KPMG

Economic modelling of sector specific costings of cyber attacks

A KPMG report for the Department for Science, Innovation and Technology

April 2025

This research was supported by the Department for Science, Innovation & Technology and the R&D Science and Analysis Programme at the Department for Culture, Media & Sport. It was developed and produced according to the research team's hypotheses and methods. Any primary research, subsequent findings or recommendations do not represent Government views or policy.

Important notice

This Report has been prepared by KPMG LLP ("KPMG") solely for the Department of Culture, Media and Sport ("DCMS" or the "Client") in accordance with the terms of engagement agreed between DCMS and KPMG, dated 4th November 2024.

This Report is for the benefit of only the Client and the other parties (specifically the Department for Science, Innovation and Technology ("DSIT") that are included as beneficiaries of this research within the Agreement) that we have agreed in writing to treat as parties to the Agreement (together the "Beneficiaries").

This Report has not been designed to be of benefit to anyone except the Beneficiaries. In preparing this Report we have not taken into account the interests, needs or circumstances of anyone apart from the Beneficiaries, even though we may have been aware that others might read this Report. We have prepared this Report for the benefit of the Beneficiaries alone.

We have not verified the reliability or accuracy of any information obtained in the course of our work, other than in the limited circumstances set out in the Agreement.

This Report is not suitable to be relied on by any party wishing to acquire rights against KPMG LLP (other than the Beneficiaries) for any purpose or in any context. Any party other than the Beneficiaries that obtains access to this Report or a copy (under the Freedom of Information Act 2000, the Freedom of Information (Scotland) Act 2002, through Beneficiary's Publication Scheme or otherwise) and chooses to rely on this Report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility or liability in respect of this Report to any party other than the Beneficiaries.

In particular, and without limiting the general statement above, since we have prepared this Report for the benefit of the Beneficiaries alone, this Report has not been prepared for the benefit of any other Government Department nor for any other person or organisation who might have an interest in the matters discussed in this Report.

Our work commenced on 4th November 2024 and our fieldwork was completed on 31st March 2025. We have not undertaken to update our Report for events or circumstances arising after that date.

Contents

Executive summary

Context for the study

DCMS and DSIT are commissioning various programmes of work to quantify the cost of cyber attacks to the UK economy. As part of this, KPMG, with support from Professor Madeline Carr and Chloe Colomer from University College London (UCL), was commissioned to undertake research into the sector specific costs associated with cyber attacks in the UK, including how the costs of cyber attacks on businesses vary by size of firm and by type of cyber attack. This report sets out the findings from the research.

In the development of this study, a number of steps were taken to gather evidence and establish and implement an appropriate methodology for modelling the sector specific costs of cyber attacks on businesses in the UK. The steps involved a systematic literature review; analysis of existing surveys and databases, including DSIT's Cyber Security Breaches Survey (CSBS)[1], KPMG's Industry Insights Database (IID) and other sources; as well as workshops with DSIT and cyber sector subject matter experts from both KPMG and UCL to refine the modelling and assumptions.

Modelling of sector specific costs of cyber attacks

In order to model the sector specific costs of cyber attacks on businesses, rather than conduct new primary research in the form of surveys (which carry significant limitations including poor response rates and lack of knowledge on the subject matter from participants, particularly around the cost of a cyber attack), existing data and literature on such costs was drawn upon. A range of existing surveys and databases containing data on the costs of cyber attacks, split by sector, were investigated and analysed. These included:

- DSIT's CSBS[2] which, since 2017, has surveyed UK businesses to inform government policy on cyber security and which collects information on both the prevalence and costs of cyber attacks experienced by UK businesses.
- KPMG's Industry Insights Database (IID) which is a database of cyber attack costs containing approximately 1,500 individual datapoints on the costs of cyber attacks affecting organisations.
- A range of publications drawn from the literature review which estimate the costs of cyber attacks split by sector. The most notable of which included (but was not limited to): Cyentia's Information Risk Insights Study (IRIS) 2022[3], the Cybersecurity and Infrastructure Security Agency (CISA) Cost of a Cyber Incident: Systematic Review and Cross-Validation report[4] and the IBM Cost of a Data Breach Report[5].

These sources were used to obtain estimates of the value of costs associated with cyber attacks on businesses, as well as to sense check some of the estimates derived from our modelling. Where available, additional sources were used to sense check the estimates for the costs of cyber attacks by sector, size of firm and type of cyber attack. This was done in order to provide a more comprehensive assessment of how the estimates from the model compare to other estimates/information (e.g. estimates of the probability of a cyber attack and the cost of a cyber attack).

The study identified that robust and comprehensive data on the costs of cyber attacks is scarce. Moreover, where reports and databases, like those outlined above, do provide information on the costs of cyber attacks, they each have their limitations. As a result, and following a consideration of the relative merits of the various available data sources, data on costs of cyber attacks reported by Cyentia[6] was identified as the most appropriate source for estimating the costs of cyber attacks for

[1] Cyber Security Breaches Survey - GOV.UK
[2] Cyber Security Breaches Survey - GOV.UK
[3] IRIS-2022_Cyentia.pdf
[4] Cost of a Cyber Incident: Systematic Review and Cross-Validation
[5] Cost of a data breach 2024 | IBM
[6] IRIS-2022_Cyentia.pdf

this study. The Cyentia report provides data drawn from a large dataset of cyber incidents predominantly from the United States (US), and provides information on a range of factors including the costs of significant (see below for more detail) cyber attacks split by sector, size of firm, and type of cyber attack – all on a consistent basis. Importantly for the purposes of this study, the use of the Cyentia report provides for transparency and replicability (the report is publicly available and can be used by DSIT to update the model inputs as needed in the future as and when new data is released); and robustness (being based on a large dataset of cyber incidents and associated costs).

The CSBS is the only source of UK cyber attack cost and likelihood estimates that was identified as part of this work. While the data on the likelihood of UK businesses experiencing a cyber attack is used in parts of this study, the sampling approach used in the survey means that it will likely exclude the most financially damaging cyber security attacks that affect a very small number of UK organisations in a very extreme way.[7] Moreover, even where cyber attack costs are reported in the CSBS, the accuracy of the financial costs reported is questionable.[8] For these reasons the Cyentia report is used to estimate cyber attack costs rather than the CSBS.

As a result, the modelling uses data from the Cyentia report to produce estimates of the average costs[9] of significant cyber attacks split by both sector and size of business converted from US dollars into UK pound sterling using the OECD's purchasing power parity (PPP). The Cyentia data captures cost data on successful cyber attacks, typically those with a cost of over £500.[10] In this study we refer to such cyber attacks as significant cyber attacks. To then scale the average costs of a significant cyber attack to an estimate of the overall cost to businesses of significant cyber attacks at the UK economy level, information on the likelihood of a significant cyber attack[11] from the CSBS[12] is coupled with business count data from the Office for National Statistics (ONS)[13]. Full details of the approaches to the modelling, including assumptions applied and data sources used, are provided in Section 4.

When interpreting the findings of this study on the costs of cyber attacks there are some key limitations to be aware of:

— There is a lack of reliable evidence on the cost of cyber attacks experienced by businesses within the UK (and other countries) which contributes to a heavy reliance within available literature on data from the US. This is likely to be, in part, due to the regulatory requirements in the US, where multiple legal frameworks[14,15,16] oblige organisations to publicly disclose breaches or cybersecurity attacks. While the Cyentia report relies on US data, which represents the largest drawback to using the Cyentia report, there are reasons to believe that the costs of cyber attacks reported will be broadly representative of the costs experienced by organisations within the UK. As set out in

[7] Given the CSBS is a sample survey, rather than a census of businesses, it may well miss some of the most financially damaging cyber security attacks that tend to affect a very small number of UK organisations, in a very extreme way. This is recognised by DSIT in the technical report accompanying the CSBS 2024 report (Section 1.2).
[8] This is because, as noted in the CSBS technical report, many organisations do not monitor their costs (in relation to cyber incidents) and given the survey may miss some of the most financially damaging cyber security attacks respondents may underestimate the true economic cost of breaches or attacks.
[9] As noted in the literature review (see Appendix 1), the distribution of cyber attack costs usually exhibits a long tail – i.e. there are a very small number of very costly attacks. This means that taking the arithmetic mean of costs (that is adding up all the costs of cyber attacks experienced by businesses and dividing by the number of firms experiencing a cyber attack) is likely to overstate the actual cost of most cyber attacks because of the existence of a few very costly attacks. As a result, this report makes use of the geometric mean to estimate the average cost of a significant cyber attack. Using the geometric mean (which multiplies all the 'n' observations of cyber costs together and then takes the nth root) provides a means of reducing the impact of outliers in the data
[10] IRIS-2022_Cyentia.pdf
[11] The CSBS 2024 provides information on 'negative outcomes' resulting from a cyber attack which include things like: website taken down; money stolen; software or systems corrupted; personal data stolen; and loss of access to files or networks among others. See Section 4.5 of Cyber security breaches survey 2024 - GOV.UK. This is coupled with attacks that are recorded as costing at least £500 to derive what is called in this report a significant cyber attack.
[12] Specifically the CSBS is used to understand the proportion of cyber attacks by size of firm that result in both a negative outcome (as defined by the CSBS) and a cost of at least £500 (so a not insignificant cyber attack).
[13] The analysis used data the number of businesses in the micro, small, medium and large size categories from: UK business: activity, size and location - Office for National Statistics
[14] O. for C. Rights (OCR), 'Summary of the HIPAA Privacy Rule'. Accessed: Feb. 04, 2025. [Online].
[15] 'Gramm-Leach-Bliley Act | Federal Trade Commission'. Accessed: Feb. 04, 2025. [Online].
[16] 'SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies'. Accessed: Feb. 04, 2025. [Online].

Section 3.5, given the similarity of the two economies[17]; the global nature of cyber threats; similar cyber vulnerabilities in both the US and UK (as illustrated by the joint initiatives to tackle such vulnerabilities[18]); and a similar commitment to cyber security[19]; it is reasonable to assume that the costs of a cyber attack on US organisations are likely to be similar to those experienced by organisations in the UK.

— Where data does exist, it is generally not available at a sufficiently granular level to allow for disaggregation by sector, size of business, and attack type in the way required for this work.

As a result of these limitations, to generate estimates for costs split by sector, size and attack type, a number of assumptions have to be applied. While assumptions were informed by available data and information from the literature review and other sources, alongside expert input, inherent data limitations mean that the results of the modelling should be treated as indicative only.

Results of the modelling

The average cost of a significant cyber attack for an individual business in the UK is estimated in this study to be £194,729 (in 2024 prices and based on underlying US data). When scaled based on the proportion of UK businesses estimated to experience a significant cyber attack[20], the modelling estimates a total cost to businesses at the UK economy level of £14.7 billion (based on underlying US data), representing 0.5% of the UK's annual Gross Domestic Product (GDP)[21].

However, it is noted that estimates of the total cost of cyber attacks to an economy vary widely and are based on a range of different methodologies.[22] In this study the total cost to businesses of significant cyber attacks at the UK economy level is primarily based on two variables: the average cost to business of a significant cyber attack and the likelihood of experiencing a significant cyber attack. Robust data on both variables is scarce. As a result, the estimate of the total cost of significant cyber attacks on businesses at the UK economy level should be considered as indicative only.

Considering costs at the sector level, Table 1.1 shows the modelling estimates of the average cost of a significant cyber attack for an individual business in the UK split by sector and size of firm and based on underlying US data.

[17] See for instance the share of service sector in both economies in OECD Economic Surveys: United Kingdom 2024 | OECD and OECD Economic Surveys: United States 2024 | OECD

[18] CISA Partners with ASD's ACSC, CCCS, NCSC-UK, and Other International and US Organizations to Release Guidance on Edge Devices | CISA and ASD's ACSC, CISA, and US and International Partners Release Guidance on Choosing Secure and Verifiable Technologies | CISA

[19] See: Global Cybersecurity Index which illustrate that both the UK and US are in the top 10 countries for commitment to cyber security reflecting legal, technical and organisational measures in the two countries.

[20] Using data from CSBS 2024

[21] This figure uses GDP at market and current prices for 2024

[22] Cost of a Cyber Incident: Systematic Review and Cross-Validation

Table 1.1: Estimates of the average cost of a significant cyber attack for a UK organisation split by sector and size of firm by turnover (2024 prices and based on underlying US data)[23]

Sector	Micro	Small	Medium	Large	Average across all firms
Utilities	£93,665	£137,687	£124,245	£436,443	£210,837
Construction	£39,540	£58,926	£53,173	£149,340	£46,695
Manufacturing	£203,071	£293,337	£264,699	£846,619	£330,406
Trade	£161,644	£233,603	£210,797	£591,913	£224,280
Retail	£206,264	£306,183	£276,290	£919,026	£250,457
Transportation	£215,176	£326,481	£294,607	£951,442	£261,070
Information	£240,843	£364,709	£329,103	£1,101,588	£336,773
Financial	£203,811	£304,920	£275,151	£908,294	£309,181
Real Estate	£81,227	£122,551	£110,586	£374,666	£92,683
Professional	£240,453	£363,889	£328,363	£968,187	£271,683
Management	£225,566	£281,715	£254,211	£681,067	£333,943
Administrative	£115,702	£177,210	£159,909	£505,734	£129,474
Education	£69,771	£104,952	£94,706	£244,622	£98,343
Healthcare	£121,503	£181,636	£163,903	£483,312	£149,284
Entertainment	£298,780	£455,160	£410,723	£1,354,368	£331,113
Hospitality	£137,661	£206,022	£185,908	£555,397	£153,529
Other Services	£67,102	£102,043	£92,081	£246,037	£72,873
Public	£101,197	£113,848	£102,733	£216,653	£102,588
All sector average	**£152,766**	**£236,832**	**£216,818**	**£712,349**	**£194,729**

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data.
Note: The data in this table is based, predominantly, on underlying US data and is converted from US dollars to UK pound sterling using the OECD's PPP.

When interpreting these results, it is helpful to compare to existing cost estimates. Looking at the overall average cost across sectors and by size of firm, the figures from the modelling are substantially higher than those produced by the CSBS. However, as noted earlier, there are questions around the accuracy of financial costs reported in the CSBS. The average cost figures across sectors from the modelling are generally higher than the figures quoted in reports that use insurance data (such as NetDiligence). However, the sector average estimates from the modelling are lower than the figures reported in the IBM cost of data breach report – which only considers the costs of data breaches but also incorporates the wider costs of these cyber attacks. Whilst the IID does not provide estimates of the average total cost of significant cyber attacks, the estimates in the table above fall within the range of cost estimates produced for different significant cyber attacks for the financial, information, retail, manufacturing and real estate sectors from the IID. As a result, the cost estimates set out in Table 1.1 above fall within the broad range of different cost estimates available in the literature as well as the cost estimates contained in the IID (used for commercial cyber security purposes).

In terms of the average costs of a significant cyber attack by sector, Table 1.1 shows that it is estimated the information sector faces the highest average cost of a significant cyber attack overall, with the entertainment, management and manufacturing sectors also experiencing high average costs. The construction and real estate sectors are among those with the lowest average costs of a significant cyber attack. This ranking appears to be broadly consistent with other reports and analysis – for instance, whilst the IBM report[24] (on the cost of data breaches) finds healthcare to have the highest cost of a data breach, it highlights the financial, industrial and technology sectors as also experiencing high costs. From a UK perspective, whilst there is a lack of sector specific data on costs of cyber attacks, the Department for Education (DfE) does collect information on the costs of cyber attacks experienced by state schools through its risk protection arrangement (RPA). The data collected by the RPA is confidential so underlying data cannot be reported, however, the data does suggest that the average cost of a cyber attack for the education sector estimated in this study (as set

[23] The size bands used in this study are: Micro: turnover up to £0.65 million (including unknown); Small: turnover of £0.65 million to £6.5 million; Medium: turnover of £6.5 million to £65 million; and Larger: turnover over £65 million. See Section 4 for more detail. Whilst Cyentia data relates to 2022, cost figures have been uprated to 2024 prices using GDP deflators.
[24] Cost of a data breach 2024 | IBM

out in Table 1.1 above) is in line with their own data. This provides some corroboration of the modelled estimates regarding their applicability to UK sectors.

There are no consistent definitions of the different types of cyber attacks experienced by businesses across different reports and data. This makes it difficult to assess the reliability of the costs of different types of significant cyber attacks estimated by the model, and, as a result, such estimates should be considered as indicative only. Nevertheless, in relation to average costs of a significant cyber attack by type of attack, Table 1.2 sets out estimated costs below. Modelling to split these costs across sectors would rely on an underlying assumption that the prevalence of each of these types of attacks is the same across sectors, which evidence from the Cyentia report suggests is not the case. Therefore, results are split by type of attack only.

Table 1.2: Estimates of the average cost to a UK organisation of a significant cyber attack split by type of attack (2024 prices and based on underlying US data)

Type of cyber attack	Total
Accidental disclosure	£43,546
DoS attack	£97,560
Insider misuse	£89,817
Physical threat	£62,083
Ransomware	£210,128
Scam or fraud	£2,564,422
System failure	£1,170,714
System intrusion	£236,818

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data.
Note: The data in this table is based, predominantly, on underlying US data and is converted from US dollars to UK pound sterling using the OECD's PPP.

In terms of the different components of the cost of a significant cyber attack, (i.e. Home Office categories of: costs in response; costs as a consequence; and cost in anticipation[25]) the literature notes that studies typically fail to disentangle costs into these categories.[26] It is therefore difficult to be definitive about the share of significant cyber attack costs that can be attributed to each of the Home Office definitions. However, the available evidence[27] suggests that costs are reasonably evenly split between costs in response to, and costs as a consequence of, a significant cyber attack (and do not include costs in anticipation which are considered as business as usual costs).

[25] The economic and social costs of crime and Understanding the costs of cyber crime
[26] See for instance: 'Cost of a data breach 2024 | IBM' - https://www.ibm.com/reports/data-breach and Cybersecurity and Infrastructure security agency, 'Cost of a cyber incident: systemic review and cross validation', 2020.
[27] See for instance: NetDiligence (2019); Ponemon Institute (2017); and Kaspersky Lab (2017, 2018). Data and information for these reports are summarised in CISA - Cost of a Cyber Incident: Systematic Review and Cross-Validation

2 About the study

2.1 Introduction to the study

The UK Government Department for Culture, Media and Sport (DCMS) is running a Research & Development Science and Analysis Programme across DCMS and the Department for Science, Innovation and Technology (DSIT). The Programme is focused on delivering longer term (3-5-10 years in the future), more cross-cutting, and more experimental approaches to research than traditional methods of evidence development within the Departments.

One area of work under this Programme relates to quantifying of the cost of cyber attacks to the UK economy. Quantifying the cost of cyber attacks to the economy is a challenging exercise, and is currently without an established, consensus methodology. To demonstrate the importance and urgency of enhancing the UK's cyber resilience and capabilities, the UK government is looking to develop a robust and comprehensive methodology to estimate the economic impact of cyber attacks on the UK.[28]

To support this programme of work, KPMG, with support from Professor Madeline Carr and Chloe Colomer from University College London (UCL), was commissioned by DCMS and DSIT to undertake research to improve the UK Government's understanding of the sector specific socio-economic costs associated with cyber attacks, including how the costs of cyber attacks vary by size of firm and by type of cyber attack. Such costs include, but are not limited to, costs associated with reputational damage to organisations post attack, direct and indirect costs to organisations of personal data lost/stolen, ransom payments made and recovery time cost for business.

In addition to the impact on individual organisations, DCMS and DSIT also want to understand how cyber attacks and fear of attacks may impact specific sectors and the economy more widely.

This report sets out the findings of this research.

2.2 Scope of the study

At the inception of this study, a workshop was held with DSIT and UCL to co-design the questions and objectives for the research. A research plan was developed as a result of the workshop, which included the following agreed research questions and sub questions:

- What are the sector specific[29] socio-economic costs associated with cyber attacks in the UK?
- How do these costs vary by type of cost?[30]:
  - costs in anticipation[31]
  - costs as a consequence[32]
  - costs in response[33]

[28] Department for Culture, Media & Sport (2024) Invitation to Tender (ITT) For: Contract for services: R&D Science and Analysis Programme – Economic modelling of sector specific costings of cyber attacks
[29] Following the research design workshop, DSIT confirmed that the main sectors to consider were: financial services; manufacturing; retail; real estate legal services (i.e. conveyancing); and broadband services (part of the information and communication sector).
[30] The three different types of cost outlined (i.e. anticipation; consequence; and response) are derived from the Home Office's cost of cyber crime framework: Understanding the costs of cyber crime
[31] This should include but is not limited to the costs associated with the implementation of specialist staff or money spent on upskilling existing cyber security technicians and staff across an organisation and the implementation of new cyber security technology and process. This could also look at more technical memory safety fixes and estimate the costs of improving these.
[32] This should include but is not limited to costs associated with reputational damage to organisations post attack, direct and indirect costs to organisations of personal data lost/stolen, ransom payments made and recovery time cost for business.
[33] This should include but not be limited to costs associated with reporting and administrative costs, fines and legals costs, PR costs, new IT/training/intervention as a direct response to the incident, people employed via private sector to investigate (as opposed to law enforcement investigating)

- How do these costs vary by type of cyber attack?:
  - phishing
  - hacking of bank details
  - hacking of emails
  - devices being targeted with other malware (e.g. viruses or spyware)
  - takeovers or attempts to take over email or social media accounts
  - ransomware
  - distributed denial of Service (DDoS)
- How do these costs change depending on organisation size?:
  - large (employees >=250 and turnover > £50 million)
  - medium (employees >=50 and < 250 and turnover <= £50 million)
  - small (employees >=10 and < 50 and turnover <= £10 million)
  - micro (employees < 10 and turnover <= £2 million)
- How do these costs vary by sector[34] and what factors drive costs by sector?
- How prevalent are cyber attacks by sector? Including:
  - are some sectors impacted more so by attacks than others?
  - are some sectors targeted more so than others?
  - are some sectors better prepared than others?
  - are some sectors better equipped to deal with attacks than others?
  - are there any unique considerations for the DCMS and DSIT sectors[35]?

