KPMG

The economic impact on consumers 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 29 October 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.

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 29 October 2024 and our work was completed on 28 April 2025. We have not undertaken to update our Report for events or circumstances arising after that date.

Contents

Glossary

Key Term	Definition
Cyber attack	A malicious and deliberate attempt to breach the information system of an individual or organisation.
Cyber security	A process, practice or technology put in place by organisations to secure networks, devices, programs or data they hold.
Denial of service attack	Attacks that try to slow or take down online services, to render the service inaccessible.
Hacking	The unauthorised access of files, networks, etc.
Malware	A type of computer program designed to infiltrate and damage computers without the user's consent e.g. viruses.
Phishing	Fraudulent attempts to extract information such as passwords or personal data.
Ransomware	A type of malicious software designed to block access to a computer system until money (a ransom) is paid.

Source: Definitions are based on the Cyber Security Breaches Survey, 2024. DSIT. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#appendix-b-glossary

Executive summary

Overview of the study

Digital transformation has the potential to improve lives in the UK and modernise the way government works.[1] However, as IT systems have become increasingly vital to the functioning of society and the economy, they have become valuable targets for cyber attacks.[2] Such cyber attacks impact consumers, businesses, and government, and have also resulted in anticipatory costs to help prevent future attacks.

While the impact on organisations is reasonably well-understood, the impact on consumers of cyber attacks has not often been considered when assessing harm from cyber attacks. DSIT therefore commissioned KPMG to conduct this study to assess the consumer harm arising from a loss of access to goods and services as a result of cyber attacks.

The study focuses on developing methodologies and producing estimates of the harm to consumers from cyber attacks on businesses that result in the loss of provision of specific goods and services in the following five sectors:

- Financial services: online banking, and motor vehicle insurance
- Health care sector: GP practices, and major hospitals
- Creative industries and arts: online ticketing, online video streaming services, and cultural institutions
- Real estate and renting: property purchases and renting
- Manufacturing: pharmaceutical manufacturing

Further details of the scope of the study and the rationale for the selection of the sectors and impacted goods/ services is explained in section 1.

The study involved:

- A literature review undertaken by academics at UCL Consultants Ltd. This included review of academic and grey literature, as well as of news articles and government and industry reports, to understand the existing evidence on the impact on consumers of the loss of provision of goods and services as a result of cyber attacks. The findings from the literature review are described in section 2.
- Impact maps were developed to show visually how cyber attacks may affect the provision of the goods and services of interest, how consumers may respond to the loss of access to these goods and services, and the resulting impacts on consumers. These are set out in section 3.
- Methodologies to assess, in monetary terms where feasible, the consumer impacts identified in the impact maps were developed in line with HMT Green Book guidance. These methodologies drew on the secondary data sources, and primary data collected through a consumer survey. The methodologies and associated limitations are set out in section 4.
- To estimate the impact on consumers of a loss of access to online banking services, online ticketing services, and online streaming services, a consumer survey was developed to obtain data on consumers' willingness to pay (WTP) to retain access to these services in the event of a hypothetical cyber attack scenario resulting in a loss of access to these services, and their willingness to accept (WTA) compensation . WTP and WTA are methods used to estimate how much consumers value a good or service.[3] The survey achieved 1,000

[1] Transforming for a digital future: 2022 to 2025 roadmap for digital and data - updated September 2023 - GOV.UK
[2] For example, Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? | Request PDF
[3] WTP reflects the maximum amount a consumer will pay for something, and WTA reflects the minimum amount a consumer will accept in compensation for a loss. Such stated preference techniques are in line with HMT Green Book guidance on the valuation of costs and benefits where there is no market price.

completed survey responses and the data was weighted to be representative of the UK population. Further details on the approach taken is set out in section 4.[4]

Summary of findings

For each sector, the findings from the literature review (as detailed in section 2 and Literature Review Appendix 2), and the estimated consumer impacts (as detailed in section 4) are summarised below.

Key findings: Financial services

Evidence shows that the financial sector is one of the most targeted industries for cyber attacks. The International Monetary Fund found that nearly one-fifth of all reported cyber incidents target financial firms.[5] The types of attacks discussed in the literature include phishing, ransomware and data breach incidents.

The literature reports that consumers act in various ways in response to cyber attacks. Some consumers switch to alternative providers,[6] while others attempt to adapt by using traditional banking methods, such as in-person visits to bank branches.

As for all sectors, the impact on consumers of cyber attacks targeting financial services varies depending on the type, scale, and duration of the attack. Across studies, frequently reported impacts on consumers include the inability to access funds, compromised personal information, and loss of trust in digital banking platforms.[7,8] For consumers who switch to alternative providers, impact can include fees, lost access to previous banking tools and disruptions to automated payments.[9]

Online banking

The estimated impact on consumers from a cyber attack scenario resulting in the loss of access to online banking services for a three-day period is shown in Table 1 below. This was estimated using the WTP and WTA values derived from the survey data, and the estimated number of consumers potentially impacted based on bank market share data.

Table 1: Estimated consumer impact of a cyber attack resulting in a three day loss of access to online banking services, 2024 prices

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Years per incident (approx.)
	Low	High		
Online Banking	£5.5m	£231m	0.27 per year	Once every four years

The impact on consumers per cyber attack resulting in the loss of access to online banking services is estimated to range from approximately £5.5m to £231m depending on the market share of the bank affected. The estimated frequency of a successful cyber attack in the sector leading to consumer impacts is once every four years.[10]

[4] Two approaches to elicit the WTP and WTA were used in the consumer survey; a double-bounded dichotomous choice approach, and an open-ended elicitation approach.
[5] International Monetary Fund, The Last Mile: Financial Vulnerabilities and Risks, 2024. Accessed: Jan. 08, 2025. [Online].
[6] L. Ali, F. Ali, P. Surendran, and T. Bindhya, 'The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services', IJEEEE, vol. Volume 7 Number 1, 2017, doi: 10.17706/IJEEEE.
[7] C. Castañeda, Patelco Credit Union ransomware attack halts banking services for nearly half a million members - CBS San Francisco. Accessed: Jan. 08, 2025. [Online].
[8] J. Flores, Massive Patelco cyberattack is still affecting half a million people. Here's how to protect yourself, San Francisco Chronicle. Accessed: Jan. 08, 2025. [Online].
[9] L. Ali, F. Ali, P. Surendran, and T. Bindhya, 'The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services', IJEEEE, vol. Volume 7 Number 1, 2017, doi: 10.17706/IJEEEE.
[10] This is based on the rate of successful ransomware attacks estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024) at 2.45% per large company per year.

The impact per consumer: The estimated WTP and WTA values derived from the survey data, varied from a WTP £4.34[11] to a WTA of £15.14. The scenario described to respondents was where the loss of access to their main online banking service was expected to last for three days and this would happen at a random time. It may be at a time when access to online banking services is not required, or when there is a greater need for access, such as when setting up a new recurring payment or before making a large purchase.

The number of consumers impacted: To estimate the number of consumers potentially impacted by a cyber attack, data on bank market shares by volume of main Personal Current Accounts (PCAs) is used from the CMA Retail Banking Market Investigation in 2016.[12] Taking the market shares by volume of PCAs (ranging from 2.5% to 30%), together with the estimated number of UK adults using online banking services (51 million), the number of consumers who may be impacted by a cyber attack resulting in the loss of access to online banking services for the customers of one major bank is estimated to range from 1.3 million (i.e. 2.5% of 51 million) to 15 million (i.e. 30% of 51 million).

Motor vehicle insurance

The estimated impact on consumers from a cyber attack scenario affecting a motor vehicle insurance provider resulting in 11 days[13] of disruption to services is shown in Table 2 below. This is based on the financial impact, in terms of the opportunity cost of payment delays, as a result of the cyber attack.

Table 2: Estimated consumer impact of a cyber attack resulting in 11 days of disruption to a motor vehicle insurance provider, 2024 prices

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Years per incident (approx.)
	Low	High		
Motor Vehicle Insurance	£0.011m	£0.688m	0.20 per year	Once every five years

The impact of a cyber attack on a motor vehicle insurance provider is estimated at £11,000 (for a small insurance firm and the lowest rate of interest) to £688,000 (for a large insurance firm and the highest rate of interest) per attack. The estimated frequency of a successful cyber attack in the sector leading to consumer impacts is once every five years.[14]

Motor vehicle insurance payments per provider: Using data on the estimated share of UK motor vehicle insurance payouts by motor insurance provider from the 2023 SFCR (Solvency and Financial Conditions Report) regulatory filings, and the annual value of motor vehicle insurance payments,[15] the payout per provider is estimated to range from £0.5bn to £2.3bn annually.

