report externally.

As seen previously, some participants and by inference corporates feel more comfortable than others reporting cybercrimes to authorities, but even the most committed of reporters described poorly perceived, inadequate reporting arrangements, with only one participant (EU based) describing reporting arrangements as *"pretty easy"*:

> *"If you look at the UK, Action Fraud has a reputation you'd want to wipe off your shoe, in their inactivity, and it's not their fault".*
> (Participant 6)

> *"They (UK authorities) don't really make it easy to report a cybercrime".*
> (Participant 11)

Most UK based participants described unresponsive, unwieldy and over-bureaucratic reporting processes, inappropriately skilled and understaffed agencies with inadequate resources:

> *"The people I spoke to didn't have a clue what I was talking about, it was just beyond them technically, what was going on. They didn't have time to follow it up. They barely had time to take notes of what was going on and we never heard from them again".*
> (Participant 11)

> *"We reported something before on an intelligence basis and then a few years later, they're 'Oh, we've got this other thing that's got a lead and it kind of links into this thing that you reported'. But that's the best-case scenario, the police don't have resource to investigate anything that's minor, and to be fair, they don't have the expertise either".*
> (Participant 6)

At the same time as heralding a need for improved data fidelity for better planning and response, that participants agreed is primarily achieved through reporting, some articulated a sense of aggrievement at 'wasting time' reporting, only for their reported data to end up in a data lake or as government statistics:

“Reporting to (UK) Action Fraud is an absolute drain on resources and for no benefit, other than making law enforcement feel good about themselves that they've got some extra data, they don't have any resources to deal with it. It takes us ages to report something, absolutely, ages”.

(Participant 6)

“Is [reporting data] it going into a data void? Yes, it is. (pauses) Yes, it is. Does it get lost? Yes, it does”.

(Participant 7)

There were differences in the level of expectation of different participants in relation to law enforcement response capabilities, most participants described a total absence of law enforcement incident response capabilities:

“You don't get police cars turn up, with laptops to save the day”.

(Participant 5)

A number of participants felt a gap still exists in corporate awareness of reporting mechanisms, despite steadily improving outreach activities of central agencies such as the UK’s National Cyber Security Centre (NCSC):

“There are still organisations (in the UK) who haven't heard of the NCSC, who haven't heard of Action Fraud through to the police”.

(Participant 8)

Participants most clearly articulated a lack in sense of purpose associated with reporting to central or law enforcement agencies, with no feedback, and low visibility of successful investigation and/or prosecution results:

“Attackers generally, unless they get to a level of noise, i.e., that they've done significant damage, that gets the attention of, shall we say, the government; very little will be arrayed against those cybercriminals that is effective and dissuasive”.

(Participant 10)

Failure to bring criminals to justice due to a combination of under resourcing and geographic limitations or constraints of law enforcement agencies were also highlighted subthemes identified by participants as contributing factors to the generally held view of law enforcement being inadequate and ineffective.

6.6. No Corporate Benefit to Report

If *"nothing is going to happen anyway",* disenfranchised corporates will struggle to find compelling reasons to report:

> *"What is the point of an external reporting if it's actually just going to have a negative impact, in that case, you don't have any positive impact on the business, or on the group have perpetrated the crime?"*
> (Participant 8)

Invariably, participants felt that there was no point or incentives to report,

> *'What really contributes to under-reporting is mostly business incentives...a business is trying to run as a business".*
> (Participant 12)

Participants for the most part, spoke with an overriding sense of futility:

> *"The drivers to keep it quiet are, in this strange regulated, GDPR world, are bigger, partly because of the regulations, they are bigger than the any benefit of actually reporting it, well, there isn't the benefit of reporting it".*
> (Participant 11)

In various forms, participants described a vicious circle of disincentives:

> *"Because of the lack of visibility of government activity and law enforcement activity against the cybercriminal, the organisations that have been victimized are probably sitting there going: 'Well, why bother reporting it as nothing will come of it, right?' So, you have demoralisation and then you have a nativity of the size of the problem".*
> (Participant 10)

Reporting is invariably seen amongst senior information security professionals as a vital tool to improve data fidelity needed to form better cyber-crime response strategies. Corporates are however disincentivised to report due to ineffective reporting mechanisms. Reporting yields no clear benefits or outcomes, and in many cases, is perceived as a threat to corporate objectives that may result in regulatory actions being taken.

7. Under-Reporting Consequences

Having found widespread corporate under-reporting of cybercrime, this chapter seeks to gain a deeper understanding of corporate views on the consequences of under-reporting.

Three key themes are contrived from the analysis of findings relating to the consequences of under-reporting. The first addresses difficulty to deter cybercriminals. The second, a reduced ability to effectively defend against cybercrime, analysis in this area reflects on the lack of data fidelity key theme previously discussed in chapters 5 and 6. The third revisits the blurred lines key theme previously discussed within Chapter 4, concentrating on links between cybercrime and organised crime and the associated societal consequences of under-reporting.

7.1. Difficult to Deter Cybercriminals

Where law enforcement processes start with reporting, from a deterrence perspective, many participants described the message given to cybercriminals as an open invitation to keep offending. It is a favourable risk / benefit equation for cyber-criminals , safe in the knowledge that so few corporates report cybercrimes. Combined with inadequate law enforcement resources, the chances of being caught are remote, resulting in further cybercrime proliferation:

> *"It's hard to provide a deterrent to people that are thinking about doing it, because they know that, actually, it's easy, the likelihood of an attribution and prosecution is so low, it's a pyramid".*
> (Participant 6)

Some participants were concerned at the level of tolerance or normalisation of under-reporting, since without reporting cybercrime, it is difficult to deter, finding the low number of corporates reporting externally worrying:

> *"If there are no consequences to under-reporting (for corporates), then it becomes the norm…And if we're saying it's [non-reporting] acceptable*

and allowing that - is it acceptable that a cybercrime has been committed? It's a crime because it's illegal, unauthorised access to your people, systems, and processes. If you are saying I'm not reporting it to anywhere, you're saying that's OK, what you're doing is saying, come on, we don't care, attack us again. Do what you like…It's called corporate lack of responsibility".

(Participant 7)

The question of corporate social responsibility surfaced briefly, this is however a topic of interest when considering the ranging sophistication of cybercrimes that now affect corporates, some with links to organised crime, this is further discussed within Section 7.3.

7.2. Reduces Ability to Effectively Defend

This section shows a circular relationship identified by participants between a lack of information sharing, resulting in a lack of data fidelity and the reduced ability to defend against cybercrime that this causes.

From a defence perspective, the impact of under-reporting was said by many participants to result in failure to share and disseminate useful attack information A lack of reporting generates 'negative awareness' where corporates are kept in the dark and starved of better information sharing that could assist them in their ability to effectively defend against cybercrimes. This was described as enabling cyber criminals to "*hold the initiative for longer":*

"There is a danger that the people that don't share information potentially could lead to future breaches, of similar threat vectors, that could be prevented ultimately".

(Participant 9)

Fundamental concerns were raised by some participants relating to corporate prohibition of information sharing:

"So, we've actually built a system, I think that actively suppresses the sharing of information, that is somewhat prejudice to involving law

enforcement or regulatory authority, if it can be avoided, in order to essentially try to move the narrative of that company's security failing along as quickly as possible…Law firms are using client confidentiality to suppress the information sharing that folks have widely lauded as basically being one of the solutions to the cybercrime problem; which is information sharing amongst peer and industry vertical organisations. But that's actually being actively suppressed and there is a calculation out there right now".