As part of the research design workshop, the following broader research interests were also discussed, but were identified as lower priority:

- Who are the bearers of the costs of cyber attacks? To include:
  - organisations who are directly and indirectly the victim of an attack
  - costs associated to the wider supply chain as a result of an attack
  - costs to the individual
  - cost to the sector
  - cost to the wider economy
- What proportion of attacks are related to memory safety?
- Does the malicious use of Artificial Intelligence (AI) in cyber attacks increase the prevalence of successful cyber attacks?
- Does the malicious use of AI in cyber attacks increase the likelihood of harm associated with cyber attacks?
- Does the malicious use of AI in cyber attacks increase the cost of harms associated with successful cyber attacks?

It was agreed that the study would report on any relevant insights or evidence in relation to these themes that were identified through the course of the research rather than prioritising them.

The vast majority of the research questions were to be answered through research and analysis conducted in the development of a model. The model provides estimates of the cost of significant cyber attacks split by sector, size of firm and by type of cyber attack. These estimates would then be scaled to the UK economy wide level. The model design is intended to allow for DSIT to update

[34] Following the research design workshop, DSIT confirmed that the main sectors to consider were: financial services; manufacturing; retail; real estate legal services (i.e. conveyancing); and broadband services (part of the information and communication sector).
[35] These include among others: arts, creative industries, digital, media, tourism and sport sectors.

estimates of the costs of significant cyber attacks over time as new data and information become available.

2.3 Approach to the study

2.3.1 Overview of approach

In the development of this study, the following key steps were taken to gather evidence and establish and implement an appropriate methodology for modelling the sector specific costs of cyber attacks in the UK:

- Systematic literature review to understand the availability and robustness of data on the costs of cyber attacks split by sector, size of firm and type of attack.
- Analysis of existing surveys and databases, including DSIT's Cyber Security Breaches Survey (CSBS), KPMG's Industry Insights Database (IID) and other sources to understand how they could contribute to the research.
- Workshops with DSIT and cyber sector subject matter experts from both KPMG and UCL to discuss the literature review and the methodology for building a model of costs.
- Iterative model development alongside DSIT to test and review assumptions.

More detail on each of these steps and the approach taken is provided in the sections below.

2.3.2 Literature review

A systematic literature review was undertaken to gather evidence on the sector specific costs of cyber attacks in the UK. A literature review protocol was developed by academics at UCL to set the parameters of the systematic review. The literature review protocol and the findings from the literature review are set out in Appendix 1.

The literature review followed a dual search strategy, combining a systematic review of academic literature together with a focused search of grey literature and news reports. The studies reviewed cover a wide range of geographies, with a particular prominence of studies from the US where the reporting of cyber attacks is more prevalent than in many other countries, largely driven by regulatory requirements.

The literature review identified numerous reports containing data and information which have informed the scope and approach to the analysis and modelling as part of this study. These reports have been used to obtain estimates of the value of costs associated with cyber attacks, as well as to justify or evidence some of the assumptions made to distribute costs of cyber attacks by sector, size of firm and type of cyber attack. The literature review also provides insights into a number of the wider research questions within the scope of this study.

2.3.3 Analysis of existing surveys and databases

In developing the approach to estimating the costs of cyber attacks on different sectors of the economy, a range of existing surveys and databases containing data on the costs of cyber attacks, split by sector, were investigated and analysed.

This included:

- DSIT's CSBS[36] which, since 2017, has surveyed UK businesses to inform government policy on cyber security. The survey explores a number of issues including: the policies, processes, and approach to cyber security for businesses; the different cyber attacks and cyber crimes these organisations face; as well as how these organisations are impacted and respond to attacks.

[36] Cyber Security Breaches Survey - GOV.UK

— KPMG's Industry Insights Database (IID) which is a database of cyber attack costs containing approximately 1,500 individual datapoints on the costs of cyber attacks affecting organisations – taken from a variety of sources including industry publications, other public sources, as well as data from KPMG's internal Cyber Response Services team.

— A range of publications drawn from the literature review which estimate the costs of cyber attacks split by sector. The most notable ones included, but are not limited to: Cyentia's Information Risk Insights Study (IRIS) 2022[37], the Cybersecurity and Infrastructure Security Agency (CISA) Cost of a Cyber Incident: Systematic Review and Cross-Validation report[38] and the IBM Cost of a Data Breach Report[39].

These sources were used to obtain estimates of the value of costs associated with cyber attacks, as well as to sense check some of the estimates derived from our modelling. Where available, additional sources were used to sense check the estimates for the costs of cyber attacks by sector, size of firm and type of cyber attack in order to provide a more comprehensive assessment of how the estimates from the model (e.g. estimates of the probability of a cyber attack and the cost of a cyber attack) compare to other estimates/information.

2.3.4 Workshops to discuss the literature review and methodology for building a model of costs

To support the development of the approach to modelling the costs of cyber attacks on different sectors of the economy, a number of workshops were convened with DSIT and KPMG subject matter experts. They were used to discuss the evidence available, the best way to use available evidence to build a model of cyber costs split by sector, size of firm and type of cyber attack, as well as how the model is intended to be used by DSIT going forward.

The approach to modelling the costs of cyber attacks was developed iteratively with DSIT, allowing for the broad approach to estimation to be interrogated; assumptions to be tested; and datasets/ information to be used to be discussed in more detail.

2.4 Key caveats and limitations

When interpreting the findings of this study on the costs of cyber attacks across different sectors of the economy, sizes of firms and attack types, there are a number of caveats and limitations to be aware of.

The main limitation relates to the lack of reliable evidence on the cost of cyber attacks experienced by businesses. This is driven by two main factors:

— First, a significant proportion of cyber attacks go unreported, making it difficult to accurately assess their prevalence and impact. Businesses often fear reputational damage that may result from disclosing they have experienced a cyber attack and choose not to disclose attacks publicly unless there is a requirement to do so.[40]

— Second, even when cyber attacks are reported, information on the associated costs is often unavailable or unreliable. This may be due to a combination of firms not being able to accurately assess the full costs of an attack, and/or not wanting to disclose this information for reputational or other reasons.[41]

These factors contribute to a heavy reliance within available literature on data from the US due to regulations governing the reporting of cyber attacks in the US compared to other countries.5[42] The

[37] IRIS-2022_Cyentia.pdf
[38] Cost of a Cyber Incident: Systematic Review and Cross-Validation
[39] Cost of a data breach 2024 | IBM
[40] See for instance the CISA report (Cost of a Cyber Incident: Systematic Review and Cross-Validation)
[41] See for instance S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity
[42] For instance, the Securities and Exchange Commission sets out regulations and guidelines regarding incident reporting for public companies in the US and public sector bodies in the US have mandatory reporting requirements (to the US Computer Emergency Readiness Team) around malware events, for example.

Cyentia report relies predominantly on US data. This represents the largest drawback to using the Cyentia report because it relies predominantly on data from a different, much larger, economy than the UK economy, and data from another country subject to different legislation to the UK. However, there are reasons to believe that, despite these issues, the costs of cyber attacks reported in the Cyentia report will be broadly representative of the costs experienced by organisations within the UK. As set out in the literature review, at present there is no documented difference in expected costs between US and UK firms of similar size and sector in responding to or recovering from a cyber attack. Moreover, as set out in Section 3.5, given the similarity of the two economies[43]; the global nature of cyber threats; similar cyber vulnerabilities in both the US and UK (as illustrated by the joint initiatives to tackle such vulnerabilities[44]); and a similar commitment to cyber security[45]; it is reasonable to assume that the costs of a cyber attack on US organisations are likely to be similar to those experienced by organisations in the UK.

In addition, where data is available it is generally not at a sufficiently granular level to allow for disaggregation by sector, size, and attack type. As a result, to generate estimates for costs split by sector, size and attack type, a number of assumptions have to be applied. In Sections 3 and 4, the strength of the available evidence supporting the assumptions made in the modelling is considered.

While steps have been taken to limit any bias or inaccuracies stemming from data limitations[46], results of the modelling should be treated with caution. Where there are known factors that could influence results, but which were not incorporated into the modelling due to a lack of sufficient evidence to do so, these are considered qualitatively in the reporting of results in Section 4, including the expected magnitude and direction of impact on estimates.

2.5 Report structure

The remainder of this report is structured as follows:

- Section 3 considers the data on cyber attacks (predominantly the likelihood of attacks and the costs of cyber attacks) available from existing surveys, databases and literature.
- Section 4 describes the development of the model of sector specific costs of cyber attacks.
- Section 5 provides a brief summary of wider research insights.

[43] See for instance the share of service sector in both economies in OECD Economic Surveys: United Kingdom 2024 | OECD and OECD Economic Surveys: United States 2024 | OECD

[44] CISA Partners with ASD's ACSC, CCCS, NCSC-UK, and Other International and US Organizations to Release Guidance on Edge Devices | CISA and ASD's ACSC, CISA, and US and International Partners Release Guidance on Choosing Secure and Verifiable Technologies | CISA

[45] See: Global Cybersecurity Index which illustrate that both the UK and US are in the top 10 countries for commitment to cyber security reflecting legal, technical and organisational measures in the two countries.

[46] See the discussion in Sections 3 and 4. For example selecting the input data with a large number of datapoints; testing the validity of simplifying assumptions by drawing on wider evidence from the literature review; and sense-checking the robustness of results through comparison with other datasets.

3 Data from existing surveys, databases and literature

3.1 Introduction

In order to model the sector specific costs of cyber attacks on businesses, rather than conduct new primary research in the form of surveys (which carry significant limitations including poor response rates and lack of knowledge on the subject matter from participants, particularly around the cost of a cyber attack), existing data and literature on such costs was drawn upon. This section details the main sources used in the modelling of costs of cyber attacks split by sector, size, and type of attack. It sets out the nature of the different sources including aspects such as the coverage of the data, the underlying source of the data, and the data's reliability. From this, consideration is given to the strengths and weaknesses of each source prior to its use in the modelling.

3.2 Cyber Security Breaches Survey (CSBS)

Since 2017, HM Government (via DCMS and DSIT) has surveyed UK businesses via the CSBS to find out how they approach cyber security and learn more about the cyber security issues faced by organisations.[47] This research informs government policy on cyber security.

The 2024 CSBS survey[48] followed a similar approach to previous years – consisting of two strands:

- A random probability telephone and online survey of 2,000 UK businesses – with the data for businesses weighted to be statistically representative of the business population. This comprised a quantitative element carried out in winter 2023/24 and a qualitative element carried out in early 2024.
- 44 in-depth interviews conducted between December 2023 and January 2024, to gain further qualitative insights from some of the organisations that answered the survey.

Sole traders and public-sector organisations are outside the scope of the survey. In addition, businesses with no IT capacity or online presence are deemed ineligible (exclusions that are consistent with previous years).

Whilst the CSBS technical report[49] states that the survey aims to produce the most representative, accurate and reliable data possible with the resources available, it acknowledges that there are inevitable limitations of the data. The following main limitations are outlined in the technical report:

- Organisations can only inform on the cyber security breaches or attacks that they have detected. There may be other breaches or attacks affecting organisations, but which are not identified as such by their systems or by staff, such as a virus or other malicious code that has so far gone unnoticed. Therefore, the survey may tend to systematically underestimate the real level of breaches or attacks.
- Whilst the survey intends to represent businesses of all sizes, the UK business population is predominantly made up of micro and small businesses. These businesses, due to their smaller scale and resource limitations, typically have a less mature cyber security profile which may limit the insights the survey can generate.
- Organisations may be inclined to give answers that reflect favourably on them in surveys about cyber security (a form of social desirability bias), given the common perceptions of reputational damage associated with cyber security attacks. Whilst the anonymity of the CSBS should reduce this impact to some extent, organisations that have suffered from more substantial cyber security

[47] Cyber Security Breaches Survey - GOV.UK
[48] Cyber Security Breaches Survey 2024 - GOV.UK
[49] Cyber security breaches survey 2024: technical report - GOV.UK[50] IRIS-2022_Cyentia.pdf

attacks may be less inclined to take part because of this. This may result in surveys like the CSBS under-counting the true extent and cost of cyber security attacks.

- There is a significant challenge in accurately capturing the financial implications of cyber security attack, given that survey findings necessarily depend on self-reported costs from organisations (which may not be equipped to measure such costs). Indeed, the financial costs of an attack are likely to be best understood by parts of the organisation (e.g. finance) that are not the main responders to the survey. As a result, respondents may underestimate the true economic cost of their most disruptive breaches or attacks in the survey, and the averaged results may miss critical cases within the population. Moreover, a sample-based survey may well miss some of the most financially damaging cyber security attacks that affect a very small number of UK organisations, in a very extreme way.

In addition, whilst the CSBS is a large survey of business organisations, the fact that it is a sample survey, means that disaggregation to some of the breakdowns required for the model in this study is not reliable. That is, when split by sector and size of firm – some of the breakdowns will rely on a very small number of observations from the survey. This is particularly the case for cost estimates in the survey.

It should be noted that while some of these limitations are specific to the CSBS, a number are inherent to the nature of cyber attacks and available information on their costs and, therefore, similar limitations apply across other datasets and sources.

Some of the limitations set out above relate to the robustness of cost estimates that the CSBS generates only. Of these, some, but not all, also apply to CSBS estimates of the prevalence of cyber attacks. For example respondents do not have to estimate a financial cost or value to register an attack (or type of attack), therefore data on attack prevalence may be more reliable than specific cost data. As a result, as shown later in the report, the CSBS is used to help in understanding the prevalence of cyber attacks in the UK.

Table 3.1: Strengths and weaknesses of the CSBS for this study

	Description of strength/weakness
Strengths	Large survey, broadly representative sample of UK businesses
	Covers sector, size and type of attack
	Provides estimates of both likelihood and costs of attack
Weaknesses	Sample based survey, meaning data on some cyber attacks will be missed (particularly the most financially damaging attacks, that affect a very small number of organisations in a very extreme way)
	Sample size means that some levels of disaggregation are not reliable
	Survey based, meaning it is reliant on accuracy of self-reported responses

3.3 KPMG's Industry Insights Database (IID)

KPMG's IID is a database of expected costs to businesses from cyber attacks containing approximately 1,500 individual datapoints on the costs of cyber attacks. Data for these costs derive from several sources including: industry publications such as Cyentia's IRIS[50]; other publicly available sources such as press reports; and data from KPMG's internal Cyber Response Services team. The datapoints are mapped to five company turnover bands across 20 industries and to 12 cyber attack threat scenarios (which include scenarios such as business email compromise, data breach and widespread ransomware).

The individual datapoints can be split into two types of cyber attack costs:

- Total costs: the entire cost of the breach to the affected party
- Partial costs: a proportion of total costs, for example a ransom payment or a GDPR fine

[50] IRIS-2022_Cyentia.pdf

Given limited data points on the total costs of cyber attacks, an extrapolation-based approach has been used to incorporate and make use of the larger sample of partial cost data. That is, estimates are made as to what proportion of total costs the partial cost estimates are likely to make up (across industries and turnover bands). This is done using the relationship between total costs and partial costs exhibited in the raw dataset. Partial cost estimates are then scaled up by this factor to generate total cost estimates.

This complete database can then be used to identify the expected loss based on a given cyber attack threat scenario, industry sector and level of turnover.

As with all sources investigated for this study, there are some limitations of the IID for use in this study. These limitations include:

- Not all datapoints in the IID relate to the UK. As a result, use of this source would require an implicit assumption that the costs of cyber attacks in other countries are similar to the costs of cyber attacks experienced by businesses in the UK.
- Some of the costs in the database are estimated. Whilst these estimations are based on the best available evidence, it is possible that the actual costs of a cyber attack differ to the estimations made.
- The proprietary nature of the IID means it is not easy for DSIT to investigate the individual costs of cyber attacks contained in the dataset and, similarly, it would not be easy for DSIT to replicate the estimation of costs set out in this study on an on-going basis.

Table 3.2: Strengths and weaknesses of the IID for this study

	Description of strength/weakness
Strengths	Numerous (approx. 1500) observations of costs of cyber attack
	Covers sector, size and type of attack
	Provides estimates of both likelihood and costs of attack
Weaknesses	Proprietary nature of data means lack of transparency of individual cyber attack loss events for this work
	Proprietary nature of data means lack of replicability
	Data cover a number of countries (not just UK), meaning costs may not directly translate to UK firms

3.4 Other data sources

3.4.1 Overview of other data sources

The literature review (see Appendix 1) identifies a number of reports which provide further estimates of the costs of cyber attacks. These include: Cyentia's Information Risk Insights Study (IRIS) 2022[51]; the Cybersecurity and Infrastructure Security Agency (CISA) Cost of a Cyber Incident: Systematic Review and Cross-Validation report[52]; the IBM Cost of a Data Breach Report[53]; Ponemon Institute annual report series[54]; NetDiligence annual cyber claim studies[55]; and Romanosky - Examining the costs and causes of cyber incidents[56], amongst others.

As identified in the literature review set out in Appendix 1, the cost estimations in these reports are often on different bases. For example, the Ponemon Institute work includes the opportunity costs of dealing with cyber attacks (among other costs) in its estimates; whereas most other reports do not include such costs. Other reports, like those produced by NetDiligence, cover the insurance costs

[51] IRIS-2022_Cyentia.pdf
[52] Cost of a Cyber Incident: Systematic Review and Cross-Validation
[53] Cost of a data breach 2024 | IBM
[54] Ponemon Library | Ponemon Institute
[55] NetDiligence Publishes Fourteenth Annual Cyber Claims Study | NetDiligence
[56] S.Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001

relating to cyber attacks; which are, arguably, more restricted than the cost categories considered in other reports.

The result of the literature review was the identification of three pieces of analysis that are particularly useful with respect to estimating the costs of cyber attacks. These were selected as providing useful, often consistent over time estimates of costs from cyber attacks across sectors. These reports are: the IBM (cost of data breach report); the CISA report; and the Cyentia report. Each of these is considered in turn in the following sections.

3.4.2 IBM Cost of Data Breach report

The IBM Cost of Data Breach report[57] covers research, conducted by Ponemon Institute (but sponsored, analysed and published by IBM), on 604 organisations impacted by data breaches. The 2024 report includes data on breaches that occurred between March 2023 and February 2024.

For the purposes of the report, a data breach is defined as an event in which records containing: Personally Identifiable Information (PII); financial or medical account details; or other secret, confidential or proprietary data are potentially put at risk. The research covers organisations of various sizes across 17 industries and over 16 countries. The research involved Ponemon Institute's researchers interviewing 3,556 security and business leaders with knowledge of the data breach incidents at their organisations.[58]

The research collects data on both direct and indirect expenses incurred by the organisation as a result of the breach. Direct expenses include: costs of engaging forensic experts; outsourcing hotline support; and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include: in-house investigations and communications along with the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.[59]

As with all sources investigated for this study, the IBM report has a number of limitations for use in this study. These limitations include:

- The data and information relate to data breaches only. As a result, the report does not cover cyber attack costs which are not related to data breaches.
- No organisation-specific information is collected on the respondents so there is no information on how costs vary by size of organisation for instance.
- The report covers organisations in 16 countries with the UK representing about 8 per cent of the sample. As a result, an implicit assumption if the IBM report were to be used for this study would be that the costs of a data breach in other countries are similar to the costs of cyber attacks experienced by businesses in the UK.
- The report surveys organisations, so is reliant on accurate responses; the report acknowledges that respondents may not provide accurate or truthful responses.
- The report, whilst being based on a survey, reports data and information as averages which restricts the ability to interrogate individual cyber attack events.