Payments during the period impacted by the cyber attack: The value of payments impacted during the period over which insurance payments are delayed due to a cyber attack is estimated to range from £14m to £39m, based on an estimated 11 day duration of disruption.[16]

Opportunity cost of payment delays: The opportunity cost to consumers of not receiving the payment earlier is estimated by applying a daily interest rate to the value of delayed payments associated with a cyber attack. The daily interest rate faced by individuals will depend on the financial

[11] The estimated WTP from the open-ended elicitation approach was £0 but this is not used in the subsequent analysis.
[12] Retail banking market investigation final report, table 5.1.
[13] Estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024).
[14] This is based on the rate of successful ransomware attacks estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024) at 2.45% per large company per year.
[15] The Association of British Insurers (2024) Motor insurers pay out record amounts to help keep motorists mobile | ABI
[16] Estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024).

circumstances of affected consumers, being higher for consumers who take out credit compared to those who otherwise would have saved the payment and foregone interest on this.

Key findings: Health care

Ransomware attacks, data breaches, and attacks on sub-contractors were all found to impact the provision of healthcare. The literature indicates that patients adapt in various ways when faced with disruptions. Evidence from the US shows that some patients sought care from private health care providers to avoid delays, incurring substantial out-of-pocket expenses, while others delayed or entirely avoided treatments, placing their health at further risk.[17]

The literature suggests that the impact on consumers of cyber attacks in the health care sector depends on the scale and duration of the attack, as well as the type of care patients required. Across reports and studies, patients frequently reported delays in accessing essential services (e.g. surgery, blood tests, prescriptions, etc.), often with serious consequences for their health and well-being.[18,19] News articles also discussed the psychological impact of disruptions, reporting it as distressing for patients, especially those requiring urgent care.

Major hospitals and GP Practices

The methodology used to estimate the health impacts on patients of cancelled appointments and procedures at hospitals and GP surgeries is based on a methodology used by the Department for Health and Social Care (DHSC) to estimate the impact of cancelled care as a result of the Covid-19 pandemic.[20] The estimated impacts are shown in Table 3 below.

Table 3: Estimated consumer impact of a cyber attack affecting major hospitals and GP Practices, 2024 prices

Service	Consumer impact per successful cyber attack	Estimated frequency (approx.)	Annual consumer impact
Major Hospitals	£11.141m	3 per year	£33.424m
GP Practices	£0.020m	37 per year	£0.740m

The consumer (patient) impacts per cyber attack are estimated at £11.14m per cyber attack on a major hospital, and £0.02m per cyber attack on a GP practice. Given an estimated three incidents per year for major hospitals,[21] and an estimated 37 incidents per year for GP Practices,[22] the annual patient impact is estimated to range from approximately £33.4m for cyber attacks on major hospitals to £0.74m for GP Practices.[23]

The impact per patient: It is assumed that of the patients affected by disrupted appointments and procedures, 50% go without care, while 50% would wait for care and lengthen the waitlist.[24] For those who forego care, the impact per patient is estimated using NHS data on the cost per appointment and

[17] M. Bohannon, Change Healthcare Cyberattack Disrupts Services Nationwide—Here's What To Know, Forbes. Accessed: Jan. 07, 2025. [Online].
[18] National Audit Office, Investigation: WannaCry Cyber Attack and the NHS. Report by the Comptroller and Auditor General, 2018. Accessed: Jan. 07, 2025. [Online].
[19] Cyber attack on hospitals impacts 1,130 operations in London, BBC News. Accessed: Jan. 07, 2025. [Online].
[20] Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity. Shared by DHSC via email.
[21] This is based on the observed frequency of cyber attacks in major hospital over the 2024 calendar year.
[22] This is based on the rate of successful ransomware attacks estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024) at 0.475% per year for the charities and education section.
[23] For the other services in scope of this study, the estimated annual frequency is not a whole number and therefore DSIT requested that an annual consumer impact was not estimated given the binary nature of cyber attacks.
[24] This assumption is sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity.

converting this into a Quality Adjusted Life Years (QALY),[25] using a marginal value per QALY of £15,000.[26] For those waiting for care, the impacts on the waitlist were modelled in line with the DHSC methodology, with a group of patients experiencing reduced quality of life for the duration of their wait, resulting in an estimated QALY impact due to the lengthened waitlist. The QALY impacts were monetised using the HMT Green Book value of £70,000 per QALY.[27]

Number of patients impacted: Data from the 2024 Synnovis cyber attack on London hospitals, and the reduction of GP appointments during the 2024 CrowdStrike cyber incident[28] was used to estimate the percent reduction in hospital and GP appointments during a cyber attack. These percentages were combined with annual activity data from major hospitals and GP practices in order to estimate the reduction in appointments at hospitals and GP practices. Per cyber attack on a major hospital, an estimated 5,143 appointments may be disrupted. Per cyber attack on a GP practice, an estimated 237 GP appointments may be disrupted.

Key findings: Creative industries and arts

While there was less evidence on cyber attacks in the creative industries compared to the health and financial services sectors, the available literature indicates that attacks in the creative industries predominantly target systems storing sensitive data, catalogues, and operational tools.

The impact on consumers of cyber attacks and their response, depends on the institution targeted and the services disrupted in the creative industries. Examples of recent cyber attacks provide useful evidence:

- The cyber attack on the British Library severely disrupted services and operations including catalogue and collection access, research tools, and on-site activities. It therefore impacted both regular consumers and scholars using services for academic work. Scholars with access to alternative catalogues or resources could redirect their efforts, while others reliant on specific services experienced prolonged setbacks.[29]
- Following the Gallery Systems attack, consumers noted the inconvenience of losing access to online collections.[30]

Online ticketing

As shown in Table 4 below, the impact on consumers of a cyber attack scenario affecting online ticketing services for one day is estimated to range from approximately £0.6m to £161m, depending on the market share of the online ticketing service affected. The estimated frequency of a successful cyber attack affecting online ticketing services, with resulting consumer impacts, is once every four to five years.[31]

[25] This is a commonly used measure to assess health impacts of policy interventions, as it captures both the level of health and longevity of life impact.
[26] This value is sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity.
[27] HMT (2022) The Green Book
[28] Although the 2024 CrowdStrike incident was not a cyber attack it was identified as a relevant proxy for the reasons provided in section 4.2.2.
[29] Museums Association, Cyber security is an urgent priority for the sector, Museums Association. Accessed: Jan. 08, 2025. [Online].
[30] Z. Small, Museum World Hit by Cyberattack on Widely Used Software, The New York Times, Jan. 03, 2024. Accessed: Jan. 08, 2025. [Online].
[31] This is based on the rate of successful ransomware attacks estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024) at 2.45% per large company per year.

Table 4: Estimated consumer impact of a cyber attack resulting in one day loss of access to online ticketing services, 2024 prices

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Years per incident (approx.)
	Low	High		
Online Ticketing	£0.6m	£161m	0.22 per year	Once every four to five years

The impact per consumer: The estimated WTP and WTA values, derived from the survey data, varied from a WTP of £0.48[32] to a WTA of £10.00 for online ticketing services. The scenario described to respondents was where the loss of access was expected to last for one day, at a time of attempting to purchase tickets for an event.

The number of consumers impacted: To estimate the number of consumers potentially affected by a cyber attack resulting in the loss of access to online ticketing services, the percentage of event tickets purchased using Ticketmaster (60%)[33] vs. other providers (5%),[34] and the estimated number of UK adults using online ticketing services (27 million)[35] is used. The number of impacted consumers is therefore estimated to range from 1.3 million (5% of 27 million) to 16 million (i.e. 60% of 27 million).

Online video streaming services

As shown in Table 5 below, the impact on consumers of a cyber attack scenario resulting in the loss of access to streaming services for one day is estimated to range from £2.8m to £197m. The estimated frequency of a successful cyber attack affecting online video streaming services, with resulting consumer impacts, is once every eight years.[36]

Table 5: Estimated consumer impact of a cyber attack resulting in one day loss of access to video streaming services, 2024 prices

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Years per incident (approx.)
	Low	High		
Video Streaming	£2.8m	£197m	0.12 per year	Once every eight years

The impact per consumer: The estimated WTP and WTA values, derived from the survey data, varied from a WTP of £0.59[37] to a WTA of £5.00 for streaming services. The scenario described to respondents was where the loss of access was expected to last for one day, and respondents were asked to consider their average use of the online video streaming service they primarily use.

