Analysis of the full costs of cyber security breaches

Final report

Harry Heyburn, Andrew Whitehead, Leonardo Zanobetti
and Jayesh Navin Shah, Ipsos MORI
Professor Steven Furnell, University of Plymouth

Ipsos MORI

Contents

Executive summary

The Department for Digital, Culture, Media and Sport (DCMS) commissioned Ipsos MORI to carry out research to better understand the full costs of cyber security breaches. It involved the creation of a methodology for categorising and grouping costs.

This categorisation informed the drafting of a cost tool, for organisations to use to improve their own cost estimates. For the purpose of this project, the cost tool took the form of a self-completion Word questionnaire, which we tested across 15 case study interviews. The interviews were with UK businesses and charities of varying sizes and sectors, although due to sampling constraints, we did not include very large organisations (e.g. FTSE 350 companies). As a result, the tool is not intended to be a final product, but an initial draft for further testing and development beyond this project.

Below is a summary of our key findings, which we have split into three parts:

1. the benefits that a cost tool based on the one from this study is likely to provide for organisations
2. the challenges this research has raised for capturing this kind of cost information in depth
3. our recommendations for further development of a cost tool, based on the one from this study.

Firstly, the study captured many benefits associated with organisations using a cost tool such as this, not just for the organisation as a whole, but for management boards and also third parties:

- **A cost tool will enable organisations to better understand the true cost of a cyber security breach, which tends to be different from their initial estimates.** The existing literature suggests that there is low awareness, understanding and monitoring of the costs associated with cyber security breaches and no unified way of estimating costs. Evidence from our case studies suggests that this tool helps organisations to appreciate and anticipate the wide range of potential costs they face, including indirect and non-immediate costs. The cost estimates from this tool were typically higher than those recorded for the same breaches in the Cyber Security Breaches Survey (CSBS).

- **The tool can help to change organisations' attitudes and behaviours towards cyber security.** Many of those completing the tool felt they could show the cost information collated via the tool to management boards, to improve their understanding of the cost of breaches, and justify additional investment, training or increased cyber insurance coverage (to cover the potential costs). Interviewees also raised the idea of using the cost data to demonstrate the importance of cyber security to employees, encouraging them to be more vigilant and follow good practice.

- **The tool is likely to be helpful for third parties who can support organisations to manage their cyber risks, such as cyber security consultancies and insurance companies.** One stakeholder highlighted that these bodies had historically struggled to obtain robust and standardised data on breaches. Their hope was that a cost tool based on the one from this project could be used as a consistent way to collect information on the impact of a cyber breach. This would allow for better cost comparisons across different types of organisations (e.g. different sectors) and an understanding of the *types* of costs that are more common in certain sectors.

Secondly, we captured the recurring challenges that organisations faced when using the cost tool:

- **Filling in the tool is likely to require significant input from a range of people in different roles and teams within an organisation and can therefore be burdensome.** In our case studies, this included a mix of IT staff, finance staff, senior management and frontline staff. We also found that many case study participants considered the cost tool to be time consuming and repetitive in its current Word format. This is, partly, a reflection of its comprehensiveness. It should also be noted that the tool drafted for this project is not a final product, but something that may be developed further by government or industry before being rolled out.

- **Some case study participants found it particularly difficult to measure time costs accurately.** In some organisations, the time spent responding to breaches had not been formally logged. In some cases, it was challenging to monetise if wages were not hourly or if those filling in the cost tool were not privy to other employees' salaries.

- **The opportunity cost of time spent responding to breaches is an especially difficult concept for employees to grasp**, even with the aid of this cost tool, as people engaged in immediate incident response management may feel that this time is simply part of their job, and therefore not a cost. This suggests that, where feasible, it may be better for people outside of immediate incident response teams to be put in charge of completing the tool. Chief Risk Officers and Chief Data Officers may be appropriate people to take responsibility for filling in the tool in large organisations.

- **The cost estimates generated in the case studies are still subjective and depend on how engaged interviewees were with the tool.** We had examples of the same type of breach leading to a varied and inconsistent use of the tool. In some instances of invoice fraud or phishing attacks, interviewees only filled out one or two sections. In other cases, similar attacks were felt to have had far more wide-ranging impacts. This was typically linked to how interviewees perceived their cyber security breaches – if the breaches were, in their minds, relatively simple, they were less likely to use the tool comprehensively and more likely to ignore certain types of costs.

Considering these challenges, we make the following recommendations around the further development of the cost tool:

- **The cost tool likely be more useful to small and medium enterprises (SMEs) if there was a "lite" version of the tool that was less burdensome for them.** SMEs typically do not have dedicated cyber teams and often lack reliable data on the cost of a cyber breach. A "lite" version of the cost tool for SMEs, removing some of the medium and long-term costs that they would be less likely to incur (such as PR or marketing costs) or less able to accurately measure, would still allow them to get a more robust sense of the cost of their breach than without any tool.

- **A future tool might try to capture additional costs raised in the research, with an acknowledgement that these estimates are likely to be very subjective.** These include losses in staff time (e.g. through illness) and productivity brought about due to the emotional and physical impact of breaches on staff, and the reputational impact on individual employees.

- **Organisations could receive more written guidance on certain aspects, or even assistance from third parties to help them complete the tool more consistently.** This includes, for example, more explicit guidance on opportunity costs and guidance for deciding the percentage of a cost that is attributable to a single breach. It might be helpful for cyber security consultants or insurance companies to administer the tool, as well as other organisations highlighted in the most recent CSBS, such as banks, accountants or other organisations conducting audits.

- **Any future cost tool developed from this study is likely to work best as an online tool or app.** An online tool or app would help respondents to navigate and provide the required information more easily and complete the process more quickly. It would also make the subsequent extraction of the data easier, allowing them to easily develop summary reports which could, for example, be presented to management boards or shareholders.

1 Introduction

The Department for Digital, Culture, Media and Sport (DCMS) commissioned Ipsos MORI to carry out secondary research and case studies to better understand and measure the full costs of cyber security breaches. This final report has been produced alongside a list of annexes, covered in the appendix.

The UK Government's approach to ensuring the population is secure and resilient to cyber threats is set out in the National Cyber Security Strategy 2016-21 (NCSS). Under the *develop* strand of the NCSS, DCMS works to improve the UK economy's resilience to cyber attacks. This involves ensuring that UK organisations are able to appropriately manage their cyber risks, which in turn requires them to have an informed understanding of the true costs of cyber security breaches.

The qualitative analysis in previous Cyber Security Breaches Surveys (CSBS) found that organisations tend to overlook indirect, long-term and intangible costs when thinking about the impact of a cyber security breach or attack. Furthermore, they do not capture the full extent of direct losses.

The lack of transparency, awareness and nuanced understanding of these costs represents a barrier to organisations' ability to make appropriate, risk-based investment decisions and potentially results in an underinvestment in cyber security. Providing the evidence base for organisations to understand the true costs of cyber security breaches and attacks should allow them to better direct resources when managing and mitigating cyber risks.

As such this study's aims are to:

1. produce a comprehensive list of all the cost categories and considerations that could be associated with a cyber security breach or attack
2. produce a cost tool, encompassing these cost categories, that will allow the government, organisations and market actors[1] to better estimate the total cost of a cyber incident – not intended to be a final product, but an initial draft for further testing and development beyond this project
3. produce insight and estimates of the full extent of these costs through a set of case studies with organisations who have experienced a breach.

The cost tool, for the purpose of this project, took the form of a self-completion Word questionnaire. We describe its development in detail in Chapter 2.

[1] Within organisations, this might include, for example, management boards, IT, finance and procurement leads and others that advise boards on risk management (e.g. Chief Risk officers). It might include third parties that work with organisations, such as auditors, insurers, cyber security consultancies and risk management consultancies. Other interested parties could also include investors, shareholders and clients.

2 Methodology

This section describes the methodology used to produce and test the cost mapping and cost tool, and to recruit and carry out the case studies. We also outline the methodological challenges the project faced and the mitigation strategies we used to address them.

2.1 Literature review

A review of the relevant existing literature formed the first stage of the study. The aim of this review was to assess the methodologies that have previously been used to estimate the cost of a cyber security breach and to identify which costs have been estimated in previous studies.

A longlist of documents to review came from two places. Firstly, we utilised documents included in an internal policy review (from summer 2019) by the Department for Culture, Media and Sport (DCMS). Secondly, we added additional documents provided by DCMS and Professor Steven Furnell. In total, the longlist contained 22 documents, which are listed in an annex (sent separately alongside this report).

We reduced the longlist to a set of 15 key documents to review in depth. We prioritised literature that focused on the costs of a cyber security breach, as opposed to literature that looked at impacts in general but did not attempt to monetise impacts or discuss monetary costs. We also focused on the costs for individual organisations, rather than consumers or society as a whole. We deprioritised literature that was focused on a very specific area that limited its wider relevance. In addition, when reports were published annually, only the latest version was included.

For each of the shortlisted documents, the following information was collected:

- description of the report contents and objectives
- countries included
- the types of cyber security breaches or attacks included, including definitions
- the methodologies used, including methodological challenges, strengths and weaknesses
- sample sizes and descriptions of sample characteristics (e.g. business sizes and sectors included)
- lists of the costs identified, including definitions
- the applicability of the costs identified to this research project.

In addition to the summaries of the individual papers, we wrote an overall summary, which is presented in Chapter 3 of this report.

2.2 Stakeholder interviews

The study team conducted interviews with five stakeholders across government and industry between December 2019 and March 2020.These encompassed:

- government departments
- trade associations and institutes (interviewing the relevant cyber security lead from these bodies)
- third parties from the private sector including a cyber security consultancy and an insurance firm.

The earlier interviews fed into the development of the cost mapping and cost tool. The later interviews asked stakeholder how the cost tool could be refined and how it might be most usefully deployed.