[57] Cost of a data breach 2024 | IBM
[58] Cost of a data breach 2024 | IBM
[59] Cost of a data breach 2024 | IBM

Table 3.3: Strengths and weaknesses of the IBM report for this study

	Description of strength/weakness
Strengths	Covers data on different sectors
	Cost estimates cover wider, indirect, costs of a data breach (e.g. lost business revenues)
	Publicly available report which provides for transparency and replicability of analysis
Weaknesses	Data is provided as averages - lack of transparency of individual data points for this work
	Data cover multiple countries (UK is 8% of global sample), meaning costs may not directly translate to UK firms
	No data/information on cyber attack costs by size of firm
	Survey based, meaning it is reliant on accuracy of self-reported responses
	Data cover cost of data breach only (not costs of other types of cyber attack)

3.4.3 Cyentia IR2022

The Cyentia Information Risk Insights Studies[60] investigate the losses experienced as a result of cyber attacks. The data underpinning the Cyentia report is taken from the Advisen dataset[61] and is made up of over 77,000 cyber incidents (with 1,800 of these incidents including data on the costs of attacks). Advisen maintains a repository of more than 100,000 cyber events. It compiles this information through publicly available sources, such as breach disclosures; company filings; litigation details; and Freedom of Information Act requests. Whilst the majority of incidents in the Advisen dataset do not include information on costs, Cyentia argue that the recorded losses, due to the increased scrutiny of public records, "suitably reflect known financial losses from publicly visible cyber incidents". The dataset is also matched to known company IDs (e.g., using Dunn & Bradstreet (D&B) and Standard & Poor's (S&P) data) allowing for the characteristics of organisations to be linked to the costs of a cyber attack.

For the 2022 report, Cyentia uses the July 2022 release of the Advisen dataset, which focuses on a 10-year window ranging from 2012 to 2021. Cyentia removes incidents that are exclusively privacy-related. The sample contains organizations predominantly from the US (74%), Europe (9%), and Latin America (9%).

As with all sources investigated, the Cyentia report has a number of limitations for use in this study. These limitations include:

- The sample is predominantly taken from the US. As a result, the implicit assumption for this information's use in this study is that the costs of a cyber attack in the US (and other countries covered in the data) are similar to the costs of cyber attacks experienced by businesses in the UK.
- The report presents data and information as averages which, although presented in a number of different ways (e.g. by sector and by size of firm), restricts the ability to interrogate individual cyber attack events.

Table 3.4: Strengths and weaknesses of the Cyentia report for this study

	Description of strength/weakness
Strengths	Numerous observations of costs of cyber attack
	Covers sector, size and type of attack
	Provides estimates of both likelihood and costs of attack
	Publicly available report which provides for transparency and replicability of analysis
Weaknesses	Data is provided as averages - lack of transparency of individual data points for this work
	Data cover a number of countries – predominantly the US – meaning costs may not directly translate to UK firms

[60] IRIS-2022_Cyentia.pdf
[61] Cyber Loss Data - Advisen Ltd.

3.4.4 CISA report

The CISA, Cost of a Cyber Incident: Systematic Review and Cross-Validation report[62], looks to understand the impacts, costs and losses from cyber attacks. The report sets out the results from a systematic analysis of existing cyber attack cost studies to document cost estimates. To do this the report sets out an in-depth review of the cyber loss literature; identifies estimates of cyber losses that are based on historical data; and to understand the limitations of the currently available estimates.

As a result, the CISA report does not provide any primary evidence on cyber attack losses but it is useful in providing evidence in support of assumptions made, or the estimates generated, in the modelling.

3.5 Conclusions on the use of data sources in the final model

It is clear from the literature that robust and comprehensive data on the costs of cyber attacks is scarce. Moreover, as detailed in this section, where reports and databases do provide information on the costs of cyber attacks, they have their limitations.

Nevertheless, following the consideration of the various available data sources, the Cyentia report was identified as the most appropriate source for estimating the costs of cyber attacks for this study. The Cyentia report provides data drawn from a large dataset of predominantly US cyber incidents and costs, and provides information on a range of factors including the costs of significant cyber attacks split by sector; size of firm and type of cyber attack – all on a consistent basis. Importantly for the purposes of this study, the report is publicly available and therefore allows for DSIT to use the data on an ongoing basis to update the model. As a result, the use of this report for this study provides for transparency and replicability (the report is publicly available and can be used by DSIT to update the model inputs as needed in the future as and when new data is released); and robustness (being based on a large dataset of cyber incidents and costs).

The largest drawback of the Cyentia report is its reliance on predominantly US data for the prevalence of cyber attacks and their associated costs. The CSBS is the only source of UK cyber attack cost estimates that was identified and analysed as part of this work. However, the sampling approach used in this survey means that it will likely exclude the most financially damaging cyber security attacks that affect a very small number of UK organisations in a very extreme way. Moreover, even where cyber attack costs are reported in the CSBS, there are questions around the accuracy of financial costs reported. This is because survey findings necessarily depend on self-reported costs which may underestimate the true economic cost of breaches or attacks. Indeed, the average costs of cyber attacks (calculated using arithmetic means, medians and/or geometric means) drawn from the CSBS appear to significantly underestimate the cost of a cyber attack when compared to other published information on the costs of cyber attacks (e.g. from insurance claims and publicly announced cyber attack costs).

Whilst the Cyentia report draws data from a much larger economy than the UK economy and from a different country with different legislation, there are reasons to believe that the cyber attack costs experienced in the US are likely to be similar to those experienced in the UK. The US and UK economies are similar in nature with both being heavily orientated to the service sector. Indeed, 80.5% of the value added in both countries relates to the service sector (compared to an OECD average of 70%).[63] As such both countries have a similar industrial structure, with significant financial and business services as well as information and communication technology sectors, which are often the target of cyber attacks.[64] Moreover, many cyber threats are global in nature such that many of the attack vectors, tactics, and malware, for example, used in the US are also prevalent in the UK.[65] This is particularly the case given much of the software and IT platforms used in the UK is similar to those used in the US and results in similar cyber vulnerabilities across the two countries. These common

[62] Cost of a Cyber Incident: Systematic Review and Cross-Validation
[63] OECD Economic Surveys: United Kingdom 2024 | OECD and OECD Economic Surveys: United States 2024 | OECD
[64] IRIS-2022_Cyentia.pdf
[65] Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments

cyber vulnerabilities are illustrated by the joint efforts by cyber agencies in the UK and US (as well as other countries) to address cyber threats.[66,67,68] Indeed, whilst it is subject to change, the UK's close relationship with the US and its involvement in international conflicts might, arguably, make it a target for state-sponsored cyber espionage in a similar way to the US, particularly from countries with adversarial relationships with the US.[69] Lastly, both the US and UK are ranked as being in the top 10 countries for commitment to cyber security, reflecting broadly similar types of legal, technical and organisational measures in the two countries.[70]

As a result, in what follows, the Cyentia report is used to obtain estimates of the average costs of significant cyber attacks across sector, size of firm and type of cyber attack. These cost estimates are compared against the information contained in other data sources and reports to sense check the modelled estimates where that is possible, as well as to support the assumptions used in the model.

To provide an estimate of the costs to businesses of significant cyber attacks at the UK economy level, the average cost estimates on a per attack basis are coupled with information on the likelihood of a significant cyber attack[71] taken from the CSBS (UK data on the prevalence of cyber attacks) alongside UK data on firm size distribution by sector[72].

Data and information from the literature review and other sources are used to test and evidence the robustness of simplifying assumptions where they are made.

[66] 2023 Top Routinely Exploited Vulnerabilities
[67] CISA Partners with ASD's ACSC, CCCS, NCSC-UK, and Other International and US Organizations to Release Guidance on Edge Devices | CISA
[68] ASD's ACSC, CISA, and US and International Partners Release Guidance on Choosing Secure and Verifiable Technologies | CISA
[69] Russian foreign intelligence poses global threat with... - NCSC.GOV.UK
[70] Global Cybersecurity Index
[71] The CSBS 2024 provides information on the negative outcomes resulting from a cyber attack which include things like: website taken down; money stolen; software or systems corrupted; personal data stolen; and loss of access to files or networks among others. See Section 4.5 of Cyber security breaches survey 2024 - GOV.UK. This is coupled with attacks that are recorded as costing at least £500 to derive a significant cyber attack.
[72] UK business: activity, size and location - Office for National Statistics

4 Development of the model of sector specific costs of cyber attacks

4.1 Overview of the approach to developing the model of sector specific costs of significant cyber attacks

This section sets out the approach to the modelling of costs of significant cyber attacks across sector, firm size and type of attack. The modelling aims to provide DSIT with a transparent and repeatable approach for estimating sector specific costs of significant cyber attacks. This is intended to allow DSIT to update the estimates of the costs of significant cyber attacks when additional data and evidence becomes available and to adjust modelling assumptions if required.

Each stage of the model's development is set out in brief below and then expanded upon in the following sections.

Step 1: Average cost of a significant cyber attack to an organisation split by sector and size of firm

The first step in the modelling is to estimate the average cost of significant cyber attacks across sector and size of firm:

- Cyentia data is used to first estimate the proportion of businesses experiencing a significant cyber attack split by sector and size band.
- This data is then used together with information from the Cyentia report on:
  - the average cost of a significant cyber attack by sector, and
  - the average cost of a significant cyber attack by size of firm

  to produce estimates for the total costs of significant cyber attacks both by sector and by size of firm.
- The model is then constrained to these total costs. That is, the total costs of significant cyber attacks on businesses for all sectors and across all firm size bands are fixed and the individual estimates of significant cyber attack costs by sector and size of firm are iterated to be consistent with the fixed total cost figures.

This process generates estimates of the costs of significant cyber attacks split by both sector and size of firm.

Step 2: Average cost of different types of significant cyber attack to an organisation

The next step is to estimate the average cost of a significant cyber attack for an organisation split by the different types of cyber attack:

- Information from the Cyentia report on the frequency of different types of significant cyber attacks is applied to estimates of the total number of firms experiencing significant cyber attacks generated in Step 1. This produces estimates for the number of firms experiencing the different types of significant cyber attack.
- Information from the Cyentia report on the proportion of costs associated with different types of significant cyber attacks is applied to the total cost of significant cyber attack estimates generated above. This produces estimates for the total cost for different types of significant cyber attack.
- Dividing the estimates of the total financial costs by type of significant cyber attack by the number of firms experiencing the different types of significant cyber attack produces an estimate of the average cost of the different types of significant cyber attack.

Step 3: Total cost of significant cyber attacks to businesses at the UK economy level

The final step is to estimate the cost to businesses of significant cyber attacks at the UK economy level:

- Information on the likelihood of a significant cyber attack from the CSBS is coupled with data from the ONS on the firm size distribution by sector. This provides an estimate of the number of businesses experiencing a significant cyber attack split by size of firm in the UK using UK data.
- These figures are then applied to the estimates of the average cost of significant cyber attacks to an organisation split by size of firm generated above to provide an estimate of the total cost of significant cyber attacks to businesses at the UK economy level.
- This figure is compared against UK GDP figures to put the figure in context.

Further details on each step, including the assumptions applied, evidence to support and justify these assumptions, and any associated limitations, are provided in the sections below.

4.2 Modelling of average costs by sector, firm size and type of attack based on Cyentia data

4.2.1 Prevalence of attacks by sector and firm size

The first step in modelling the average costs of significant cyber attacks by sector and firm size is to estimate the prevalence of attacks across these same characteristics. This prevalence data is subsequently used to scale the Cyentia cost of significant cyber attack data and then redistribute significant cyber attack costs across sectors and size bands (see Section 4.2.2 below).

Attack prevalence by firm size band is considered first.

The Cyentia IR 2022 report provides information on the likelihood of experiencing a significant cyber attack for firms in different size bands. To derive annualised loss event frequency (i.e. the annual likelihood of experiencing a significant cyber attack – that is, a cyber attack that results in a cost), Cyentia divided its dataset into 12-month rolling windows. This provides a larger sample that Cyentia employed to model the annualised loss event frequency more confidently. The report provides estimates of the proportion of firms within a given size band experiencing at least one significant cyber attack. Two estimates are provided for this proportion. An upper bound estimate looks at the proportion of firms recorded in the Advisen dataset that have experienced at least one significant attack over the 12-month period. This shows the likelihood of experiencing a significant attack in any one year – drawn from a population that has experienced a significant attack at some point in the last 10 years (and recorded in Advisen dataset). A lower bound estimate looks at the proportion of firms attacked over this period among all registered organisations in the US (using Dunn and Bradstreet (D&B) data)..[73]

Data on the likelihood of significant attack is provided by Cyentia for larger firms only. Therefore, to derive an estimate for the proportion of firms experiencing at least one significant cyber attack across all size bands a line of best fit is generated for the upper bound proportions and a line of best fit for the lower bound proportions – as shown in Table 4.1 below.

The values reported in the Cyentia report are in US dollars. For the purposes of this study, and in all that follows in this report, the values from the Cyentia report are converted from US dollars into pound sterling using the OECD's PPP rate for 2022 (the date relating to the data used in the Cyentia report)..[74]

[73] The Cyentia report uses all registered organisations in the US for this lower bound estimate. Whilst the Advisen dataset does include data and information from other countries the majority of information is from the US. As a result, and similarly to the Cyentia report, the data is assumed to relate to the US business population for the purposes of estimating the likelihood of a cyber attack as well as the costs of a cyber attack in this study.

[74] The OECD PPP is used here to control for differences in price levels, in this instance as between the UK and US. In this study it is used to convert the value of cyber attack costs across all sectors of the economy (in US dollars) into UK pound sterling. Costs are also inflated to 2024 prices using the UK GDP deflator.

Table 4.1: Estimates of the proportion of firms experiencing at least one significant cyber attack by size of firm (based on underlying US data)

Size distribution (annual turnover)	Upper bound	Lower bound
More than £65bn	**29.33%**	**29.30%**
£6.5bn to £65bn	**21.93%**	**14.20%**
£0.65bn to £6.5bn	**17.04%**	6.99%
£65m to £0.65bn	**12.95%**	3.39%
£6.5m to £65m	**11.53%**	1.64%
£0.65m to £6.5m	8.55%	0.80%
£65k to £0.65m	6.73%	0.39%
Less than £65k	5.30%	0.19%
Unknown	1.60%	0.01%

Source: Cyentia IR 2022 Table 2 (bold figures) and KPMG analysis (estimated figures in italics).

The lower bound proportion is then multiplied by the number of US firms in each size band to generate an estimate of the number of firms experiencing a significant cyber attack in any single year. The data used for the number of firms in the US by turnover bands and sector is sourced from the NAICS Association[75] (a source which uses the same D&B data as used in the Cyentia report).

The NAICS data includes a single size band for firms over £0.65 billion. Therefore, in order to utilise the more granular Cyentia prevalence data, Fortune 500[76] data is used for the distribution of large firms over £0.65 billion of revenue across these size bands.

The prevalence data, set out in Table 4.1, is then combined with the firm population within each size band for each sector to arrive at the number of firms experiencing significant cyber attacks by firm size split by sector. To maintain the detail within the more granular breakdowns, analysis is conducted at the greatest level of disaggregation possible before being re-aggregated to the size bands set out in the original specification for this work (i.e. micro, small, medium and large).

However, it should be noted that the size bands that are aggregated to are not exactly the same as those that tend to be used by the UK Government or the ONS[77]. The size bands reported in this study (after aggregation) are: up to £0.65 million (including unknown); £0.65 million to £6.5 million; £6.5 million to £65 million; and over £65 million. These size bands are reported in this study because they represent a direct aggregation of the size bands used in the Cyentia report.

This process provides an estimate of the number of firms experiencing attacks by size band split by sector – as shown in Table 4.2.

[75] US Business Firmographics - Company Size
[76] Fortune Global 500 – The largest companies in the world by revenue | Fortune
[77] UK business: activity, size and location - Office for National Statistics

Table 4.2: Total number of firms in the US experiencing a significant cyber attack by sector and size of firm by turnover (unadjusted for relative probability of attack across sectors)

Sector	Micro	Small	Medium	Large	Total
Agriculture	692	81	15	7	794
Mining	45	41	25	41	152
Utilities	73	38	33	65	209
Construction	2,747	902	248	68	3,966
Manufacturing	940	845	499	364	2,647
Trade	1,005	823	412	168	2,408
Retail	2,887	879	294	107	4,167
Transportation	1,212	260	88	52	1,612
Information	613	138	64	74	890
Financial	1,166	329	196	223	1,913
Real Estate	1,638	247	55	37	1,976
Professional	4,539	818	228	76	5,662
Management	12	18	18	11	58
Administrative	2,830	322	102	55	3,309
Education	517	185	197	98	997
Healthcare	2,912	647	264	170	3,992
Entertainment	703	104	26	8	841
Hospitality	1,522	241	52	24	1,840
Other Services	3,545	454	104	29	4,133
Public	14	0	0	0	14
Total	29,611	7,372	2,922	1,676	41,580

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data

To this point in the model development the assumption is that the experience of significant cyber attacks by size of firm was common across all sectors. However, the literature highlights that the likelihood of experiencing a significant cyber attack varies by sector. Information on how cyber attacks vary by sector is also provided in the Cyentia report.

Table 4.3 below shows the relationship between different sectors, in terms of likelihood of attack, relative to the public sector, as reported in the Cyentia report.

Table 4.3: Probability of experiencing one or more significant cyber attacks across sectors relative to the public sector (based on underlying US data)

Sector	Relative probability
Hospitality	1.17
Information	1.16
Financial	1.15
Retail	1.12
Transportation	1.05
Healthcare	1.03
Public	1
Education	0.98
Real Estate	0.95
Administrative	0.94
Entertainment	0.93
Manufacturing	0.92
Professional	0.91
Other services	0.91
Utilities	0.91
Management	0.91
Trade	0.86
Construction	0.77

Source: Cyentia IR 2022 – Figure 5.
Note: Given the low number of publicly recorded cyber attacks in the agriculture and mining sectors - no data is provided on the relative probability of experiencing a cyber attack in the agriculture and mining sectors as compared to the public sector.

To incorporate this data, the total number of significant attacks by sector is constrained to fit the relationship between sectors (as set out in Table 4.3). For example, the number of significant attacks experienced in the finance sector is increased by a factor of 1.15 (relative to the public sector) and the number of significant attacks experienced in the construction sector is reduced by a factor of 0.77. This results in a distribution of significant attacks by sector and size of firm that is consistent with these two data sources from the Cyentia report (i.e. the proportion of businesses experiencing a significant attack by turnover band and the relative probability of a significant cyber attack by sector). Table 4.4 below shows the resulting estimated distribution of firms experiencing significant attacks in the US.

Table 4.4: Total number of firms in the US experiencing a significant cyber attack by sector and size of firm by turnover (adjusted for relative probability of attack across sectors)

Sector	Micro	Small	Medium	Large	Total
Utilities	69	36	31	60	196
Construction	2,178	725	198	53	3,154
Manufacturing	890	810	477	339	2,516
Trade	888	737	368	146	2,139
Retail	3,331	1,027	342	121	4,822
Transportation	1,312	285	96	55	1,749
Information	734	167	78	87	1,066
Financial	1,384	395	234	259	2,272
Real Estate	1,605	245	54	36	1,939
Professional	4,259	777	215	71	5,322
Management	11	17	17	10	55
Administrative	2,745	316	100	52	3,213
Education	521	189	200	98	1,009
Healthcare	3,092	696	282	177	4,248
Entertainment	674	101	26	7	808
Hospitality	1,837	295	64	29	2,224
Other Services	3,328	432	99	27	3,886
Public	14	0	0	0	15
Total	28,873	7,250	2,882	1,628	40,633

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data
Note: Cyentia does not provide figures on the relative probability of cyber attacks for the agriculture or mining sector as compared to the public sector. As a result the totals in this table do not match totals in Table 4.2.

To arrive at the estimated probability of a significant cyber attack by sector and firm size, the estimated numbers of businesses experiencing at least one significant cyber attack (as reported in Table 4.4) is divided by the total number of firms in the US split by firm size and sector sourced from NAICS. These probabilities are presented in Table 4.5.

Table 4.5: Estimated proportion of businesses experiencing at least one significant cyber attack in a single year (based on underlying US data)

Sector	Micro	Small	Medium	Large
Utilities	0.2%	0.8%	1.6%	5.8%
Construction	0.2%	0.6%	1.3%	3.4%
Manufacturing	0.2%	0.8%	1.6%	4.9%
Trade	0.2%	0.7%	1.5%	3.8%
Retail	0.2%	0.9%	1.9%	6.4%
Transportation	0.2%	0.9%	1.8%	5.7%
Information	0.2%	1.0%	2.0%	6.7%
Financial	0.2%	1.0%	2.0%	6.5%
Real Estate	0.2%	0.8%	1.6%	5.6%
Professional	0.2%	0.8%	1.6%	4.3%
Management	0.0%	0.8%	1.6%	3.9%
Administrative	0.2%	0.8%	1.6%	4.9%
Education	0.1%	0.8%	1.7%	4.0%
Healthcare	0.2%	0.9%	1.8%	4.9%
Entertainment	0.2%	0.8%	1.6%	5.2%
Hospitality	0.2%	1.0%	2.0%	5.7%
Other Services	0.2%	0.8%	1.6%	3.9%
Public	0.0%	0.9%	1.8%	3.6%

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data

The data generated in this section, particularly the number of US firms experiencing at least one significant cyber attack (Table 4.4), is used in the next section to estimate the average cost of significant cyber attacks split by sector and size of firm.

4.2.2 Average costs by sector and firm size

Having estimated the probability of a significant cyber attack on an annual basis by sector and firm size, this is then used in the modelling of the average cost of significant cyber attacks across both sector and firm size.