The number of consumers impacted: To estimate the number of consumers potentially impacted by a cyber attack on streaming services, data on the percentage of households with subscriptions to video streaming services was used from the Ofcom Media Nations 2023 report,[38] together with data on the number of households in the UK and the number of people per household.[39] The number of consumers who may be impacted by a cyber attack resulting in the loss of access to online video streaming services is estimated to range from 4.7 million to 39.5 million, depending on the size of the streaming service affected.

[32] The estimated WTP from the open-ended elicitation approach was £0 but this is not used in the subsequent analysis.
[33] ticketmaster brand profile UK 2022 | Statista
[34] A report on the completed merger between Ticketmaster Entertainment, Inc and Live Nation, Inc
[35] Based on 50% of adults using online ticketing services as indicated in the consumer survey.
[36] This is based on the rate of successful ransomware attacks estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024) at 2.45% per large company per year.
[37] The estimated WTP from the open-ended elicitation approach was £0 but this is not used in the subsequent analysis.
[38] Media Nations: UK 2023, Ofcom
[39] Families and households in the UK - Office for National Statistics

Cultural institutions – museums and galleries

As shown in Table 6 below, the impact on consumers per cyber attack resulting in the loss of access to museums and galleries for an 11 day period is estimated at c. £271,000. The estimated frequency of a successful cyber attack affecting museums and galleries, with resulting consumer impacts, is once every three years.[40]

Table 6: Estimated consumer impact of a cyber attack resulting in 11 days of disruption to museums and galleries, 2024 prices

Service	Consumer impact per successful cyber attack	Estimated annual frequency (approx.)	Years per incident (approx.)
Museums & Galleries	£0.271m	0.37 per year	Once every three years

The impact per consumer: The value of museum online offerings was estimated at £3.90 per month (2021/22 prices, £4.47, 2024 prices) per attendee in a 2023 report by Simetrica Jacobs and Creative Industries Policy Evidence Centre for The Department for Culture, Media and Sport (DCMS) and Arts Council England.[41] This study surveyed individuals about four different museums across England, asking for their WTP for access to digital content.

The number of consumers impacted: To estimate the number of consumers impacted by a cyber attack on cultural institutions, data from museums and galleries with over 1 million annual visitors (as larger institutions are more likely to be targets for cyber attacks) was collected from a range of sources to cover the four nations,[42] together with data from DCMS-sponsored museum and galleries KPIs on attendance by overseas visitors.[43] Across the 18 museums and museum groups identified, there was an average domestic attendance of 2.01 million annual visitors per museum. Assuming 11 days of disruption (based on the typical duration until restoration following a ransomware attack across large companies in the 2019 to 2024 Cyber Security Breaches Surveys (CSBS) this would be associated with approximately 61 thousand visitors impacted.

Libraries

As shown in Table 7 below, the estimated consumer impact of a cyber attack scenario affecting a library service and resulting in a loss of access to services for consumers for 11 days is £17,000. The estimated frequency of a successful cyber attack affecting library services, with resulting consumer impacts, is once every seven months.[44]

Table 7: Estimated consumer impact of a cyber attack resulting in 11 days of disruption to library services, 2024 prices

Service	Consumer impact per successful cyber attack	Estimated annual frequency (approx.)	Months per incident (approx.)
Local Libraries	£0.017m	1.8 per year	Once every seven months

The impact per consumer: The DCMS commissioned Culture and Heritage Capital Evidence Bank[45] was searched to identify relevant WTP and WTA values for library services. The value of library services was taken from a 2015 WTP study commissioned by Arts Council England.[46] The WTP value

[40] This is based on the rate of successful ransomware attacks estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024) at 2.45% per large company per year.
[41] Table 4.22 WTP a monthly household subscription fee for Digital Offer if Covid-19 had not happened Simetrica Jacobs and Creative Industries Policy Evidence Centre (2023) Measuring the economic value of museums and galleries digital offers: an exploratory use of contingent valuation techniques - GOV.UK
[42] See section 4.2.3.
[43] DCMS (2024) DCMS-sponsored museums and galleries annual performance indicators - GOV.UK
[44] This is based on the rate of successful ransomware attacks estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024) at 0.475% per year for the charities and education section.
[45] Simetrica-Jacobs (2022) Rapid Evidence Assessment: Culture and Heritage Valuation Studies - GOV.UK
[46] Fujiwara, Lawton and Mourato (2015) The health and wellbeing benefits of public libraries. Report for Arts Council England. The health and wellbeing benefits of public libraries.pdf

for those who had used public libraries in the past year was £19.51 per year per household (2014 prices, equivalent to £26.03 in 2024 prices).[47]

Converting the annual WTP value to an 11 day value (based on typical duration until restoration following a ransomware attack across large companies in the CSBS), the value per household of the lost access to library services is estimated at £0.78 per household.

The number of consumers impacted: To estimate the number of library users that may be impacted as a result of a cyber attack, the average number of households per local authority (LA) was estimated (at c. 74,000),[48] and combined with the reported 30% of adults that used libraries in the period May 2023 to March 2024,[49] giving an estimated 22,000 library user households per LA.

Real estate and renting: property purchases and renting

There was significantly less literature relating to cyber attacks on the housing sector than on the health and financial services sectors. However, the ransomware attack on Hackney Council in October 2020 illustrates how cyber attacks within local government can impact housing, creating challenges for consumers. Evidence from the literature[50,51,52] shows that the impacts include delays in accessing housing, financial losses, and heightened psychological stress. Consumers responded in various ways to the disruptions, such as pursuing private housing options at higher costs or delaying housing applications altogether. However, for vulnerable populations, these alternatives were often unfeasible, exacerbating their housing instability.

Property purchases

The estimated impact on consumers from a cyber attack affecting property purchases is shown in Table 8 below. This is based on a scenario whereby a cyber attack on a LA results in inaccessible property transaction systems, therefore impacting property purchases. The consumer impact estimated is based on the financial impact, in terms of moving delays and cancellation costs, and indemnity insurance costs.

Table 8: Estimated consumer impact of a cyber attack affecting property purchases for three months, 2024 prices

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Months per incident (approx.)
	Low	High		
Land Registry Searches (Local Authorities)	£0.135m	£0.237m	1.71 per year	Once every seven months

The estimated impact per cyber attack is £135,000 to £237,000. The estimated frequency of a successful cyber attack affecting property purchases due to an attack on a LA, with resulting consumer impacts, is once every seven months.[53]

Share of purchases cancelled or delayed: To estimate the share of property purchases delayed or cancelled by a cyber attack, the number of property purchases in the London Borough of Hackney

[47] In this study the WTP was framed around a hypothetical increase in annual council tax payments.
[48] This was estimated based on a total of 28.4 million UK households and 382 LAs across the four nations.
[49] DCMS, Arts Council England and DSIT (2025) Headline findings for the Participation Survey (May 2023 to March 2024) - GOV.UK
[50] Hackney Council, Services available, but not back to normal – devastating impact of cyberattack one year on, Services available, but not back to normal – devastating impact of cyberattack one year on. Accessed: Jan. 08, 2025. [Online].
[51] BBC News, Hackney cyber-attack causes collapse of property purchases, BBC, Dec. 12, 2020. Accessed: Jan. 08, 2025. [Online].
[52] Information Commissioner's Office, Iboh updated reprimand with redactions, 2024. Accessed: Jan. 08, 2025. [Online].
[53] This is based on the rate of successful ransomware attacks estimated from the Cyber Security Breaches Survey (DSIT, 2019 to 2024) at 0.475% per year for the charities and education section.

was compared to the number in the surrounding areas over the three-month period following the ransomware attack on Hackney in October 2020, given neighbouring areas are generally comparable in terms of property purchase activity. Over the three-month period the reduction in volume in Hackney was estimated at 17%.

Volume of purchases impacted: To estimate the volume of sales impacted per LA, data from the Land Registry UKHPI data from the last available 12 months was used.[54] The number of transactions over the 12-month period ranged from 148 in the City of London, to 10,953 in the City of Edinburgh, with a median volume of transactions per LA of 1,621.

Taking the median LA transaction volume of 1,621, and the estimated 17% reduction in transactions, means approximately 69 transactions are estimated to be impacted in the three-months following a cyber attack.