(Participant 10)

Justification for active suppression is intended to protect corporates from the negative consequences of external reporting or over exposure (discussed with Section 6.2.1 above), rather than allowing information to be used to defend against cybercrime more effectively. As a result, lack of awareness is raised as a concern. Corporate victims are described as potentially opening themselves up unnecessarily to further attacks, through failure to effectively learn from an incident, relying only on in-house knowledge, rather than pooling current knowledge and drawing on the skills and expertise of external agencies:

"I think at that point you're isolating yourselves from various industry bodies that share information that is helpful and useful. By trying to draw less attention to your position, equally draws less knowledge and information that you can consume from other parties".

(Participant 9)

From a risk management perspective, a few participants questioned how many attacks of a similar nature corporates would be able to withstand, with a rising tide of attack sophistication:

"Corporates will manage the risk of being struck by an attack once, but won't potentially think about it for the second, third or fourth time".

(Participant 9)

The majority of participants considered under-reporting to have some effect on risk management, although participants were generally unclear on the precise extent to which this is an influence. Several participants, however, asserted that

under-reporting certainly makes quantifying cybercrime risk more challenging, an additive consequence of under-reporting linked to the lack of data fidelity.

As well as the challenges of cybercrime risk quantification within corporations, from governmental policy making to law enforcement resourcing, participants described the challenges that lack of visibility presents to deliver efficacious cybercrime response strategies:

> *"If you don't report crime, the police of course have no idea that crime is occurring and therefore the allocation of resources to combat that crime is proportionately decreased. At the policy level of government, if government doesn't have accurate measurements about the type of crime that's occurring, the hotbeds and or regions that are victimizing the citizens, the lack of capacity for anti-fraud initiatives, all of these things combined into skewing the picture of the policy makers of the government and therefore degrading the resources available to combat a growing threat".*
>
> (Participant 10)

7.3. Blurred Lines (Links to Organised Crime)

Participants opinions on links between cybercrime and organised crime were mixed, the prevailing view that, within a certain portion of cybercrime activity, links to organised crime exist :

> *"Linkage definitely does exist between cybercrime and organised crime, with proceeds of crime being used to fund organised crime and terrorist activities, there is always a chain to follow. What happens to it the money? Where does it go? How do you hide it? Legitimate businesses like empty restaurants can make it legitimate, pay tax, so what? It wasn't your money to start with. But that's the thin end of the wedge, the money is being used to fund organised crime".*
>
> (Participant 3)

Some participants were particularly concerned with money laundering being used to conceal the proceeds of cyber-crimes, said to fund organised crime:

“In cyber criminality, what's been gained, is actually funding dreadful crimes, dreadful, dreadful crimes, and it is human trafficking, it is child sexual exploitation, it is modern day slavery, it is drugs, it is funding everything”.

(Participant 7)

A small number of participants did not know if links exist between the cybercrimes they experience and organised crime; there was however acknowledgement of the collusion and professional structures operationalising more sophisticated attacks:

“I don't know how easy it is for any organisation to differentiate between those two. I think for the more sophisticated attacks, that becomes even harder because that approach becomes a layered attack that may not be focused at single points in the entities environment, where you don't have full visibility. The more sophisticated attacks will typically have elements of collusion”.

(Participant 9)

It was noted by a few participants that establishing the nature or categorising some of the attacks now seen by corporates could be difficult due to the blurring of lines due to the increasing collusion of threat actors, and their varied roles in attacks:

“But how you then categorise them, I'm not too sure how you’d separate what is organised crime and what was described as crime that is organised, it is very difficult because there is a huge grey zone in the middle; you have like an individual, then moving up to a group, then moving up to an organised group”.

Corporates’ understanding and recognition of the consequences of under-reporting of cyber-crime is vital to combatting the proliferating problem of cybercrime, particularly as lines between low level opportunistic cybercrimes and organised crime become increasingly blurred.

8. Potential Strategies to Improve Reporting Cultures

The need for change and improvement of corporate reporting cultures is evident, in both the extent of under-reporting and the reluctant corporate reporting positions described by participants. Within this chapter, potential strategies to improve reporting cultures are explored. First, the strategies offered by interview participants directly are discussed. Other potential improvement strategies subsequently proposed to and socialised with interview participants are further explored.

8.1. Participant Suggested Strategies

8.1.1. Anonymous Information Sharing

Most participants proposed the need for improved centralised, anonymised information sharing. These participants suggested sharing attack methods, and other relevant incident learning, recognising the need for a more proactive ability to manage and defend against cybercrimes:

> *"If you reported cybercrime more, if it went into a central pot and if the information related to these attacks was made available on it quicker, the ability of criminals to professionalise their industry and for less tech savvy criminals to buy this and utilise this software would be massively interdicted".*
>
> (Participant 2)

Consistent with the widespread reluctance to report and fear of over exposure, proposal for sharing such information were predicated on guaranteed anonymity:

> *"So, potentially some sort of a standard that is across the board, anonymising, a way where you can share reports without it being attributed to an organisation can change the game".*
>
> (Participant 6)

Despite many not being in favour of punitive regulations, participants were pragmatic about the role of any potential central reporting agency, demanding a better structure and protection to share information easily and anonymously, potentially under Chatham House rules[22]:

> *"A body where we could report events to within certain bounds, where we're not, I don't want to say, we're not then going to get prosecuted,, no guarantees there, but, something where we could actually say 'Do you know what, we had this issue and some bad thing's happened', where we could contribute that in an environment where we weren't then going to be a) immediately fined, b) pilloried in the press etc".*
> (Participant 11)

Whilst the UK National Cyber Security Centre (NCSC) has established itself to fulfil such a central agency brief, through its Cyber Security Information Sharing Partnership (CISP) and other initiatives such as its Industry 100 initiative[23], improvement in outreach, accessibility and response are needed according to participants' majority calls to fill such a void.

8.1.2. Industry Led Threat Intelligence Sharing

In a similar vein to the calls for anonymised information sharing, several participants discussed the successes of industry specific intelligence sharing groups, such as US Information Sharing and Analysis Center (ISAC) groups, and UK industry specific intelligence sharing groups, including those coordinated by the UK NCSC, with participants advocating support for more private / trusted intelligence sharing:

---

[22] Chatham House Rule helps problems to be shared confidentially, where information disclosed may be used without divulging identity

[23] The UK's NCSC Industry 100 initiative draws on security skills of private industry, with 100 security professionals seconded to work in partnership with the NCSC.

"[Corporates] need to understand intelligence and utilise intelligence better".

(Participant 2)

Some limitations of industry specific groups were at the same time discussed:

"At the outset you're not going to achieve anything significant for at least 12 months, right? Because the first 12 months is all about building trust with each other. And then, if you manage to build trust with each other and people don't change jobs halfway through, then you can really get that amazing threat intel sharing".

(Participant 6)

However:

"They are still little silos of painfully learned intelligence which could be shared much more efficiently, if there was a way of doing it".

(Participant 11)

In parallel, a smaller number of participants gave strong views on the tensions created through commercialisation of threat intelligence:

"We've kind of monetised intelligence sharing. There are organisations out there that do provide for a significant membership fee, Intelligence sharing amongst vertical markets. Perhaps a new model of where those are turned into, not for profit trusts, and that there's a governance framework that goes all the way up to and including the various intelligence and law enforcement agencies".

(Participant 10)

The convergent points of theme being that for threat intelligence to be used to greater effect, not-for-profit, centralised threat intelligence gathering and controlled dissemination are needed.

8.1.3. Better Reporting Mechanisms

The overwhelming majority of participants were critical of existing reporting mechanisms, whilst some called for existing mechanisms to be abolished

entirely and a greenfield approach to be taken, others were keen to adapt and build on existing mechanisms, whilst most participants were in agreement that better reporting mechanisms are needed:

> *"I think it would be a game changer if someone got rid of Action Fraud and came up with something that would actually be an easier way for businesses to report stuff to the police…However, if they gave me an API that I could automatically fire stuff at, and I didn't have to use the time of my team, then, then I probably would hook it up".*
> (Participant 6)

Building better law enforcement relationships, offering better real time incident support and better agency outreach were also popular suggestions among participants.