2.3 Cost mapping

The costs identified in the literature review were mapped according to a typology developed by the study team. The typology was informed by the work from previous studies identified in the literature review, as well as expert input from Professor Steven Furnell, the DCMS project team and the stakeholders.

2.4 Cost tool

The cost categories identified during the cost mapping exercise were used to develop a cost tool, in the form of a self-completion Word questionnaire, which could be used by organisations to estimate each of the identified costs. The tool is provided as an annex, alongside this main report.

The Ipsos MORI team developed and tested the tool to ensure it was easy to understand and that it was comprehensive in the costs it covered. However, it is important to note that the version created for this research project is not a final product. Getting to a stage where such a tool is ready to roll out to organisations would require further development work and user testing, beyond the scope of this single project. We also acknowledge that an online tool would be better than a Word version – feedback from case study participants on this is captured in Chapter 5 – but it was not in the scope of this project to create this online version.

The estimation of long-term and intangible costs involves many methodological challenges. These challenges, and the mitigation strategies we used, are listed below. In some cases, this also explains why we have opted to exclude certain cost categories (e.g. loss of share value) from the tool entirely.

- **Identifying the correct person within an organisation** – as the costs of a cyber security breach or attack are wide-ranging, it may be the case, especially within large organisations, that multiple people are required to complete the questionnaire. This might include people from cyber security teams, wider IT teams, legal and compliance teams, finance teams and management boards. To make it easier for organisations to identify the best person to provide specific cost estimates, the questionnaire is ordered into sections based on which department or team the costs are likely to be associated with and specific guidance on this is provided at the start of each section.

- **Attribution (external factors)** – many costs are influenced by a range of external factors beyond a cyber security breach or attack, such as the wider economic environment or physical security factors. This creates methodological challenges when asking organisations what proportion of a cost is attributable to a breach, and not to external factors. One example is the effect of a breach on the share price. The share price of a firm will vary due a myriad of factors, which no individual in the firm could reasonably be expected to accurately understand. Therefore, while changes to share value is accounted for in our cost mapping, it was excluded from the questionnaire. This could, potentially, lead to the cost tool still underestimating the cost of a cyber attack in cases where a reduced share price anecdotally represents a significant cost for a firm.

  This may also affect other costs that we do currently try to capture, including downgraded credit ratings and loss of donors or other (non-share) investment. In these cases, we acknowledge the relative difficulty of making these costs completely attributable to a cyber incident. Their inclusion may make the final estimate represent the *upper limit* of the cost, rather than the true cost.

- **Attribution (other breaches)** – some of the costs that are associated with a firm's response to a cyber security breach or attack may be the cumulative result of multiple breaches. Organisations are asked to self-identify the extent to which a cost is directly the result of a specific cyber security breach. However, we acknowledge that this approach may lead to bias. Where there is uncertainty, respondents are asked to provide a cost range (e.g. more than £1,000, up to £2,000), to avoid providing false degrees of precision.

- **Uncertainty and permanence of impacts** – some of the costs included in the cost tool, such as loss of intellectual property (IP), are associated with a degree of uncertainty. The cost tool includes specific guidance for respondents when completing these questions in order to ensure that robust and consistent estimates are provided. For example, for lost IP, firms are asked to first clarify how they determined a loss in competitive advantage and later to sense-check how they arrived at the cost they provide, by providing a written description.

  One stakeholder especially highlighted the importance of allowing contextual comments alongside these kinds of costs, so those reviewing the costs could judge which elements were less certain.

  Some long-term costs such as loss of share value, downgraded credit ratings, and customer and supplier attrition also have uncertainty around the permanence of the cost. For example, many of our stakeholders indicated that share prices are known to fall in the aftermath of a breach and then rapidly recover their value months later. Again, the inclusion of these costs (except for loss of share value, which is omitted in the questionnaire) may make the final estimate represent the *upper limit* of the cost, rather than the true cost.

2.5 Case studies

Once the cost tool was developed by the study team and modified following the interviews with stakeholders, the tool was tested with 15 UK businesses and charities that had previously suffered a cyber security breach. These case studies involved the organisation self-completing the cost tool, followed by an in-depth interview with the Ipsos MORI team.

Recruitment

For the most part, these case study participants were recruited from the recontact sample for the Cyber Security Breaches Survey (CSBS) 2020, for which fieldwork took place between October and December 2019. In some cases, we also recruited participants through our recruiter's own business networks.

A purposive sampling strategy was employed, with quotas set to achieve case studies with organisations of different sizes and sectors, and with different types of cyber security breaches. The achieved sample should not be seen as representative of UK organisations as a whole. In addition, while a range of large businesses have been included, the constraints of the CSBS 2020 recontact sample meant that we could not interview very large organisations (e.g. FTSE 350 companies) for these case studies.

In order to recruit organisations for participation in the case studies the study team used a pre-approved business recruiter – the same recruiter that worked on the CSBS 2020 qualitative strand. In addition, we offered participants an incentive (either bank transfers or charity donation) for taking part. This was initially set at £100 and later increased to £200 to improve participation rates (one of the recruitment challenges discussed at the end of this chapter).

We carried out an initial three pilot case studies to test the suitability of the case study topic guide and initial experiences of organisations completing the cost tool. These findings feed into the development of the cost tool for the remaining case studies.

Case study write-ups

The interviews examined how the tool was completed, probed the accuracy of the estimates provided, asked how the tool could be made more useful and whether use of the tool had prompted or could prompt behaviour change within the organisation. The individual case study reports can be found in Chapter 6. They have all been systematically written up with the following information:

- the type of organisation (by size and sector)
- the type of breach they suffered and when it occurred
- their initial estimate of the cost (from CSBS 2020) and how they arrived at this estimate
- the revised cost estimate after using the cost tool
- a summary of their feedback on the cost tool and overall approach to defining and measuring costs (e.g. in terms of sensitivities on the data collection, and how to best encourage or incentivise this kind of assessment and data collection in the future)
- the expected impact on their organisation of using the tool.

Recruitment challenges and revisions in the approach

Recruitment for this project presented a number of challenges, which we document below.

Challenge	Mitigation strategy
Length of the cost tool – as the questionnaire was designed to be comprehensive in the costs captured, it was very detailed and represented a substantial time commitment for respondents. Many potential respondents were put off agreeing to an interview by the length of the Word document or dropped out after starting to complete the survey.	▪ To reflect the detailed nature of the task the study team offered a substantial incentive to motivate participation (£100). This was then increased further during the study (to £200). ▪ In addition, the survey was reformatted to minimise the length and make navigation through the survey easier. Finally, clear instructions were included to provide more instructions for the respondent and reassure that respondents would only be required to answer the questions that were relevant for the cyberbreach experienced by their organisation.
Self-selection of organisations with relatively minor breaches – the initial participants tended to have had relatively simplistic breaches (e.g. a one-off invoicing fraud). This reflects the fact that the time taken to complete the cost tool increases according to the range of impacts that the breach caused. These initial participants were not able to test the whole tool.	▪ Once this issue became apparent, the recruiter was provided with additional instructions to probe the potential respondent during the recruitment stage, to ensure that the breach experienced by the organisation was significant. ▪ The project team also reviewed the CSBS 2020 sample to prioritise organisations that had incurred multiple types of breaches regardless of the cost estimate they gave in that survey – not just those that had incurred single, high-cost breaches.
Identifying the correct person within the organisation – the job title of the person within the organisation with the access to the information required to complete the cost survey may vary by organisation and may be different to the person who completed the CSBS (intended to be the senior individual with most responsibility for cyber security in the organisation). In addition, depending on the organisation multiple people within the organisation may be required to complete the cost tool.	▪ The contact provided in the CSBS acted as a starting point and were asked to engage the relevant people within the organisation when trying to complete the tool. ▪ To assist completion, the cost tool was divided into sections according to which department or team would potentially be best placed to answer the questions in that section. The recommended job titles for each section came from the consultations with industry stakeholders and the pilot case studies. ▪ Where respondents were not able to complete parts of the questionnaire, we also used the interviews to probe who in their organisation would have been best placed to fill those sections in, and why they could not do it for the interview (e.g. due to being busy or not having the relevant information themselves).

Challenge	Mitigation strategy
Limited recontact sample – the initial sample of organisations was taken from the recontact sample from CSBS 2020 and was restricted to the organisations from this survey that had experienced a cyber security breach or attack. This was the best approach within the time constraints for this study (as opposed to trying to screen for eligible businesses through commercial business databases) but left us with a relatively small starting sample.	A number of alternative recruitment strategies were employed in order to increase the number of case studies, including: ▪ snowballing from existing recruits, requesting case study participants to provide additional contacts of peers that might have also experienced a cyber security breach ▪ using contacts within Ipsos MORI, e.g. links from our own IT and cyber resilience team's employees to their peers in other organisations ▪ expanding the scope of the interviews, to carry out more interviews with stakeholders to get a wider perspective of the cost tool. These contacts were provided by DCMS.

3 Literature review

This chapter highlights the key methodological challenges identified in the literature review, the various approaches that previous studies have used to address these challenges, and an overview of the costs and cost categories that have been used in previous studies.

All references for this chapter are included at the end of this report rather than in footnotes.

3.1 Previous work

A internal policy review conducted by the Department for Digital, Culture, Media and Sport (DCMS) in summer 2019 presented a thematic summary of 15 sources. Costs arising from breaches were categorised into *direct costs* and *indirect and long-term costs*, with a series of key categories being identified within each grouping. It was also recognised that costs could be incurred and analysed at several levels – to individuals and to businesses, as well as nationally and globally.

The analysis identified some notable limitations and gaps in current approaches. There was a lack of uniformity in how costs were gathered and calculated, resulting in figures that were not directly comparable between different sources. In addition, there was a lack of continuity in the data collected across different years, with an absence of longitudinal studies based on a consistent sample group and data collection method.