The impact per consumer: The monetised impacts per consumer include moving delays and cancellations at £500 to £1,000 per transaction,[55] and indemnity insurance at £300 to £500 per transaction.[56]

Manufacturing

The manufacturing sector, particularly in pharmaceuticals and logistics, depends on automated systems for production, storage, and distribution. In the pharmaceutical industry, literature reports that cyber incidents may have cascading effects, disrupting supply chains, halting production lines, and compromising patient care.[57]

Cyber attacks on the pharmaceutical industry can impact consumers at the end of the supply chain of goods and services. Schachenhofer et al. (2024), in their study focusing on the pharmaceutical sector under cyber attack conditions, stated: “For patients, the implications of [drug shortage] can be severe as drug shortages can cause serious harm to the patient's health.”[58]

Pharmaceutical manufacturing

DSIT and DHSC agreed that estimated values of the potential impacts on patients of a cyber attack on UK manufacturers of prescription and non-prescription medication should not be included in this study (see section 4.2.5 for the reasons for this). Therefore, a methodology for the estimation of consumer impacts that could be used in the future is described in the report, without providing quantified estimates of potential impacts.

The methodology has been developed working with DHSC’s supply and resilience colleagues. The health impacts on patients of cyber attacks on UK pharmaceutical manufacturing which result in a medicine shortage can be estimated in QALY terms. This can be done by combining the impact per patient day of a lack of medication by the shortfall in the number of daily doses of the affected medication. These are defined as:

Health impact per patient day: The impact on a patient per day of a lack of access to medication can be estimated by the difference in Quality of Life (QoL) between those with and without access to the affected medication.

[54] HM Land Registry’s UK House Price Index.
[55] Homeowners Alliance Moving Day Delays - 115,000 Delayed Moves; Cost To Homeowners £15 Million - HomeOwners Alliance
[56] Bollanack & Bishop Solicitors Can You Sell Land With Possessory Title? | Property Lawyers
[57] L. Schachenhofer and P. Hirsch, ‘Pharmaceutical Logistics under Cyberattack Conditions’, in Proceedings of the 14th International Defense and Homeland Security Simulation Workshop DHSS, CAL-TEK srl, 2024. doi: 10.46354/i3m.2024.dhss.004.
[58] Ibid

Patient days of disruption: If the number of units of medication disrupted is known, the extent of patient disruption can be estimated by dividing the quantity disrupted by the daily dose.

Summary of key limitations

The methodologies for estimating the impacts on consumers of hypothetical cyber attack scenarios affecting the availability of certain goods and services in select sectors of the economy have been developed in line with HMT Green Book guidance. They utilise available secondary data, as well as primary data collected through the consumer survey carried out as part of this study.

There are a number of key limitations that should be noted when considering the results, which are set out alongside each of the methodologies described in section 4. Some of these are specific to the methodologies used but the following general limitations should be noted:

- Survey data: Where the consumer survey data is used, it should be noted that the estimated WTP and WTA values are associated with the specific scenarios described in the survey and may not be representative of all cyber attacks, respondents answers may be biased because the scenarios are hypothetical and there are no real financial consequences of the amounts stated, and the stated values in the survey may influence respondent's WTP and WTA.
- Assumptions: The quantified impacts are highly dependent on the assumptions used in the analysis. Therefore, ranges of potential impacts and sensitivity analysis is presented in the analysis. However, there remains considerable uncertainty.
- Non-monetised impacts: The methodologies seek to quantify the key consumer impacts identified. However, there are a number of additional consumer impacts, as set out in the impact maps for each area, which are not monetised.
- Number of consumers impacted: While an attempt has been made to estimate the number of consumers potentially affected by a cyber attack across the areas considered, there is considerable uncertainty around this. In particular, it will depend on the type, scale and duration of a cyber attack.

1 About the study

1.1 Introduction to the study

1.1.1 The study context

Digital transformation has had a substantial and positive impact on society and the economy, particularly in recent years, with businesses able to offer more innovative products and services, and consumers able to enjoy the efficiencies and opportunities brought about through improvements in technology. Increased digitalisation permeates most sectors in the economy. In the Transforming for a Digital Future (2023) policy paper the Government recognised the "unrivalled potential that digital transformation has to improve the lives of citizens throughout the UK and modernise the way government works."[59]

However, as IT systems have become increasingly vital to the functioning of society and the economy, they have become valuable targets for cyber attacks. As an example, Carr (2019) finds that "while the Internet of Things offers significant benefits… and promises societal and economic progress through productivity gains and cost savings, it also creates profound challenges and coordination problems in terms of security and privacy."[60]

Such cyber attacks impact consumers, businesses, and government, and have also resulted in anticipatory costs to help prevent future attacks. The impact of cyber attacks on organisations is reasonably well-understood and despite the challenges in quantifying the impacts, it is accepted that the financial impact can be significant. Although such estimates are contested, with some suggesting that costs are overestimated and others that they are underestimated.

The impact of cyber attacks on consumers, however, is often not considered when assessing the harm caused by cyber attacks. Previous work has focused on the impact on consumers of losing personal data,[61] but there is limited evidence on the impact on consumers of losing access to particular goods and services as a result of a cyber attack.

DSIT have therefore commissioned this study to assess the consumer harm arising from a loss of access to goods and services as a result of cyber attacks. This is part of a wider research programme to develop robust methodologies to estimate the economic impact of cyber attacks on the UK economy.

1.1.2 The purpose of the study

The overarching purpose of this study is to develop methodologies and produce estimates of the harm to consumers from cyber attacks on businesses that result in the loss of provision of goods and services in the following five sectors:

1. Financial services
2. Health sector
3. Creative industries and arts
4. Manufacturing
5. Real estate and renting

DSIT held the following specific rationales for focusing the study on each of these five sectors.

[59] Transforming for a digital future: 2022 to 2025 roadmap for digital and data - updated September 2023 - GOV.UK
[60] Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? | Request PDF
[61] Review of literature relevant to data protection harms

- Financial services, and real estate and renting were selected due to the high participation in these sectors among consumers.
- The health sector was chosen given recent high profile cyber attacks affecting health care provision.
- Creative industries and arts was included as it was considered that there potentially may be different consumer impacts to the other sectors; and
- Manufacturing was chosen to consider the supply chain impacts on consumers.

In this study, the consumer is defined as the end-user i.e. a person who uses the goods or services under consideration, it does not include purchasers in the distribution chain or business-to-business transactions where one business provides goods or services to another.

The study was commissioned to answer the following research questions:

- What are the direct economic impacts on consumers when access to goods and services are disrupted as a result of cyber attacks?
- How do the economic impacts on consumers vary across sectors?
- How do the economic impacts on consumers vary by consumer characteristics? (e.g. income, geographic location and demographic factors)
- What is the impact of AI on the nature and severity of the economic impacts on consumers?

This report presents the findings from the research and analysis undertaken to answer these questions.

1.2 Overview of the approach

In the development of this study a range of approaches were used to agree the scope of analysis, to gather evidence and to conduct the analysis. This included workshops, a literature review, impact mapping, a consumer survey and quantitative analysis. The approaches were agreed with DSIT and the project Steering Group at the outset in order to answer the research questions.

There are a number of different types of cyber attacks which manifest in different ways across different businesses and sectors. This in turn gives rise to very different consumer impacts. In order to meet the objectives of the research and quantify the impacts on consumers of cyber attacks resulting in the loss of goods and services, within the budget and timeframe available, there was a need to focus on specific types of attacks affecting agreed parts of the broad sectors under consideration.

A workshop of government stakeholders was therefore held to agree the sector parameters and the specific goods and services within the sectors that should be the focus of the study.

The following areas of focus within the sectors were agreed for the reasons set out:

- Financial services: online banking given this is an area where building operational resilience is likely to be important, and motor vehicle insurance as it is a legal requirement for driving.
- Health sector: GP practices and major hospitals given recent high profile attacks affecting these services.
- Creative industries and arts: online ticketing due to the interest in the market across government, online video streaming services as it was considered to be an important digital service used by a high proportion of consumers and captured purely digital provision of the arts, and cultural institutions given the recent cyber attack on the British Library.[62]
- Real estate and renting: property purchases and renting given the high profile Hackney Council cyber attack which affected housing services.
- Manufacturing: pharmaceutical manufacturing as it is a significant contributor to the UK's manufacturing sector and one of the largest contributors to the value of manufacturing goods that are consumed in the UK. Pharmaceutical products account for the largest amount of

[62] British Library (2024) Learning Lessons from the Cyber-Attack: British Library cyber incident review

direct economic value consumed domestically across the 47 manufactured product categories included in ONS data.[63]

To understand the existing evidence on the impact on consumers of the loss of provision of goods and services as a result of cyber attacks, a detailed literature and documentation review was undertaken by academics at UCL Consultants Ltd. This included review of the academic and grey literature, as well as of news articles and government and industry reports. A dual approach was adopted including a systematic literature search which followed a search protocol, and a focused search to prioritise the most relevant case studies and policy documents. The literature reviewed was recorded in an evidence bank to capture information about the evidence source and key insights obtained. Section 2 presents a summary of the evidence from the literature review, with further detail on the approach to conducting the literature review and detailed findings set out in Appendix 2.