As interview data suggests, whilst improving reporting mechanisms is important, as cumbersome, slow, and unresponsive, the mechanisms themselves are dissuading corporates to engage in the reporting process; improving such arrangements however, will only encourage greater reporting amongst corporates who are already invested in the process, the 10%, according to the UK Government Department for Digital, Culture, Media, and Sport Cyber Security Breaches Survey (Department for Digital, Culture, Media, and Sport, 2020), and not to wider reluctant reporters and thereby failing to address the cause.

8.1.4. Less Punitive Regulations (that Incentivise)

Liability and fines, a prevalent subtheme within discussions on the consequences of external reporting (see Section 6.2.1), saw many participants singling out the EU GDPR, with its punitive approach towards corporates threatening large fines, as a major barrier to report externally. Expectedly therefore, a popular improvement strategy suggested by many participants would be to reappraise the approach taken to regulation, calling for less punitive regulations that incentivise corporates to report and better protect themselves and others:

“Revising regulations so that they're less avoidable, and they're not punitive and they help solve the problem”.

(Participant 4)

Participants were divided, with few participants in favour of more hard-line legislation or regulation concerning mandatory reporting of cybercrimes:

“When the Computer Misuse Act gets updated, make it to oblige certain things to happen. It depends how far policy makers and politicians want to take it, but it could be anything from ‘It's criminal offense not to tell the Board or Trustees’ to ‘It's a criminal offense not to let the police know, even if it's on an intelligence basis”.

(Participant 6)

Others emphasised the need to provide corporates with incentives to report, even if this needed to be achieved through regulation by introducing rewards for meeting foundational security standards and reporting responsibly:

“We need to incentivize AND regulate”.

(Participant 10)

The GDPR landscape proved to be a high frequency data feature across the data corpus; it was described by some participants as fuelling negative publicity with fervent media coverage, heavily impacting brand and reputation. A regulatory approach that incentivises corporates (potentially through mechanisms such as corporate taxation incentives), to better protect and defend themselves to a foundational level was largely favoured, rather than the application of blanket regulatory penalties that serve only to punish the corporate (itself a victim of cybercrime).

8.1.5. Increased Reporting Awareness

Some participants described a lack of board security expertise as a risk to not disclosing, suggesting a need to educate, on how to identify attacks, making the right determination when it’s appropriate to engage with authorities and the

right channels to use for reporting, showing the negative impacts to Boards of not reporting. Some participants went further and were more insistent and specific on need for better Board level security expertise:

> *"The best thing to do for most organisations is, if they can find someone that can advise them at Board level; either have another ex CISO, as an advisor to the Board on cyber security, or a Board level cyber security advisory committee, or non-execs that have security backgrounds".*
> (Participant 6)

Continuing the key theme of reporting awareness, other participants focused more generally on public awareness and suggested that corporates themselves would benefit from greater disclosure of other corporates, collectively improving the ability of others to defend against similar attacks. A few participants connected public awareness with the need for more effective media management strategies:

> *"(On Fireye), they handled the Solarwinds breach better than any other company – upfront, straightway, hand in hand with forensics and how to mitigate, consequently have not seen the dire impact on their business that we usually expect – all corporates should learn lessons from their media strategy. If you try to bury something like this it's going to be much worse, they'll always be journalists around to find the scoop. But they used the media as their channel".*
> (Participant 2)

One idiosyncratic perspective on improvement strategies stood out as noteworthy, relating to awareness of the consequences of cybercrime and corporate social responsibility. The participant's suggestion that corporates are acting irresponsibly through under-reporting, with a need for increased awareness of the consequences of both cybercrime and under-reporting (referring to links with organised crime). Framing the suggestion against the context of recent social movements standing up against racism and abuse; the participant expressed the need to take a parallel approach to address the proliferation of cybercrime, highlighting the protection currently being afforded to cybercriminals through corporates turning a blind eye:

"Do we want the corporates to start being responsible? And protecting themselves better? Educating their staff better?" Education is needed - it's about providing information for the good of all, isn't it? …Being silent isn't good enough anymore, it's not acceptable anymore".
(Participant 7)

Having the right corporate governance in place, with appropriate Board level security expertise to navigate reporting decisions and engage with external agencies at the right time, under the right circumstances, is also an important part of the under-reporting equation. It remains however, that if disincentives to external corporate reporting prevail, potentially getting in the way of corporates achieving business objectives; education and awareness is likely only to improve reporting cultures by narrow margins, without any significant groundswell that makes an intrinsic change to corporate motivation.

8.2. Proposed Potential Strategies

Two additional potential improvement strategies were shared with participants, where participants opinions in support or opposition of each proposed strategy were analysed.

8.2.1. Role of a Bystander

A complimentary approach to intelligence sharing for stronger defence may rest in the application of Mary Rowe's (2018) 'bystander' theory. Rowe argues that bystanders are routinely 'a missing link in conflict systems' (Rowe, 2018). This study argues that through the juxtaposition of a conflict system with a cybercrime environment, using Rowe's theory, bystanders (such as ISPs, hosting providers, security service providers, or insurers) could be used to greater effect, to anonymously share the reconnaissance, intelligence, or attack information they see to strengthen both central defence and deterrence.

- **Support – Concept of Utilising Third Party Visibility**

Most participants initially received the idea of a Bystander mechanism with interest, some identifying software vendors, hosting providers and ISPs as potential Bystander candidates:

> *"I actually think that's a really interesting point. If you want to know how many systems are breached, don't talk to the customers. Talk to the supplier of the system about the questions they get asked by their customers".*
> (Participant 11)

> *"I think the Google's and the Microsoft's and the Amazon's who run world infrastructure, or some of it, are bystanders to a tremendous amount of adversarial activity. And if they were given an incentive to not go after the other guys, but just build more awareness, I think that could do nothing but good; but right now, they have no reason to".*
> *"We could tackle this problem at the level of the ISP's. Use ISP's as much more of a central reporting point and collation point".*
> (Participant 4)

Participants' preconceptions of how information would be reported, used and protected rapidly overtook the initial positive reception the proposal received. Two subthemes summarise participants' fundamental concerns:

- **Opposition - Breach of Trust**

Rejection of the concept was predicated on the likely existence of a commercial relationship between the bystander and corporate cybercrime victim; whereby the bystander could share information with authorities that the corporate is unwilling to disclose, resulting in a fundamental breach of trust. Some participants suggested that this may depend on the method of bring the concept to life:

> *"There's a difference between empowering those bodies to report on your behalf in a certain, anonymised way that you buy into, versus them being a bystander and noticing it, and then reporting*

it, regardless of what your position on it [reporting] is as an organisation, or whether they're aligning with you as to how they're reporting on it. So that breaks the trust and that actually takes us back. That builds walls".

(Participant 12)

- **Opposition - Privacy Versus Security**

Some participants were concerned at the level of intrusion into traffic or access to hosted environments that would be needed to make the bystander concept feasible:

"If an ISP is served with a warrant, they will fall over backwards to assist. But if you ask an ISP to tell you about attacks about X; 'So you want me to breach every transaction on my network?'. It means you have to look inside, there are no signs or patterns otherwise, you have to crack the egg open to see the yolk; unless its DDOS which is really a networks thing, otherwise there is very little to go on…the collision is between protection and privacy. What gives them the right to scan through this on mass? To look for IPs, and code".

(Participant 5)

Participants primary concerns of the bystander, breach of trust and anonymisation of data, could be mooted and potentially addressed by means of implementation, particularly if bystanders were only to report fully anonymised data to a central agency, on a level playing field with all other such third parties legally required and incentivised to do so.