3.2 Summary of findings

The literature provides highly useful context and direction for our study. There are a number of key insights and learnings that have been derived from the literature. The Cyber Security Breaches Survey (CSBS) series (Ipsos MORI, 2019) suggests that the cost of cyber security breaches and attacks to UK organisations is substantial and may have increased over time. In 2019, the mean cost of all breaches for organisations that lost data or assets as a result was estimated to be £4,180, up from £2,450 in 2017.

Although it is understood that the cost of dealing with cyber security incidents is increasing, the actual estimates of these costs vary significantly from study to study. This is because there is no consensus on what cost is being measured (e.g. attacks, incidents, breaches, crimes), which elements to include (e.g. direct, indirect, short term and long term), or how to capture and measure them effectively (e.g. surveys or secondary data collection).

As a result of the fragmented nature of cost estimation, it appears that greater focus has been placed on costing cybercrimes, with less effort going into looking at the costs of non-criminal cyber security breaches, such as incidents related to device failures and staff misuse (intentional as well as accidental). As such, they are taking a narrower view of what can actually constitute a breach and may be amplifying the significance of some cost categories, while overlooking others.

The literature suggests that the disparity in cost estimates can also be partially explained by the fact that businesses display low rates of awareness, monitoring and understanding of the costs associated with cyber security breaches. This makes it challenging for senior decision makers, who may not have cyber security expertise, to conceptualise costs beyond the direct costs of the breach. In addition, the literature suggests that some businesses simply do not even tend to capture the necessary information for calculating costs. These findings have implications for our study, highlighting the need for our costing framework, including the subcategories, to be clearly defined, easy to apply and be underpinned by data which organisations can easily collect.

3.3 Methodological challenges identified in the literature

This section outlines the methodological challenges observed in the reviewed literature in calculating the cost of cyber security breaches.

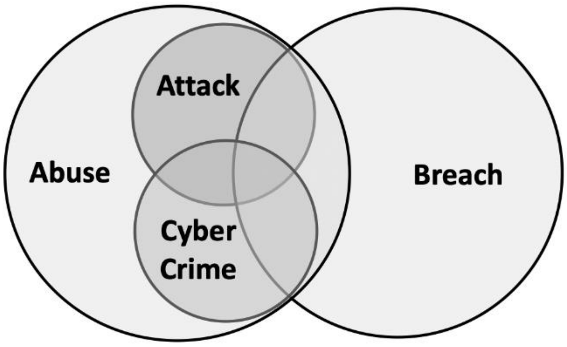
Defining cyber security breaches

Fundamentally, the starting point in unpicking the methodological challenges in costing cyber security breaches, is defining what constitutes a cyber security breach. The literature in this field often presents costing frameworks or methodologies in terms of cybercrimes, attacks or incidents, and not specifically cyber security breaches.

Cyber security breaches and attacks can both be considered forms of incidents. Breaches can, however, occur for reasons other than cyber attacks, and attacks will not necessarily result in breaches.

Cybercrime and cyber security breaches overlap significantly in terms of associated costs. However, cybercrime includes incidents which do not fall within the scope of a cyber security breach. Similarly, breaches can extend far beyond the overlap with cybercrime – device failures and staff misuse can all lead to a cyber security breach but would not ordinarily be considered within the scope of cybercrime.

Furnell (2020) provides an illustration (reproduced below) of how the terms breach, attack and cybercrime, while often used interchangeably, are not the same. The accompanying definitions are below.



- Abuse encompasses any negative and/or undesirable use of technology.
- A breach occurs when security has in some way been compromised and can extend beyond deliberate causes (e.g. accidental or environmental events).
- Attack refers to a deliberate action targeted against another party and may or may not result in a breach (it depends if it is successful).
- Cybercrime results from any illegal use of technology, not just those that constitute attacks.
- An overarching term encompassing all the above would be a cyber security “incident”.

The 2018 Home Office study, Understanding the cost of cybercrime, references their Serious and Organised Crime Strategy’s definition, which theorises that cybercrime can be broken down in two types of criminal activity:

- Cyber-dependent crimes: those which can only be committed using computers, computer networks or other forms of information and communications technology (ICT). They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage.
- Cyber-enabled crimes: those which can be conducted on or offline, but online may take place at unprecedented scale and speed.

The Home Office notes that the costs of cyber terrorism, online hate crimes, cyber bullying, digital piracy or online sexual crimes, should not be considered within the material scope.

As noted above, there is limited consideration in the literature of the costs specifically linked to cyber security breaches. The CSBS does, however, focus on cyber security breaches. It asks individuals to self-report based on a range of categories that are intended to be comprehensive of all types of breaches. However, it stops short of explicitly defining a cyber security breach.

Defining the costs categories within a cyber security breach

Having clearly defined what constitutes a cyber security breach, and therefore which costs are in and out of scope, the next step becomes unpicking the same methodological challenge in determining the boundaries of the specific cost elements associated with a cyber security breach.

Fundamentally, costs can be considered from two perspectives, timeframe and direct vs. indirect. The CSBS considers these as follows:

- direct costs, include:
  - staff not being able to work
  - lost, damaged or stolen outputs, data, assets, trade secrets or intellectual property
  - lost revenue or income if customers or donors could not access your services online
- indirect costs: all other costs can be considered indirect in nature
- long-term costs, include:
  - loss of share value
  - loss of investors, donors or funding
  - long-term loss of customers (including potential new customers or business)
  - handling customer complaints or PR costs
  - compensation, fines or legal costs
- short-term costs: all other costs can be considered short-term in nature.

Therefore, all costs will sit in one of the four quadrants below:

	Short-term cost	Long-term cost
Direct cost	Quadrant 1	Quadrant 2
Indirect cost	Quadrant 3	Quadrant 4

The short-term, direct costs are often the easiest to identify and measure. This is because their impact is realised almost immediately and there is a direct link between the event and the cost that makes it highly tangible to most observers. However, as aforementioned, the direct costs are not always fully captured by organisations.

The key challenges in costing cyber security breaches relate to accurately capturing the indirect and long-term costs (quadrants 2, 3 and 4). Often the issue here is determining what degree of indirect cost or long-term costs can be justified for inclusion. A common example relates to intellectual property (IP) theft. Intuitively, one might expect this to reduce an organisation’s competitiveness within its given market, leading to a loss in profitability. The direct impact on profitability can be captured relatively easily, through a reduction in the market value or revenue of the organisation. However, the indirect, long-term or knock-on effects of the direct impact on profitability may be substantial. These include costs relating to the possible loss in human capital, as employees switch to other organisations as a result of the reduced profitability of the organisation. The problem becomes creating a clear cut, in terms of defining which of these indirect costs can evidently be included within a costing framework.

The indirect and long-term costs included should be based on empirical evidence, rather than theoretical or anecdotal evidence. As such the cost mapping exercise should set clear definitional boundaries for what indirect and long-term costs can be justified for inclusion.

Appropriate inclusion or exclusion of costs

Once costs have been defined, the question becomes which of these costs can be justified for inclusion. Determining the grounds on which certain costs should or should not be included presents a methodological challenge for the accurate calculation of the true cost of cyber security breaches to organisations.

The nature and complexity of cyber security breaches mean that organisations often experience costs of different types and magnitudes depending on the specific breach, as well as the size and sector of the organisation in question. This wide variation within certain cost categories (e.g. reputational damage) makes it challenging to accurately estimate average costs robustly. Consequently, we must determine whether or not estimates are robust enough to justify inclusion within a costing methodology. An interesting example of a cost with a high degree of variance across breaches is emotional harm costs. The issue here is that the magnitude of the cost often rests on the specificities of a given breach.

Although this may be an extreme case, the vast majority of breaches which result in a financial loss will impact upon stakeholders' wellbeing. This includes the wellbeing of employees of the organisation experiencing the breach as well as the individuals who have had their personal data taken, and perhaps misused. In short, the potential for emotional harm could be quite widespread.

The Home Office cost of crime work captures this emotional harm cost through a reduction in an individual's quality of life. Methodologically, this is captured through a reduction in one's quality adjusted life years (QALY). This can be considered as an economic cost but not a financial one.

As emotional harm costs, in terms of quantitative measurement, are somewhat intangible in nature and vary significantly by individual and by breach, it is statistically challenging to create representative samples to accurately capture the nature of these costs. Furthermore, estimates of emotional harm are underpinned by self-reported outcomes data and are thus susceptible to bias of human nature. However, there is potential that, with adjustments to collection approaches, emotional harm costs would be considered robust enough to include within our framework.

A number of potential other cost items can be identified that are not clearly or strongly represented within the existing literature, but which can nonetheless be foreseen as likely to be incurred as a consequence of breaches. Examples here would include costs associated with handling customer complaints, opportunity cost of staff time caused by the disruption to business-as-usual activities, provision of post-breach customer protection, and increases in insurance premium costs. These must nonetheless be recognised within the overall context of estimating the costs arising from breaches and are therefore included in the cost mapping approach proposed by this study.

Self-reporting

The consistency and validity of self-reported data is inherently influenced by factors of human nature such as one's emotional state. Estimating certain costs associated with a cyber security breach rest on self-reported data provided by individuals within an organisation. The element of subjectivity involved in estimating these figures may lead to either an upward or downward bias in estimated costs. Therefore, accounting for self-reporting bias is a key consideration in survey design.

In addition, the self-reported nature of direct data collection means that individuals will only disclose the costs they have recorded, the costs they are *aware of*, as well as the breaches they are aware of (not unidentified ones). Each of these three points highlights the inherent weakness with self-reported data.