Whilst the Cyentia report provides information on the average costs of significant cyber attacks by sector and by size band separately, the full matrix of significant cyber attack costs by sector and size band is not provided. To estimate the full matrix, first prevalence data (set out in Table 4.5) and data on the average cost of a significant attack by sector is used to estimate the total costs of significant cyber attacks split by sector (for the US). This provides for a matrix of costs by sector and size (with the distribution across size purely based on number of firms). Then separately, prevalence data and data on the average cost of a significant attack by firm size is used to estimate the total cost of significant cyber attacks by firm size (for the US). The model is then constrained to fit these two totals (total costs by sector and total costs by size band) in order to generate estimates of the matrix of significant cyber attack costs split by both sector and by size band based on the estimated distribution of costs across each.

This is set out in the following sections.

Costs by sector

The Cyentia report provides information on the average cost of a significant cyber attack across businesses which have experienced a significant cyber attack, split by sector. As noted in the literature, the distribution of cyber attack costs usually exhibits a long tail – i.e. there are a very small number of very costly attacks.[78] This means that taking the arithmetic mean of costs (that is adding up all the costs of cyber attacks experienced by businesses and dividing by the number of firms experiencing a cyber attack) is likely to overstate the actual cost of most cyber attacks because of the existence of a few very costly attacks which could occur in any of a number of sectors. As a result, the Cyentia report makes use of the geometric mean[79] to estimate the average cost of a significant cyber attack. Using the geometric mean (which multiplies all the 'n' observations of cyber costs together and then takes the nth root) provides a means of reducing the impact of outliers in the data.

Table 4.6 below sets out the average costs of a significant cyber attack (geometric mean) and also the 95th percentile of costs reported in the Cyentia report, converted into pound sterling. The results, as set out in the table, show that the average (geometric mean) cost of a significant cyber attack varies across sector from a low of just under £47,000 in the construction sector to a high of £1.4 million in the mining sector (all based on predominantly US data). The 95th percentile costs provide an indication of the scale of costs of what might be considered as a worst case cyber attack across different sectors. These costs vary substantially from a low of £2 million in the agriculture sector through to a high of £125 million in the transportation sector (all based on predominantly US data). The results set out in the table also provide an illustration of how long the tail of the distribution of significant cyber costs is. This is illustrated by how much larger the 95th percentile cost is than the average (geometric mean) cost. For example, despite having an average significant cyber attack cost of around £129,000, the administrative sector has a 95th percentile cost of £35 million (based on predominantly US data). The implication is that rather than clustering around the average cost, significant cyber attack costs exhibit a very wide distribution with a few instances of very significant costs.

[78] Cyentia IR2022 and P. Dreyer *et al.*, 'Estimating the Global Cost of Cyber Risk: Methodology and Examples', RAND Corporation, Jan. 2018

[79] The formula for the geometric mean of n numbers a_1 to a_n is: $\sqrt[n]{(a_1 \times a_2 \times ,,, \times a_n)}$

Table 4.6: Average cost (geometric mean) of a significant cyber attack and the 95th percentile cost for an organisation split by sector (2024 prices)

Sector	Geometric mean	95th percentile
Administrative	£129,474	£35,000,000
Agriculture	£43,158	£2,000,000
Construction	£46,695	£4,000,000
Education	£98,343	£4,000,000
Entertainment	£331,113	£65,000,000
Financial	£309,181	£62,000,000
Healthcare	£149,284	£9,000,000
Hospitality	£153,529	£37,000,000
Information	£336,773	£76,000,000
Management	£333,943	£96,000,000
Manufacturing	£330,406	£76,000,000
Mining	£1,415,014	£6,000,000
Other Services	£72,873	£9,000,000
Professional	£271,683	£64,000,000
Public	£102,588	£10,000,000
Real Estate	£92,683	£3,000,000
Retail	£250,457	£37,000,000
Trade	£224,280	£8,000,000
Transportation	£261,070	£125,000,000
Utilities	£210,837	£13,000,000

Source: Cyentia IR 2022 Table 4 with KPMG analysis.
Note: The data in this table is based, predominantly, on underlying US data and is converted from US dollars to UK pound sterling using the OECD's PPP.

Multiplying the estimates of the geometric mean cost of significant cyber attacks in Table 4.6 with the estimates of the number of significant attacks by sector and size of firm (as set out in Table 4.4) provided values for the cost of significant cyber attacks by sector, prior to adjustment for the average cost of significant cyber attacks by size of firm. The results are shown in

Table 4.7 below.

Table 4.7: Estimates of total costs of significant cyber attacks in the US (using estimates of the number of attacks from Table 4.4 and the geometric mean cost of cyber attacks by sector from Table 4.6, unadjusted for the average cost of cyber attacks by size of firm – 2024 prices)

Sector	Micro	Small	Medium	Large	Total
Utilities	£14,520,887	£7,679,556	£6,633,636	£12,577,800	£41,411,879
Construction	£101,723,253	£33,834,252	£9,264,635	£2,475,177	£147,297,318
Manufacturing	£294,183,293	£267,789,071	£157,503,416	£111,844,125	£831,319,905
Trade	£199,218,579	£165,293,494	£82,448,824	£32,773,710	£479,734,608
Retail	£834,365,045	£257,165,225	£85,699,477	£30,406,687	£1,207,636,434
Transportation	£342,434,286	£74,424,231	£25,187,557	£14,488,918	£456,534,992
Information	£247,337,345	£56,282,934	£26,211,249	£29,230,427	£359,061,955
Financial	£427,757,794	£122,114,232	£72,453,785	£80,216,260	£702,542,070
Real Estate	£148,736,073	£22,694,806	£5,005,478	£3,321,260	£179,757,617
Professional	£1,157,071,777	£211,224,407	£58,533,905	£19,154,055	£1,445,984,145
Management	£3,592,186	£5,615,885	£5,731,440	£3,282,988	£18,222,499
Administrative	£355,370,608	£40,909,860	£12,929,468	£6,770,571	£415,980,507
Education	£51,278,654	£18,580,005	£19,714,828	£9,667,062	£99,240,550
Healthcare	£461,627,774	£103,891,724	£42,137,135	£26,487,342	£634,143,975
Entertainment	£223,273,101	£33,394,209	£8,464,009	£2,348,284	£267,479,603
Hospitality	£282,004,596	£45,270,280	£9,762,431	£4,435,074	£341,472,381
Other Services	£242,506,261	£31,474,132	£7,189,006	£1,982,870	£283,152,268
Public	£1,461,355	£28,693	£16,577	£14,975	£1,521,599
Total	**£5,388,462,868**	**£1,497,666,995**	**£634,886,857**	**£391,477,586**	**£7,912,494,306**

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data.
Note: This table relates to US data and uses the Cyentia lower bound estimate for the likelihood of a cyber attack so should not be compared to aggregated UK cost estimates.

To this point in the model development the assumption is that the cost of significant cyber attacks by size of firm is common across all sectors. In the next section the total costs presented in

Table 4.7 are used alongside average costs of significant cyber attacks split by firm size to estimate average costs by both sector and firm size.

Costs by firm size

The Cyentia report provides information on the average cost (geometric mean) of a significant cyber attack by firm size band, aligned to the prevalence firm size bands reported earlier (see Table 4.1 for example). This data is set out in Table 4.8 below (converted into pound sterling).

Table 4.8: Estimated average significant cyber attack costs for an organisation by firm size by turnover (2024 prices)

Size distribution (annual turnover)	Geometric mean
More than £65bn	£734,392
£6.5bn to £65bn	£365,074
£0.65bn to £6.5bn	£539,828
£65m to £0.65bn	£195,272
£6.5m to £65m	£91,976
£0.65m to £6.5m	£100,466
£65k to £0.65m	£85,608
Less than £65k	£62,261
Unknown	£87,023

Source: Cyentia IR 2022 Figure 7 with KPMG analysis.
Note: The data in this table is based, predominantly, on underlying US data and is converted from US dollars to UK pound sterling using the OECD's PPP.

Multiplying the total number of significant attacks by size band (from the lower bound estimates set out in the prevalence section) by the average cost of a significant attack by size band and then constraining to the sector level total generates an estimate of the total cost of significant cyber attacks by size band (as shown in Table 4.9).

Table 4.9: Estimated total costs of significant cyber attacks in the US by firm size by turnover (2024 prices)

Size distribution (annual turnover)	Total costs
More than £65bn	£199,328,576
£6.5bn to £65bn	£435,894,403
£0.65bn to £6.5bn	£95,920,898
£65m to £0.65bn	£428,536,921
£6.5m to £65m	£624,907,554
£0.65m to £6.5m	£1,717,103,113
£65k to £0.65m	£614,511,368
Less than £65k	£3,776,775,758
Unknown	£19,515,715
Total	**£7,912,494,306**

Source: Cyentia IR 2022 with KPMG analysis.
Note: This table relates to US data and uses the Cyentia lower bound estimate for the likelihood of a cyber attack so should not be compared to aggregated UK cost estimates.

4.2.3 Average costs by sector and firm size

Using estimates of the total cost of significant cyber attacks by sector and the total cost of significant cyber attacks by firm size, the model is constrained to fit these two totals alongside the distributions of costs across sector and firm size identified in Table 4.6 and Table 4.8. This generated estimates of the cost of significant cyber attacks by sector and by size band.

The simplifying assumption used in this modelling is that distribution of significant costs across firm size bands is similar across sectors. Whilst this is a simplifying assumption, the literature review identified no definitive evidence to suggest that this assumption would not hold; most of the evidence

suggests that the costs of cyber attacks increase with firm size and that this holds, in general, across all sectors.

This process generated a table of estimates of the total cost of significant cyber attacks in the US split by sector and firm size (as an intermediate step in the modelling) shown in Table 4.10.

Table 4.10: Estimates of total costs of significant cyber attacks in the US (constraining estimates to fit with total costs of cyber attacks by sector and total costs of cyber attacks by size of firm – 2024 prices)

Sector	Micro	Small	Medium	Large	Total
Utilities	£6,450,946	£5,015,122	£3,909,149	£26,036,663	£41,411,879
Construction	£86,135,037	£42,696,345	£10,549,882	£7,916,054	£147,297,318
Manufacturing	£180,808,448	£237,745,200	£126,181,017	£286,585,239	£831,319,905
Trade	£143,581,846	£172,164,917	£77,492,292	£86,495,554	£479,734,608
Retail	£687,140,595	£314,383,040	£94,538,820	£111,573,980	£1,207,636,434
Transportation	£282,237,264	£93,071,234	£28,423,157	£52,803,336	£456,534,992
Information	£176,883,066	£60,951,650	£25,614,246	£95,612,993	£359,061,955
Financial	£281,976,235	£120,431,520	£64,479,269	£235,655,046	£702,542,070
Real Estate	£130,351,028	£30,008,296	£5,972,355	£13,425,939	£179,757,617
Professional	£1,024,068,264	£282,911,577	£70,745,571	£68,258,733	£1,445,984,145
Management	£2,426,386	£4,737,561	£4,363,003	£6,695,550	£18,222,499
Administrative	£317,572,208	£55,993,151	£15,968,815	£26,446,333	£415,980,507
Education	£36,380,418	£19,828,528	£18,985,533	£24,046,070	£99,240,550
Healthcare	£375,719,892	£126,406,775	£46,263,612	£85,753,696	£634,143,975
Entertainment	£201,470,380	£45,904,895	£10,499,028	£9,605,300	£267,479,603
Hospitality	£252,858,298	£60,748,680	£11,821,342	£16,044,061	£341,472,381
Other Services	£223,300,998	£44,072,778	£9,083,864	£6,694,629	£283,152,268
Public	£1,441,533	£31,842	£16,600	£31,624	£1,521,599
Total	**£4,410,802,841**	**£1,717,103,113**	**£624,907,554**	**£1,159,680,799**	**£7,912,494,306**

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data.
Note: This table relates to US data and uses the Cyentia lower bound estimate for the likelihood of a cyber attack so should not be compared to aggregated UK cost estimates.

These estimates are then divided by the estimated number of firms experiencing a significant cyber attack in any single year. This provides an estimate of the average cost of a significant cyber attack (by sector and by firm size), as shown in Table 4.11.

In effect, Table 4.11 illustrates the average cost of a significant cyber attack split by sector and size of firm for US businesses. The simplifying assumption used in the modelling is that the average cost of a significant cyber attack for a UK business is the same as for a US business. As noted in Section 3.5 there are reasons to believe that the cyber attack costs experienced in the US are likely to be similar to those experienced in the UK. These include: the similar nature of US and UK economies (with both being heavily orientated to the service sector); the global nature of many cyber threats; and the similar nature of software and IT platforms meaning similar cyber vulnerabilities across the two countries.

Table 4.11: Estimates of the average cost of a significant cyber attack for a UK organisation split by sector and size of firm by turnover (2024 prices)

Sector	Micro	Small	Medium	Large	Average across all firms
Utilities	£93,665	£137,687	£124,245	£436,443	£210,837
Construction	£39,540	£58,926	£53,173	£149,340	£46,695
Manufacturing	£203,071	£293,337	£264,699	£846,619	£330,406
Trade	£161,644	£233,603	£210,797	£591,913	£224,280
Retail	£206,264	£306,183	£276,290	£919,026	£250,457
Transportation	£215,176	£326,481	£294,607	£951,442	£261,070
Information	£240,843	£364,709	£329,103	£1,101,588	£336,773
Financial	£203,811	£304,920	£275,151	£908,294	£309,181
Real Estate	£81,227	£122,551	£110,586	£374,666	£92,683
Professional	£240,453	£363,889	£328,363	£968,187	£271,683
Management	£225,566	£281,715	£254,211	£681,067	£333,943
Administrative	£115,702	£177,210	£159,909	£505,734	£129,474
Education	£69,771	£104,952	£94,706	£244,622	£98,343
Healthcare	£121,503	£181,636	£163,903	£483,312	£149,284
Entertainment	£298,780	£455,160	£410,723	£1,354,368	£331,113
Hospitality	£137,661	£206,022	£185,908	£555,397	£153,529
Other Services	£67,102	£102,043	£92,081	£246,037	£72,873
Public	£101,197	£113,848	£102,733	£216,653	£102,588
All sectors	**£152,766**	**£236,832**	**£216,818**	**£712,349**	**£194,729**

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data.
Note: The data in this table is based, predominantly, on underlying US data and is converted from US dollars to UK pound sterling using the OECD's PPP.

As would be expected, the results set out in Table 4.11 align with the broad findings from the Cyentia report as regards to how the costs of significant cyber attacks vary by sector and by size of firm.

Focusing on the size of firm, cyber costs tend to increase with the size of firm with micro firms experiencing the lowest average costs of a significant cyber attack and large firms experiencing the largest average cost from a significant cyber attack. This relationship does not hold for the difference between small and medium sized firms, with medium sized firms, on average, experiencing a slightly lower average cost of a significant cyber attack when compared to small firms. This is a direct result of the data in the Cyentia report (and set out in Table 4.8 above) which suggests that medium sized firms, on average, experience a slightly lower average cost of a significant cyber attack when compared with small sized firms.

There is no explanation for this difference in the Cyentia report, however, one possible explanation is that medium sized firms may be better prepared for, or able to deal with, a significant cyber attack than smaller firms. For instance, they may have more efficient incident response plans or invest more in cybersecurity which could, potentially, reduce the costs of a significant cyber attack for medium sized firms as compared to small firms. The CSBS 2024 provides some evidence to support this point, finding that 55% of medium-sized businesses have a formal cyber incident response plan (compared to 22% of all businesses). More specifically, the CSBS asks questions about the technical controls that businesses employ regarding cyber security. These include: boundary firewalls and internet gateways; secure configurations; user access controls; malware protection; and patch management (i.e. applying software updates). In total 22% of businesses report having technical controls in all five areas. This is considerably higher for medium businesses at 53%. To this end, the survey notes that, "… larger organisations tend to treat cyber security more seriously, and consequently allocate more resources to it".[80]

[80] Cyber security breaches survey 2024 - GOV.UK

Whilst the average costs are lower in absolute terms for micro firms as compared to large firms, the Cyentia report points out that, as a share of annual revenues, the cyber attack costs can be more significant for micro firms as compared to large firms.

In terms of the average costs of a significant cyber attack, the modelling estimates that the information sector faces the highest average cost overall, with the entertainment, management and manufacturing sectors also experiencing high average costs of a significant cyber attack. The construction and real estate sectors are among those with the lowest average costs of a significant cyber attack.

This ranking appears to be broadly consistent with other reports and analysis – for instance, whilst the IBM report[81] (on the cost of data breaches) finds healthcare to have the highest cost of a data breach, it highlights the financial, industrial and technology sectors as also experiencing high costs. From a UK perspective, whilst there is a lack of sector specific data on costs of cyber attacks in the UK, DfE does collect information on the costs of cyber attacks experienced by state schools through its RPA team. The data collected by the RPA is confidential, so underlying data cannot be reported, however the data does suggest that the average cost of a cyber attack for the education sector estimated in this study (as set out in Table 4.11 above) is in line with RPA data. This provides some corroboration of the modelled estimates regarding their applicability to UK sectors.

4.2.4 Average costs by type of cyber attack

Having estimated costs of significant cyber attacks by sector and firm size, the average costs by type of attack are then considered.[82]

The results from the literature review highlight that there is no consistent, agreed upon, definition for the different types of cyber attack experienced by firms. As a result, data or information on the cost of significant cyber attacks split by the type of attack tends to be inconsistent.

The Cyentia report, which is used for the majority of inputs to the model, classifies the type of cyber attack into the following categories:

- Accidental disclosure: data stores that are inadvertently left accessible to unauthorised parties, typically through misconfigurations on the part of the data custodian.
- Denial of Service (DoS) attack: any attack intended to render online systems, applications or networks unavailable, typically consuming processing or bandwidth resources.
- Insider misuse: inappropriate use of privileged access, either by an organisation's own employees and contractors or a trusted third party.
- Physical threats: threats that occur via a physical vector, such as device tampering, snooping, theft, loss, sabotage and assault.
- Ransomware: a broad family of malware that seeks to encrypt data with the promise to unlock upon payment or seeks to completely eradicate data/systems without the pretence of collecting payment.
- Scam or fraud: any incident that primarily employs various forms of deception to defraud the victim of money, property, identity, information etc.[83]
- System failure: unintentional service disruption, e.g. environmental hazards or network malfunctions.

[81] Cost of a data breach 2024 | IBM
[82] As set out in Section 4.2.2, the geometric mean is used for the average costs of a cyber attack.
[83] It should be noted that whilst this attack type is included in the Cyentia report (and so reported here for consistency), the resulting estimates for scams and frauds should not be viewed as appropriate standalone estimates of fraud and are not comparable to other estimates of fraud costs, including those published elsewhere by the Home Office. Other published estimates of fraud, including those of the Home Office, are undertaken using a different methodology and use the available UK-focused data. The Cyentia data is also anticipated to capture higher value losses, rather than being representative of all fraud loss to business.

— System intrusion: all attempts to compromise systems, applications, or networks by subverting logical access controls, elevating privileges, deploying malware etc.

However, other reports define different categories of type of cyber attack. For instance, the reports by NetDiligence (which primarily look at cyber insurance claims) cite various other types of cyber attack, including categories such as: business email compromise; malware/virus; and phishing. Similarly, the categories of cyber attack defined in the CSBS do not fully align to the categories used in other reports. Furthermore, Cyentia includes fraud/scams as a form of cyber attack, which would also not be captured as a cyber attack in other reporting. For example, from a Home Office perspective, whilst cyber attacks / cyber crimes can help facilitate fraud, they are defined, counted and reported on differently as part of other crime recording measures

For the purposes of this study, the Cyentia definitions are used, given the availability of data on both cost and prevalence across these categories of attack type, and for consistency with other elements of the modelling.

Estimating the cost of different types of significant cyber attacks, requires data on the prevalence of different types of attack. Whilst the CSBS does provide data on the prevalence of different types of cyber attack, the definitions of the type of attack are not consistent with the information in the Cyentia report. This means it would be difficult to align prevalence data by type of attack from CSBS with the financial impact of different types of cyber attacks set out in the Cyentia report.[84] As a result, the Cyentia data alone is used for this part of the modelling.

As well as information on the prevalence of different types of attack, estimating the cost of different types of cyber attacks also requires data, or information, on the relative costs of different cyber attacks. Information provided by the Cyentia report on both the frequency and financial impact of significant cyber attacks is set out in Table 4.12 below. The frequency data shows the number of each type of attack as a share of the total number of significant attacks recorded; whist the cost data shows the total cost of all attacks of a certain type as a share of the total cost of all significant attacks. Combined the data also provides an indication of the relative average cost of significant attacks. For example, there are some types of attack (e.g. system failure) which have low prevalence, but a make up a relatively high share of total costs, implying a high average cost of these attacks; whilst others (e.g. accidental disclosure) are relatively common but make up a relatively lower share of total costs, indicating a low average cost of these attacks. Table 4.12 also indicates why definitions of what constitutes a cyber attack are important. This is because both Table 4.12 and Table 4.13 show that, according to the Cyentia report and data, scam or fraud constitutes a sizeable share of the total costs of cyber attacks.