8.2.2. Safety Culture

Promotion of safety culture was proposed as a strategy to participants through summary of Matthew Syed's treatment of safety culture, within popular book, Black Box Thinking (Syed, 2015). Syed takes cultural safety learnings from the aviation industry and looks at how they might be applied to improve performance, requiring transparency of reporting.

- **Support – Concept of Open Learning from Near Misses**

Generally, participants were open to the concept of structured, open learning from incidents, as would be expected where information security management systems [24] are based on continuous improvement (although this concept is applied introspectively by most corporates), as promoted within Syed's safety culture. A few participants qualified their support only to apply to near misses, or low impact events:

> *"I think looking at near misses, you know, near miss reporting in safety management, you could liken to event reporting within security management, the more we can learn from things that didn't result in, or, you know, resulted in less of a consequence, I think gives us far more opportunity to learn and evolve than we have at the moment within security management".*
>
> (Participant 9)

- **Opposition – Safety Style Regulation**

Opposition from most participants did not relate to the concept of safety culture itself but to the regulatory approach that might be taken to implement it:

> *"Staggeringly strange things go on in a very, very well-regulated industries, because people just hide from the regulations".*
>
> (Participant 11)

> *"Fundamentally what happens in some of these small organisations is they've got a million different compliance related things to worry about, probably none of which they're experts in; it could be anything, it could be safeguarding, financial crime, health and safety, data protection, the list goes on, right? So where do you put your focus? You have to be compliant with all of them, but you're not that expert in any of them".*

[24] Such as continuous improvement requirements set out within BS EN ISO/IEC 27001:2017, the International Standard for information security management.

(Participant 6)

The ultimate concern over adoption of a safety culture applied to cybercrime incidents, as previously seen across multiple themes and other proposed strategies, was of over exposure of incident data, with a greater degree of acceptance that learnings from near misses or low impact events might be shared, rather than any incident of a level for which there may be some form of recourse against the corporate. This indicates a trend of broader reticence to embrace wider cultural change, based on the issues surfaced within the corporate fear of reporting key theme, including liability and fines, negative publicity, and brand and reputation (as described previously within Chapter 6).

9. Conclusion

The aim of this study was to answer five core research questions. Within this concluding chapter, I compare interview findings (discussed within Chapters 4 to 8) with relevant literature and theories (discussed in Chapter 2) alongside conclusions drawn in relation to each core research question, which are set out in order below.

9.1. What Does the Corporate Cybercrime Landscape Look Like?

Interview findings from this study suggest that cybercrime affects corporates to a far greater degree than official cyber-incident cyber breach statistics show (see Section 2.2.1). In the main, low level, opportunistic attacks including phishing attacks, whether successful or unsuccessful, were described by participants as occurring at high frequency, with corporates affected by more severe or higher impact cyber-attacks at a somewhat lower frequency, but with the universal agreement of participants that frequency of cybercrime incidents far outstrips official statistics. Participants were critical of cybercrime statistics due to differences in cybercrime definitions, as also seen within academic literature (Gordon and Ford, 2006, Wall, 2007). They were supportive of the need for common definitions in reporting, as seen also seen within Anderson et al. (2013) study on costs of cybercrime. These signal a pressing need for better data fidelity to inform the development of more effective cybercrime response strategies, data fidelity that can only be achieved through reporting cybercrimes.

Changes in the cybercrime landscape, such increasing Ransomware-as-a-Service, potentially disrupt theories such as those of Seebruck (2015). Attacks may no longer be executed by the actor responsible for instigating them . A threat actor is likely several threat actors fulfilling different cybercrime roles, that might or might not have links to organised crime, but with a rising tide of sophistication, I argue corporates have to now expect the worst and be prepared to respond, and report accordingly.

9.2. What Is the Extent of Corporate Under-Reporting?

As seen in Chapter 5, the UK Government Department for Digital, Culture, Media, and Sport's (2020) Cyber Security Breaches Survey suggests that less than 10%vof corporates, report cybercrimes to law enforcement. There was consensus among participants that whilst the statistics may not be entirely reliable, the majority of corporates under-report cybercrime externally, suggesting a more endemic lack of reporting than merely situational gaps.

It was also clear from the responses of interview participants that many similarities exist between corporate under-reporting of cyber-crime and the disclosure gaps observed with US listed corporations failing to meet Securities and Exchange Commission (SEC) disclosure requirements (Etzioni, 2011, Trope, 2012, Ferraro, 2013, Young, 2013, Amir et al. 2018). Similarities were found not only with the calculations corporates make in determining when to disclose or report (with SEC disclosures determined by a materiality threshold), but also in the shared reasons identified for under-reporting, examined within section 9.3 below.

Despite the purpose of reporting to law enforcement or cyber response agencies being to reduce cybercrime and its impacts, even if realised in the long term, reporting should be serving the interests of corporates. However, reporting was generally seen by participants as countering business interests; in a similar vein, Etzioni (2011) identifies corporates withholding SEC disclosure information in the interests of corporate shareholders. I suggest this reveals a prevalent 'protectionist' reporting culture, centred on corporate protection of immediate business interests, that I argue requires an array of aligned strategies in combination to even begin to shift the dial on change.

9.3. What Reasons Are There for Corporate Under-Reporting?

This study finds corporates generally proactively taking or falling into one of three reporting positions:

- Corporates unable to report

- Corporates unwilling to report
- Corporates making calculated reporting decisions

The inability to detect and therefore report cybercrime incidents was identified by participants as a significant factor in relation to corporate under-reporting, supporting Etzioni's (2011) view that not all corporates are aware of having been affected by cybercrime. Participants generally asserted that 100% of business suffer cybercrime incidents, many of whom are unaware and unable to report. Large corporates are not immune to monitoring and detection omissions either, often with vast technology footprints to selectively rather than exhaustively monitor. The inability to detect cyber-attacks, however, is in the main associated in with small, less cyber mature corporates, that is concerning when according to the World Bank (2021), small-medium enterprises represent the majority of businesses worldwide. Schemes such as the UK's Cyber Essentials[25], have been heavily invested in, to encourage corporates of all sizes to implement foundational information security practises. I contend however that greater education and incentivisation (not fines) for small businesses is needed to adequately protect against, detect and crucially report cybercrimes.

Participants largely supported the claims of corporate unwillingness to identify as cybercrime victims made by Wall (2007). In relation to the potential relationship between willingness and crime impact (Graham et al., 2019), whist participants within this study identified crime impact as a potential factor driving reporting, this was seen to relate more to internal rather than external reporting to law enforcement. Impact should however be conflated with breach materiality determinations, described in relation to GDPR as a legal pre-occupation, and the most influential factor in making calculating reporting decisions.

[25] Cyber Essentials and Cyber Essentials Plus are two levels of certification available as part of a UK government backed scheme to assist organisations of all sizes achieve a foundational level of protection against most common cyber-attacks.

Corporates are fiercely protective of their brands, as seen by Wang et al. (2013) corporates' main concerns are managing public perceptions and avoiding negative publicity. Additively, under threat of punishment for data breaches with significant fines levied by regulators, corporates are potentially more fearful of reporting cybercrimes, than cybercriminals of breaking the law and being apprehended.

In comparison with many studies (Laube and Böhme, 2016, Juma'h and Alnsour, 2020, Klaus and Elzweig, 2020) relating to the impacts of data breaches on share price, most participants recognised share price as consequential factor in relation to reporting. The view of participants implied significant, long term stock impacts were feared, somewhat in opposition to the study by Juma'h and Alnsour (2020) suggesting that stock losses suffered as a consequence of data breaches are generally short lived, although different studies present slightly varying findings in this area, making it difficult to assert a conclusive position.