Additionally, the scale and structure of some large organisations may simply dictate that no one individual can adequately conceptualise the scale of cost across an entire organisation[2], leading to inaccurate self-reported figures. We have sought to address this in our case studies by involving individuals from across the organisation (with varying perspectives of the cost landscape) in completing the cost tool. This will include finance directors, technical cyber security personnel who deal with breaches from operational standpoint, and Governance, Regulation and Compliance (GRC) stakeholders who might deal with breaches more from a training, culture and compliance perspective. This comprehensive coverage will ensure no tangible costs go uncaptured.

Creating a representative sample for calculating average costs

As previously noted, cyber security breaches are not uniform events. The specificity of each individual breach presents a statistical challenge in terms of creating a large enough sample size to accurately reflect the true cost of a breach. For example, the costs borne by a large organisation as a result of a cyber security breach will be significantly different from the costs borne by small and medium enterprises (SMEs). Therefore, applying average costs to SMEs based on a sample which included cost data skewed towards large organisations would seriously misrepresent the estimated loss to the SME. To mitigate this, we must understand what variables drive variances in costs. Here we have used the example of organisation size. However, empirical evidence also shows that the type of breach experienced (e.g. spread of malware, hacking and Distributed Denial of Service attacks) is one of the key determinants of cost, and must be taken into consideration when looking at subgroups to derive average costs.

Measurement metrics

The complex nature of cyber security breaches and the difficulties in accurately capturing costs has resulted in a lack of consistency in measurement approaches within the field. For example, some studies capture costs as a per-incident cost, others capture costs as an annual cost, or even as a percentage of revenue generated.

Further complicating matters is the fact that a breach could be a single event or a collection of events, for example the Wannacry ransomware attack. Wannacry was one ransomware attack, however an organisation could have had a sustained period of hacking attempts (many incidents) that they class as a single “breach” – part of the same set of incidents that would have always occurred together.

This lack of consistency in how cyber security breaches are quantified means that building upon previous work within the field becomes challenging, as direct comparisons of costs or variables used to calculate costs require greater analytical capacity or, in some instances, may not even be quantitatively possible.

3.4 Methodological approaches

To address the challenges described above, a range of methodological approaches have been employed in the literature, these are described in the following section.

[2] One of the aims of this piece of work is to provide a methodology which organisations can use to accurately calculate their costs.

Survey approaches

One way to estimate costs is to apply a bottom-up approach, which involves identifying each cost separately and then aggregating the costs to arrive at a total cost estimation. In general, costs are identified in consultation with industry experts and estimates are then generated using a firm-level survey.

An example of this approach can be seen in Oxford Economics (2014). Based on existing literature, Oxford Economics developed an economic framework for the impact of cyber attacks on UK firms which explored the motivations and returns for a cyber attack and implications for UK firms. In order to develop the firm-level survey, Oxford Economics worked with the Ponemon Institute, using their existing database of IT professionals, IT security practitioners and other IT related roles. By using a convenience sample as opposed to random probability sampling, the sample cannot be seen as representative of UK firms. Survey respondents self-reported the losses they experienced as a result of a cyber attack.

Another example of the survey approach is Kaspersky (2016). The study surveyed over 4,000 business representatives in 25 countries to assess the economic burden of budgets used to safeguard businesses against potential losses. A component of the survey explored the costs of data breaches and security incidents – beyond cybercrimes. However, the methodology is not explained in detail in the report.

The Ponemon Institute, alongside Accenture Security conduct an annual study on the impact of cyber attacks. Ponemon Institute & Accenture Security (2019), collected data through over 2,600 interviews conducted with 355 companies in 11 countries. Organisations reported their spending in relation to cybercrime over a four-week period. These figures were validated (though the checks and balances used were not disclosed in the report) and aggregated to estimate the average cost to a company over the course of a year.

Survey-based estimates suffer from several methodological limitations. For instance, the non-uniform nature of losses means that a significant proportion of estimates are likely to come from a small number of respondents. In addition, results have often been characterised by the presence of large outliers.

The estimates taken from the survey approach are typically considered to contain a number of biases, although direction of any bias is disputed. Florencio and Herley, 2011 explore these methodological issues in detail. Florencio and Herley, 2011 state that all such cost studies are upwardly biased (due to the fact that cost estimates can only take positive values and so all bias is upwards). However, this is disputed by Oxford Economics, 2014, which argues that the fact that the firms have an incentive to understate the impact of cyber security breaches might in fact lead to a downward bias.

The Cyber Security Breaches Survey (Ipsos MORI, 2019) attempts to address many of these short comings, for example by surveying a representative sample of UK businesses, including those that have different levels of engagement with cyber security. However, the qualitative interviews carried out as part of this study series have regularly revealed that the survey estimates do not capture the full range of costs experienced by firms. This includes, for example, a lack of consideration for intangible or indirect costs, such as reputational damage, and underreporting of time costs.

Causal models

Another approach that has been used to provide cost estimates is a causal model, which provides a framework to assess the impact of cybercrime on businesses. This approach relies on estimates and assumptions, rather than specific examples of cybercrime.

An example of this approach is Detica (2011). In this approach different types of cybercrime are mapped to broad categories of impact. Estimates of specific cost are then made using a three-point estimate (worst case, most likely case and best case). These estimates are informed by consultation from experts in cyber security, business, law enforcement and economics. However, the authors believe the most likely case estimate still underestimates the full cost, due to data sensitivities and underreporting of cybercrime.

The model provides a snapshot, using 2010 as a baseline for market conditions. Therefore, many costs that are associated with a high degree of situational complexity, such as fluctuations in share price value as a result of a cyber security breach, are excluded.

In addition to relying on the suitability of the 2010 baseline, the authors make a number of key assumptions that significantly impact their estimates, such as assuming that all criminal attacks from the National Fraud Authority (NFA) Annual Fraud Indicator were cyber attacks. The strength of the cost estimate depends on the reliability of the assumptions made. While some assumptions are explained, a number of others are made without fully outlining the method behind their derivation.

RAND (2018) also uses a model approach to estimate present and future global costs of cyber risk, reflecting the considerable uncertainty in the frequencies and costs of cyber incidents. Alongside the report is an Excel-based modelling and simulation platform that allows users to alter assumptions and investigate a wide variety of research questions.

In the model, direct costs (output losses experienced by each sector in each country) are calculated based on the share of value added related to a sector *i* of a given country *c*, as well as the output value of that sector in that country. Alongside this, the model incorporates the unitless value representing the fraction of output of industry *i* that is at risk from each type of exposure type, in addition to a unitless value representing the fraction of the exposure at risk for country *c* – for sector *i* that will be destroyed or stolen due to a peril. The direct cost to sector output will be then determined by the sum of the product of the unitless values for each type of peril and exposure – multiplied by the output of a certain sector in a certain country.

As they do not use specific examples of cyber security breaches, these models rely on the strength of their underlying assumptions to produce reliable cost estimates. As stated above, many of the assumptions made in these reports are not fully explained, making it difficult to assess their appropriateness or likely direction of any estimation errors.

Event studies

Both the US Council of Economic Advisors (2018) and Oxford Economics (2014) used event studies to estimate the impact of a cyber security breach on the firms' share value. An event study is a statistical method to assess the impact of an event (the cyber security breach) on the value of a firm.

Event studies typically use the market model[3] to estimate what the return on each individual stock would have been had the event (the cyber security breach) not occurred. Event studies have the advantage of using publicly available data. Thus, their methodology is not dependent on firms disclosing private and potentially confidential information.

This methodology has specific usefulness in estimating the size of reputational costs for the firm. This method is often used alongside other methodological tools. For example, Oxford Economics (2014) captures reputational costs with an event study, alongside a firm-level survey to capture direct costs.

[3] The market model says that the return on a security depends on the return on the market portfolio and the extent of the security's responsiveness.

Case studies

Multiple studies such as US Council of Economic Advisors, 2018 and Oxford Economics, 2014 use in-depth case studies to illustrate the costs of a cyber security breach for a specific firm. Case studies are often included to supplement other methodological methods and provide more in-depth approaches for a specific number of cases. Typically, case studies comprise of a number of interviews with firms, supplemented by secondary research.

Deloitte, 2016 provides a particularly in-depth case study approach looking specifically at two firms and the impact of 14 pre-identified impact factors. Intangible costs were estimated using the following concepts:

- valuation and financial quantification at a specific point in time (i.e. when attack was discovered), calculated through a Discounted Cash Flow Method, which, broadly, entails estimating the present value of the projected economic benefits to be derived from the use of the asset
- with-and-without method, which involves estimating the value of an asset under two scenarios:

  - one, with a certain asset or situation in place (the “situation,” in this context, being the occurrence of a cyber attack)
  - the other without the asset or situation in place (in this case, the absence of a cyber attack).

The difference in these value estimates yields the isolated value impact that can be attributed to the cyber attack.

3.5 Cost typologies

The typology used to group different types of costs is a key difference amongst many of the papers reviewed. The CSBS classifies costs in three ways:

- direct costs
- recovery costs
- long-term costs.

Many UK studies follow the approach established by the Home Office (2005) for measuring the cost of crime. This typology provides a breakdown by:

- costs in anticipation of crime
- costs as a consequence of crime
- costs in response to crime.

A challenge when using this typology is isolating the costs in anticipation that are incurred as a result of the cyber security breach, as opposed to overall investment in cyber security (which the firm would have undertaken even if they had not been breached). This typology was used in the Home Office (2018), which looks specifically at cybercrime using the Cost of Crime framework, as well as in Oxford Economics (2014) and Detica (2011). The primary focus of these two latter studies was on the costs as a consequence of a cybercrime.

Other studies use a diverse range of typologies. Ponemon Institute & Accenture Security (2019) groups costs according to whether they are internal or external. Costs are further broken down into:

- direct costs (the direct expense outlay to accomplish a given activity)
- indirect costs (the amount of time, effort and other organisational resources spent, but not as a direct cash outlay)

- opportunity cost (the cost resulting from lost business opportunities as a consequence of reputation diminishment after the incident).