Table 4.12: Ranking of common types of significant cyber attack with relative frequency and attack cost statistics (based on underlying US data)

	Frequency		Cost of cyber attack	
Type of attack	Percentage	Overall rank	Percentage	Overall rank
Accidental disclosure	23.3%	2nd	5.2%	4th
DoS attack	1.6%	6th	0.8%	8th
Insider misuse	6.3%	5th	2.9%	6th
Physical threat	11.0%	3rd	3.5%	5th
Ransomware	6.5%	4th	7.0%	3rd
Scam or fraud	1.4%	7th	18.4%	2nd
System failure	0.3%	8th	1.8%	7th
System intrusion	49.6%	1st	60.2%	1st

Source: Cyentia IR 2022 Table 8.

[84] There is no consistent, agreed upon, definition for the different types of cyber attacks. Some of the Cyentia categories could be considered to read directly across to the categories of attack type in the CSBS – for instance: denial of service (DoS) attacks; ransomware; and insider misuse. However, most of the other categories covered in the CSBS are probably best considered as methods that could result in the 'system intrusion' category in the Cyentia report (these being: phishing attacks; takeovers; people impersonating the organisation or staff; and devices targeted with other malware). It is not clear what category the hacking of online bank accounts covered in the CSBS would fall into in the Cyentia report.

In the model, the frequency percentages set out in Table 4.12 are applied to the total number of significant cyber attacks in the US by sector and size (i.e. Table 4.4). This provides an estimate of the number of significant attacks split by the different types of cyber attack. The financial impact percentages are also applied to the total costs of significant cyber attacks in the US split by sector and size (i.e. Table 4.10). This provided an estimate of the total costs of significant cyber attacks in the US split by type of cyber attacks. Dividing the estimate of the total costs of significant cyber attacks split by type of cyber attack by the estimate of the total number of significant attacks split by different types of cyber attacks provides for an estimate of the average costs of significant cyber attacks by different types of cyber attack.

The simplifying assumption that would be required to produce estimates of the costs of significant cyber attacks by type of attack and by sector using this approach, and based on the available underlying data, is that the likelihood of different types of attack is 'common' across different sectors. This is unlikely to be true. For instance, the data in Figure 16 in the Cyentia report[85] shows that different sectors experience different rankings of cyber attack techniques (e.g. phishing or external remote services), which would suggest that different sectors may experience different types of cyber attack. However, there is little quantitative information or data with which to robustly adjust the estimates. As a result, the estimates of costs by type of attack are reported here as averages across all sectors, as shown in Table 4.13, and are best interpreted as indications of the costs by type of attack.

Table 4.13: Estimates of the average cost to a UK organisation of a significant cyber attack split by type of attack (2024 prices)

Type of cyber attack	Total
Accidental disclosure	£43,546
DoS attack	£97,560
Insider misuse	£89,817
Physical threat	£62,083
Ransomware	£210,128
Scam or fraud	£2,564,422
System failure	£1,170,714
System intrusion	£236,818

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data.
Note: The data in this table is based, predominantly, on underlying US data and is converted from US dollars to UK pound sterling using the OECD's PPP.

In order to test the robustness of the results, they have been compared to wider evidence on the costs of different types of cyber attacks. This shows that there is variability in the cost estimates across various sources and the existing estimates differ from the modelling results. This highlights the indicative nature of the results produced (as reported in Table 4.13). For example, the IID provides information on the cost of a DoS attack and ransomware attack and reports these costs as relatively similar to the modelling results. However, the average ransomware cost set out in Table 4.13 is lower than that suggested in the IID. The ransomware figure also is lower than some estimates provided in other data or literature, such as the Sophos report which estimates a global median recovery cost of just under £500,000[86], but is higher than other estimates, such as that contained in the Verizon Data Breach Investigations Report[87] which estimated a median cost of £17,000.

4.2.5 Breakdown of average costs by type of costs

In addition to costs of attack by sector, firm size and attack type, DSIT is also interested in identifying how costs of attacks by sector are split by type of costs.

[85] IRIS-2022_Cyentia.pdf
[86] Sophos state of ransomware 2024
[87] 2023 Data Breach Investigations Report, Verizon - Business Technology Reports | Verizon

The Home Office report into the costs of crime and cyber crime[88] breaks the cost of attacks into the following categories:

- Costs in anticipation: this should include but is not limited to the costs associated to the implementation of specialist staff or money spent on upskilling existing cyber security technicians and staff across an organisation and the implementation of new cyber security technology and process. This could also look at more technical memory safety fixes and estimate the costs of improving these.
- Costs as a consequence: this should include but is not limited to costs associated with reputational damage to organisations post attack, direct and indirect costs to organisations of personal data lost/stolen, ransom payments made and recovery time cost for business. In addition to the impact on individual organisations, the department also wants to understand how attacks and fear of attacks may impact sectors and the economic more widely.
- Costs in response: this should include but not be limited to costs associated with reporting and administrative costs, fines and legals costs, public relations (PR) costs, new IT/training/intervention as a direct response to the incident, people employed via private sector to investigate (as opposed to law enforcement investigating).

Costs in response to, and costs as a consequence of, a cyber attack both relate directly to a cyber attack experienced by a business. These are the costs that are typically cited in existing literature and datasets as the costs of a significant cyber attack. Indeed, the findings from the literature review illustrate that most research focuses on post-incident costs, such as remediation, downtime, and legal fees, while pre-attack expenditures and long-term economic impacts are inconsistently measured. Costs in anticipation tend to be incurred by businesses irrespective of whether they have been attacked or not and arguably relate to the existence of a threat of cyber attacks rather than to a specific incident. As such they largely represent business as usual costs, for example, insurance costs, training costs and general on-going cyber protection costs (e.g. software packages).

The Cyentia report does not split costs out into the Home Office categories. Indeed, findings from the literature review show that studies typically fail to disentangle costs into these categories.[89] However, some US studies of cyber costs do split out the costs of significant cyber attacks into other related classifications. These classifications are used to provide a best estimate of the share of costs that pertain to costs as a consequence of, and costs in response to, a significant cyber attack.

Three sources in particular are identified as providing information on the breakdown of significant cyber attack costs into different cost categories. These are NetDiligence, Ponemon and Kaspersky.[90]

In order to provide an indication of the relative size of costs in response to a significant cyber attack and costs as a consequence of a significant cyber attack, the cost categories from each of these three sources are matched to the Home Office cost categories. A more detailed outline of the analysis conducted is set out in Appendix 2. Given the cost categorisations do not directly align, there is some subjectivity in this analysis. Therefore, whilst the allocation of costs to Home Office categorisations were sense-checked with DSIT, Home Office and both KPMG and UCL cyber subject matter experts, the allocation is best considered as illustrative of the potential split of significant cyber attack costs into the two different Home Office categorisations.

For the reasons set out above, it is difficult to be definitive about the share of significant cyber attack costs that can be attributed to the Home Office cost categories. However, what evidence is available seems to suggest that costs are reasonably evenly split between costs in response to and costs as a consequence of a significant cyber attack. Table 4.14 (reproduced from Appendix 2 here) compares the share of significant cyber attack costs attributable to the two Home Office cost categorisations (i.e. costs in response and costs as a consequence) across the three different reports considered. A simple average (i.e. arithmetic mean) across the different estimates suggests that costs in response

[88] The economic and social costs of crime and Understanding the costs of cyber crime
[89] See for instance: 'Cost of a data breach 2024 | IBM' - https://www.ibm.com/reports/data-breach and Cybersecurity and Infrastructure security agency, 'Cost of a cyber incident: systemic review and cross validation', 2020.
[90] Data and information for all three reports are summarised in CISA - Cost of a Cyber Incident: Systematic Review and Cross-Validation

to a significant cyber attack could vary between 41% and 45% compared to between 55% and 59% for costs as a consequence. The data analysed suggests that for small and medium sized businesses slightly more than half the costs of a significant cyber attack may relate to costs as a consequence of a significant cyber attack. That situation is reversed for large businesses.

Table 4.14: Comparison of share of cost categories across different reports

Report	Size of firm considered	Share of costs in response (%)	Share of costs as a consequence (%)
Net Diligence	SMB*	47.0	53.4
	Large entities	52.6	47.1
Ponemon	All	28.0	72.0
Ponemon (excluding lost business)	All	54.9	45.1
Kaspersky	SMB* 2017	41.0	59.0
	SMB* 2018	49.7	50.3
	Large entities	53.1	46.9
Simple average of all reports		**45.2**	**54.8**
Simple average of SMBs		**41.4**	**58.7**
Simple average of large entities		**44.6**	**55.3**

Source: NetDiligence (2019); Ponemon Institute (2017); and Kaspersky Lab (2017, 2018) with KPMG analysis.
Note: All simple averages (arithmetic means) include the Ponemon report (but exclude the Ponemon report excluding lost business). * Small and Medium sized businesses (SMB)

4.3 Total cost to businesses of significant cyber attacks at the UK economy level

4.3.1 Overview of approach to scaling average costs

To estimate the total cost to businesses of significant cyber attacks at the UK economy level, information on the likelihood of a significant cyber attack from the CSBS is coupled with data from the ONS on the number of firms split by firm size and by sector. This provides an estimate of the number of businesses experiencing a significant cyber attack in the UK per annum using UK data.

A significant cyber attack is categorised as an attack resulting in both a negative outcome (as defined by the CSBS) and a cost of at least £500. That is, the CSBS is filtered to focus on the number of significant cyber attacks only. This is because the CSBS records a large number of cyber attacks that have no impact, outcome or cost. Indeed, the report notes that, "… a large proportion of attacks are unsuccessful." As a result, filtering the CSBS to focus on significant cyber attacks is necessary in order to align the data with the types of cyber attack that are considered in the cost estimates covered in the Cyentia report (which, being publicly available costs, tend to cover the more significant costs of cyber attacks).

The figures on the number of firms experiencing a significant cyber attack are then applied to the estimates of the average total cost of significant cyber attacks (from Table 4.11) to provide an estimate of the total cost to businesses of significant cyber attacks at the UK economy level.

More detail on these steps is set out in the following sections.

4.3.2 Prevalence of significant cyber attacks in the UK

The CSBS provides data for the UK on the proportion of businesses experiencing a cyber attack and, of these, the proportion that result in negative outcomes. The CSBS finds that 50% of UK businesses experienced a cyber attack or breach in 2024. Of these businesses, just over one in ten (13%) experienced a negative outcome from the attack (so around 6.5% of all businesses experienced a

cyber attack with a negative outcome in 2024). The CSBS report notes that the low proportion stating a negative outcome indicates that a large proportion of attacks are unsuccessful.[91]

Focusing on negative outcomes, provides an indication of cyber attacks that are successful in breaching a firm's defences and result in an impact; it helps to filter out the cyber attacks that have no impact. Negative outcomes are described in the survey as being one of the following:

— website or online services taken down or made slower
— temporary loss of access to files or networks
— money stolen
— lost access to relied-on third party services
— compromised accounts or systems used for illicit purposes
— money was paid as a ransom
— software or systems corrupted or damaged
— personal data altered, destroyed or taken
— damage to physical devices or equipment
— permanent loss of files (not personal data)
— lost or stolen assets, trade secrets or intellectual property

However, in the CSBS many of these cyber attacks still result in minimal financial (or other) costs to businesses. Given the data reported by Cyentia captures publicly reported, significant, cyber attacks, the data used for the prevalence of cyber attacks needs to be consistent with that.

As a result, to estimate the proportion of firms experiencing a significant cyber attack, records from the CSBS are filtered to include only those experiencing a cyber attack that costs more than £500. The cut off of £500 in the CSBS is used because data from the Cyentia report[92] suggest that very few publicly reported cyber attacks involve a cost of less than £500 (based on predominantly US data). Table 4.15 below sets out how this likelihood of attack varies by size of business in the UK. Results are split by size of business because this provides for a larger sample of responses from the CSBS (for each category considered) than if the results were split by sector (although the number of responses is still relatively low). In addition, the cost of cyber attacks varies more by size of business than by sector.

Table 4.15: Likelihood (%) of UK business experiencing a cyber attack with a negative outcome and a cost of cyber attack of more than £500, split by size of business in 2024

	Micro	Small	Medium	Large	All
Proportion of businesses experiencing a cyber attack with a negative outcome and a cost of more than £500	2.9%	4.3%	6.6%	10.9%	3.1%

Source: CSBS with KPMG analysis.
Note: The number of observations for some of the subgroups reported in this table are less than 30 (the normal level for CSBS reports); nevertheless all subgroups have 18 or more observations.

Applying the percentages in Table 4.15 to the 2.7 million businesses in the UK distributed across firm size[93] (as set out in Table 4.16) means that almost 85,000 businesses in the UK are estimated to have experienced a significant cyber attack in 2024 (as shown in Table 4.17).

[91] Cyber security breaches survey 2024 - GOV.UK (Section 4.5)
[92] See Figure 7 at: IRIS-2022_Cyentia.pdf
[93] UK business: activity, size and location - Office for National Statistics

Table 4.16: Size distribution of UK businesses, 2024

	Micro	Small	Medium	Large	Total
Number of employees	0-9	10-49	50-249	250+	
Total number of firms	2,428,740	241,165	43,580	11,285	2,724,770

Source: ONS with KPMG analysis

Table 4.17: Number of UK businesses estimated to experience a significant cyber attack, 2024

	Micro	Small	Medium	Large	Total
Number of employees	0-9	10-49	50-249	250+	
Total number of firms	70,242	10,357	2,880	1,229	84,708

Source: KPMG analysis based on data from CSBS and ONS

Applying the average costs of a significant cyber attack by size of firm (from Table 4.11 and based predominantly on US data) to the number of businesses experiencing a significant cyber attack by size of firm (from Table 4.17) results in a total cost to businesses from significant cyber attacks at the UK economy level in 2024 of £14.7 billion. To put this figure in context, it represents around 0.5% of UK Gross Domestic Product (GDP) for 2024.[94]

4.4 Summary of results

Average costs to businesses from a significant cyber attack

Estimates of the average cost of a significant cyber attack split by sector and size of firm is shown in Table 4.11 (repeated below).

Table 4.11 (repeated): Estimates of the average cost of a significant cyber attack for a UK organisation split by sector and size of firm by turnover (2024 prices)

Sector	Micro	Small	Medium	Large	Average across all firms
Utilities	£93,665	£137,687	£124,245	£436,443	£210,837
Construction	£39,540	£58,926	£53,173	£149,340	£46,695
Manufacturing	£203,071	£293,337	£264,699	£846,619	£330,406
Trade	£161,644	£233,603	£210,797	£591,913	£224,280
Retail	£206,264	£306,183	£276,290	£919,026	£250,457
Transportation	£215,176	£326,481	£294,607	£951,442	£261,070
Information	£240,843	£364,709	£329,103	£1,101,588	£336,773
Financial	£203,811	£304,920	£275,151	£908,294	£309,181
Real Estate	£81,227	£122,551	£110,586	£374,666	£92,683
Professional	£240,453	£363,889	£328,363	£968,187	£271,683
Management	£225,566	£281,715	£254,211	£681,067	£333,943
Administrative	£115,702	£177,210	£159,909	£505,734	£129,474
Education	£69,771	£104,952	£94,706	£244,622	£98,343
Healthcare	£121,503	£181,636	£163,903	£483,312	£149,284
Entertainment	£298,780	£455,160	£410,723	£1,354,368	£331,113
Hospitality	£137,661	£206,022	£185,908	£555,397	£153,529
Other Services	£67,102	£102,043	£92,081	£246,037	£72,873
Public	£101,197	£113,848	£102,733	£216,653	£102,588
All sector average	**£152,766**	**£236,832**	**£216,818**	**£712,349**	**£194,729**

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data.
Note: The data in this table is based, predominantly, on underlying US data and is converted from US dollars to UK pound sterling using the OECD's PPP.

When interpreting these results it is helpful to compare to existing estimates of costs. Looking at the overall average cost across sectors and by size of firm, the figures from the modelling are

[94] GDP – data tables - Office for National Statistics

substantially higher than those produced by the CSBS. As noted in Section 3, there are questions around the accuracy of the financial costs reported in the CSBS. This is because survey findings necessarily depend on self-reported costs which may underestimate the true economic cost of breaches or attacks.[95] Indeed, the average costs of cyber attacks (calculated using arithmetic means, medians and/or geometric means) drawn from the CSBS appear to significantly underestimate the cost of a cyber attack when compared to other published information on the costs of cyber attacks (e.g. from insurance claims, publicly announced cyber attack costs and UK evidence on the cyber attack costs experienced by schools). For instance, the 2024 CSBS estimates a median average total cost of the most disruptive breach or attack (which resulted in a negative outcome or impact) as £500 across all businesses (£970 for large businesses) which is significantly lower than the estimates set out in Table 4.11.

The average significant cyber attack cost estimates are generally higher than the figures quoted in reports that use insurance data (like the NetDiligence reports). However, they are lower than the figures reported in the IBM cost of data breach report – which only considers the costs of data breaches and also incorporates wider costs of these cyber attacks. Whilst the IID does not provide estimates of the average total cost of significant cyber attacks, the estimates in Table 4.11 fall within the range of cost estimates produced for different significant cyber attacks for the financial, information, retail, manufacturing and real estate sectors from the IID. As a result, the cost estimates set out in Table 4.11 above fall within the broad range of different cost estimates available in the literature as well as the cost estimates contained in the IID (used for commercial cyber security purposes).

Average costs to businesses of significant cyber attacks by sector

Looking at sectors, in terms of the average costs of a significant cyber attack, the information sector is estimated to experience the highest average cost overall with the entertainment and manufacturing sectors also experiencing high average costs of a significant cyber attack. The construction and real estate sectors are among those with the lowest average costs of a significant cyber attack. This ranking appears to be broadly consistent with other reports and analysis – for instance whist the IBM report[96] (on the cost of data breaches) finds healthcare to have the highest cost of a data breach – it highlights the financial, industrial and technology sectors as also experiencing high costs.

From a UK perspective, whilst there is a lack of sector specific data on costs of significant cyber attacks in the UK, the Department for Education (DfE) does collect information on the costs of cyber attacks experienced by state schools through its risk protection arrangement (RPA). The data collected by the RPA is confidential, so underlying data cannot be reported, the data does suggest that the average cost of a significant cyber attack for the education sector estimated in this study (as set out in Table 4.11 above) is in line with their own data. This provides some corroboration of the modelled estimates regarding their applicability to UK sectors.

Average costs to businesses of a significant cyber attack by type of cyber attack

In relation to average costs of a significant cyber attack by type of attack, Table 4.13 sets out estimated costs below. Modelling to split these costs across sectors would rely on an underlying assumption that the prevalence of each of these types of attacks is the same across sectors, which evidence from the Cyentia report suggests is not the case. Therefore, results are split by type of attack only. The estimates set out in Table 4.13 are of a broadly similar scale to those estimated from the IID.

[95] As noted in the technical report accompanying the CSBS 2024 report (Section 1.2) - many organisations do not monitor their costs (in relation to cyber attacks) and given the survey may miss some of the most financially damaging cyber security attacks – respondents may underestimate the true economic cost of breaches or attacks. In the technical report, DSIT note that designing a methodology that accurately captures the financial implications of cyber security attacks is a, "significant challenge".

[96] Cost of a data breach 2024 | IBM

Table 4.13 (repeated): Estimates of the average cost to a UK organisation of a significant cyber attack split by type of attack (2024 prices)

Type of cyber attack	Total
Accidental disclosure	£43,546
DoS attack	£97,560
Insider misuse	£89,817
Physical threat	£62,083
Ransomware	£210,128
Scam or fraud	£2,564,422
System failure	£1,170,714
System intrusion	£236,818

Source: KPMG analysis based on Cyentia IR 2022, NAICS and Fortune 500 data.
Note: The data in this table is based, predominantly, on underlying US data and is converted from US dollars to UK pound sterling using the OECD's PPP.

Average costs to businesses of a significant cyber attack by type of cost

The Home Office report into the costs of crime and cyber crime[97] breaks the cost of cyber attacks into three categories: costs in anticipation; costs as a consequence; and costs in response of a cyber attack. Costs in response to, and costs as a consequence of, a cyber attack both relate directly to a significant cyber attack experienced by a business. These are the costs that are typically cited in existing literature and datasets as relating to the costs of a significant cyber attack. In contrast, costs in anticipation tend to be incurred by businesses irrespective of whether they have been attacked or not and arguably relate to the existence of a threat of cyber attacks than to a specific incident. As such they largely represent business as usual costs.

The Cyentia report does not split costs out into the Home Office categories. Indeed, studies typically fail to disentangle costs into these categories.[98]

However, three US studies of cyber costs are used (which do split out the costs of cyber attacks into different cost categories)[99] and these cost categories are allocated to the Home Office cost categorisations. This methodology provided for a best estimate of the share of costs that pertain to costs as a consequence and costs in response of a significant cyber attack.