As suggested by Wall (2007), ineffective law enforcement impacts corporate (un)willingness to report. Participants also described laborious, time-consuming reporting mechanisms that fail to offer practical response support or investigation feedback as obvious disincentives for corporates to engage in any reporting process, particularly if the starting position to report is one of reluctance.

In summary, the reasons for under-reporting are business centric, reporting decisions are believed to made with the protection of corporate interests in mind.

I suggest the reporting balance needs to be recalibrated. Protection needs to be weighted in favour of the corporate rather than the criminal. Corporates reporting benefits need to be visible with tangible business incentives created to report. Strategies considered to improve reporting are discussed within Section 9.5 below.

9.4. What Are the Consequences of Under-Reporting?

Corporate under-reporting of cybercrime impedes deterrence, sending a clear message to criminals that cybercrime pays, with low likelihood of apprehension or prosecution. Cybercrime was generally seen by participants as a proliferating problem, in agreement with Wall (2008).

Cybercriminal operations are increasing in effectiveness. Cybercrime services such as Ransomware-as-a-Service are becoming increasingly accessible, with sophisticated cyber-attack tools being made available to non-technical or novice cyber-criminals. These growing trends, I argue if uncurbed, will make cybercrime more difficult to defend against, with the potential to become significantly more impactful to corporates, and more consequential to society.

In terms of consequence, of what is at stake, of the criminals being harboured by corporates through under-reporting, some (but not all), participants recognised connections between cybercrime and organised crime in relation to low-level cyber-attacks, such as those found by Leukfeldt et al. (2017). Other participants felt that links to organised crime could still only be seen as edge cases. Most participants did however recognise the increasingly blurred lines between potential threat actors, supporting the assessment of cybercriminals made by Sailio et al.(2020) finding that it may not always be possible to differentiate between threat actors. Participants rarely identified the intersection of cybercrime and cyber politics as a corporate concern (Dunn Cavelty and Wenger, 2020).

I contend that these increasingly blurred lines between opportunistic, low-level criminality and high end, sophisticated, organised crime, should be sounding alarm bells, particularly when considering the current protectionist reporting cultures identified. Corporates and Boards require greater awareness of the nature of the threats they could be facing and criminal activities they could be harbouring, accepting that some attacks may not be what they seem, there is a need to consider the potential consequences of organised crime as part of incident response and responsible reporting decisions.

As seen in Chapter 6, participants agreed that data fidelity is important to plan effective cybercrime response strategies and provide adequate resources, this is largely dependent on external reporting; yet corporates continue to disregard the value of reporting. This highlights a wider cultural discrepancy between security professionals' perceived need for better information sharing (see Section 9.5 below) to improve cybercrime defence, and an overriding business objective to suppress information to avoid over exposure of weaknesses.

9.5. What Potential Strategies Could Improve Reporting Cultures?

Participants suggested multiple strategies that could be used to improve reporting cultures. The most popular strategy proposed was for anonymised cyber incident information sharing with authorities, reflecting Dutta and McCrohan's (2002) advocacy of public-private sector collaboration. Sector specific intelligence sharing[26] predicated on trust (Wagner et al. 2019) can be impactful, with participants also calling for the promotion of greater closed-group intelligence sharing to benefit sectors with common aims.

Participants were divided with respect to legal and regulatory approaches to reporting. Some suggested mandatory reporting and augmentation of existing Computer Misuse legislation is necessary to improve reporting, particularly if underpinned by a legally required minimum technical standard against which compliance could be recognised and negligence penalised, somewhat echoing Laube and Böhme's (2016) and Tang and Whinston's (2020) proposals. Other participants were entirely dismissive of the effectiveness of any legal or regulatory approach taken to mandate reporting, particularly the punitive approach seen with the EU GDPR, articulating more cautious opinions towards increasing legal and regulatory requirements, closer to (Holt, 2018).

[26] Such as US Information Sharing and Analysis Center (ISAC) groups and UK NCSC coordinated threat intelligence groups.

Additional strategies presented to and explored with participants received a mixed reception. Building on Perset's (2010) positioning of internet intermediaries, I suggest that the application of Rowe's (2018) 'bystander' theory could be used to greater effect, to anonymously share the reconnaissance, intelligence, or attack information, to strengthen both central defence and deterrence. Whilst some degree of conceptual support was afforded, participants posed fundamental objections centred on breach of trust, demonstrating the potential complexity involved in the implementation of such a strategy.

The adoption of reporting principles seen within safety management, as proposed by Syed (2015), were also largely dismissed, from two primary standpoints. One of adding a further layer of unrealistic compliance demands on corporates, particularly small businesses. The other concerned with over exposure of weaknesses, reiterating, rather than resolving reporting concerns. However, blame cultures were described to exist and to shape how cybercrime information is shared and there may still be benefit in consideration of the safety approach outlined by Dekker and Breakey (2014).

I argue that a range of strategies in alignment and combination are needed to improve corporate cybercrime reporting cultures. Law enforcement needs to be seen as a positive and worthwhile endeavour, corporates need to feel protected and supported reporting to law enforcement agencies, reporting needs to be made quick and easy and crime information needs to be seen to be used more effectively by authorities. In the pursuit of deterrence and defence against cybercrime, allied methods need to be developed for centralised anonymous information sharing, governed by a central, not for profit body. Opportunities need to be explored to incentivise corporates (potentially through tax breaks) to achieve a basic standard / level of a defence as a mandatory requirement that demonstrates corporate responsibility that is recognised by regulators.

9.6. Concluding Remarks

The majority of corporates do not report cyber-crimes to law enforcement authorities, either because they are unaware of having been a victim or because they are acting in the interests of protecting their business. Corporates need to be better incentivised to share cybercrime information in the wider interests of industry and society, to improve both deterrence and defences against the rising tide of cybercrime, in changing cybercrime landscape.

Bibliography

Amir, E., Levi, S. and Livne, T. (2018) 'Do Firms Underreport Information on Cyber-Attacks? Evidence From Capital Markets', *Review of Accounting Studies,* 23(3), pp. 1177-1206. doi:10.1007/s11142-018-9452-4.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.,G., Levi, M., Moore, T. and Savage, S. (2013) 'Measuring the Cost of Cybercrime *The Economics of Information Security and Privacy*' Berlin, Heidelberg: Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 265-300.

Ashford, W. (2018) 'Why Businesses Must Report Cyber Crime, *Computer Weekly* (14-20 August 2018), pp.29-36. https://www.computerweekly.com/feature/Cyber-crime-why-business-should-report-it (Accessed: 23 August 2021).

Berry, K. (2018) 'Equifax Misled Public on Data Breach, Warren Claims, *The American Banker',*183(27), p.1. Available at: http://web.b.ebscohost.com.ezproxy01.rhul.ac.uk/ehost/detail/detail?vid=0&sid=9f534171-4f51-410c-b943-222557b3db51%40sessionmgr103&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=127841142&db=bth (Accessed: 21 March 2021).

Bidgoli, M., Knijnenburg, B.P., Grossklags, J. and Wardman, B. (2019) '*Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting'* (From the 2019 APWG Symposium on Electronic Crime Research (eCrime)), pp. 1-10, doi:10.1109/eCrime47957.2019.9037577

Braun, V. and Clarke, V. (2006) 'Using Thematic Analysis in Psychology *Qualitative Research in Psychology',* 3(2), pp. 77-101. doi:10.1191/1478088706qp063oa.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, *International Journal of Electronic Commerce,'* 9(1), pp. 69-104. https://www.jstor.org/stable/27751132 (Accessed: 20 August 2021).