Looking beyond the costs to the firm, RAND (2018) aims to create a methodology for estimating the present and future global costs of cyber risk. It classifies costs according to whether they are:

- direct costs, which are the costs experienced by each sector in each country
- systemic costs, which are the macroeconomic impacts to output experienced by other sectors, because of the damages by each sector in each country.

The US Council of Economic Advisors (2018) examines the economic cost of malicious cybercrime activity on the US economy. It classifies costs into three groups:

- effect on a firm's value – the Cumulative Abnormal Return (CAR) effect on a firm's stock value
- prevention costs – costs associated with acquiring security products (spam filters, anti-virus protection), training, fraud detection and tracking efforts
- wider economic costs – the wider impact of IP theft in slowing down the rate of development and adoption of new technologies, and thereby lowering the efficiency gains that can be achieved through these new technologies.

Looking at the prior categorisations, it becomes apparent that none of them provide sufficient granularity to enable the costs to an organisation to be clearly understood:

- the Home Office cost categories (i.e. in anticipation, as a consequence, and in response) do not differentiate between those that are directly and indirectly incurred. Additionally, while they appear to be distinct in terms of the time periods relative to a breach, some costs could potentially end up sitting in two or three of these categories depending on when they get addressed (e.g. cost of security controls).

- The CSBS categories (i.e. direct, long term, and recovery) do not necessarily provide a coherent set of distinct labels. While the direct costs are those specifically arising from the breach (e.g. staff prevented from carrying out work; lost, damaged or stolen assets; and lost revenue from customers), the other two relate to the timeframe of the cost and the reason for it. This does not result in a clean partitioning of costs, as there will be some costs that are neither long-term nor recovery-related, and some that might be both, as well as being direct or indirect.

As such, rather than adopting a simple linear categorisation, a more appropriate means of categorisation is to recognise that several distinct dimensions can be applied to the same cost, in order to give an overall characterisation of it. Proposed aspects here are:

- **type** – the binary choice of direct or indirect, denoting those costs specifically linked to a breach and those arising elsewhere as result of it
- **timeframe** – generally, this would be how long after a breach a cost is likely to be incurred, and it is considered useful to identify three periods:

  - **short-term** – relating to the period immediately following the breach or its discovery. These are most likely to be related directly to the impact of the breach or the heightened awareness resulting from it. Examples would be costs of investigation, response, recovery etc.
  - **medium term** – relating to costs incurred once the immediate period of breach is passed. These are likely to involve the cost of resulting investments (e.g. additional security measures) and consequential costs (e.g. fines, compensations payable as a result of the breach).

- **long-term** – relating to costs that persist well after the breach and the initial aftermath of it have passed. Examples would be additional ongoing costs such as insurance premiums, product or service subscriptions and salaries for new cyber security team members.

A further category (e.g. pre-emptive) would need to be added if there is a desire to take account of costs incurred in anticipation of a breach.

As an example of how this might be applied, dealing with customer complaints might be an indirect, medium-term cost. Bringing in data recovery specialists might be a direct, short-term cost.

Some additional points to qualify and explain the proposed approach:

- The approach taken in the cost mapping specifically considers costs at the level of the organisation, rather than focusing on the individual or considering wider contexts such as national or global costs. These other perspectives would change the nature of the potential costs involved, and while this could arguably represent a further dimension in a fully comprehensive framework, it is out of scope in the context of this study.
- It will be relevant to consider how each of the costs are captured. For example, some costs will be estimated or self-reported (e.g. data loss and lost productivity), whereas others will be actual monetary exchanges or be independently verifiable (e.g. loss of share value and payment of fines).
- The 3-point estimates used in the Detica (2011) study (i.e. worst, likely and best-case scenarios) are potentially interesting in understanding what the resulting cost outcomes might look like. However, there would still be a need to utilise, and assess against, the other cost categories in order to determine what the figures here might be. As such, the outcome scenarios could be regarded as an optional layer that could be added onto the main mapping framework.

3.6 Cost identified

The following section outlines some of the main cost categories identified in the literature and describes the different methodological approaches employed in their estimation.

Prevention and defence costs

These can broadly be defined as the costs associated with acquiring security such as spam filters, anti-virus protection, training, fraud detection and tracking efforts. NCC Group Whitepaper (2018) uses the SANS security costing model, which estimates the costs of implementing operational security. Additional costs such as staffing, and consultancy are also added to the existing model.

The cost of prevention and defence could feasibly be included in a firm-level survey. It is likely that many of the firms that have experienced a cyber security breach will have engaged in some prevention or defence costs. However, it is important to isolate which of these are as a result of a cyber security breach and which would have occurred regardless.

This also touches on a more fundamental issue regarding the scope of this research project. Prevention and defence costs could be considered as an organisation’s overall investment in cyber security – costs that they would incur regardless of the breaches or attacks they experience. As such, these costs fall outside the scope of the study, which is focused on the costs incurred as a result of breaches or attacks.

Recovery and response costs

These costs include the ex-post costs of the steps taken to organise the recovery and response to the cyber security breach. These typically include activities associated with repairing and remediating the organisation’s systems and core business processes. These encompass the restoration of damaged information assets and other IT assets, staff not being able to carry out work during the breach, customers or service users not being able to access products or services during the breach, immediate lost productivity, and implementing new controls or processes post-breach to deal with future breaches. Ponemon Institute & Accenture Security (2019) and Ipsos MORI (2019) estimate these costs using a firm-level survey, while Detica (2011) assesses them in their causal model.

Regulatory compliance

Many studies include fines and penalties levied by governments and regulators resulting from the cyber security breach as a direct cost to firms. Crucially, these costs would not be included in studies looking at the overall cost of cybercrime to the economy (such as the Home Office, 2018) as fines are a transfer, and therefore have a net cost of zero. However, for studies estimating costs at firm level, fines and penalties represent a cost which is equal to the size of the fine or penalty paid.

Deloitte (2016) includes the cost of fines or fees levied as a result of noncompliance with cyber security breach-related laws and regulations in their case study approach. However, such an approach may be difficult to replicate, as their methodology relies on accessing sensitive accounting information.

The cost of regulatory compliance could be feasibly included in a survey approach, although this is likely to only be applicable in a small number of high-profile cases.

Extortion

Another direct cost experienced by firms is the cost of extortion, broadly defined as the ransom costs paid by firms to resolve denial of service, flooding of a company server or manipulating the company website. Detica (2011) estimates the cost of extortion to firms in their causal model approach by considering the turnover of small, medium and large businesses, and multiplying these by:

- an estimate made of the proportion of companies that would be vulnerable to extortion
- the probability of an extortion attempt being made
- the probability that it would be successful.

The direct costs to a firm of extortion payments could feasibly be included in a firm-level survey, although it is important to consider that the overall cost of extortion may be above the ransom paid. It may also include additional costs such as reputational damage, further explained below.

Reputational costs

Damage to a firm’s reputation may result in lost business and loss of both existing and potential customers. Due to the intangible nature of a firm’s reputation, these costs are often measured using the effect of the cyber security breach on the firm’s share value as a proxy for reputational damage.

Share price

Several studies look at the effect of cyber security breaches on a firm’s share price. One such study is Comparitech (2018) which attempts to assess the extent to which investors react to data breaches and whether Wall Street punishes companies that leak customer data. To do this the authors analysed the closing share prices of 28 companies listed on the New York Share Exchange that had suffered data breaches resulting in the release of at least 1 million customer records, starting the day prior to the public disclosure of their respective data breaches. The performance of each share was compared with the NASDAQ, which was used as a common standard for overall market performance for the same time period. The study calculated the difference in performance between the NASDAQ baseline and the breach companies.

The US Council of Economic Advisors (2018) and Oxford Economics (2014) also attempt to estimate the effect of a cyber security breach on a firm's value. They use an event study methodology to calculate how market prices react to the news of a cyber attack. A market model is used to calculate the Cumulative Abnormal Return (CAR)[4] to estimate the impact of the cyber attack over the event window.

A challenge faced by all studies that attempt to investigate the impact of a cyber security breach is the quantity of external factors, which also have the potential to affect a firm's share price. Moreover, looking at a firm's share price as a proxy for reputational damage is only relevant for firms listed on the share market.

Intellectual Property (IP) theft

IP theft, defined as the loss of intangible creative knowledge such as trade secrets or patents, is the focus of many studies attempting to estimate the cost of cybercrime, due to its importance in the rate of development and the adoption of new technologies. Costing the impact of IP theft presents several methodological challenges that have been addressed in multiple ways in the literature.

Detica (2011) presents two methods for estimating the cost of IP theft through cybercrime. The first method uses the total research and development (R&D) expenditure for each UK industry sector as a starting point. The expected return on investment as a percentage for this R&D spend was estimated, which created an overall market value for the IP. This value recognises that IP theft does not just lead to short-term losses from R&D spend, but also to future losses from the value that industry sectors would wish to recoup from their initial expenditure.

The second method started with the total cash flow for each UK industry sector, and then estimated the fraction that was attributable to IP within the industry. This calculated the subsequent economic value. Numerous assumptions were made in the calculation of these estimates regarding:

- the total amount of R&D spending in each UK business sector
- the average estimated return on investment that each UK business sector would expect from its R&D spending
- the level of IP exploitability for cyber criminals.

Once the economic value of the IP had been derived from both methods, predictions were made of the probability of cyber theft for each industry sector using three-point estimates, with the subsequent IP exploitability and revenue impact also calculated as a percentage. The scenario approach is necessary as a result of the number of variables involved and the lack of official data. The authors acknowledge that the proportion of IP theft cannot be measured with any degree of confidence. The level of theft depends on the level of motivation of cybercriminals to steal it, which requires additional assumptions to calculate.

