Corporate under reporting of cybercrime:
Why does reporting to authorities matter?

Author
Laure Lydon, MSc (Royal Holloway, 2021)

Abstract

Reporting crimes to law enforcement agencies is the starting point for any crime response or criminal investigation process. Without reporting, cybercrimes cannot be investigated, prosecutions cannot be pursued, and more crucially, effective prevention strategies cannot be developed. Yet despite the catalytic role of cybercrime reporting, the majority of corporates fail to report cybercrimes. In this article we explain why this is an increasing cause for concern. [a]

[a] This article is published online by Computer Weekly as part of the 2022 Royal Holloway information security thesis series https://www.computerweekly.com/ehandbook/Royal-Holloway-Corporate-under-reporting-of-cyber-crime. It is based on an MSc dissertation written under the supervision of Rikke Jensen as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

While acknowledging that there are significant challenges in comparing different cybercrime statistics, many statistics still suggest a prevalence of corporate under-reporting of cybercrime, with remarkably few cybercrime prosecutions[1], compared to both official[2] and commercial[3] cyber incidents (that may not all constitute crimes), and breach statistics. Even when taking into consideration the likely bias of commercial statistics, alongside the limitations and issues relating to cybercrime categorisation that narrow prosecution statistics (where some types of security incidents might not be classified as cybercrimes in different jurisdictions, such as denial of service or phishing attacks, which may only be considered enablers rather than computer misuse crimes in themselves), these statistical sources remain several orders of magnitude apart. Without a common definition of cybercrime, there is no 'apples for apples' statistical comparison.

Corporates are unlikely to publicly discuss issues relating to cybercrime victimisation or their reporting positions. Understanding corporate under-reporting of cybercrime has therefore been largely shaped by flawed cybercrime statistics, and industry and media coverage of data breaches, with sources often lacking data fidelity. However, recent academic research into corporate under reporting of cybercrime, its extent and consequences, has now also shown that the majority of corporates do not report cybercrimes to law enforcement agencies. The full report can be found on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

What is at stake?

Over a decade ago, established academic on cybercrime, David Wall, outlined the fundamental concern with under-reporting, allowing cyber criminals to stay in the shadows, without fear of being apprehended[4]. When lucrative criminal behaviour goes unchecked, it proliferates, as seen in significant year on year increases in ransomware attacks since 2013.

[1] https://www.ons.gov.uk/aboutus/transparencyandgovernance/freedomofinformationfoi/convictionsunderthecomputermisuseact1990

[2] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

[3] https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[4] 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime', International Review of Law, Computers & Technology, 22(1-2), pp.45-63. (Wall, D.S, 2008)

The last two years have seen an uptick in general access to cybercrime tools and services, coupled with a rising tide of cyber-attack sophistication. Differentiation, therefore, between organised crime and lower-level cyber-attacks routinely affecting corporates presents a growing challenge.

Commercialised cybercrime service offerings have increased in effectiveness. Services such as Ransomware as a Service (RaaS) and the sale of access to systems and data now mean that cybercriminals no longer need their own capabilities to carry out end-to-end attacks and are increasingly likely to outsource or delegate roles based on capability or assignment requirements. Additionally, the cellular structures adopted by some organised crime groups to evade detection, combined with potential nation state sponsorship of cybercrime activities, introduce further complexity and difficulty for corporates to really know what type of threat actors they are dealing with.

Corporates defending against cyber-attacks need to be prepared for increasing ambiguity. Novice, non-technical cybercriminals 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.

Reasons for corporate underreporting of cybercrime

There are many reasons why corporates fail to report cybercrimes to authorities. Many small/medium or less mature organisations are oftentimes simply unaware of breaches, unable to detect attacks. Typically, smaller organisations may also not have adequate access to the security management experience needed to appropriately navigate reporting issues, often lacking security advice at Board level.

Large corporates are not immune to monitoring and detection omissions either, with vast technology footprints, monitoring selectively rather than exhaustively. More generally however, larger corporates may be unwilling to report. Large corporates are concerned with potential negative impacts of breach disclosure, such as impacts on share price, brand reputation or financial penalties. Calculated decisions are commonly made by corporate lawyers, based on thresholds of breach materiality, to determine the legal or regulatory requirement for any external disclosure. Reporting decisions are not only driven by regulation, but also internal, business centric factors, and other external issues including public perception and cyber insurance.

Despite what might be described as corporate preoccupation with the negative impacts of breach disclosure, there is a lack of consensus across academic analyses relating to the extent and longevity of impacts on stock and share price following security incident disclosures[5], with some researchers finding only marginal short-term impacts on corporates, rather than the devasting consequences feared.

Equally, the anticipated volume of astronomic fines expected to rain down on corporates never reached the dizzy heights that many predicted before the inception of the European General Data Protection Regulation. Hefty fines are however still feared, underpinning a reluctance to report cybercrimes to authorities, where it is perceived by corporates that reporting may open organisations up to regulatory scrutiny.

Additional reasons cited for corporate under reporting within recent academic research include inadequate cybercrime reporting mechanisms and law enforcement challenges, where even the most willing corporates are deterred from reporting due to bureaucratic and ineffective reporting mechanisms, with a sense of aggrievement over wasting time reporting, only for reports to end up in a data lake or as government statistics.