Crowdstrike (2020) '*Crowdstrike 2020 Global Threat Report'* Available at: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/?utm_campaign=brand&utm_content=neu&utm_medium=sem&utm_source=bing&utm_term=%2Bcrowdstrike&msclkid=e831597b8dcb16d66aea394ad2cb2779 (Accessed: 17 February 2021).

Dekker, S.W.A. and Breakey, H. (2016) 'Just Culture: Improving Safety by Achieving Substantive, Procedural and Restorative justice', *Safety Science,* 85, pp.187-193. doi:10.1016/j.ssci.2016.01.018.

Department for Digital, Culture, Media, and Sport (2020) '*Cyber Security Breaches Survey 2020'* Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020 (Accessed: 20 February 2021).

Dunn Cavelty, M. and Wenger, A. (2020) 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science, *Contemporary Security Policy',* 41(1), pp.5-32. doi:10.1080/13523260.2019.1678855.

Dutta, A. and McCrohan, K. (2002) 'Management's Role in Information Security in a Cyber Economy, *California Management Review,'* 45(1), pp.67-87. doi:10.2307/41166154.

Etzioni, A. (2011) 'Cybersecurity in the Private Sector: The Nations Businesses Manage a Significant Share of Online Activity Related to National Security and Must Play a Larger Role in Ensuring the Overall Integrity of the System' *Issues In Science and Technology,* 28(1), pp.58. Available at: https://https//www.jstor.org/stable/43315569 (Accessed: 20 February 2021).

Feiner, L. (2021) 'Microsoft President: The Only Reason we Know About Solarwinds Hack is Because Fireeye Told Us', *CNBC,* 23 February 2021. Available at: https://www.cnbc.com/2021/02/23/microsoft-exec-brad-smith-praises-fireeye-in-solarwinds-hack-testimony.html (Accessed: 6 March, 2021).

Ferraro, M.F. (2013) '"Groundbreaking" or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, its Effectiveness, and Implications', *Albany Law Review,* 77(2), pp.323. Available at: https://heinonline.org/HOL/license (Accessed: 21 March 2021).

Festinger, L. (1957) *A Theory of Cognitive Dissonance.* Evanston, Ill.: Evanston, Ill. : Row, Peterson.

Finnemore, M. and Hollis, D.B. (2020) 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity', *European Journal of International Law,* 31(3), pp.969-1003. doi:10.1093/ejil/chaa056.

Finnemore, M. and Hollis, D.B. (2016) 'Constructing Norms for Global Cybersecurity', *The American Journal of International Law',* 110(3), pp.425-479. doi:10.1017/S0002930000016894.

Fruhlinger, J. (2020) 'Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?', *CSO Online,* (12 February 2020) Available at: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (Accessed: 21 August 2021).

Glaessner, T.C., Kellermann, T. and Mcnevin, V. (2004) 'The World Bank: Electronic Safety and Soundness', *World Bank Working Paper,* 26. The International Bank for Reconstruction and Development / The World Bank, Available at: https://openknowledge.worldbank.org/handle/10986/15029 (Accessed: 21 August 2021).

Gordon, S. and Ford, R. (2006) 'On the Definition and Classification of Cybercrime, *Journal In Computer Virology',* 2(1), pp.13-20. doi: 10.1007/s11416-006-0015-z.

Graham, A., Kulig, T.C. and Cullen, F.T. (2019) 'Willingness to Report Crime to the Police, *Policing : An International Journal of Police Strategies & Management',* 43(1), pp.1-16. doi: 10.1108/PIJPSM-07-2019-0115.

Hakimi, M. (2019) 'Introduction to the Symposium on Cyber Attribution, *AJIL Unbound',* 113, pp.189-190. doi:10.1017/aju.2019.30.

Hay Newman, L. (2017) 'All the Ways Equifax Epically Bungled Its Breach Response', *Wired*, (24 September 2017), Available at: https://www.wired.com/story/equifax-breach-response/ (Accessed: 28 March 2021).

Haynes, D. (2021) *Into The Grey Zone: Exploring the Murky Evolution of Warfare.* Available at: https://news.sky.com/story/into-the-grey-zone-exploring-the-murky-evolution-of-warfare-12184358 (Accessed: 23 March 2021).

Higgins, K.F. and Zatylny, M. (2018) 'SEC Issues New Cybersecurity Disclosure Guidance, *Insights',* 32(3), pp 3-7. . Available at: http://web.a.ebscohost.com.ezproxy01.rhul.ac.uk/ehost/detail/detail?vid=0&sid=383cc061-3a82-4d3f-b0c2-76250aca6185%40sessionmgr4008&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=128981139&db=bth (Accessed: 23 March 2021).

Holt, T.J. (2018) 'Regulating Cybercrime through Law Enforcement and Industry Mechanisms', *The Annals of the American Academy of Political and Social Science,*679(1), pp.140-157. doi:10.1177/0002716218783679.

Home Office (2019a) *Crime Against Businesses: Findings from the 2018 Commercial Victimisation Survey.* GOV.UK, Available at: https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-2018-commercial-victimisation-survey (Accessed: 19 August 2021).

Home Office (2019b) *Crime Against Businesses: Findings from the 2018 Commercial Victimisation Survey: Months Crime-Against-Businesses-Headline-2018-Tables – RV.* GOV.UK, Available at: https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-2018-commercial-victimisation-survey (Accessed: 19 August 2021).

Information Commissioner's Office (2016) *TalkTalk cyber attack – How the ICO's Investigation Unfolded.* Available at: https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded (Accessed: 20 August 2021).

Jhaveri, M., Cetin, O., Gañán, C., Moore, T. and Eeten, M. (2017) 'Abuse Reporting and the Fight Against Cybercrime', *ACM computing surveys,* 49(4), pp.1-27. doi:10.1145/3003147.

Juma'h, A.,H. and Alnsour, Y. (2020) 'The Effect of Data Breaches on Company Performance', *International Journal of Accounting and Information Management,*28(2), pp.275-301. doi:10.1108/IJAIM-01-2019-0006.

Klaus, T. and Elzweig, B. (2020) 'The Impact of Data Breaches on Corporations and the Status of Potential Regulation and Litigation', *Law and Financial Markets Review,* 14(4), pp.255-260. doi:10.1080/17521440.2020.1833432.

Knowles, T. (2020) 'Firms pay £200m in ransoms to hackers', *The Times,* 31 July 2020.

Krishna, A. and Vibber, K.S. (2017) 'Victims or Conspirators? Understanding a Hot-Issue Public's Online Reactions to a Victim Cluster Crisis', *Journal of Communication Management (London, England),* 21(3), pp.303-318. doi: 10.1108/JCOM-08-2016-0067.

Laube, S. and Böhme, R. (2016) 'The economics of Mandatory Security Breach Reporting to Authorities', *Journal of Cybersecurity (Oxford),* 2(1), pp.29-41. doi:10.1093/cybsec/tyw002.

Leukfeldt, E.R., Leukfeldt, E.R., Lavorgna, A., Lavorgna, A., Kleemans, E.R. and Kleemans, E.R. (2017) 'Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime', *European Journal on Criminal Policy and Research,* 23(3), pp.287-300. doi:10.1007/s10610-016-9332-z.

Lewis, D.J. and Weigert, A. (1985) 'Trust as a Social Reality', *Social forces,* 63(4), pp.967-985. doi:10.1093/sf/63.4.967.

Morse, E.A. and Ramsey, I. (2017) 'Navigating the Perils of Ransomware', *The Business lawyer,* 72(1), pp. 287-294. Available at: https://heinonline-

org.ezproxy01.rhul.ac.uk/HOL/P?h=hein.journals/busl72&i=299. (Accessed: 20 February 2021).

Newman, G. (2017) 'Held to Ransom', *Canadian Underwriter,* 84(8), pp.19-21. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=125079732&site=ehost-live Accessed: 20 August 2021).