IP theft results in a range of potential indirect knock-on effects, including:

- reduced turnover through direct loss of business
- reduced profitability by losing first-to-market advantage and increasing price-competition
- reputational damage caused by disclosure of the theft and arrival on the market of counterfeit goods
- reduction in share price, which may be particularly acute if the company also happens to be an acquisition target

[4] Cumulative abnormal return is a financial term used to describe the value of an investment. Specifically, it describes the relationship between the expected value of a stock given the performance of the market as a whole and the stock's actual value.

- loss of competitive advantage, which may be more apparent in overseas markets
- additional costs incurred through attempts to protect future IP
- opportunity costs, as the company becomes less willing to invest
- redundancies, as R&D facilities and product lines decrease in capacity or are closed
- company failures, particularly if the theft has occurred from an SME, reliant upon IP-enabled sales
- a reduction in investment from overseas.

Oxford Economics (2014) estimates costs to the firm of IP theft, alongside impact on research and development (R&D), through a survey approach where it asks firms to quantify losses due to theft of IP. This form of self-reporting is typically associated with reporting bias, which may diminish the reliability of these estimates. While only a small proportion of firms reported a loss of IP or commercially sensitive business information, these costs were estimated to be significant for the firms affected.

While there are considerable measurement challenges associated with the estimation of IP theft, the literature indicates that they are a significant cost for firms impacted. Therefore, their exclusion would lead to a significant underestimation of the full cost of cyber security breaches for firms.

4 Cost mapping

We created the following cost mapping using a typology of costs that took into account the findings from the literature review and further expert input from Professor Steven Furnell. We first describe the typology used, then provide a definition for all the cost categories included in the mapping, as well as the mapping itself in a table.

4.1 Typology

In developing the cost typology, it was important to make a distinction between costs that were the result of a specific breach and investment in cyber security in general. This study aims to come up with a more comprehensive measurement of the cost *of a specific breach*. As such, the spending associated with preventing breaches in general is outside the scope of the study and is excluded from the cost mapping. This represents a significant deviation from previous cost of crime work, for instance undertaken by the Home Office (2018), where costs in anticipation of crime are an important category.

In addition, the study only focuses on the costs of a cyber security breach experienced by *organisations*, excluding the costs associated with an individual or the economy in general.

We considered replicating the typologies from previous studies. However, these were, in general, not clearly defined or were not mutually exclusive. As a result, a new typology was developed which defined costs according to their type (direct or indirect) and timeframe (short, medium and long term). These are defined as follows.

Type

- **Direct costs** are costs of a cyber security breach that involve a direct monetary exchange.
- **Indirect costs** are costs of a cyber security breach that do not involve a monetary exchange.[5]

Timeframe

- **Short term** relates to the period immediately following the breach or its discovery.
- **Medium term** relates to costs incurred once the immediate period of breach has passed.
- **Long term** relates to costs that persist well after the breach and the initial aftermath of the breach have passed.

We have not put a specific time limit on what is considered short, medium or long term, as this will vary depending on the nature and duration of the breach. For instance, the immediate incident response could last several hours or several days depending on the severity of a cyber attack.

4.2 Cost definitions

The costs included in the cost mapping exercise are defined as follows:

- **change in cyber security practices** – cost of switching Internet Service Providers (ISPs), security providers or products to increase security
- **compensation/discounts –** payments or discounts given to customers affected by the breach
- **complaints (external) –** the cost of contracting additional staff or services to deal with the additional complaints as a result of the breach

[5] These definitions are taken from Cost of Crime: A systematic review, Wickramasekera et al. (2015) and differ from those used in the CSBS which refer more informally to direct, recovery and long-term costs.

- **complaints (internal)** – the additional staff time required to deal with the additional complaints as a result of the breach including the cost of creating a customer service function to respond to the incident
- **consultant fees** – the costs of hiring external consultants to respond to the breach
- **containment** – the costs of activities required to contain the breach such as shutting down other high-risk areas such as insecure applications or networks such as websites or email
- **credit rating/insurance premiums –** damage to long term credit rating/insurance premiums
- **customer attrition** – loss revenue from lost customers including lost future customers
- **cyber ransom and extortion losses –** the costs of any ransom payment made to retrieve access to services denied by the cyber security breach
- **cyber security improvements (opportunity costs) –** the opportunity cost of staff time associated with cyber security improvements to security controls, monitoring capabilities, or surrounding processes, to prevent a similar occurrence in the future
- **cyber security improvements –** the costs associated with cyber security improvements such as improvements to the infrastructure to prevent a similar occurrence in the future
- **data and software loss** – costs of reconstitution, replacement, restoration or reproduction of data or software which have been lost, corrupted, stolen, deleted or encrypted
- **financial theft** – financial losses arising from the cyber security breach including theft of money or theft of other financial assets (e.g. shares)
- **fines –** the cost of fines made to regulators or authorities as a result of the breach
- **insurance excess** – in the case that financial losses arising from a cyber security breach is covered by insurance this cost includes any insurance excess paid by the firm
- **intellectual property theft –** loss of value of an intellectual property asset
- **interruption of business as usual activities (opportunity cost) –** opportunity cost when staff are stopped from carrying out their usual work
- **interruption of service –** revenue loss incurred when customers are unable to access the service during the breach
- **investigation (external) –** the fees paid for external activities employed to uncover the source, scope, and magnitude of the cyber security breach
- **investigation (internal) –** the cost of internal activities necessary to thoroughly uncover the source, scope, and magnitude of the cyber security breach
- **investment/donor/funding loss –** the loss of investors, donors or other funding sources (e.g. crowdfunding) as a result of the breach
- **IT equipment damage** – the cost to damage to IT equipment and other it assets
- **legal –** the cost of legal advice required as a result of the breach
- **long term productivity –** the costs associated with a fall in research and development (R&D) expenditure if firms become more risk averse as a result of the breach resulting in a fall in long term productivity
- **notification costs (authorities) –** the cost involved in cost of reporting the incident to the relevant authorities
- **notification costs (customer) –** the direct expenses associated with informing individuals whose data has been compromised
- **physical equipment damage** – if the IT system affected by the breach is controlling machinery then this may also be damaged as result of the breach (N.B. this does not include damage to the it equipment itself)
- **post-breach customer protection** – the costs associated with additional services to detect and protect against potential efforts to use an individual's compromised personal data for unauthorised purposes
- **PR/marketing activities (external) –** the cost of hiring third parties to repair the brand damage incurred in the breach

- **PR/marketing activities (internal) –** the cost of internal activities to repair the brand damage incurred in the breach
- **recruitment costs –** increase in recruitment costs
- **share value –** the loss in the firm's value as a result of the breach
- **staff costs (long term) –** increased spending on cyber security as a result of the breach including hiring additional cyber security staff
- **staff response (overtime)** – the overtime costs required to respond to the breach
- **staff response costs (contracting external staff)** – the cost of contracting additional staff to respond to the breach
- **supply chain attrition** – lost revenue caused by members of the supply chain no longer willing to do business with an organisation as a result of a breach
- **third party liability** – any pay-outs that are incurred as a result of any law suit that is brought as a result of the breach
- **training costs (opportunity cost) –** the opportunity cost of staff participation in additional cyber security training
- **training costs (internal resources) –** the cost of any non-staff internal resources required for the purpose of additional cyber security training, e.g. room use
- **training costs (external resources) –** the cost of any non-staff resources required for the purpose of additional cyber security training, e.g. hiring a training space for the duration of training
- **training costs –** the cost of hiring external trainers to conduct additional cyber security training.

The following table maps these cost categories against our bespoke typology. The full cost tool (questionnaire) developed to allow organisations to collect estimates of these various cost categories is attached as an annex to this report.

	Short term	**Medium term**	**Long term**
Direct cost	▪ Consultant fees ▪ Cyber ransom and extortion losses ▪ Financial theft ▪ Insurance excess ▪ Staff response (overtime) ▪ Staff response costs (contracting external staff)	▪ Changes in cyber security practices ▪ Compensation/discounts ▪ Complaints (external) ▪ Fines ▪ Investigation (external) ▪ Legal ▪ PR/marketing activities (external) ▪ Recruitment costs ▪ Third party liability	▪ Credit rating/insurance premiums ▪ Cyber security improvements ▪ Investment/donor/funding loss ▪ Staff costs (long term) ▪ Training costs ▪ Training costs (external resources) ▪ Share value[6]
Indirect cost	▪ Containment ▪ Data and software loss ▪ Intellectual property theft ▪ Interruption of staffs' business as usual activities (opportunity cost) ▪ IT equipment damage ▪ Notification costs (authorities) ▪ Notification costs (customer) ▪ Physical equipment damage (not including it equipment damage) ▪ Interruption of service	▪ Complaints (internal) ▪ Investigation (internal) ▪ Post-breach customer protection ▪ PR/marketing activities (internal)	▪ Customer attrition ▪ Cyber security improvements (opportunity cost) ▪ Long term productivity ▪ Supply chain attrition ▪ Training costs (internal resources) ▪ Training costs (opportunity cost)

[6] This has potential to have impacts across the short to long-term timeframe. Several studies have looked at the persistence of a share price depreciation. See Comparitech (2018) for further discussion: https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/.

5 Main insights on the cost tool from the primary research

This chapter brings together the common themes across all the case studies and stakeholder interviews based on their use of the cost tool. It covers organisations' and stakeholders' overall impressions of the tool, the impact it had or could have on organisations, and how they thought it might be refined and taken forwards beyond this research project.

The individual case studies, as well as being synthesised here, have been written up as mini case study reports. These mini reports are provided as an annex alongside this main report.