To show visually the routes through which impacts on consumers from cyber attacks resulting in the loss of goods and services occur, impact maps were developed. The impact maps were developed based on the findings from the literature review as well as input from stakeholders across relevant government departments. The impact maps show how cyber attacks affect the provision of the goods and services of interest, how consumers may respond to the loss of access to these goods and services, and the resulting impacts on consumers. Section 3 presents and describes the impact maps developed for each sector.

In order to quantify the impact on consumers of cyber attacks resulting in the loss of goods and services, methodologies were developed to quantify the consumer impacts identified in the impact maps. These methodologies drew on secondary data sources and primary data collected through a consumer survey. To estimate the impact on consumers of a loss of access to online banking services, online ticketing services, and online streaming services, a consumer survey was developed to obtain data on consumers' willingness to pay (WTP) to retain access to these services in the event of a cyber attack, and their willingness to accept (WTA) compensation in the event of a cyber attack resulting in a loss of access to these services. The consumer survey was developed with specialist input provided by academics at UCL Consultants Ltd. and fieldwork partners YouGov. The fieldwork was conducted by YouGov among their online panel of consumers, between Tuesday 21st and Friday 31st January 2025, achieving 1,000 completed survey responses. Appendix 1 provides further detail on consumer survey including the fieldwork and data processing.

The methodologies were developed in line with HMT Green Book Guidance, including the supplementary guidance on stated preference techniques. Section 4 describes the methodologies in detail, together with the sources of information used, and presents the results of the analysis. Table 9 below provides an overview of the methodologies used:

[63] CPA_C21 Basic pharmaceutical products and pharmaceutical preparations accounted for £3.9 billion of direct GVA in the Final Consumption Expenditure section of the 2019 Input-Output Analytical Tables. While the more recent 2021 Input-Output Analytical Tables were available at the time of writing, the ONS notes in the 2021 edition that due to COVID-19 'Users wanting a more "typical" IOT reflecting the UK economy may wish to use the 2019 input-output table instead.' Source: UK input-output analytical tables: product by product - Office for National Statistics

Table 9: Overview of methodologies for quantifying the consumer impacts from cyber attacks

Sector	Good/ service of focus	Overview of methodology
Financial services	Online banking	WTP and WTA estimates from the consumer survey are combined with the estimated number of consumers impacted
	Motor vehicle insurance	Foregone interest from delays in insurance payments
Health care	Major hospital	The health impact on patients of disrupted appointments and procedures at hospitals and the impact of longer wait times at A&E departments are valued
	GP practice	The health impact on patients of disrupted appointments at GP surgeries is valued
Creative industries and arts	Online ticketing	WTP and WTA estimates from the consumer survey are combined with the estimated number of consumers impacted
	Streaming services	WTP and WTA estimates from the consumer survey are combined with the estimated number of consumers impacted
	Cultural institutions	WTP and WTA estimates from existing studies are combined with the estimated number of consumers impacted
Real estate and renting	Property purchases	The impact per consumer from disruptions to property purchases are combined with the estimated number of consumers impacted
Manufacturing	Pharmaceuticals	The impact per patient per day of a lack of medication is combined with the patient days of disruption

Source: KPMG analysis.

The key limitations associated with the quantified impacts on consumers are specific to the methodologies used for each of the goods and services considered within the sectors in scope of this study. Therefore, the key limitations are set out alongside the methodologies in section 4.

1.3 Report structure

The remainder of the report is structured as follows:

- Section 2 sets out the evidence from the literature review including the approach to the literature review and key findings including sector specific consumer impacts of cyber attacks resulting in the loss of access to goods and services, the variability in consumer response and impact, and the role of Artificial Intelligence (AI) in cyber attacks.
- Section 3 describes the expected impacts on consumers from cyber attacks resulting in the loss of goods and services, including a summary impact map and impact maps for each of the sectors within scope of the study which show visually the routes through which consumer impacts may arise together with an explanation for each impact map.
- Section 4 presents the estimated costs to consumers from cyber attacks resulting in the loss of goods and services, including the valuation methodologies and results for each of the sectors within scope of the study.
- Appendix 1 is a technical appendix detailing the methodological approach to the consumer survey analysis.
- Appendix 2 presents the literature review including the detailed methodological approach to conducting the review and the findings.

2 Evidence from the literature review of consumer impacts from cyber attacks

2.1 Purpose of the literature review

As part of the research a literature review was undertaken by UCL Consultants Ltd. led by Professor Madeline Carr and Chloé Colomer, UCL Department of Computer Science. The literature review was designed to:

- identify and summarise the existing evidence on the consumer harms from cyber attacks resulting in the loss of goods and services; and
- gather evidence and insights to inform the development of the impact maps setting out the impacts on consumers from cyber attacks resulting in the loss of goods and services.

The approach to conducting the literature review and the detailed findings from the review, including case studies, are set out in Appendix 2. This section provides an overview of the approach and a summary of key findings.

2.2 Overview of the approach to the literature review

To answer the research questions, a dual approach was adopted to undertake the literature review:

1. A systematic literature search: This approach followed a search protocol using specified search terms to gather evidence from peer-reviewed academic sources.
2. A focused search: This approach focused on identifying relevant case studies and policy documents in grey literature and news reports.

In the early stages of implementing the systematic search of academic literature, it became clear that most existing studies focused on the impacts of cyber attacks on organisations, rather than the impact on consumers. Therefore the research methodology was amended and additional literature that was relevant to the COVID-19 pandemic was included. This was based on the assumption that the reduced access to goods and services experienced by consumers during COVID-19 could be a proxy for the disruption to goods and services caused by cyber attacks, and therefore provide insights into the impacts on consumers.

Only publications related to the sectors within the scope of this study (financial services, health care, creative industries and arts, manufacturing, and real estate and renting) were included in the literature review, and the focused search targeted case studies related to the specific goods and services of interest within the sectors (as described in section 1.2).

2.3 Summary of literature review findings

2.3.1 Sector specific consumer impacts of cyber attacks

This section sets out the findings from the literature review for each sector. For each sector, the types of cyber attacks occurring, the consumer response to disruption and the impact on consumers is described using examples from the literature and publications reviewed.

Health care

A range of cyber attacks have been shown to impact the provision of health care:

- Ransomware attacks: McGlave et al. (2023) found ransomware attacks in the US typically decreased hospital service volume by 17 to 26 percent during the first week of an attack, with

recovery taking up to three weeks.[64] Neprash et al. (2024) found ransomware attacks on US hospitals disrupt operations in both rural and urban hospitals.[65] However, while the scale of disruption was similar across both settings, rural patients faced exacerbated challenges, having to travel greater distances to access alternative care.

- Data breaches: Portela et al. (2023), in a case study on medical data breaches from Portugal hospitals, found data breaches can compromise access to critical patient information and support systems, delaying essential hospital activities.[66] These breaches could not only endanger patient health during the attack but also have financial and health consequences after the attack for patients and health practitioners.
- Attacks on sub-contractors such as pathology services or insurance companies: A recent example is the ransomware attack on Synnovis, a pathology service provider for NHS Trusts in London, which led to widespread delays across hospitals and GP practices. BBC News reported over 1,294 outpatient appointments and 320 planned operations were postponed at King's College Hospital and Guy's and St Thomas' NHS Foundation Trusts.[67] Similarly, the attack on the health insurance provider Change Healthcare in the US disrupted claims processing and prescription refills.[68]

The literature indicates that patients adapt in various ways when faced with disruptions. Evidence from the US shows that some patients sought care from private health care providers to avoid delays, incurring substantial out-of-pocket expenses, while others delayed or entirely avoided treatments, placing their health at further risk.[69]

The literature suggests that the impact on consumers of cyber attacks in the health care sector depends on the scale and duration of the attack, as well as the type of care patients required. Across reports and studies, patients frequently reported delays in accessing essential services (e.g. surgery, blood tests, prescriptions, etc.), often with serious consequences for their health and well-being. Pathology backlogs heightened risks for chronic patients reliant on routine bloodwork, as delays in monitoring and managing critical conditions left them vulnerable. News articles also discussed the psychological impact of disruptions, reporting it as distressing for patients, especially those requiring urgent care such as chemotherapy or organ transplants.