Office for National Statistics (2019) *Number of Recorded Incidents of Hacking and Cybercrime.* Available at: https://www.ons.gov.uk/aboutus/transparencyandgovernance/freedomofinformationfoi/numberofrecordedincidentsofhackingandcybercrime (Accessed: 30 November 2019).

Osborne, C. (2014) *How Hackers Stole Millions of Credit Card Records from Target.* Available at: https://www.zdnet.com/article/how-hackers-stole-millions-of-credit-card-records-from-target (Accessed: 23 August 2021).

Perset, K. (2010) 'The Economic and Social Role of Internet Intermediaries', *OECD Digital Economy Papers, (*171). doi:10.1787/5kmh79zzs8vb-en.

Porcedda , M.G. and Wall, D.S (2019) 'Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk Hack', *2019 IEEE European Symposium on Security and Privacy Workshops (4th Euro S&P)*, Stockholm. 17-19 June 2019. IEEE, pp.443.

Rogers, M.K. (2006) 'A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy', *Digital investigation,* 3(2), pp. 97-102. doi:10.1016/j.diin.2006.03.001.

Rowe, M. (2018) 'Fostering Constructive Action by Peers and Bystanders in Organizations and Communities', *Negotiation Journal,* 34(2), pp.137-163. doi:10.1111/nejo.12221.

Sailio, M., Latvala, O. and Szanto, A. (2020) 'Cyber Threat Actors for the Factory of the Future', *Applied Sciences,* 10(12), pp.4334. doi:10.3390/app10124334.

Seebruck, R. (2015) 'A Typology of Hackers: Classifying Cyber Malfeasance Using a Weighted Arc Circumplex Model', *Digital Investigation,* 14, pp. 6-45. doi:10.1016/j.diin.2015.07.002.

Spring, T. (2021) *Black Hat: New CISA Head Woos Crowd with Public-Private Task Force.* Available at: https://threatpost.com/cisa-head-woos-security-crowd/168426 (Accessed: 23 August 2021).

Syed, M. (2015) *Black Box Thinking, Marginal Gains and the Secrets of High Performance.* London: John Murray.

Tang, Q. and Whinston, A.B. (2020) 'Do Reputational Sanctions Deter Negligence in Information Security Management? A Field Quasi-Experiment', *Production and Operations Management,* 29(2), pp.410-427. doi:10.1111/poms.13119.

Tidy, J. (2021) 'REvil: Ransomware gang websites disappear from internet', *BBC News,* Available at: https://www.bbc.co.uk/news/technology-57826851 (Accessed: 23 August 2021).

Trope, R.L. (2012) '"There's No App for That": Calibrating Cybersecurity Safeguards and Disclosures', *The Business Lawyer,* 68(1), pp. 183-195. Available at: https://www.jstor.org/stable/23527083 (Accessed: 18 August 2021).

Turner, M.J.L. (2021) *MoJ analysis of Computer Misuse Act 1990 Case Outcomes 2008 - 2018.* Available at: https://www.computerevidence.co.uk/CMA%20index.htm (Accessed: 18 August 2021).

Verizon (2020) *Data Breach Investigations Report.* Verizon. Available at: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (Accessed: 17 February 2021).

Wagner, T.D., Mahbub, K., Palomar, E. and Abdallah, A.E. (2019) 'Cyber Threat Intelligence Sharing: Survey and Research Directions', *Computers & Security,* 87, pp.101589. doi:10.1016/j.cose.2019.101589.

Wall, D.S. (2007) *Cybercrime : The Transformation of Crime in The Information Age.* Cambridge: Polity.

Wall, D.S. (2008) 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime', *International Review of Law, Computers & Technology,* 22(1-2), pp.45-63. Available at: https://www-tandfonline-com.ezproxy01.rhul.ac.uk/doi/citedby/10.1080/13600860801924907?scroll=top&needAccess=true (Accessed: 17 February 2021).

Wang, P. and Johnson. Christopher (2018) 'Cybersecurity Incident Handling: A Case Study of the Equifax Data Breach', *Issues in information systems.,* 19(3), pp. 150-159. Available at: http://iacis.org/iis/iis.php Accessed: 23 August 2021).

Wang, T., Ulmer, J.R. and Kannan, K. (2013) 'The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities', *Journal of Organizational Computing and Electronic Commerce,*23(3), pp.200-223. doi:10.1080/10919392.2013.807712.

Williams, M.L., Levi, M., Burnap, P. and Gundur, R.V. (2019) 'Under the Corporate Radar: Examining Insider Business Cybercrime Victimization Through an Application of Routine Activities Theory', *Deviant Behavior,* 40(9), pp. 1119-1131. doi:10.1080/01639625.2018.1461786.

Young, S. (2013) 'Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches', *The Journal of Corporation Law,*38(3), pp. 659. doi:TN_cdi_proquest_journals_1368563396.

Appendices

Appendix 1 – Literature Search Results

The following tables provide a summary of literature search results:

Royal Holloway University of London (RHUL) Library Search

Search Date	Source	Search Terms	Active Filters	Number of Hits	Total Number of Extended Search Results	Articles (Including Journal Articles)	Book Chapters	Books	Conference Proceedings	Newspaper Articles	Reference Entries	Reports
28-Feb-21	RHUL Library Search	Corporate AND Under-Reporting AND Cybercrime	2001 - 2021 Excluding Reviews, Excluding Standards	0	**3248**	2995	162	6	13	31	16	25
			Directly Relevant Sources: From Top 1000 Search Results, Specifically Referring to Corporate Under-Reporting	**0**	**15**	11	1	1	0	2	0	0

Other Database Searches

Date of Search	Database	Search Terms	Active Filters	Total Number of Results	Number Directly Relevant
6-Feb-2021	Web of Science	Cybercrime AND Under Reporting	2001-2021	1	0
6-Feb-2021	Google Scholar	Cybercrime AND Under Reporting	2001-2021	17,300	2* from top 100 results
6-Feb-2021	IEEE Explore	Cybercrime AND Under Reporting	2001-2021	85	1

Appendix 2 – Literature Review - Subject Categories

As outlined within Chapter 2, listed below are literature subject categories analysed within the literature review undertaken, supporting exploration of wider issues associated with under reporting:

- Artificial Intelligence and Big Data,
- Criminology / Victimology,
- Cybercrime,
- Cyber Politics,
- Cyber Terrorism and Cyber War,
- Defence / National Security,
- Economics,
- Finance and Accounting,
- Insurance,
- Law and Enforcement,
- Media Studies - Public Perception,
- National Cyber and Data Protection Authorities,
- Regulation and Disclosure Obligations,
- Safety Culture and Fault Analysis,
- Security Culture,
- Security Management,
- Governance, Risk and Compliance, "
- Sociology – Trust,
- Statistics,
- Strategy,
- Threat Intelligence,
- Under-reporting/ Disclosure.