5.1 Completing the tool

Comprehensiveness of the questionnaire and missing costs

There was a consensus across interviews that the cost tool was extremely comprehensive and allowed organisations to think through every possible cyber security cost. The language used throughout the tool, including the descriptions of the different costs, was also felt to be easy to understand. As a result, participants who completed the questions in the cost tool often emerged with a new appreciation for all the possible different costs that can be incurred.

Nevertheless, there were a small set of potential cost areas missing from the tool that arose in both the case studies and stakeholder interviews:

- **emotional and physical costs**, related to staff wellbeing and morale – for example, staff having to go on sick leave after being directly targeted or impacted by a cyber attack
- **reputational costs that affect individual employees within the organisation** – for example, one interview from an organisation that suffered an invoicing fraud suggested that it had created an air of mistrust around colleagues associated with the incident, affecting working relationships
- **avoidance behaviours** – the cost of an organisation becoming more risk averse and choosing not to invest in certain technologies, or to abandon existing technologies.

These are all indirect costs (i.e. where there is no exchange of money) making them naturally difficult for organisations to estimate. The Home Office (2018) study suggests it is not possible to monetise the softer aspects of these costs, such as the stress to the individual and the impact on working relationships. However, it is possible to monetise certain aspects of staff time, such as the working days lost to sick leave or a loss of productivity – which could be a result of less positive working relationships, staff having to be redeployed or being given reduced access to data or systems.

This kind of estimate would be easier for certain occupations, where the expected output of a team or individual is documented and any loss in productivity can be measured against this. However, for many occupations where the expected day-to-day output for teams or individuals is fluid, estimates of lost short-term productivity would carry great uncertainty. Another consideration is the difficulty of attributing this loss of staff time or productivity to the breach, meaning that these estimates would probably represent the upper bound of such a cost.

Looking at avoidance behaviours, it might be possible to adapt the existing questions estimating reductions in research and development spending as a result of the breach. We expect that these costs would be very bespoke, reflecting cases where organisations were explicitly aware of foregone investment activities. They are also unlikely to be very robust unless there has been specific forecasting done on the expected return on investment.

Another issue that arose in the case studies was the *perception* that certain costs had been missed, when in fact these had been captured in different places within the cost mapping and cost tool. A recurring example is reputational damage, which is split into more granular cost categories such as customer attrition and the cost of PR or marketing activities. The rationale behind this split was to make it easier for users to provide more specific costs, as opposed to an ambiguous single cost figure for reputational damage. However, this raises the point that users may benefit from a fuller explanation of how reputational damage is accounted for in the tool. They might also benefit from seeing the full cost mapping framework (the table in Chapter 4) within a future tool.

Difficult or unclear costs to estimate

In the case studies, a recurring theme was the difficulty of estimating and monetising time costs. One aspect of this was that interviewees often neglected to acknowledge the opportunity cost of their own time – something we discuss in more detail below. Other challenges included:

- time spent on specific tasks or activities not being systematically recorded in some organisations (e.g. if staff do not have to complete timesheets)
- estimates of time being very uncertain for breaches that took place several months ago – which highlights the importance of recording costs when breaches are still fresh in employees' minds
- the people completing the tool not being privy to the salaries of other people in the organisation
- calculating the time cost in hours for staff that are not paid hourly – something which might be automated in a more developed cost tool in the future.

The result of this uncertainty was sometimes a very wide range for the estimated time cost. In one case, an interviewee suggested that the cost of staff working overtime to resolve a breach could have been between £1,000 and £5,000.

Some interviewees also commented on the difficulty of attributing certain spending to a single breach or incident. There was uncertainty around big spending decisions such as investment in new staff training, which might have been introduced at a later stage, but was potentially fast-tracked as a result of the breach. One interview suggested it would be helpful to have more written guidance in the cost tool for deciding the percentage of a cost that is attributable to a single breach. One solution may be for the tool to ask businesses how likely they would have been (between 0% and 100%) to take a particular action anyway and use this in calculating the expected cost attributable to the breach.

Stakeholders and case study participants also raised the likelihood that some of the cost estimates collected in a self-completion tool such as this one would naturally be ambiguous at the point of collection, with the true cost revealing itself years later, or never. The main examples of this included:

- the impact on the share price, which might drop initially but then recover a few weeks later
- the loss of intellectual property (IP), for which the true loss in business competitiveness is not realised until many years down the line
- customer and supply chain attrition, since there was no clear counterfactual to show what these business relationships would have been like in the absence of a breach
- loss of services that are not directly linked to revenue generation, such as organisation websites that are not used to log orders, or access products or services.

Stakeholders agreed that it was the right approach to exclude loss of share value from the cost tool (for the reasons mentioned in Chapter 2, as well as the one above).

By contrast, one stakeholder considered the loss of IP as too important to exclude, given that it would be the most valuable type of asset susceptible to cyber attacks in certain industries. The pharmaceutical, digital tech and life science sectors were mentioned. However, they acknowledged that losses of IP and trade secrets are difficult to address for insurers. Businesses are typically poor at valuing their IP objectively. The real cost may depend on the extent to which the IP is exploited by others in time.

Burden of completion

As we mentioned in the introduction to this report, several individuals in our sample declined to take part because of the length of the document and the sense that it would take them a long time to complete. In some cases, these people were the sole individual in a cyber role in their organisation, and they felt that spending time on this exercise would distract them from their job.

There was also a sense that the tool could be repetitive, asking the same kinds of questions across multiple sections. While this is a side effect of its comprehensive nature and the fact that it tries to collect costs in a systematic way, it makes it more tedious for people to complete.

Perceived irrelevance of certain sections

Some interviewees felt that several sections were irrelevant for the type of breach they had experienced. They felt that the list of questions could potentially be filtered by the type of breach.

However, this is not straightforward, as we had examples of the same type of breach leading to a varied and inconsistent use of the tool. In some instances of invoice fraud or phishing attacks, interviewees only filled out one or two sections, typically relating to the direct costs (e.g. the amount on the invoice). In other case studies, similar attacks were felt to have had far more wide-ranging impacts (e.g. having to notify customers or bringing in cyber security consultants).

Ultimately, this suggests that there may be more appetite to use this tool among organisations that already have an awareness of the range of potential impacts that their breach may have had. By contrast, it may be more difficult to convince those that have had, in their minds, a relatively simple breach with narrow impacts to use the tool – and they are less likely to look through it comprehensively.

Low understanding of opportunity cost

Stakeholders flagged that organisations would find it more challenging to talk about indirect and intangible costs generally. This also reflects findings from the Cyber Security Breaches Survey (CSBS) series, which has regularly found that organisations naturally focus on the immediate direct costs that they can most easily see and understand.

In the case studies, we commonly found that the opportunity cost of time spent responding to breaches was a difficult concept for people to grasp. This was particularly acute when the people completing the tool were the ones at the frontline of the organisation's breach response. These employees were among the least likely to record their own time spent dealing with the breach as a cost, because they felt that this was part of their job and therefore not a cost. This suggests that, where feasible, it may be better for people outside of immediate incident response teams to be put in charge of completing the tool. It also suggests that additional guidance is needed to ensure that people consider their own time as a cost, regardless of whether it is part of their job role to respond to cyber security breaches.

Who is best placed to complete the cost tool?

One of the key unknowns during recruitment was who within the organisation would be the most appropriate person to take charge of completing the questionnaire. In the development stage, it became clear that in many large organisations it would require the input of multiple teams or individuals. In our case studies, this included a mix of IT staff, finance staff, senior management and frontline staff.

In one stakeholder interview, we also discussed the extent to which this mix of people in different roles would differ across organisations. There was a sense that, if the tool was developed and used by FTSE 350 companies, it would be easier to pick out specific management layers or people with specific job titles to take charge of completing the questionnaire – because incident response management in these larger companies had, in recent years, started to follow a very common structure. This includes people in bronze, silver and gold crisis roles, where bronze includes the people dealing with the crisis on the ground and gold would be the senior directors tasked with looking at existential impacts across the whole firm. Someone leading on operational resilience would likely act across all three layers and may be the best person to take the main responsibility for tool completion.

The same stakeholder mentioned a range of people with common job titles that might be called on to help fill in specific parts of the questionnaire, including Chief Risk Officers and Chief Data Officers. Another stakeholder suggested that those responsible for risk management across the business should be put in charge of this cost tool, as they would be a more credible voice than finance or IT teams when presenting the results to a management board.

Confidentiality

Typically, case study participants did not have concerns related to the confidentiality of the data provided, *with the exception of salary levels*. Since the cost tool uses salary levels as part of the calculation to estimate the monetary cost of staff time, it requires the employees using the tool to write down the salaries of the staff impacted by the breach. Some interviewees were unwilling to share the exact salaries or, as previously mentioned, were not privy to this information themselves. This led to the estimates being based on assumed wages or salary bands, leading to greater uncertainty.

It is important to note that the relaxed attitudes towards sharing cost data overall may have partially reflected the type of firms that we included in the case studies – they were generally small and medium enterprises (SMEs) with few reputational concerns relative to larger organisations. Moreover, when probed on this topic, they anticipated that *other* organisations might have confidentiality concerns if providing this kind of information to a third party. Industry stakeholders also suggested that large organisations would be more cautious about completing the tool if they felt that there was a risk of the information being shared (e.g. on reputational damage).

During the recruitment process and interviews, we provided reassurances around confidentiality and the anonymity of organisations and individuals taking part. One potential solution to this problem if the tool's use becomes more widespread may be for some parts of the tool to be administered with the help of a third party like an insurance company and other parts (e.g. on topics like customer complaints) to be handled internally, not for wider sharing.

5.2 Potential impact of the tool

More accurate and precise (but still subjective) costs

One of the key objectives of this study was to ascertain whether organisations were systematically underestimating the cost of cyber security breaches, and whether a tool such as the one we developed could help them to better understand the true cost. Broadly speaking, interviewees felt that the cost estimates they collected with the help of the tool were better informed than the cost estimates they provided in the CSBS (which were recorded again when we recruited case study participants).