The available evidence suggests that costs are reasonably evenly split between costs in response to and costs as a consequence of a significant cyber attack. The data analysed suggests that for small and medium sized businesses very slightly more than half the costs of a significant cyber attack may relate to costs as a consequence of a significant cyber attack. That situation is reversed for large businesses with the limited data available suggesting that this may be because of higher notification and legal costs for larger businesses as compared to smaller businesses.[100]

Total cost to businesses of a significant cyber attack at the UK economy level

Combining data on the likelihood of businesses experiencing a significant cyber attack from the CSBS with ONS data on the UK business population and estimates of the average cost of a significant cyber attack (based on predominantly US data) all split by size of firm results in an estimated cost to businesses of significant cyber attacks at the UK economy level of £14.7 billion, representing 0.5% of the UK's annual GDP.[101]

[97] The economic and social costs of crime and Understanding the costs of cyber crime
[98] See for instance: 'Cost of a data breach 2024 | IBM' - https://www.ibm.com/reports/data-breach and Cybersecurity and Infrastructure security agency, 'Cost of a cyber incident: systemic review and cross validation', 2020.
[99] Data and information for all three reports are summarised in CISA - Cost of a Cyber Incident: Systematic Review and Cross-Validation
[100] See Appendix 2 for more detail.
[101] This figure uses GDP at market and current 2024 prices

In relation to this total cost estimate, it is noted that, in general, estimates of the total cost of significant cyber attacks to an economy vary widely..[102] The estimate from this study relies on two key variables. The first is the estimated average cost of a significant cyber attack (as set out in Table 4.11 and based predominantly on US data), while the second is the estimated number of firms in the UK that experience such an attack per annum.

The estimated average costs of a significant cyber attack, being derived from publicly quoted figures and with a range of existing estimates against which the figures can be sense-checked, means that these figures are considered to provide reliable estimates of the costs of a significant cyber attack on businesses in the UK. Although the estimates are derived from US data there is no reason to believe there is a systematic difference between the costs incurred by US businesses as compared to UK businesses. Moreover, UK data for the education sector validates the cost estimates for that sector.

The estimated number of businesses that experience a significant cyber attack is considered to carry greater uncertainty. The CSBS is used in this study to estimate the number of UK businesses experiencing a significant cyber attack, and as set out in Section 4.3.2, steps have been taken to align the estimated prevalence of significant attacks with the nature of attacks captured within the Cyentia data on which average costs of attacks are based. However there remains a risk that the figures reported in the CSBS could overstate the number of firms experiencing a significant cyber attack and so there is a risk that the estimate for the cost to businesses of significant cyber attacks at the UK economy level reported here is an overestimate.

[102] Cost of a Cyber Incident: Systematic Review and Cross-Validation

5 Wider research insights

5.1 Introduction

As noted in the introduction to the scope of the study (Section 2.2), there are a number of agreed research questions in the research plan that are not explicitly covered by the modelling. These include some research questions considered as lower priority for this study.

The lower priority research questions are:

- Who are the bearers of the costs of cyber attacks? To include:
  - organisations who are directly and indirectly the victim of an attack
  - costs associated to the wider supply chain as a result of an attack
  - costs to the individual
  - cost to the sector
  - cost to the wider economy
- What proportion of attacks are related to memory safety?
- Does the malicious use of AI in cyber attacks increase the prevalence of successful cyber attacks; increase the likelihood of harm associated with cyber attacks; and/or increase the cost of harms associated with successful cyber attacks?

The following sections provide some evidence and findings, where available, on the broader research questions in turn.

5.2 Who are the bearers of the costs of cyber attacks?

Most of the literature investigated for the purposes of this study focuses on the direct costs to the organisation experiencing a cyber attack. However, attacks on some sectors have the potential to impact on individuals. For instance, findings from the literature review show that because attacks on the retail sector can implicate hundreds of thousands of retail store cardholders, the direct costs can reach millions in response, remediation, and card re-issuance fees. To this end, the review highlights previous breaches at Target in 2013 and Home Depot in 2014.[103]

In terms of the wider impacts of cyber attacks, evidence identified through the literature review highlights that attacks on the information, communication and technology (ICT) sector could have knock-on impacts on other sectors. The European Systemic Risk Board and IMF highlight ICT's cross-sector relevance with an attack on a major cloud or software provider, for instance, potentially cascading into widespread operational interruptions across client organisations in finance, manufacturing, and beyond.[104] Indeed, the IMF study highlights that highly interconnected sectors, such as finance or ICT, face amplified contagion risks where a single attack could cascade across multiple organisations, elevating the likelihood of extreme tail events. Another study identified through the literature review discusses how localized attacks on ICT nodes may propagate to education or trade sectors via shared digital infrastructures.[105]

Another example, cited in the literature review, relates to the potential impact of a cyber attack on the finance sector. Simulation-based approaches used by Federal Reserve analysts illustrate that a breach at a mid-sized bank can propagate liquidity shocks through the entire payment network.[106]

[103] G. Gavett, 'Could Target Have Prevented Its Security Breach?', Harvard Business Review; C. Brooks, 'The Target Breach 10 Years Later', Security Info Watch; and J. Stempel, 'Home Depot reaches $17.5 million settlement over 2014 data breach', Reuters, Nov. 24, 2020

[104] IMF, Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks and European Systemic Risk Board, 'Systemic cyber risk.', Publications Office, LU, 2020

[105] A. Agosto and P. Giudici, 'Cyber Risk Contagion', Risks, vol. 11, no. 9, Art. no. 9, Sep. 2023

[106] T. M. Eisenbach, A. Kovner, and M. J. Lee, 'Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis', 2021

Such systemic contagion will not be captured by purely incident-based analyses or analyses focused on direct costs.

Some studies, as referenced in the literature review, use scenario modelling or macro-level input–output analysis to simulate potential cascading effects across sectors. These models sometimes generate aggregate cost estimates that attempt to estimate not only the immediate financial losses for organisations subject to the cyber attack, but also second-order disruptions, such as supply chain bottlenecks, knock-on effects on trading partners, and long-term reputational harm. As noted in the literature review, while scenario modelling can illustrate how a single cyber attack could escalate to billions in economic damage, its outputs depend heavily on assumptions about attack severity, response speed, and intersectoral dependencies, assumptions that, if shifted, may alter estimates.

In addition, the CISA report[107] provides a summary of some reports that consider the aggregate costs of cyber attacks to the sector or wider economy level – although like most of the literature in this area it relates predominantly to the costs pertaining to US sectors and the wider US economy. The estimates in the reports covered by the CISA report tend to derive from an aggregation of individual organisation costs of cyber attacks to the sector or economy level rather than a consideration of the potential knock on impacts of cyber attacks to the sector or whole economy.

5.3 What proportion of attacks are related to memory safety[108]?

As noted elsewhere in this report, there is no consistent definition in the literature of the type of cyber attack that businesses experience. Similarly, it is difficult to find information in the literature, considered as part of this study, on the causes of different cyber attacks. As a result, it is not possible to robustly estimate the proportion of attacks that are related to memory safety within the parameters of this study.

5.4 How does the malicious use of AI in cyber attacks impact?

The review of literature, which focused primarily on the costs of cyber attacks, did not identify any information on the impact of AI on cyber attacks. However, it did highlight that one of the difficulties or challenges with estimating the costs of cyber attacks is the continuously evolving cyber threats. The literature review notes that new techniques relating to cyber threats can render historical data less useful in understanding future outcomes. Indeed, other literature illustrates that AI is being used as a new means of launching cyber-attacks, automating the attack process and arguably making it more efficient and effective.[109, 110, 111] As well as a means of launching cyber attacks, some literature notes the increasing use of AI to combat and defend against cyber attacks, with AI having the potential to improve cyber security in several areas, including automation, threat intelligence, and increased cyber defence.[112, 113]

[107] Cost of a Cyber Incident: Systematic Review and Cross-Validation
[108] Memory safety is a concept in computer programming that ensures programs access memory locations securely and correctly. It plays an important role in maintaining the security and reliability of software applications.
[109] The New Threat - Offensive AI vs. Cybersecurity
[110] An Overview of Cyber Threats Generated by AI - Neliti
[111] The AI-Based Cyber Threat Landscape: A Survey: ACM Computing Surveys: Vol 53, No 1
[112] Threats and Opportunities with AI-Based Cyber Security Intrusion Detection: A Review by Bibhu Dash, Meraj Farheen Ansari, Pawankumar Sharma, Azad Ali :: SSRN
[113] The Effects of Cyber Security Attacks on Data Integrity in AI | IEEE Conference Publication | IEEE Xplore

Appendix 1: Detailed literature review

A1.1 Overview of the approach to the literature review

Aim of the literature review

This literature review synthesises existing evidence on the prevalence and economic costs of cyber attacks across multiple sectors, including financial services, manufacturing, retail, real estate, and ICT. It examines the evidence suggesting estimates for both the prevalence and cost of cyber attacks and the methodologies used to measure these. Where possible, the review also considers sector-specific costs and prevalence, differentiating between types of cyber attacks, firm sizes, and categories of economic losses.

Literature review protocol

The overarching research question guiding this review is:

What are the socio-economic costs of cyber attacks across different sectors in the UK, and how do these costs vary depending on attack type, firm size, and industry preparedness?

The review is structured around two key research strands. The first strand explores the financial impact of cyber attacks across industries, analysing how different types of cyber threats, such as phishing, hacking of bank details, malware, or ransomware, result in varying levels of financial losses. The second strand investigates sectoral differences in how cyber attacks are experienced, focusing on which industries are most frequently targeted, how prepared they are to prevent attacks, and how effectively they respond when an attack occurs.

The review followed a dual search strategy, combining a systematic review of academic literature with a focused search of grey literature and news reports. The systematic review is conducted using structured search queries within academic databases (Web of science, Scopus, Google scholar, Nexis), covering peer-reviewed studies published from 2019 onwards. This strategy is divided into two sub-strands:

- Cost-related evidence – identifying studies that quantify the economic impact of cyber attacks, distinguishing between different attack types, sectors, and firm sizes.
- Prevalence and resilience – analysing research on the frequency of attacks across industries, differences in preparedness levels, and the effectiveness of sectoral responses.

Search terms are designed to retrieve publications discussing any type of cyber attack and their financial, business, or economic effects as described in Table A1.1.

Table A1.1: Search terms for costs and prevalence of cyber attacks per sector

Strands	Cost of cyber attacks per sector	Prevalence of cyber attacks per sector
Search terms	("cyber incident*" OR "cyberattack*" OR "cyber-attack*") AND ("economic cost*" OR "financial impact*" OR "cost*" OR "monetary impact" OR "business impact*" OR "individual impact*" OR "economic impact" OR "wider economy" OR "financial harm" OR "financial loss*" OR "socio-economic impact" OR "socio-economic cost" OR "socioeconomic impact" OR "socioeconomic cost") AND ("financial service*" OR "bank*" OR "manufacturing" OR "pharmaceuticals" OR "motor vehicles" OR "cars" OR "metals" OR "retail" OR "wholesale" OR "real estate legal services" OR "conveyancing" OR "broadband services" OR "information and communication" OR "broadband" OR "internet service provider*")	("cyber incident*" OR "cyberattack*" OR "cyber-attack*") AND ("prevalence" OR "probability" OR "incidence" OR "resilience" OR "preparedness" OR "readiness" OR "defence" OR "ISO270001" OR "essential*") AND ("financial service*" OR "bank*" OR "manufacturing" OR "pharmaceuticals" OR "motor vehicles" OR "cars" OR "metals" OR "retail" OR "wholesale" OR "real estate legal services" OR "conveyancing" OR "broadband services" OR "information and communication" OR "broadband" OR "internet service provider*")

Besides academic sources, a targeted review of grey literature and news reports was conducted to capture real-world case studies and practical insights that may be absent from academic research. This includes analysing cybersecurity reports from government agencies, regulatory bodies, and industry organisations. To ensure the relevance, quality, and applicability of the findings, studies were selected based on the following inclusion criteria:

- Academic literature: peer-reviewed articles
- Grey literature: industry reports, policy briefs, and government/NGO publications relevant to the cost of cyber attacks
- News articles: recent news articles covering specific cyber attacks, economic impacts, and sector-specific cases
- Topic relevance: studies specifically addressing sectoral impacts of cyberattacks or AI's role in cyber attack likelihood and costs
- Date range: publications from 2019 onwards (the last 5 years)
- Language: English only
- Geographic: mainly UK focus for news articles

Applying these criteria, 26 studies and reports were selected for inclusion in this review consisting of:

- 12 peer-reviewed academic studies
- 11 grey literature sources
- 3 news articles and case studies

These studies and reports are set out in Table A1.2 below.

Table A1.2: Studies and reports used in literature review

Publication type	Authors	Title	Journal	Year
Grey	International Monetary Fund (IMF)	Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks (chapter 3 on cyberrisks)	International Monetary Fund (IMF)	2024
Grey	Thomas M. Eisenbach, Anna Kovner, Michael Junho Lee	Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis	Federal Reserve Bank of New York, Staff Report No. 909	2021
Academic	Chris Florackis, Christodoulos Louca, Roni Michaely, Michael Weber	Cybersecurity Risk	The Review of Financial Studies	2022
Academic	Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, René M. Stulz	Risk management, firm reputation, and the impact of successful cyberattacks on target firms	Journal of Financial Economics	2021
Grey	European Systemic Risk Board (ESRB)	Systemic Cyber Risk	Publication of European Systemic Risk Board (ESRB)	2020
Academic	Arianna Agosto and Paolo Giudici	Cyber Risk Contagion	risks	2023
Academic	Angelo Corallo, Mariangela Lazoi, Marianna Lezzi, Pierpaolo Pontrandolfo	Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level	IEEE Transactions on Engineering Management	2023
Academic	Rokhaya Dieye, Ahmed Bounfour, Altay Ozaygen, Niaz Kammoun	Estimates of the macroeconomic costs of cyber-attacks	Risk Management and Insurance Review	2020
Academic	Maryam Firoozi and Sana Mohsni	Cybersecurity Disclosure in the Banking Industry: A Comparative Study	International Journal of Disclosure and Governance	2023
Academic	Mohammed S. Shafae, Lee J. Wells, Gregory T. Purdy	Defending Against Product-Oriented Cyber-Physical Attacks on Machining Systems	The International Journal of Advanced Manufacturing Technology	2019
Grey	IBM Corporation and Ponemon Institute	Cost of a Data Breach Report 2024	NA	2024
Academic	Olha Kovalchuk, Mykola Shynkaryk, Mariia Masonkova	Econometric Models for Estimating the Financial Effect of Cybercrimes	Proceedings of the 11th International Conference on Advanced Computer Information Technologies (ACIT)	2021

Grey	Published by McAfee	The Hidden Costs of Cybercrime	NA	2021
Grey	US Cybersecurity and Infrastructure Security Agency (CISA)	Cost of a Cyber Incident: Systematic Review and Cross-Validation	NA	2020
Academic	Sasha Romanosky	Examining the costs and causes of cyber incidents	Journal of Cybersecurity	2016
Grey	Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z.	Estimating the Global Cost of Cyber Risk	RAND publication	2018
Academic	Bennet Simon von Skarczinski, Arne Dreißigacker, Frank Teuteberg	Toward Enhancing the Information Base on Costs of Cyber Incidents: Implications from Literature and a Large-Scale Survey Conducted in Germany	Organizational Cybersecurity Journal: Practice, Process, and People	2022
Academic	Muriel F. Franco, Fabian Künzler, Jan von der Assen, Chao Feng, Burkhard Stiller	RCVaR: An Economic Approach to Estimate Cyberattacks Costs Using Data from Industry Reports	Computers & Security	2024
Academic	Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage	Measuring the Cost of Cybercrime	Book chapter	2013
Grey	European Union Agency for Cybersecurity (ENISA).	ENISA Threat Landscape 2024.	European Union Agency for Cybersecurity (ENISA).	2024
News	BBC News	NZ Takes Action Over Stock Market Cyber Attacks	BBC News	2020
News	Maria Henriquez	Banking Industry Sees 1,318% Increase in Ransomware Attacks in 2021	Security Magazine	2021
News	SEC	SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies	SEC newsroom	2023
Grey	Cyentia Institute	IRIS 2022: The Information Risk Insights Study	Not applicable; published by Cyentia Institute.	2022
Grey	Thales Group	2022 Thales Data Threat Report: Retail Edition	NA	2022
Grey	Ponemon Institute LLC, Accenture	Ninth Annual Cost of Cybercrime Study	NA	2019

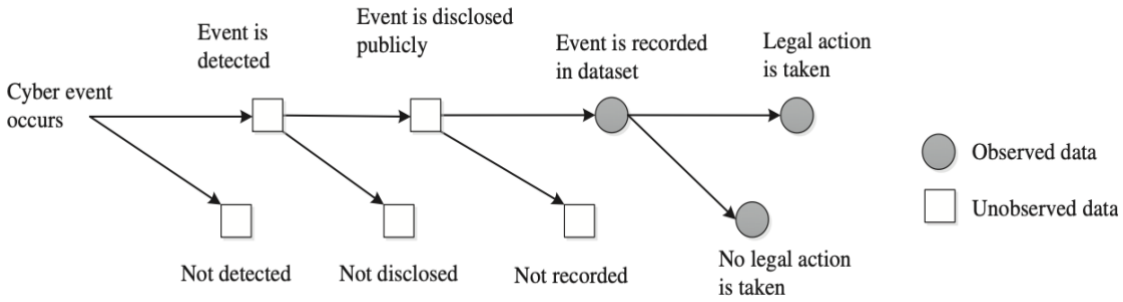
A1.2 Definitions of costs and prevalence

Definition and methodologies for estimating the prevalence of cyber attacks in the literature

In theory, one can understand the prevalence of cyber attacks as all attempts or incidents of cyber attacks, whether successful or unsuccessful, affecting a targeted group, such as businesses, governments, or individuals, within a timeframe. But in practice, the prevalence of cyber attacks is difficult to measure.

When Romanosky sought to study the costs and causes of cyber incidents, he described his data-generating process, as shown in Figure A1.1.[114] The figure illustrates the gaps between the theoretical occurrence of cyber attacks and their measurable prevalence. It shows the various stages through which a cyber event must pass to be included in a dataset. Initially, a cyber event occurs, but it might go undetected, particularly in cases of advanced persistent threats or attacks targeting less-secure systems. Even when detected, not all events are disclosed publicly, as organisations may withhold information to protect their reputation or avoid legal implications. Among publicly disclosed events, some may still not be recorded in datasets, as data collection frameworks may rely on voluntary reporting or specific regulatory mandates.

Figure A1.1: Data generating process (from Romanosky 2016)



This report uses Romanosky's data generation process as a proxy to understand prevalence as the frequency of successful cyber attacks being detected, disclosed, and ultimately included in the used datasets of that report:

- Detected by the targeted organisation, which excludes undetected and unsuccessful attacks.
- Publicly disclosed by the organisation.
- Recorded in the used datasets.

Definition and methodologies for estimating the cost of cyber attacks in the literature

As for measuring the cost of cyber attacks, the Home Office's framework defines the costs of cyber attacks as three-fold:[115]

- Costs in anticipation: spending on security solutions (e.g., antivirus software), cyber insurance, and compliance activities (e.g., meeting regulatory standards).
- Costs as a consequence: direct (e.g., ransomware payments) and indirect impacts (e.g., erosion of competitive advantage if intellectual property is compromised, reputational damages).
- Costs in response: compensation payments to victims, regulatory penalties, costs of breach notifications, investigation, and remediation.

[114] S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.
[115] UK Home office, 'The economic and social costs of crime Second edition', 2018. Accessed: Feb. 04, 2025. [Online].

In effect, the Home Office's conceptual three-category framework can help practitioners and researchers think systematically about where and how cyber attack costs arise. But it mainly exists in theory, insofar as actual measurement and reporting fail to disentangle each category. Studies converge on simplified divisions such as "direct versus indirect" or group multiple types of costs under broader umbrella terms such as "per-incident losses", "average cost of a data breach" or "total economic impact of an attack". For instance, IBM and the Ponemon institute in their 2024 Cost of data breach reports merge immediate technical remediation, legal fees, and lost customer trust into its headline figure for "average breach cost".[116] Likewise, the US Cybersecurity and Infrastructure Security Agency uses "median loss per incident" including wide-ranging expenditures and impacts.[117]

For this report, the literature gathered focuses primarily on costs arising after a cyber attack. That is, the monetary and non-monetary impacts incurred as direct or indirect results of a cyber attack. This includes outlays for incident response, investigation, and remediation, as well as the knock-on effects of downtime, reputational loss, and any penalties or compensation. Whenever a specific study's methodology deviates from this definition (for instance, by including pre-emptive security spending or solely quantifying direct financial losses), it is clarified in the text to ensure consistency and transparency in how the cost of a cyber attack is being reported.

A1.3 Challenges of exploring costs and prevalence of cyber attacks

C1: Variation of reported incidents across regions, sectors and firm sizes

The datasets and case studies available in the literature focus disproportionately on the US. One possible explanation could be the sheer volume of attacks targeting the US, often ranked as one of the most frequently attacked countries.[118, 119] While it is difficult to pinpoint all the underlying reasons, an additional likely factor is the regulatory requirements. On the regulatory side, the US has introduced multiple legal frameworks such as Health Insurance Portability and Accountability Act (HIPAA) for healthcare providers[120], the Gramm-Leach-Bliley Act for financial institutions[121], and US Securities and Exchange Commission guidelines for publicly traded firms[122] which all oblige organisations to publicly disclose breaches or cybersecurity attacks. These legal frameworks encourage more robust record keeping and produce a stream of publicly accessible data on cyber attacks for researchers to analyse. In comparison, other sectors, regions and small firms lack equivalent frameworks, which could explain why fewer attacks are documented, shared or analysed.