Reasons for under-reporting are ultimately business centric, reporting decisions are believed to be made with the protection of corporate interests in mind. Corporates are somewhat disincentivised to report, where reporting yields no clear benefits or outcomes, and in many cases, is perceived as a threat to corporate objectives that may result in regulatory action being taken.

[5] '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. (Cavusoglu et al. 2004). See full report for more references.

Disclosure strategies that restrict reporting

Corporates have learned lessons from catastrophically mismanaged breaches, epitomised by the former TalkTalk and Equifax breaches, large corporate media management strategies have generally matured in recent years. Breach disclosure and media communications plans have commonly become structured components of broader corporate cyber incident response plans. They typically deliver minimum facts, take a conciliatory tone, and follow a 'responsibly under control' messaging formula, with external communications tightly and carefully managed to protect corporate reputation. Consequently, there is mainstream perception that external reporting risks weakening an organisation post-breach, rather than reporting to authorities being seen as a positive, protective measure.

In October 2015 Talk Talk Telecom Group PLC customer records database suffered a security breach, compromising the personal data of 15,656 of its customers.

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.

In stark contrast to the tight-lipped reporting norm, in December 2020, media channels around the world covered Fireye's corporate disclosure of the Solarwinds breach. Announcing the breach as an 'unprecedented attack' demonstrating an entirely new level of sophistication affecting both the private sector and US government systems, FireEye's CEO, Kevin Mandia, proactively, transparently and publicly disclosed the breach, telling the world what FireEye had found, how they had found it, and sharing indicators of compromise. Despite the attack remaining unknown for months, the disclosure approach taken by Fireye, working in collaboration with Big Tech companies including Microsoft, as well as with US agencies, has been widely heralded and was certainly effective in spurring quick and effective responses to mitigate compromise and further threats for organisations affected.

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.

But not every breach is an 'unprecedented breach' of a level of sophistication that evokes empathy with the corporate victim. The proven need for careful media management now also implies corporates withholding essential reporting information, that could enable more effective law enforcement response.

Can reporting really help?

Reporting is vital, not only to deter and pursue actions against cybercriminals, but to improve data fidelity, better informing corporate cybercrime prevention and response strategies.

Some security professionals have voiced concerns over the existing level of tolerance, or normalisation of corporate under reporting of cybercrime; but with limited business consequences for under reporting, nor any real incentivisation to create compelling business reasons to report, failing to report is simply being treated as acceptable. Albeit crimes have been committed.

By extension, failing to report sends the message to cybercriminals that it is 'ok' to attack corporates. Corporates are looking away. This naturally raises the question of corporate social responsibility, particularly when considering the ranging sophistication of cybercrimes that now affect corporates, some with links to organised crime or potential nation state involvement.

Improving reporting cultures

From a defence perspective, intelligence sharing is hugely powerful. 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 National Cyber Security Centre (NCSC), generate valuable threat intelligence for participating entities.

Many security professionals advocate the need to go beyond sector specific intelligence sharing and recognise the need for broader information sharing. Reporting cybercrimes to authorities to enable dissemination of anonymised information could help corporates to defend themselves more effectively and proactively against cyber threats. Practical implementation of any such initiatives would, nevertheless, be very complex, with significant administrative challenges and limitations.

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.

Crucially, for information sharing to be trusted and truly effective, a range of measures are needed in combination, to improve corporate reporting cultures over time. In the UK, the 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, but fundamental improvements to reporting mechanisms, outreach activities and availability of technically skilled response resources to support organisations reporting cybercrimes are still badly needed.

Improving reporting mechanisms may encourage greater reporting amongst corporates who are already receptive to reporting, roughly 10% of corporates, according to the UK Government Department for Digital, Culture, Media, and Sport Cyber Security Breaches Survey 2020[6], but may fail to engage the wider community of reluctant reporters.

Moving the needle on corporate under reporting undoubtedly requires changes in both corporate reporting cultures and shifts in public opinion towards corporates that have fallen victim to cybercrimes. Greater access to practical guidance for organisations experiencing cybercrime is essential, but real business incentives are also needed for corporates to report. Less punitive legal and regulatory approaches are needed, with less sensational media disclosure coverage. Without these cultural shifts, access to support and awareness measures alone are likely to fall short in combatting corporates' reporting concerns and fail to address the stigma of having been breached.

In the wake of the Solarwinds breach, the U.S has ramped up its efforts to foster greater public/private partnership, with the Cybersecurity and Infrastructure Security Agency's (CISA) establishment of the Joint Cyber Defense Collaborative (JCDC) in August 2021[7]. CISA's corporate support resources and communications have also significantly increased in profile, set against a dynamic landscape of new legislation that paves the way for more widespread requirements for mandatory reporting.

Whether driven by legislation or not, under reporting of cybercrime is a significant concern that demands corporates to be better informed, supported and incentivised to report and share cybercrime information with authorities, in the wider interests of industry and society, to improve both deterrence and defences against the rising tide of cybercrime.

Biographies

Laure Lydon is an information security Masters graduate of Royal Holloway, University of London, with an interest in security cultures and ethics. Laure has over 15 years experience within senior security management and leadership roles across multiple sectors, including technology, healthcare, communications and logistics.

Series editor: S.- L. Ng

[6] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

[7] https://www.cisa.gov/jcdc