Excluded from analysis were the following subject categories:

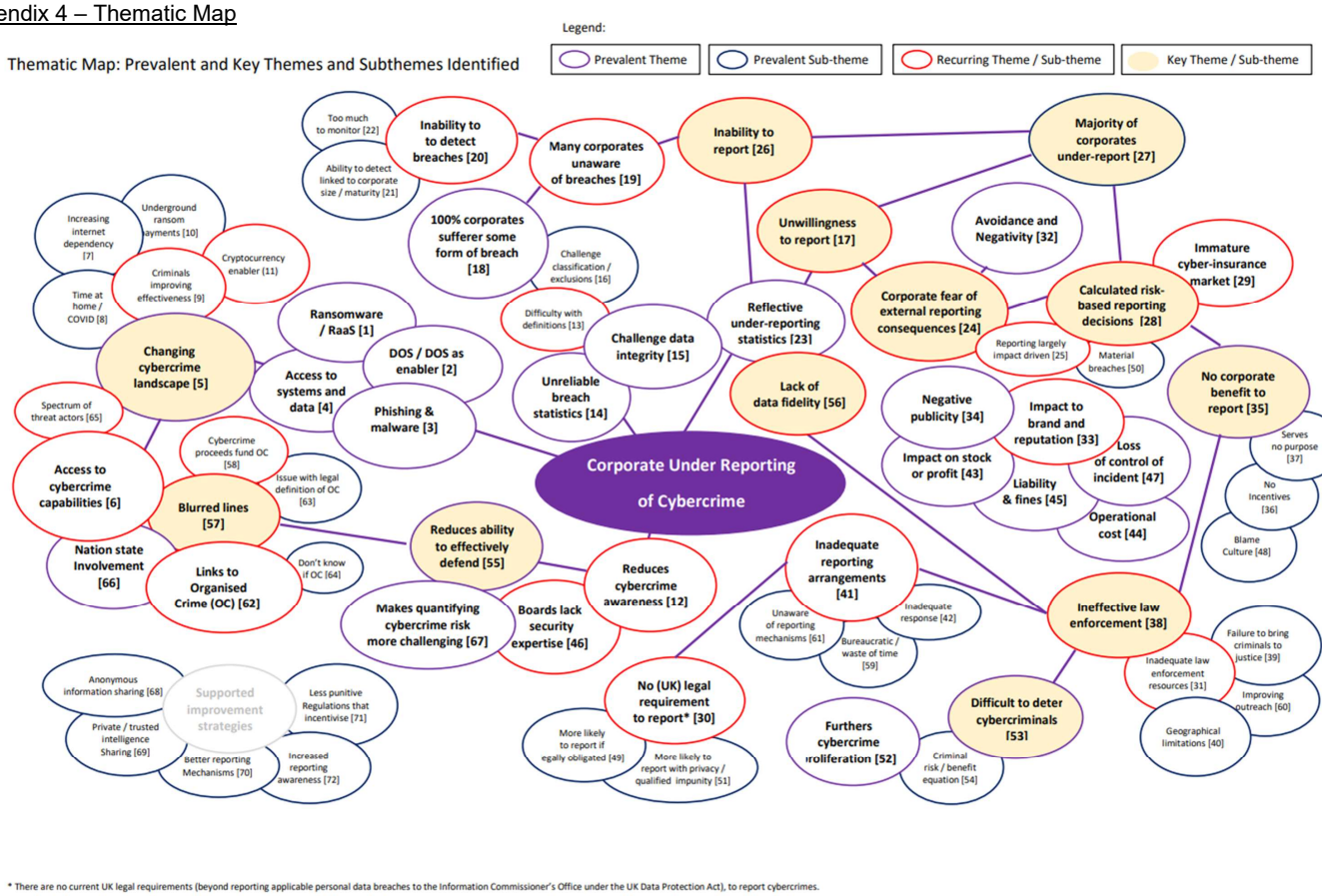
- Blockchain,
- Child Exploitation,
- Cyber Risk to Citizens,
- Device Security,

- Digital Forensic Investigation,
- E-commerce,
- Incident Response / Crisis Management,
- Identity and Authentication,
- Industrial Control Systems,
- Intellectual Property Rights,
- IOT,
- Medical Awareness,
- Privacy,
- Psychological Assessment,
- Security Education, Training and Awareness,
- Security Metrics,
- Social Engineering,
- Social Media,
- Software Security,
- Threat Detection,
- Youth Offending.

Appendix 3 – Interview Questions

1. In your experience, what would you say are the most prevalent or significant types of cybercrime affecting corporates?
2. Do you see the cybercrime landscape changing?
3. Looking at (Home Office, 2019) and (Verizon, 2020) statistics how closely do you feel they reflect current levels of cybercrime experienced by businesses?
4. How do (Department for Digital, Culture, Media, and Sport, 2020) statistics on corporate internal and external cybercrime reporting compare with your experience?
5. What do you think potential reasons for corporate under reporting, or potential barriers to reporting might be?
6. Under what circumstances do you feel corporates might be most inclined to report externally?
7. From your experience, do you feel that there are adequate arrangements in place for corporations to report cybercrimes?
8. Based on what you have seen, what do feel are the most significant consequences of under reporting?
9. How sophisticated are the majority of cybercrimes that affect corporates, are we dealing with organised crime or crime that is organised?
10. Do you feel that under-reporting has any bearing on how effectively Boards are being appraised of cybercrime risks?
11. Are there any strategies that you feel could be effective in improving reporting cultures?
12. Of the proposed strategies, which do you think could be the most effective?

Appendix 4 – Thematic Map



* There are no current UK legal requirements (beyond reporting applicable personal data breaches to the Information Commissioner's Office under the UK Data Protection Act), to report cybercrimes.

Appendix 5 – Thematic Analysis: Key and Prevalent Themes and Subthemes

A full list of key themes (denoted by bold underline), prevalent themes and subthemes (denoted in brackets) analysed is provided below:

	Key Themes and Prevalent Themes & (Subthemes)
1	Ransomware / Raas
2	DOS / DOS as enabler
3	Phishing and malware
4	Access to systems and data
5	**Changing cybercrime landscape**
6	(Access to cybercrime capabilities)
7	(Increasing internet dependency)
8	(Time at home / COVID)
9	(Criminals improving effectiveness)
10	(Underground ransom payments)
11	(Cryptocurrency enabler)
12	Reduces cybercrime awareness
13	Difficulty with definitions
14	Unreliable breach statistics
15	Challenge data integrity
16	(Challenge classification / exclusions)
17	**Unwillingness to report**
18	100% corporates suffer some form of attack or breach
19	Many corporates unaware of breaches
20	(Inability to detect breaches)
21	(Ability to detect linked to size / maturity)
22	(Too much to monitor)
23	Reflective reporting statistics
24	**Corporates fear external reporting consequences**
25	Reporting largely impact driven
26	**Inability to report**
27	**Majority of corporates under-report**
28	**Calculated, risk-based reporting decisions**
29	Immature cyber-insurance market
30	No (UK) legal requirement to report
31	Inadequate law enforcement resources
32	Avoidance and negativity
33	Impact to brand and reputation
34	Negative publicity
35	**No corporate benefit to report**
36	(No incentives)
37	(Serves no purpose)

38	**Ineffective law enforcement**
39	(Failure to bring to criminals to justice)
40	(Geographical limitations)
41	Inadequate reporting arrangements
42	(Inadequate response)
43	Impact on stock or profit
44	Operational cost
45	Liability & fines
46	Boards lack security expertise
47	Loss of control of incident
48	Blame culture
49	More likely to report if legally obligated
50	Material breaches
51	More likely to report with privacy and qualified impunity
52	Furthers cybercrime proliferation
53	**Difficult to deter cybercriminals**
54	(Criminal risk / benefit equation)
55	**Reduces ability to effectively defend**
56	**Lack of data fidelity**
57	**Blurred lines**
58	Cybercrime proceeds fund Organised Crime
59	(Bureaucratic / waste of time reporting to authorities)
60	(Improving outreach)
61	(Unaware of reporting mechanisms)
62	Links with Organised Crime
63	(Issue with legal definition of Organised Crime)
64	(Don't know if cybercrime is Organised Crime)
65	(Spectrum of threat actors)
66	Nation state involvement
67	Makes quantifying cybercrime risk more challenging
68	(Need) Anonymous information sharing
69	(Need) Industry led threat intelligence sharing
70	(Need) Better reporting mechanisms
71	(Need)Less punitive regulations (that incentivise)
72	(Need) Increased reporting awareness