Differences in detection capacity also shape the data landscape. Larger enterprises have access to specialised cybersecurity teams or third-party security providers, are more likely to spot and report breaches accurately, thereby generating detailed incident reports. Meanwhile, smaller organisations may lack these resources or not have an obligation to report what they detect. As a result, many attacks within that segment remain invisible to researchers and practitioners.

Consequently, what appears in the literature, including the present report, may skew toward large US entities, masking the broader prevalence and cost of cyber attacks in other scales, sectors and regions.

[116] 'Cost of a data breach 2024 | IBM'. Accessed: Jan. 07, 2025. [Online].
[117] Cybersecurity and Infrastructure security agency, 'Cost of a cyber incident: systemic review and cross validation', 2020. Accessed: Feb. 04, 2025. [Online].
[118] R. Dieye, A. Bounfour, A. Ozaygen, and N. Kammoun, 'Estimates of the macroeconomic costs of cyber‐attacks', Risk Manage Insurance Review, vol. 23, no. 2, pp. 183–208, Jun. 2020, doi: 10.1111/rmir.12151.
[119] IBM, 'Cost of a Data Breach Report 2024', 2024.
[120] O. for C. Rights (OCR), 'Summary of the HIPAA Privacy Rule'. Accessed: Feb. 04, 2025. [Online].
[121] 'Gramm-Leach-Bliley Act | Federal Trade Commission'. Accessed: Feb. 04, 2025. [Online].
[122] 'SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies'. Accessed: Feb. 04, 2025. [Online].

C2: Accurately measuring cost: heavy-tailed distribution, cost-per-record fallacy and contagion

A recurring theme in cost analyses of cyber attacks is that losses follow a heavy-tailed or "Pareto-like" distribution.[123] This means that a small number of extremely large events can drive a disproportionate share of total costs. Empirical studies from the Cyentia Institute and Rand Corporation suggests that, while many breaches are relatively modest, a handful can exceed hundreds of millions or even billions of dollars.[124,125] These catastrophic cyber attacks are outliers which may skew average loss figures and make it difficult to generalise and aggregate the losses of cyber events. One approach for modelling these losses had been to use log-normal distributions. It worked fairly well for moderate attacks but tend to underestimate the far-right tail, data points beyond $1B[126], where costs spike unpredictably. This disconnect between the bulk of observed cyber attacks and their most extreme exemplars complicates the task of capturing real financial exposure after a cyber attack.

In some cases, cost-per-record estimates have been used to approximate the financial impact of a cyber attacks, such as the cost of data breach reports. Recently, they have also come under scrutiny for potentially oversimplifying real-world losses. Not all expenses scale up or down with each additional record.[127] For small breaches, certain expenses, such as legal fees and forensic investigations tend to be relatively fixed. These up-front costs can push the per-record figure to high levels if few records are involved. Conversely, for massive breaches affecting tens or hundreds of millions of records, the per-record cost may sink. Many breach-related tasks do not multiply in perfect lockstep with each additional record. In other words, whether a breach involves ten million records or a hundred million, some costs may remain the same or grow at a slower rate, lowering the average cost per record. This pattern, high unit costs for small attacks and low unit costs for mega breaches, suggests a non-linear relationship between record count and total losses. Therefore, if an analysis uses a fixed per-record cost (e.g., $100 per record) to estimate breach expenses, it paradoxically risks both overestimating and underestimating the losses, depending on the breach size.

Adding yet another layer of complexity, the International Monetary Fund highlights that highly interconnected sectors, such as finance or ICT, face amplified contagion risks[128] where a single attack could cascade across multiple organisations, elevating the likelihood of extreme tail events.

Cybersecurity's empirical cost estimation remains an open question due to heavy-tailed distributions, the underestimation of the far-right tail, nonlinear costs, and sector-wide interdependencies.

C3: Range of different methodologies

One of the biggest difficulties in comparing cyber attack cost estimates is the broad variety of research methodologies.

For example, some studies adopt an incident-based approach, collecting data from insurance claims, news reporting, or mandated breach disclosures.[129,130,131] This method can be highly specific (recording precise losses, legal outcomes, or dates of occurrence) but risks under-representing attacks that are never disclosed or small firms that lack the obligation to report. And incident-based

[123] S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.
[124] S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.
[125] P. Dreyer et al., 'Estimating the Global Cost of Cyber Risk: Methodology and Examples', RAND Corporation, Jan. 2018. Accessed: Feb. 04, 2025. [Online].
[126] Cyentia institute, 'Information Risk Insights Study', 2022. Accessed: Feb. 04, 2025. [Online].
[127] Cyentia institute, 'Information Risk Insights Study', 2022. Accessed: Feb. 04, 2025. [Online].
[128] 'Global Financial Stability Report', IMF. Accessed: Feb. 04, 2025. [Online].
[129] S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.
[130] Cybersecurity and Infrastructure security agency, 'Cost of a cyber incident: systemic review and cross validation', 2020. Accessed: Feb. 04, 2025. [Online].
[131] International Monetary Fund, 'The Last Mile: Financial Vulnerabilities and Risks', 2024. Accessed: Jan. 08, 2025. [Online].

data may not fully capture contagions, indirect or long-term repercussions (e.g., reputational damage, consumer trust erosion) unfolding well beyond the initial breach window.

Other studies rely on self-reported surveys or in-depth interviews where organisations disclose their financial impacts, security spending, and downtime costs.[132,133] These can capture intangible costs and ongoing impacts more comprehensively, but they introduce challenges of inconsistent definitions: different firms might interpret "loss," "downtime," or "incident severity" quite differently. And again, some firms, especially smaller ones, may lack the resources or internal data to quantify cyber attack consequences.

A third group of studies uses scenario modelling or macro-level input–output analysis to simulate potential cascading effects across sectors.[134,135] These models may generate aggregate cost estimates where they account not only for immediate financial losses but also for second-order disruptions, such as supply chain bottlenecks, knock-on effects on trading partners, and long-term reputational harm. While scenario modelling can illustrate how a single cyber attack could escalate to billions in economic damage, its outputs depend heavily on assumptions about attack severity, response speed, and intersectoral dependencies, assumptions that, if shifted, may alter estimates.

Because of these disparate approaches, cross-study comparisons are challenging. Researchers have to rely on data with different definitions of incident, various reporting thresholds, and inconsistent approaches to calculating costs. As a result, even two rigorous analyses covering the same incident type can produce significantly different cost estimates, simply by virtue of their methodological lenses.

C4 Challenges in modelling estimates

Accurately modelling the cost, prevalence, and downstream impacts of cyber attacks remains inherently complex, owing to several factors reflected in the literature:

- Dynamic threats: Cyber threats evolve continuously with new techniques rendering historical data less usable to understand future outcomes.[136] The variation of reported incident (see C1) and delayed breach detection render difficult to build timely or precise cost models.
- Context-specific costs: Evidence from large datasets, such as those analysed by the Cyentia Institute's IRIS 2022, suggests significant variability in breach costs. For example, in one dataset, the Gawker Media incident was associated with per-record costs exceeding \$180 million, whereas the MongoDB ransomware attack saw figures closer to a fraction of a cent per record. These observations point to how disruptions in different contexts, such as media versus database services, combined with the scale and nature of the attack, can lead to highly divergent financial outcomes. It can be very challenging for one simple formula or model to account for the full complexity of cyber-related losses across different organisations, attack methods, and industry contexts.
- Aggregation across different methodologies: As discussed in C3, the diversity of approaches introduces methodological heterogeneity. Each study or dataset may apply its own definitions, measurement tools, and collection processes. Combining those sources can produce an apples-to-oranges problem. As it is difficult to draw reliable, system-wide conclusions about cyber losses (especially when attempted to scale findings from one context or dataset to another).

[132] 'Cost of a data breach 2024 | IBM'. Accessed: Jan. 07, 2025. [Online].
[133] B. S. von Skarczinski, A. Dreißigacker, and F. Teuteberg, 'Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany', Organizational Cybersecurity Journal: Practice, Process and People, vol. 2, no. 2, pp. 79–112, May 2022, doi: 10.1108/OCJ-08-2021-0020.
[134] R. Dieye, A. Bounfour, A. Ozaygen, and N. Kammoun, 'Estimates of the macroeconomic costs of cyber-attacks', Risk Management and Insurance Review, vol. 23, no. 2, pp. 183–208, 2020, doi: 10.1111/rmir.12151
[135] P. Dreyer et al., 'Estimating the Global Cost of Cyber Risk: Methodology and Examples', RAND Corporation, Jan. 2018. Accessed: Feb. 04, 2025. [Online].
[136] A. Corallo, M. Lazoi, M. Lezzi, and P. Pontrandolfo, 'Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level', IEEE Transactions on Engineering Management, vol. 70, no. 11, pp. 3745–3765, Nov. 2023, doi: 10.1109/TEM.2021.3084687.

A1.4 Sector specific costs of cyber attacks

In light to the challenges described in part C and to provide a robust and consistent comparison across sectors, three key references (IBM (2024), Romanosky (2016), and Cyentia Institute (2022)) were selected as they provide the most complete and comparable data. While various sources discuss cyber attack impacts, these three studies were the only ones with sufficient depth and granularity to support a sector-by-sector analysis.

Each of these studies employs a distinct methodology, offering complementary perspectives on cyber attack prevalence and costs:

- Romanosky (2016) analyses publicly disclosed cyber incidents from the Advisen dataset (2004–2015), focusing on litigation data and financial losses from breaches. This study provides long-term insights into how different sectors have historically incurred cyber attack costs.
- Cyentia Institute (2022) aggregates findings from 77,000 cyber events also using Advisen's Cyber Loss Data to assess sector-specific cost distributions and incident frequencies. This large-scale statistical analysis enables a comparative understanding of loss variations across industries.
- IBM (2024) applies an activity-based costing approach, based on 3,556 interviews across 604 breached organisations worldwide (March 2023 - February 2024). By excluding very small and very large breaches, IBM's study refines sector-specific average breach costs, offering insights into direct and indirect financial consequences of cyber incidents.

Together, these three studies provide a sector-by-sector comparison across diverse variables and methodology, ensuring consistency in cost estimates and prevalence rates across industries. This approach allows for an exploration of which sectors are most vulnerable, how costs are distributed, and what factors contribute to sectoral resilience.

While these three studies serve as the primary sources for comparing cost and prevalence estimates across sectors, additional sources, including industry reports, policy briefs, and case studies, have been incorporated for completeness in each section.

D1 Financial services

Financial services have been discussed in the literature as a prime target for cyber attacks, with multiple studies pinpointing both the frequency and potentially systemic impacts of breaches.

In terms of prevalence, the financial sector emerges as one of the most frequently targeted industries.[137,138,139] Romanosky's study using the Advisen dataset, which relies on publicly disclosed breaches and legal records, shows that "Finance and Insurance" ranks among the highest in reported incidents. Likewise, the Cyentia institute report notes that finance is one of the sectors claiming a large share of incidents, while the US CISA's review indicates that high incident counts are observed when cyber loss data are aggregated by industry.[140,141] These methodologies, whether counting incidents per firm or aggregating by public disclosure, suggest that the financial sector is positioned near the top in terms of reported cyber events. This high frequency might be attributable to strict regulatory requirements that compel US banks and insurers to report data breaches.

Regarding costs, the financial sector presents a dichotomy between studies and variables (such as average and median estimates) as shown by Table A1.3.

[137] S. Romanosky, 'Examining the costs and causes of cyber incidents', *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.
[138] 'Cost of a data breach 2024 | IBM'. Accessed: Jan. 07, 2025. [Online].
[139] Cyentia institute, 'Information Risk Insights Study', 2022. Accessed: Feb. 04, 2025. [Online].
[140] Cybersecurity and Infrastructure security agency, 'Cost of a cyber incident: systemic review and cross validation', 2020. Accessed: Feb. 04, 2025. [Online].
[141] Cyentia institute, 'Information Risk Insights Study', 2022. Accessed: Feb. 04, 2025. [Online].

Table A1.3: Summary of the literature estimating costs of cyber attacks in the financial sector

Study	Variable	Estimate	Methodology
Romanosky 2016	Total losses by industry Weighted losses in millions of $/events	>$1,000M >$0.5 M	Derived from analysis of publicly disclosed cyber incidents (Advisen dataset, 2004–2015), using breach and litigation data as cost proxies.
Cyentia institute 2022	Losses observed per sector (geometric mean) Losses observed per sector 95th percentile	$437k $88M	Aggregated analysis from a dataset of 77K cyber events (Advisen's Cyber Loss Data).
IBM 2024	Cost of a data breach	$6.08M	For the 2024 report IBM calculated the average cost of data breach excluding very small and very large breaches. They used an activity-based costing based on in-depth qualitative data over 3,556 separate interviews with individuals at 604 organizations that suffered a data breach between March 2023 and February 2024

Romanosky reports a mean cost per attack of approximately $5.87 million, with a median cost of only $170,000, underscoring the heavy-tailed nature of loss distributions in this sector. The cost as a percentage of annual revenue is estimated at about 0.4%, meaning that even though some breaches are very costly, most events incur relatively modest direct expenditures.[142] In contrast, studies that incorporate broader cost measures, such as the Cyentia institute's analysis, suggests a range from $437,000 for a geometric mean of losses observed in the financial sector to as high as $88 million for the 95th percentile.

For the financial sector in particular, several studies emphasise the systemic nature of cyber risk in finance.[143] For example, simulation-based approaches used by Federal Reserve analysts illustrate that a breach at a mid-sized bank can propagate liquidity shocks through the entire payment network.[144] This systemic contagion is not captured by purely incident-based analyses or analyses focused on direct costs. The financial sector's true vulnerability is multidimensional, comprising both high attack frequency and significant indirect, systemic spillover effects, even if the median cost per event remains relatively low.

D2 Manufacturing

Prevalence in the manufacturing sector is suggested to be comparatively lower than in sectors like finance or retail. Manufacturing appears among the top five or six industries when considering the number of publicly disclosed attacks[145,146], but its overall frequency is constrained by the fact that breach notification laws typically focus on personal data exposures. Cyber attacks in manufacturing appear underrepresented in datasets that rely on public disclosures; especially those involving

[142] S. Romanosky, 'Examining the costs and causes of cyber incidents', *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.
[143] IMF, Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks. Washington, D.C.: International Monetary Fund, 2024. doi: 10.5089/9798400257704.082.
[144] T. M. Eisenbach, A. Kovner, and M. J. Lee, 'Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis', 2021.
[145] Cybersecurity and Infrastructure security agency, 'Cost of a cyber incident: systemic review and cross validation', 2020. Accessed: Feb. 04, 2025. [Online].
[146] Cyentia institute, 'Information Risk Insights Study', 2022. Accessed: Feb. 04, 2025. [Online].

operational disruptions or intellectual property theft, do not trigger mandatory reporting. This empirical bias means that the recorded prevalence in manufacturing could be underestimated.

In terms of cost, compared to finance, publicly available data on cyber attacks in manufacturing are comparatively sparse, which might be because mandatory disclosure laws centre on personal data breaches rather than disruptions to production or the theft of proprietary information. Despite this reporting gap, a few studies described in Table A1.4 rank manufacturing as one of the top six sectors for total costs from known attacks, suggesting that when events come to light, they can be extraordinarily damaging.

Table A1.4: Summary of the literature estimating costs of cyber attacks in the manufacturing sector

Study	Variable	Estimate	Methodology
Romanosky 2016	Total losses by industry Weighted losses in millions of $/events	>$1,400M >$1M	Derived from analysis of publicly disclosed cyber incidents (Advisen dataset, 2004–2015), using breach and litigation data as cost proxies.
Cyentia institute 2022	Losses observed per sector geometric mean Losses observed per sector 95th percentile	$467k $108M	Aggregated analysis from a dataset of 77K cyber events (Advisen's Cyber Loss Data).
IBM 2024	Cost of a data breach for the pharmaceutical sector only	$5.10M	For the 2024 report IBM calculated the average cost of data breach excluding very small and very large breaches. They used an activity-based costing based on in-depth qualitative data over 3,556 separate interviews with individuals at 604 organizations that suffered a data breach between March 2023 and February 2024

Other academic studies, such as those employing case-study methodologies[147] or experimental setups[148], suggest that when cyber-physical attacks occur, such as those affecting industrial control systems or compromising production line integrity, the per-incident cost can reach several million dollars. The manufacturing sector has specific characteristics that differentiate it from others. With risks stemming from disruptions to production processes, sabotage of ICS, or theft of proprietary designs and trade secrets. In their study, Shafae, Wells, and Purdy highlight product-oriented cyber-physical attacks that can degrade product quality in ways that may go undetected until significant physical or reputational harm has occurred.[149] These types of incidents are less likely to trigger the public disclosure mechanisms, because there are no mandatory disclosure requirements, that drive datasets like Advisen, resulting in a lower apparent incident frequency. But, when such events occur, they are characterised by operational impacts (such as production downtime) which can translate into very high individual cost estimates.

[147] A. Corallo, M. Lazoi, M. Lezzi, and P. Pontrandolfo, 'Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level', IEEE Transactions on Engineering Management, vol. 70, no. 11, pp. 3745–3765, Nov. 2023, doi: 10.1109/TEM.2021.3084687.
[148] M. S. Shafae, L. J. Wells, and G. T. Purdy, 'Defending against product-oriented cyber-physical attacks on machining systems', Int J Adv Manuf Technol, vol. 105, no. 9, pp. 3829–3850, Dec. 2019, doi: 10.1007/s00170-019-03805-z.
[149] M. S. Shafae, L. J. Wells, and G. T. Purdy, 'Defending against product-oriented cyber-physical attacks on machining systems', Int J Adv Manuf Technol, vol. 105, no. 9, pp. 3829–3850, Dec. 2019, doi: 10.1007/s00170-019-03805-z.

D3 Retail

Retail stands out in the academic and industry literature for its prominent large-scale data breaches, typically involving the compromise of payment card data on major chains. Romanosky notes that while retail does not surpass finance in total events, it registers an especially high litigation rate [1], surpassing one in four reported incidents, reflecting a rapid consumer legal response to stolen credit card information.

Because attacks in retail can implicate hundreds of thousands of cardholders, the direct costs can reach millions in response, remediation, and card re-issuance fees, as illustrated by well-known breaches at Target in 2013 and Home Depot in 2014.[150,151,152]

Table A1.5: Summary of the literature estimating costs of cyber attacks in the retail sector

Study	Variable	Estimate	Methodology
Romanosky 2016	Total losses by industry Weighted losses in millions of $/events	>$1,200M >$1,5M	Derived from analysis of publicly disclosed cyber incidents (Advisen dataset, 2004–2015), using breach and litigation data as cost proxies.
Cyentia institute 2022	Losses observed per sector geometric mean Losses observed per sector 95th percentile	$354k $52M	Aggregated analysis from a dataset of 77K cyber events (Advisen's Cyber Loss Data).
IBM 2024	Cost of a data breach	$3,48M	For the 2024 report IBM calculated the average cost of data breach excluding very small and very large breaches. They used an activity-based costing based on in-depth qualitative data over 3,556 separate interviews with individuals at 604 organizations that suffered a data breach between March 2023 and February 2024

Again, the relative losses may vary depending on the context. For big-box retailers with annual revenues in the tens of billions of dollars, even a notable data breach may fall below one percent of turnover, remaining under typical materiality thresholds. In contrast, small or mid-tier retailers can be far more vulnerable, with multi-million-dollar losses representing a substantial portion of their yearly sales or operating margins, sometimes approaching existential scale.