An investigation by the National Audit Office of the WannaCry ransomware attack in May 2017 established that the attack disrupted NHS systems with at least 80 out of the 236 Trusts across England affected. NHS England estimated the total number of cancelled appointments as being around 19,494 with 139 urgent cancer referrals cancelled. Other impacts included ambulances diverted to unaffected hospitals, delaying emergency response times and access to critical care.[70]

An analysis by The Royal United Services Institute (RUSI), an independent think tank, also highlights the indirect effects, such as the strain on administrative and medical staff caused by ransomware disruptions.[71] When patient records and scheduling systems are rendered inaccessible, as occurred during the attack on Advanced, an IT provider for the NHS, staff had to revert to manual processes. It

[64] C. C. McGlave, H. Neprash, and S. Nikpay, 'Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients', Oct. 04, 2023, Social Science Research Network, Rochester, NY: 4579292. doi: 10.2139/ssrn.4579292.
[65] H. T. Neprash, C. C. McGlave, K. Rydberg, and C. Henning-Smith, 'What happens to rural hospitals during a ransomware attack? Evidence from Medicare data', The Journal of Rural Health, vol. 40, no. 4, pp. 728–737, 2024, doi: 10.1111/jrh.12834.
[66] D. Portela, D. Nogueira-Leite, R. Almeida, and R. Cruz-Correia, 'Economic Impact of a Hospital Cyberattack in a National Health System: Descriptive Case Study', JMIR Formative Research, vol. 7, no. 1, p. e41738, Jun. 2023, doi: 10.2196/41738.
[67] Cyber attack on hospitals impacts 1,130 operations in London, BBC News. Accessed: Jan. 07, 2025. [Online].
[68] M. Cimons, M. Beard, and T. Amenabar, How a health-care cyberattack may affect your prescription drug access, Washington Post, Mar. 05, 2024. Accessed: Jan. 07, 2025. [Online].
[69] M. Bohannon, Change Healthcare Cyberattack Disrupts Services Nationwide—Here's What To Know, Forbes. Accessed: Jan. 07, 2025. [Online].
[70] National Audit Office, Investigation: WannaCry Cyber Attack and the NHS. Report by the Comptroller and Auditor General, 2018. Accessed: Jan. 07, 2025. [Online].
[71] Beyond the Bottom Line: The Societal Impact of Ransomware. Accessed: Jan. 07, 2025. [Online].

is noted in the literature that this increased workload not only delays care but also erodes patient confidence in the health care system and patients' trust in public institutions.

Financial services

The financial sector is one of the most targeted industries for cyber attacks. The International Monetary Fund found that nearly one-fifth of all reported cyber incidents target financial firms.[72]

The types of attacks discussed in the literature include phishing, ransomware and data breach incidents and intrusions:

- Ransomware attacks: The attack on the US based Patelco Credit Union in June 2024 illustrates the disruption that can emerge.[73] This attack shut down online banking for Patelco's members meaning they were unable to access their accounts for activity such as viewing their balances, making electronic transfers and scheduling new online bill payments. Queues at branches grew as customers sought limited cash withdrawals, while delayed transactions led to financial anxieties, including the risk of overdraft penalties and missed payments. Customers expressed their trust in Patelco was shaken given the uncertainty about how their accounts and financial data had been affected.[74] Ransomware attacks on third-party providers also show how attacks on supply chains amplify vulnerabilities.
- Phishing: Successful ransomware attacks often stem from phishing campaigns, with one study finding that 65% of ransomware attacks stemmed from phishing.[75] Beyond immediate financial losses, evidence indicates that these attacks result in reputational damage, reduced consumer confidence, and prolonged recovery times for affected institutions.
- Data breaches: The IBM Cost of Data Breach Report (2025) highlights that financial services face some of the highest costs when breached globally.[76] Such breaches have exposed sensitive customer information, leading to identity theft and fraud.

In response to cyber attacks on financial services, the literature reports that consumers act in various ways. Some consumers switch to alternative providers, which can involve fees, lost access to previous banking tools, and disruptions to automated payments.[77] Others attempt to adapt by using traditional banking methods, such as in-person visits to bank branches, despite the inconvenience.[78]

As for all sectors, the impact on consumers of cyber attacks targeting financial services varies depending on the type, scale, and duration of the attack. Across studies, frequently reported impacts on consumers include the inability to access funds, compromised personal information, and loss of trust in digital banking platforms. Victims of data breaches may experience financial losses and endure lengthy processes to recover their compromised accounts. As Ali et al. (2017) noted, the fear of losing sensitive financial data leads many consumers to reduce, or even cease, their use of online banking services, eroding trust in digital financial platforms.[79] Consumers' trust in financial institutions may be further undermined when institutions fail to provide timely responses or transparency about the scope of an attack.

[72] International Monetary Fund, The Last Mile: Financial Vulnerabilities and Risks, 2024. Accessed: Jan. 08, 2025. [Online].
[73] J. Flores, Massive Patelco cyberattack is still affecting half a million people. Here's how to protect yourself, San Francisco Chronicle. Accessed: Jan. 08, 2025. [Online].
[74] C. Castañeda, Patelco Credit Union ransomware attack halts banking services for nearly half a million members - CBS San Francisco. Accessed: Jan. 08, 2025. [Online].
[75] Grant Thornton, The economic cost of cybercrime, Ireland, 2021. Accessed: Jan. 08, 2025. [Online].
[76] Cost of a data breach 2024 | IBM. Accessed: Jan. 07, 2025. [Online].
[77] L. Ali, F. Ali, P. Surendran, and T. Bindhya, 'The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services', IJEEEE, vol. Volume 7 Number 1, 2017, doi: 10.17706/IJEEEE.
[78] J. Flores, Massive Patelco cyberattack is still affecting half a million people. Here's how to protect yourself, San Francisco Chronicle. Accessed: Jan. 08, 2025. [Online].
[79] L. Ali, F. Ali, P. Surendran, and T. Bindhya, 'The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services', IJEEEE, vol. Volume 7 Number 1, 2017, doi: 10.17706/IJEEEE.

Real estate and renting

There was significantly less literature relating to cyber attacks on the housing sector than on the health and financial services sectors. However, the ransomware attack on Hackney Council in October 2020 illustrates how cyber attacks within local government can impact housing, creating challenges for consumers.

The types of attacks discussed in the literature affecting local authorities' role in relation to the housing sector includes ransomware attacks, data breaches and phishing:

- Ransomware attacks: The attack on Hackney Council in 2020 rendered its property transaction systems inaccessible for months, disrupting essential housing operations.[80]
- Data breaches and phishing: In 2024, the housing software provider Locata was compromised in a cyber attack, leading to disruptions across Greater Manchester councils.[81,82] These disruptions affected public-facing websites like Manchester Move and Salford Home Search, which are critical for managing housing applications. In some cases, the disruption also included unauthorised access to sensitive resident data, leaving them vulnerable to phishing scams.[83]

Cyber attacks on local authority housing services directly affect residents, particularly those in vulnerable situations. Evidence from the literature shows that the impacts include delays in accessing housing, financial losses, and heightened psychological stress.

The Information Commissioner's Office report investigating the Hackney Council attack noted that over 280,000 individuals were affected, with delays in benefits and housing waiting lists disproportionately impacting vulnerable residents, such as those in temporary accommodation.[84] Prospective homebuyers could also not complete transactions because of delays in land search services, incurring financial losses. A year after the attack, Hackney Council had not fully restored its systems, and some services continued to experience delays.

Consumers responded in various ways to the disruptions, such as pursuing private housing options at higher costs or delaying housing applications altogether. However, for vulnerable populations, these alternatives were often unfeasible, exacerbating their housing instability.

Creative industries and arts

The creative industries are increasingly reliant on interconnected digital systems for managing collections and delivering services. Recent incidents, such as the attack on the British Library and the targeting of Ticketmaster, illustrate the potential impacts on consumers of cyber attacks.

While there was less literature on cyber attacks in the creative industries compared to the health and financial services sectors, the available literature indicates that attacks in the creative industries predominantly target systems storing sensitive data, catalogues, and operational tools. Common attack types include ransomware, phishing scams, and breaches through third-party service providers:

- Ransomware attacks: The ransomware attack on the British Library in October 2023 rendered catalogues and special collections inaccessible for months.[85]

[80] Hackney Council, Services available, but not back to normal – devastating impact of cyberattack one year on. Accessed: Jan. 08, 2025. [Online].
[81] Greater Manchester cyber scam leaves thousands vulnerable, BBC News. Accessed: Jan. 08, 2025. [Online].
[82] BBC News, Salford housing register still down weeks after cyber attack, Aug. 28, 2024. Accessed: Jan. 08, 2025. [Online].
[83] Greater Manchester cyber scam leaves thousands vulnerable, BBC News. Accessed: Jan. 08, 2025. [Online].
[84] Information Commissioner's Office, Iboh updated reprimand with redactions, 2024. Accessed: Jan. 08, 2025. [Online].
[85] Museums Association, Cyber security is an urgent priority for the sector, Museums Association. Accessed: Jan. 08, 2025. [Online].