Typically, interviewees revised their cost estimates upwards and gave a more precise figure. Sometimes these were relatively minor adjustments, with a small number of additional types of costs added to the previous CSBS estimate. For example, one organisation that had paid a £9,000 fraudulent invoice after a phishing attack revised their total cost estimate up from £10,000 to £13,625 after a more comprehensive consideration of the following costs:

- staff being unable to carry out day-to-day work
- the cost of customised internal training following the breach
- having to remove certain information from their website.

In some cases, the rise in the cost estimates between the CSBS and the case studies was more dramatic, which indicates the ongoing uncertainty in the estimates provided. For example, one organisation that experienced regular phishing attacks – and considered these as a single group of incidents for the purpose of the case study – initially gave a cost of £0, as none of these attacks was successful. When using the cost tool, they revised this to £8,130 after considering staff time (in terms of staff being stopped carrying out day-to-day work and time dealing with the attacks) and the changes to cyber security practices and training resulting from these breaches. In another case, an IT director of a large business raised their cost estimate for a major ransomware attack from £200,000 to £300,000, after a more thorough reflection of the time cost, data losses and equipment damage.

Both these interviewees acknowledged that their revised estimates had a great deal of uncertainty, for the reasons covered in Section 5.1 (difficulty attributing costs exclusively to the breaches, poor records of staff time and not being privy to staff salary information). This suggests that, ultimately, the cost tool helps users to reflect more deeply on the range of costs they face and provides a framework for estimating costs that might otherwise be entirely overlooked (e.g. time costs), but we must acknowledge that it still creates subjective cost estimates.

In four case studies, interviewees reduced their cost estimates from the original CSBS figure. The new estimates might still, broadly, be considered a more accurate reflection of their costs. However, in one case, the interview revealed that the participant had omitted a£1,000 laptop purchase cost, which would have raised their new cost estimate above their original figure. This again flags the imperfect nature of the cost tool, with the accuracy of the output depending on the level of engagement of the user.

Attitudinal and behaviour change

Case study participants also speculated that these improved cost estimates could lead to a shift in attitudes and behaviours towards cyber security in their organisations. Many of those completing the tool felt they could show it to management boards to improve their understanding of the cost of breaches, justify additional spending or training in cyber security, increase cyber insurance coverage (to cover the potential costs) and encourage more vigilant behaviour and good practice among employees.

In one case study, for example, an organisation had part of their website taken down and their email addresses blacklisted as spam. They eventually ended up changing their email server, several days after the issue was spotted. Upon completing the cost tool, they commented that the cost of changing the email server was low relative to the estimated cost of the breach (between £8,000 and £16,000, depending on attribution of costs) and could potentially have been undertaken sooner if the full cost of inaction had been appreciated.

5.3 Possible refinements and next steps

Format of the survey

A common area of feedback was that the current format of the tool – a Word questionnaire – could be improved. Several participants and stakeholders suggested that it would work better as an online tool or even an app. This would help hide the wiring behind the tool, with respondents only seeing the questions that were relevant to them. It would help respondents complete the questionnaire as quickly as possible.

In addition, an online tool or app could add extra functionality. For example, it would make it much easier to extract the data and add up all the cost estimates that had been compiled. It could potentially make it easier to extract the compiled costs in the form of a report that could be fed back to a management board, investors or shareholders. One suggestion was that, upon completion, the respondent should receive a summary sheet providing the total cost and a breakdown of the individual cost components.

Tailoring the tool for different types of organisations

Stakeholders suggested that the current tool presented a much bigger burden for SMEs than for larger businesses. SMEs would typically not have dedicated cyber teams. They would also lack reliable data or monitoring information on the value of commercially sensitive information or competitive advantage, and they would have less time to research these topics. This also reflects our understanding from other research for DCMS, such as the cyber skills studies, which highlighted that people in cyber roles in SMEs are often performing this function alongside other fulltime duties.[7]

One idea was to produce a “lite” version of the cost tool for SMEs, removing some of the medium and long-term costs that they would be less likely to incur (such as PR or marketing costs) but still allowing them to get a truer sense of the cost of their breach than without any tool. One of our stakeholders suggested using the Pareto principle, so that 80 per cent of the total cost could be estimated in 20 per cent of the total time.[8]

Similarly, it was apparent that different sectors would be likely to face different types of costs and, in a similar way as for SMEs, the tool could be tailored to different sectors to reflect this. For instance, schools and health services would not experience a loss in IP. However, this would be an important cost area for a pharmaceutical company, who may expect to see it earlier in the list. Similarly, revenue loss would not be a factor for a public sector organisation. Reputational damage is likely to be more important for finance and insurance firms. The need to segment the tool for different audiences is another reason in favour of eventually moving its development to an online tool or app.

Use by third parties

In stakeholder interviews, we explored how the tool might benefit third parties such as cyber security consultancies, insurance companies, client organisations, and investors and shareholders. Case study interviewees also had a small amount to say on investors and shareholders seeing the cost data compiled after a breach. Our evidence on these topics is relatively anecdotal – our interviewees had not used the cost tool in this way themselves and were not listed firms with institutional investors.

- Stakeholders highlighted the potential usefulness of the tool for cyber security consultancies and insurance companies. One said that these bodies had historically struggled to obtain robust and standardised data on breaches. Their hope was that a tool such as this could be used to develop a consistent way for collecting information on the impact of a cyber breach, eventually allowing for better cost comparisons /across different types of organisations (e.g. different sectors) and an

[7] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020.

[8] The Pareto principle (also known as the 80/20 rule) states that, for many events, roughly 80% of the effects come from 20% of the causes.

understanding of the *types* of costs that are more common in certain sectors. In order to make this work, the use of the tool would need to be widespread. This was also thought to be a very long-term ambition, which would take years to achieve.

- In one stakeholder interview, we probed whether a tool like this would provide reassurance to an organisation's clients. They felt that, while it could have this function, there were already accreditations like the ISO 27001 standard that already provided this kind of reassurance effectively. Therefore, they felt it was better to develop this as an introspective tool, rather than something to promote an organisation's cyber security credentials to clients or potential clients.

- One stakeholder suggested that, in general, this tool would be of limited relevance to institutional and individual investors, as they would typically treat cyber security as a second-tier risk. Nevertheless, case study interviewees mentioned that a report based on the cost data collected in such a tool might be of interest to shareholders after a major cyber security breach, as it would help them to understand how far-reaching the impact of the breach was. On the other hand, it might also help to reassure shareholders that the cost of the breach was finite and manageable.

Future uses and promotion

As noted above, the survey has the potential to change behaviour in organisations. The case studies suggest that it could be promoted as a tool to help:

- carry out a formal cost-benefit analysis to prove the value of *existing* cyber security approaches
- build a business case for *increasing* existing investment in cyber security, including additional cyber security insurance, or associated training
- position cyber security on an organisation's risk register
- provide additional evidence to support an insurance claim or police report.

Across our case studies, the tool was generally positively received and we explored the possibility of rolling it out more widely. The primary feedback from case study interviewees was, as previously noted, to develop the tool to be more user-friendly and less burdensome, i.e. as an online tool or app, and potentially with a "lite" variant for less complex breaches.

One stakeholder commented that it would be best rolled out as a government-backed tool, potentially as part of the package of guidance and tools that the National Cyber Security Centre (NCSC) offers to organisations. They also highlighted the important role that regulators such as the Financial Conduct Authority (FCA) could play in promoting the tool and encouraging its use.

References

Comparitech (2018) How data breaches affect stock market price

DCMS (2019) Literature Review: Calculating the Costs of Cyber security breaches

Furnell (to be published in July 2020) “Technology Use, Abuse, and Public Perceptions of Cybercrime” in The Palgrave Handbook of International Cybercrime and Cyberdeviance, Holt and Bossler (Eds.), Palgrave Macmillan

Ipsos MORI (2019) Cyber Security Breaches Survey, DCMS

Deloitte (2016) Beneath the surface of a cyber attack

Detica (2011) The Cost of Cybercrime

Florencio, H (2011) Sex, lies, and cyber-crime surveys

Home Office (2005) The economic and social costs of crime against individuals and households 2003/04

Home Office (2018) Understanding the Costs of Cybercrime

Kaspersky (2016) Measuring the financial impact of IT security on businesses

OECD (2017) Enhancing the role of insurance in cyber risk management

Oxford Economics (2014) Cyber Attacks: Effects on the UK

Ponemon Institute & Accenture Security (2019) The Cost of Cybercrime

RAND (2018) Estimating the Global Cost of Cyber Risk

The NCC Group Whitepaper (2018) The Economics of Defensive Strategy

US Council of Economic Advisors (2018) The cost of malicious cyber activity to the US economy

List of annexed documents

The following documents have been provided as annexes alongside this report:

- long list of literature review documents
- literature summary table – providing summaries of the shortlist of 15 documents
- final cost tool (as a Word/PDF self-completion questionnaire to be further developed)
- 15 full case study summaries.

Ipsos MORI’s standards and accreditations

Ipsos MORI’s standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a ‘right first time’ approach throughout our organisation.

ISO 20252

This is the international market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos MORI was the first company in the world to gain this accreditation.

ISO 27001

This is the international standard for information security designed to ensure the selection of adequate and proportionate security controls. Ipsos MORI was the first research company in the UK to be awarded this in August 2008.

ISO 9001

This is the international general company standard with a focus on continual improvement through quality management systems. In 1994, we became one of the early adopters of the ISO 9001 business standard.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation.

Data Protection Act 2018

Ipsos MORI is required to comply with the Data Protection Act 2018. It covers the processing of personal data and the protection of privacy.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI Public Affairs

Ipsos MORI Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.

Ipsos MORI