Brand damage and legal consequences further shape the retail cost profile, especially reputational harm which may inflate or extend losses beyond the immediate response window. Kamiya et al. note that shareholder wealth losses in consumer-facing breaches can exceed direct out-of-pocket expenses, a difference attributed partly to the loss of consumer trust.[153] The repeated mention of

[150] G. Gavett, 'Could Target Have Prevented Its Security Breach?', Harvard Business Review. Accessed: Feb. 05, 2025. [Online].
[151] C. Brooks, 'The Target Breach 10 Years Later', Security Info Watch. Accessed: Feb. 05, 2025. [Online].
[152] J. Stempel, 'Home Depot reaches $17.5 million settlement over 2014 data breach', Reuters, Nov. 24, 2020. Accessed: Feb. 05, 2025. [Online].
[153] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, 'Risk management, firm reputation, and the impact of successful cyberattacks on target firms', Journal of Financial Economics, vol. 139, no. 3, pp. 719–749, Mar. 2021, doi: 10.1016/j.jfineco.2019.05.019

class-action lawsuits in IBM cost of databreach report and Romanosky underscores how retail data breaches typically trigger swift consumer litigation.[154,155]

D4 Real Estate

The literature focusing on the real estate sector reveals a relative dearth of publicly disclosed incidents. Romanosky uses the Advisen dataset and categorises "Real Estate, Rental, and Leasing" separately by North American Industry Classification System codes; but very few events appear in this category. Studies relying on publicly available data and legal filings rank real estate as a low prevalence sector. Romanosky, does not provide specific prevalence figures for real estate even although this may be an artifact of the data collection method rather than an accurate reflection of its underlying cyber risk.[156]

Cost estimates evidence for the real estate domain is similarly sparse. Romanosky provides weighted losses in millions of $/events as described in Table A1.6. But CISA does not provide any estimate for that sector, nor IBM offer separate monetary estimates for this sector.[157,158]

Table A1.6: Summary of the literature estimating costs of cyber attacks in the real estate sector

Study	Variable	Estimate	Methodology
Romanosky 2016	Total losses by industry Weighted losses in millions of $/events	- >$0.4M	Derived from analysis of publicly disclosed cyber incidents (Advisen dataset, 2004–2015), using breach and litigation data as cost proxies.
Cyentia institute 2022	Losses observed per sector geometric mean Losses observed per sector 95th percentile	$131k $4M	Aggregated analysis from a dataset of 77K cyber events (Advisen's Cyber Loss Data).
IBM 2024	Cost of a data breach	-	For the 2024 report IBM calculated the average cost of data breach excluding very small and very large breaches. They used an activity-based costing based on in-depth qualitative data over 3,556 separate interviews with individuals at 604 organizations that suffered a data breach between March 2023 and February 2024

A distinctive characteristic of the real estate sector is that when a breach occurs, typically involving compromised tenant or mortgage information, the litigation rate (i.e., the proportion of incidents that lead to legal settlements and remediation expenses) ranks 6th compared to other sectors.[159] Dieye et al. estimate the macroeconomic costs of cyber attacks by quantifying economic losses (in million

[154] 'Cost of a data breach 2024 | IBM'. Accessed: Jan. 07, 2025. [Online].
[155] S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.
[156] 'Cost of a data breach 2024 | IBM'. Accessed: Jan. 07, 2025. [Online].
[157] Cybersecurity and Infrastructure security agency, 'Cost of a cyber incident: systemic review and cross validation', 2020. Accessed: Feb. 04, 2025. [Online].
[158] IBM, 'Cost of a Data Breach Report 2024', 2024
[159] S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.

USD) across the top ten affected sectors during the first 180 days following an attack. Their analysis reveals that the Real Estate Activities sector ranks third, accounting for 9% of the total losses.[160]

D5 Information Communication Technology (ICT)

In many analyses, the ICT sector has a distinct significance due to its potential to amplify risks across multiple industries. Romanosky observes that ICT consistently shows one of the highest incident rates, can be above 1.5 percent of firms in the sample.[161] Both the European Systemic Risk Board and IMF corroborate ICT's cross-sector relevance: an attack on a major cloud or software provider, for instance, could cascade into widespread operational interruptions across client organizations in finance, manufacturing, or beyond.[162,163] Agosto and Giudici discuss how even localized attacks on ICT nodes may propagate to education or trade sectors via shared digital infrastructures.[164]

Table A1.7: Summary of the literature estimating costs of cyber attacks in ICT

Study	Variable	Estimate	Methodology
Romanosky 2016	Total losses by industry Weighted losses in millions of $/events	>1,600M >$1.6M	Derived from analysis of publicly disclosed cyber incidents (Advisen dataset, 2004–2015), using breach and litigation data as cost proxies.
Cyentia institute 2022	Losses observed per sector geometric mean Losses observed per sector 95th percentile	$476k $108M	Aggregated analysis from a dataset of 77K cyber events (Advisen's Cyber Loss Data).
IBM 2024	Cost of a data breach	$5.45M	For the 2024 report IBM calculated the average cost of data breach excluding very small and very large breaches. They used an activity-based costing based on in-depth qualitative data over 3,556 separate interviews with individuals at 604 organizations that suffered a data breach between March 2023 and February 2024

Cost estimates in the ICT sector reveal a heavy-tailed distribution. Table A1.7 provides granularity for ICT, reporting a typical (or "typical incident") cost of about $476,000, although extreme events in this sector are noted to reach much higher values (with the 95th percentile in the hundreds of millions).[165]

Although Agosto and Giudici do not present explicit cost figures, their study emphasises that modelling the financial impact of cyber attacks for the ICT sector must prioritise the analysis of systemic spillovers.[166] They employ a multivariate negative binomial score-driven model, an approach particularly well suited for rare events characterised by over-dispersion, to capture the costs

[160] R. Dieye, A. Bounfour, A. Ozaygen, and N. Kammoun, 'Estimates of the macroeconomic costs of cyber‐attacks', Risk Manage Insurance Review, vol. 23, no. 2, pp. 183–208, Jun. 2020, doi: 10.1111/rmir.12151.
[161] S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001
[162] IMF, Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks. Washington, D.C.: International Monetary Fund, 2024. doi: 10.5089/9798400257704.082.
[163] European Systemic Risk Board, 'Systemic cyber risk.', Publications Office, LU, 2020. Accessed: Feb. 05, 2025. [Online].
[164] A. Agosto and P. Giudici, 'Cyber Risk Contagion', Risks, vol. 11, no. 9, Art. no. 9, Sep. 2023, doi: 10.3390/risks11090165.
[165] Cyentia institute, 'Information Risk Insights Study', 2022. Accessed: Feb. 04, 2025. [Online].
[166] A. Agosto and P. Giudici, 'Cyber Risk Contagion', Risks, vol. 11, no. 9, Art. no. 9, Sep. 2023, doi: 10.3390/risks11090165.

associated with cyber attacks in the ICT sector. Their findings indicate that extreme ICT events exhibit a contagion effect: shocks in one sector significantly increase the likelihood of subsequent attacks in other sectors. This work supports the conclusions of both the ESRB and the IMF, which argue that accounting for interdependence in cyber cost analyses leads to considerably higher aggregated loss estimates due to the potential for cascading failures.[167,168]

A1.5 Conclusion of literature review

The literature review could only partially answer the question it sought to address. While it provides evidence of the socio-economic costs associated with cyber attacks across different sectors, significant gaps remain in quantifying costs by attack type, organisation size, and cost categorisation.

How do cost differences vary across sectors (with the sectors considered being: manufacturing; retail; financial services; broadband services; and real estate legal services)? Why?

The most robust and granular studies addressing costs and prevalence research questions per sectors were: Romanosky, Cyentia Institute and IBM cost of data breach with each contributing unique methodological insights.[169,170,171] However, the findings of the review underscore the difficulty in establishing a unified cost assessment, as methodologies vary across studies. Some focus on direct financial losses, while others incorporate systemic spillover effects, insurance payouts, or per-event costs. Table A1.8 provides a comparative view of these estimates.

Table A1.8: Summary by sectors of the costs of cyber attacks (underlined for lowest and bold for highest estimates)

Sectors	Total losses by industry (Romanosky 2016)	Weighted losses in millions of $/events (Romanosky 2016)	Losses observed per sector geometric mean (Cyentia institute 2022)	Losses observed per sector 95th percentile (Cyentia institute 2022)	Cost of a data breach (IBM 2024)
Financial (D1)	>$1,000M	>$0.5M	$437k	$88M	**$6.08M**
Manufacturing (D2)	>$1,400M	>$1M	**$476k**	**$108M**	$5.10M
Retail (D3)	>$1,200	>$1.5M	$354k	$52M	$3,48M
Real estate (D4)	-	>$0.4M	$131k	$4M	-
ICT (D5)	**>$1,600**	**>$1.6M**	**$476k**	**$108M**	$5.45M

[167] IMF, Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks. Washington, D.C.: International Monetary Fund, 2024. doi: 10.5089/9798400257704.082.
[168] European Systemic Risk Board, 'Systemic cyber risk.', Publications Office, LU, 2020. Accessed: Feb. 05, 2025. [Online].
[169] S. Romanosky, 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001.
[170] 'Cost of a data breach 2024 | IBM'. Accessed: Jan. 07, 2025. [Online].
[171] Cyentia institute, 'Information Risk Insights Study', 2022. Accessed: Feb. 04, 2025. [Online].

What are the socio-economic costs on different sectors of different types of cyber attack including?

Another limitation of the reviewed literature is that it does not provide a precise breakdown of costs by type of cyber attack across sectors. While some studies discuss general trends, such as the financial sector's susceptibility to bank fraud, none provide a detailed, comparative cost analysis across multiple attack vectors. Due to these gaps, no study provides a reliable breakdown of how costs vary by attack type.

Are there specific sectors that demonstrate higher resilience or preparedness to prevent and mitigate the impacts of cyber attacks, and why?

The literature indicates that certain sectors exhibit greater resilience and preparedness against cyber attacks, primarily due to regulatory mandates, financial resources, and industry-specific risk exposure. The financial sector (D1) is consistently discussed among the most cyber-resilient, as it not only experiences substantial losses but also implements stringent risk management frameworks, reducing the long-term financial impact of cyber attacks.[172,173] A study on Australian's Small and Medium Businesses (SMBs) reveals that, despite an awareness of cyber threats, many businesses lack the necessary financial resources, in-house cybersecurity expertise, and awareness of cybersecurity frameworks such as Essential Eight, and ISO 27001.[174] The study identifies significant gaps in risk identification, monitoring, and incident response preparedness, with SMBs relying heavily on external IT service providers without a clear understanding of their own security responsibilities. It also found budget constraints hinder investment in security tools and training, leaving many SMBs ill-prepared to detect and respond to cyber attacks effectively. This aligns with broader literature findings that indicate larger enterprises, particularly those in regulated industries, benefit from more mature cybersecurity strategies, while SMBs remain highly vulnerable because of financial and knowledge barriers.

How do these costs vary by type of cost (costs in anticipation; as a consequence; and in response to cyber attacks) and by firm size?

Studies on cyber attack costs by organisation size are limited, with relevant research focusing on Australian and German SMBs.[175,176] But small and micro businesses do report less cyber losses, either because of under-reporting or limited financial exposure. Medium and large firms experience higher costs, but estimates vary significantly by sector and event severity. In general, sectoral cost breakdowns by firm size remain absent from empirical studies.

Finally, the literature on cyber attack costs remains fragmented, with studies grouping expenses under broad terms like "average breach cost" or "per-incident losses", rather than systematically distinguishing between cost variations by attack type, organisation size, or cost category. Most research focuses on post-incident costs, such as remediation, downtime, and legal fees, while pre-attack expenditures and long-term economic impacts are inconsistently measured.

[172] IMF, Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks. Washington, D.C.: International Monetary Fund, 2024. doi: 10.5089/9798400257704.082.
[173] European Systemic Risk Board, 'Systemic cyber risk.', Publications Office, LU, 2020. Accessed: Feb. 05, 2025. [Online].
[174] A. Chidukwani, S. Zander, and P. Koutsakis, 'Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications', Computers & Security, vol. 145, p. 104026, Oct. 2024, doi: 10.1016/j.cose.2024.104026
[175] A. Chidukwani, S. Zander, and P. Koutsakis, 'Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications', Computers & Security, vol. 145, p. 104026, Oct. 2024, doi: 10.1016/j.cose.2024.104026
[176] B. S. von Skarczinski, A. Dreißigacker, and F. Teuteberg, 'Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany', Organizational Cybersecurity Journal: Practice, Process and People, vol. 2, no. 2, pp. 79–112, May 2022, doi: 10.1108/OCJ-08-2021-0020.

Appendix 2: Home Office cost categorisation

A2.1 Overview of the approach to Home Office cost categorisation

The Home Office report into the costs of crime and cyber crime[177] breaks the cost of attacks into the following categories:

- Costs in anticipation: this should include but is not limited to the costs associated to the implementation of specialist staff or money spent on upskilling existing cyber security technicians and staff across an organisation and the implementation of new cyber security technology and process. This could also look at more technical memory safety fixes and estimate the costs of improving these.
- Costs as a consequence: this should include but is not limited to costs associated with reputational damage to organisations post attack, direct and indirect costs to organisations of personal data lost/stolen, ransom payments made and recovery time cost for business. In addition to the impact on individual organisations, the department also wants to understand how attacks and fear of attacks may impact sectors and the economic more widely.
- Costs in response: this should include but not be limited to costs associated with reporting and administrative costs, fines and legals costs, PR costs, new IT/training/intervention as a direct response to the incident, people employed via private sector to investigate (as opposed to law enforcement investigating).

The two categories, costs in response to and costs as a consequence of a cyber attack, both relate directly to a cyber attack experienced by a business. These are the costs that are typically cited in the literature and datasets as relating to the costs of a significant cyber attack. Costs in anticipation tend to be incurred by businesses irrespective of whether they have been attacked or not and arguably relate to the existence of a threat of cyber attacks rather than a specific incident. As such they largely represent business as usual costs – for example insurance costs, training costs and general on-going cyber protection costs (e.g. software packages).

The Cyentia report, like many others, does not split costs out into the Home Office categories. Indeed findings from the literature review show that studies typically fail to disentangle costs into the Home Office categories. However, some US studies of cyber costs do split out the costs of significant cyber attacks into different classifications. These classifications are used to provide a best estimate of the share of costs that pertain to costs as a consequence of and costs in response to a significant cyber attack.

Three sources were identified as providing information on the breakdown of significant cyber attack costs into different cost categories. These were NetDiligence, Ponemon and Kaspersky.[178]

To try and provide some information around the relative size of costs in response to a significant cyber attack and costs as a consequence of a significant cyber attack, the cost categories from each of these three sources was matched with either one of the Home Office cost categories. However, each source has its own cost categorisations which are not consistent with one another or with the Home Office definitions. As a result, there is some subjectivity in this analysis and it is best considered as illustrative of the potential split of significant cyber attack costs into the two different Home Office categorisations.

[177] The economic and social costs of crime and Understanding the costs of cyber crime
[178] Data and information for all three reports are summarised in CISA - Cost of a Cyber Incident: Systematic Review and Cross-Validation

A2.2 NetDiligence report

NetDiligence reports data on cyber costs from cyber insurance claims.[179] Table A2.1 below sets out data from NetDiligence's 2019 report illustrating the per-event cost of a cyber attack split by different elements of cost. The data is further split into small and medium sized businesses and large entities. The table also shows the allocation that has been made of the different cost categories to either of the Home Office cost categorisations (consequence or response).

Table A2.1: NetDiligence (2019) per-event cost of a cyber attack by cost category

Cost category	No. of cases	Average cost ($000)	Total cost ($000)	Share of total cost (%)
SMBs				
Total Payout	1,753	136	238408	
Costs as a consequence				
Forensics Costs	935	72	67320	28.2
Credit/ID Monitoring Costs	295	45	13275	5.6
Other Crisis Services Costs	168	60	10080	4.2
Lost Business Income	95	343	32585	13.7
Recovery Expense	89	45	4005	1.7
Total share for costs as a consequence				53.4
Costs in response				
Notification Costs	350	75	26250	11.0
Legal Guidance/Breach Coach Costs	1123	28	31444	13.2
Legal Damages-Defense Costs	181	78	14118	5.9
Legal Damages-Settlement Costs	97	264	25608	10.7
Regulatory-Defense Costs	12	95	1140	0.5
Regulatory Fines	9	19	171	0.1
PCI Fines	19	700	13300	5.6
Total share for costs in response				47.0
Large Entities				
Total Payouts	51	3784	192984	
Costs as a consequence				
Forensics Costs	30	2036	61080	31.7
Credit/ID Monitoring Costs	16	1688	27008	14.0
Other Crisis Services Costs	13	218	2834	1.5
Lost Business Income	1		0	
Recovery Expense	1		0	
Total share for costs as a consequence				47.1
Costs in response				
Notification Costs	22	2400	52800	27.4
Legal Guidance/Breach Coach Costs	33	954	31482	16.3
Legal Damages-Defense Costs	8	1380	11040	5.7
Legal Damages-Settlement Costs	3		0	0.0
Regulatory-Defense Costs	5	1235	6175	3.2
Regulatory Fines	1		0	
PCI Fines	2		0	
Total share for costs in response				52.6

Source: NetDiligence (2019) data and KPMG analysis

Using the allocations to Home Office categories set out in Table A2.1 suggests that for small and medium sized businesses the costs as a consequence of a cyber attack constitutes 53% of significant

[179] See page 65 of Cost of a Cyber Incident: Systematic Review and Cross-Validation

cyber attack costs with costs in response to a cyber attack constituting 47%. These figures are reversed for large entities.

A2.3 Ponemon report

Table A2.2 below sets out data from the Ponemon Institute's 2017 report[180] illustrating the cost of a data breach split by different elements of cost. The table also shows the allocation that has been made of the different cost categories to either of the Home Office cost categorisations (consequence or response).

Table A2.2: Ponemon Institute (2017) Data breach cost by cost category (percentage)

Cost category	Percentage of total breach cost
Costs as a consequence of	
Investigations & Forensics	16
Audit & Consulting Services	4
Free or Discounted Services	1
Identity Protection Services	2
Lost Customer Business	41
Customer Acquisition	8
Total share for costs as a consequence	72
Costs in response	
Outbound Contact	3
Inbound Contact	4
PR	1
Legal - Defense	17
Legal - Compliance	3
Total share for costs in response	28

Source: Ponemon Institute (2017) data and KPMG analysis

Using the allocations to Home Office categories set out in Table A2.1 suggests that the costs as a consequence of a significant cyber attack constitutes 72% of cyber attack costs with costs in response to a significant cyber attack constituting 28%.

The Ponemon analysis separates out the figures for lost customer business and customer acquisition (which together constitute 49% of the cost of a cyber attack in the table above). If these elements are excluded from the costs of a significant cyber attack then costs as a consequence would constitute 45% of all significant cyber attack costs and costs in response 55%.

A2.4 Kaspersky Lab report

Table A2.3 below sets out data from Kaspersky Lab's 2017 and 2018 reports[181] illustrating the average costs of a breach split by different elements of cost. The data is further split into small and medium sized businesses and large entities. The table also shows the allocation that has been made of the different cost categories to either of the Home Office cost categorisations (consequence or response).

[180] See page 72 of Cost of a Cyber Incident: Systematic Review and Cross-Validation
[181] See page 78 of Cost of a Cyber Incident: Systematic Review and Cross-Validation

Table A2.3: Kaspersky Lab (2017, 2018) average breach cost by cost category

	2017		2018	
	Average breach cost ($000)	Share of breach cost (%)	Average breach cost ($000)	Share of breach cost (%)
SMBs				
Total Breach Cost	117		149	
Costs as a consequence				
Additional Internal Staff Wages	16	13.7	17	11.4
Lost Business	21	17.9	17	11.4
Employing External Professionals	21	17.9	23	15.4
Damage to Credit Rating/Insurance Premiums	11	9.4	18	12.1
Total share for costs as a consequence		59.0		50.3
Costs in response				
Extra PR	10	8.5	15	10.1
Compensation	8	6.8	7	4.7
Improving Software/Infrastructure	11	9.4	18	12.1
Training Staff	9	7.7	15	10.1
Hiring New Staff	10	8.5	14	9.4
Penalties and Fines		0	5	3.4
Total share for costs in response				
		41.0		49.7
Enterprise - total breach cost	1336			
Costs as a consequence				
Additional Internal Staff Wages	207	15.5		
Lost Business	148	11.1		
Employing External Professionals	154	11.5		
Damage to Credit Rating/Insurance Premiums	118	8.8		
Total share for costs as a consequence		46.9		
Costs in response				
Extra PR	113	8.5		
Compensation	147	11.0		
Improving Software/Infrastructure	172	12.9		
Training Staff	153	11.5		
Hiring New Staff	124	9.3		
Total share for costs in response		53.1		

Source: Kaspersky Lab (2017, 2018) data and KPMG analysis

Using the allocations to Home Office categories set out in Table A2.3 suggests that for small and medium sized businesses the costs as a consequence of a significant cyber attack constitutes between 50% and 59% of significant cyber attack costs depending on the year considered with costs in response to a significant cyber attack constituting between 41% and 50%. For large entities figures for 2017 only are available – which show the costs as a consequence of a significant cyber attack constituting 47% with costs in response to a significant cyber attack constituting 53%.

A2.5 Comparison of results

Table A2.4 compares the share of significant cyber attack costs attributable to the two Home Office cost categorisations (i..e. costs in response and costs as a consequence) across the three different reports considered. A simple average across the different estimates suggests that costs in response

to a significant cyber attack could vary between 41% and 45% compared to a between 55% and 59% for costs as a consequence.

Table A2.4: Comparison of share of cost categories across different reports

Report	Size of firm considered	Share of costs in response (%)	Share of costs as a consequence (%)
Net Diligence	SMB*	47.0	53.4
	Large entities	52.6	47.1
Ponemon	All	28.0	72.0
Ponemon (excluding lost business)	All	54.9	45.1
Kaspersky	SMB* 2017	41.0	59.0
	SMB* 2018	49.7	50.3
	Large entities	53.1	46.9
Simple average of all reports		**45.2**	**54.8**
Simple average of SMBs		**41.4**	**58.7**
Simple average of large entities		**44.6**	**55.3**

Source: NetDiligence (2019); Ponemon Institute (2017); and Kaspersky Lab (2017, 2018) with KPMG analysis.
Note: All simple averages (arithmetic means) include the Ponemon report (but exclude the Ponemon report excluding lost business). * Small and Medium sized businesses (SMB)

www.kpmg.com/uk