- Phishing and data breaches: The literature pointed out that phishing is a major attack type used to gain unauthorised entry to secure systems in the creative industry, which can in turn result in data breaches. For example, Ticketmaster was attacked in 2024, where hackers accessed sensitive customer information, including encrypted payment details.[86,87]
- Attacks on third-party software providers: For example, in December 2023 the attack on Gallery Systems, a third-party software provider, led to institutions such as the Museum of Fine Arts in Boston and the Rubin Museum of Art in New York being unable to display their collections online for a time.[88,89]

The impact on consumers of cyber attacks and their response, depends on the institution targeted and the services disrupted in the creative industries, as illustrated in the below examples:

- The cyber attack on the British Library severely disrupted services and operations including catalogue and collection access, research tools, and on-site activities. It therefore impacted both regular consumers and scholars using services for academic work. Scholars with access to alternative catalogues or resources could redirect their efforts, while others reliant on specific services experienced prolonged setbacks.[90] In addition, personal and sensitive data of British Library users and staff were leaked on the dark web, impacting public trust and leading to concerns about privacy and financial fraud, with the British Library providing identity protection services to affected individuals.[91]
- As a result of the attack on Ticketmaster, consumers had limited access to event ticketing and were encouraged to sign up for identity protection services,[92] causing frustration and distress among consumers.
- Following the Gallery Systems attack, consumers noted the inconvenience of losing access to online collections, while curators and museum staff expressed a sense of helplessness as critical tools remained inaccessible for months.[93]

Manufacturing

The manufacturing sector, particularly in pharmaceuticals and logistics, depends on automated systems for production, storage, and distribution. In the pharmaceutical industry, cyber incidents may have cascading effects, disrupting supply chains, halting production lines, and compromising patient care.[94]

Common cyber attack types targeting the pharmaceutical industry include ransomware, data breaches, and disruptions to automated logistics systems.

- Ransomware attacks: For example, the ransomware attack on Eisai, a Tokyo-based pharmaceutical company in 2023, forced the company to take its logistics systems offline, disrupting operations both domestically in Japan and internationally.[95]

---

[86] Z. Small, Museum World Hit by Cyberattack on Widely Used Software, The New York Times, Jan. 03, 2024. Accessed: Jan. 08, 2025. [Online].
[87] Ticketmaster hack: Customers told to sign up to security service, BBC News. Accessed: Jan. 08, 2025. [Online].
[88] Z. Small, Museum World Hit by Cyberattack on Widely Used Software, The New York Times, Jan. 03, 2024. Accessed: Jan. 08, 2025. [Online].
[89] No further detail on the duration of disruption was available.
[90] Museums Association, Cyber security is an urgent priority for the sector, Museums Association. Accessed: Jan. 08, 2025. [Online].
[91] British Library, British Library cyber incident review, 2024. Accessed: Jan. 09, 2025. [Online].
[92] Ticketmaster hack: Customers told to sign up to security service, BBC News. Accessed: Jan. 08, 2025. [Online].
[93] Z. Small, Museum World Hit by Cyberattack on Widely Used Software, The New York Times, Jan. 03, 2024. Accessed: Jan. 08, 2025. [Online].
[94] L. Schachenhofer and P. Hirsch, 'Pharmaceutical Logistics under Cyberattack Conditions', in Proceedings of the 14th International Defense and Homeland Security Simulation Workshop DHSS, CAL-TEK srl, 2024. doi: 10.46354/i3m.2024.dhss.004.
[95] A. Ribeiro, Ransomware attackers target Japanese pharmaceutical company Eisai, Industrial Cyber. Accessed: Jan. 09, 2025. [Online].

- Data breaches: Schachenhofer et al. (2024) emphasise the risk that data breaches pose to the pharmaceutical sector.[96] Such incidents can expose intellectual property, clinical trial data, and sensitive patient records, endangering patient safety while undermining the competitive advantage, market position, and reputation of affected companies.[97]
- Attacks on automated logistics systems: Automated systems for order picking and digital inventory tracking, while critical for efficiency, become vulnerabilities during cyber incidents. Pharmaceutical wholesalers have struggled to maintain inventory control and the timely delivery of medications in the aftermath of such disruptions.[98]

There is limited literature which focuses on the response of consumers to cyber attacks in pharmaceutical manufacturing.

Cyber attacks on the pharmaceutical industry can impact consumers at the end of the supply chain of goods and services. Drug shortages caused by cyber attacks are not immediately recoverable due to regulatory requirements for production and distribution changes. Schachenhofer et al. (2024), in their study focusing on the pharmaceutical sector under cyber attack conditions, stated: “For patients, the implications of [drug shortage] can be severe as drug shortages can cause serious harm to the patient's health.”[99]

2.3.2 Variability in consumer response and impacts of cyber attacks

The variability in the impact on consumers from a loss of access to goods or services is illustrated within the findings presented above on the consumer impacts from cyber attacks in each sector. The literature suggests that the impact on consumers depends on various factors including the consumer’s purpose for using the goods or services, the sector in which the disruption occurs and what goods and services are disrupted, the scale of disruption, geographic factors, and the affected consumer group:

- The consumer’s purpose for using the goods or services and the alternatives available: For example, the temporary inaccessibility of the British Library’s catalogue impacted consumers differently based on their needs. Scholars or students using the catalogue for academic research encountered disruptions to their work and frustration, whereas those using it for leisure may have been annoyed by the inconvenience. Scholars with access to alternative resources through their universities, for example, could redirect their efforts to other catalogues, but this ability would be contingent on the support and resources provided by their institutions.
- The type of service disrupted and the consumer group affected: During the Hackney Council cyber attack, residents depending on council services for accommodation were impacted differently to individuals attempting to buy property. While the former faced delays in securing accommodation (with vulnerable individuals in temporary housing reporting hardships), the latter incurred financial losses from being unable to process land search services.[100,101]
- Geographic factors: For example, a study on hospital cyber attacks highlighted how rural and urban patients were affected differently by care disruptions. Patients in rural areas faced travel times averaging 33 minutes to reach unaffected hospitals, compared to just nine minutes for urban patients.[102] These extended travel times delayed access to emergency care and increased financial and emotional burdens on rural patients and their families.

[96] Ibid
[97] A. Ribeiro, Ransomware attackers target Japanese pharmaceutical company Eisai, Industrial Cyber. Accessed: Jan. 09, 2025. [Online].
[98] M. Crosignani, M. Macchiavelli, and A. F. Silva, ‘Pirates without borders: The propagation of cyberattacks through firms’ supply chains’, Journal of Financial Economics, vol. 147, no. 2, pp. 432–448, Feb. 2023, doi: 10.1016/j.jfineco.2022.12.002.
[99] Ibid
[100] BBC News, Hackney cyber-attack causes collapse of property purchases, BBC, Dec. 12, 2020. Accessed: Jan. 08, 2025. [Online].
[101] M. Burgess, The Untold Story of a Crippling Ransomware Attack, Wired. Accessed: Jan. 08, 2025. [Online].
[102] C. C. McGlave, H. Neprash, and S. Nikpay, ‘Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients’, Oct. 04, 2023, Social Science Research Network, Rochester, NY: 4579292. doi: 10.2139/ssrn.4579292.

These varied impacts demonstrate the consequences of cyber attacks are multifaceted, influenced by the nature of the service disrupted and the resources and resilience of the affected consumer groups.

2.3.3 The role of AI in cyber attacks and the impact on consumers

The literature on the potential impacts of AI on cyber attacks highlights both opportunities and risks, though much remains speculative because of the nascent stage of this technology's application in malicious activities. As noted by cyber security expert Ben Buchanan, "some of the most potent cyber attacks we have seen – including Stuxnet, the 2016 blackout in Ukraine, and the 2017 attack known as NotPetya that caused at least ten billion dollars in damage – feature some forms of automated propagation and attack capability".[103]

Some experts argue AI could improve cyber security through enhanced predictive analytics, enabling the more accurate and faster identification of threats before they materialise.[104] But it could also be used on the offensive side by attackers. AI-powered attacks are predicted to enhance the scale and sophistication of cyber threats by enabling automated system reconnaissance, generating adaptive malware, and creating highly targeted phishing campaigns.[105,106] These factors mean that AI could make future cyber attacks faster and more likely to be successful.

Despite these concerns, the understanding of the role of AI in cyber attacks remains limited, with current discourse relying heavily on theoretical scenarios and controlled experiments rather than real world case studies.[107]

[103] B. Buchanan, 'The Future of AI and Cybersecurity', 2019. The-Future-of-AI-and-Cybersecurity.pdf
[104] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review, Sep. 01, 2022, Social Science Research Network, Rochester, NY: 4323317. Accessed: Jan. 09, 2025. [Online].
[105] S. M. U. H. Minhaj, STUDY OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY AND THE EMERGING THREAT OF AI-DRIVEN CYBER ATTACKS AND CHALLENGE, Jul. 17, 2023, Social Science Research Network, Rochester, NY: 4652028. doi: 10.2139/ssrn.4652028.
[106] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, 'Weaponized AI for cyber attacks', Journal of Information Security and Applications, vol. 57, p. 102722, Mar. 2021, doi: 10.1016/j.jisa.2020.102722.
[107] SS. M. U. H. Minhaj, 'STUDY OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY AND THE EMERGING THREAT OF AI-DRIVEN CYBER ATTACKS AND CHALLENGE', Jul. 17, 2023, Social Science Research Network, Rochester, NY: 4652028. doi: 10.2139/ssrn.4652028.

3 The impact on consumers from cyber attacks

3.1 Introduction to impact mapping

In order to estimate the impact on consumers from the loss of provision of goods and services caused by cyber attacks, it was first necessary to identify all potential impacts on consumers and the pathways to those impacts. This was done using the findings and insights gathered through the literature and documentation review of academic literature, news articles, and government and industry reports, as well as in consultation with officials from relevant government departments through workshops. The findings were then presented in impact maps which show visually the routes through which consumer impacts may arise from cyber attacks affecting the provision of goods and services. A summary impact map was developed in addition to individual impact maps for each of the sectors in scope of the study.

The impact maps set out how cyber attacks may affect the provision of the goods and services of interest, how consumers may respond to the loss of access to these goods and services, and the resulting impacts on consumers. They show the causal links between the different stages in the pathways to the consumer impacts. The impact maps aim to show visually the breadth of potential consumer impacts and were designed to be representative of a cyber attack affecting the provision of the goods and services generally, rather than reflecting the specific goods and services provided by certain businesses within the sectors.

3.2 Overview of consumer impacts

The impact maps summarise the potential consumer responses and the types of impacts on consumers that may arise based on the findings of the literature and documentation review.

Each element of the impact map is described below.

Sector of impact: This shows the sectors that are within scope of this study and the selected goods and services within the sectors that are impacted by the cyber attack.

Impacts on goods/ services provided: This describes how the provision of goods and services within the sectors of interest is impacted by the cyber attack.

Consumer response types: This summarises how consumers may respond to the disruption caused to the provision of goods and services. The consumer response can be broadly grouped into three categories.

1. Consumers do nothing in response to being unable to access the good or service and wait until provision resumes.
2. Consumers switch to an alternative good or service as a result of not being able to access the good or service they usually use. Consumers' propensity to switch will likely depend on the availability of substitutes in the market and how 'close' these substitutes are to the good or service impacted by the cyber attack (i.e. how similar the goods and services are in terms of function, price, availability, etc.), as well as consumers' ability to switch.
3. Consumers spend time contacting customer services or attempting to rectify the issues (e.g. by restarting devices or their Wi-Fi router, ahead of knowing it is a cyber attack affecting the provision of all services from the provider).

Consumer impacts categories: This summarises the impact on consumers depending on their response to being unable to access the good or service. Although the specific type and nature of

consumer impacts depends on the good and service impacted, the evidence suggests that the potential impacts can be broadly grouped into four impact themes:

1. Financial costs
2. Time costs
3. Wellbeing costs
4. Health costs

The wellbeing costs that are common across the goods and services considered include:

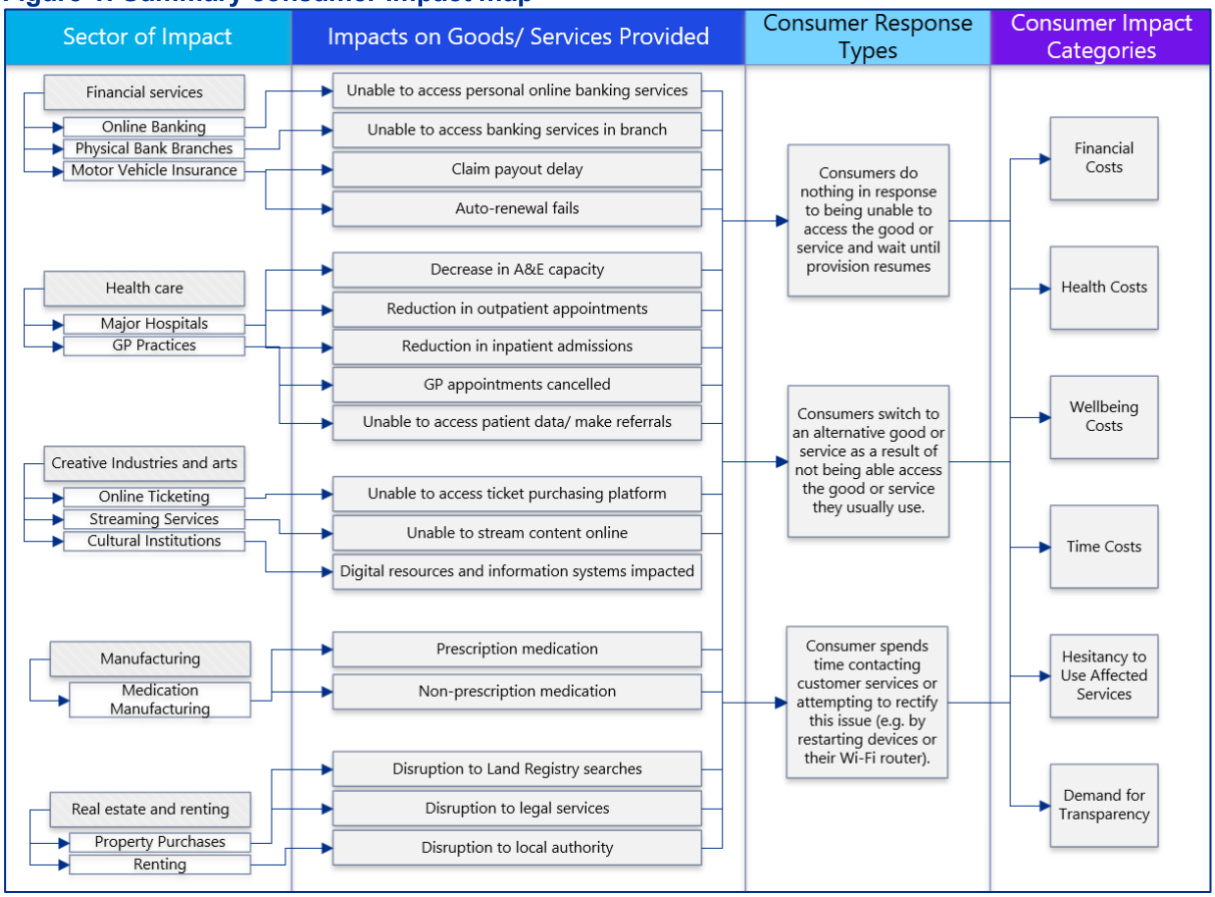
– Stress, anxiety, frustration and uncertainty: Consumers are likely to experience stress, anxiety, frustration, and uncertainty as a result of being unable to access goods and services. These feelings may be amplified by trying to deal with the loss of access and not understanding, at least initially, the reason for the loss of access.
– Loss in confidence and/ or trust with the supplier/brand/platform: When a cyber attack results in the loss of provision of goods and services, it is likely that consumer confidence in the goods and services and/ or their trust in the supplier is affected.

In addition to the broad impact themes described above there are additional consumer impacts that are common across the goods and services considered. These are:

– Hesitancy to use affected services in the future: Consumers may be hesitant to use affected goods and services in the future and have an increased preference for providers perceived as being more secure and resilient to similar cyber attacks.
– Demand for transparency in cyber attack handling: Consumers are likely to demand transparency relating to the cyber attack, such as how and why it occurred, how it was handled, and what lessons have been learnt as a result.

The summary impact map is shown below.

Figure 1: Summary consumer impact map



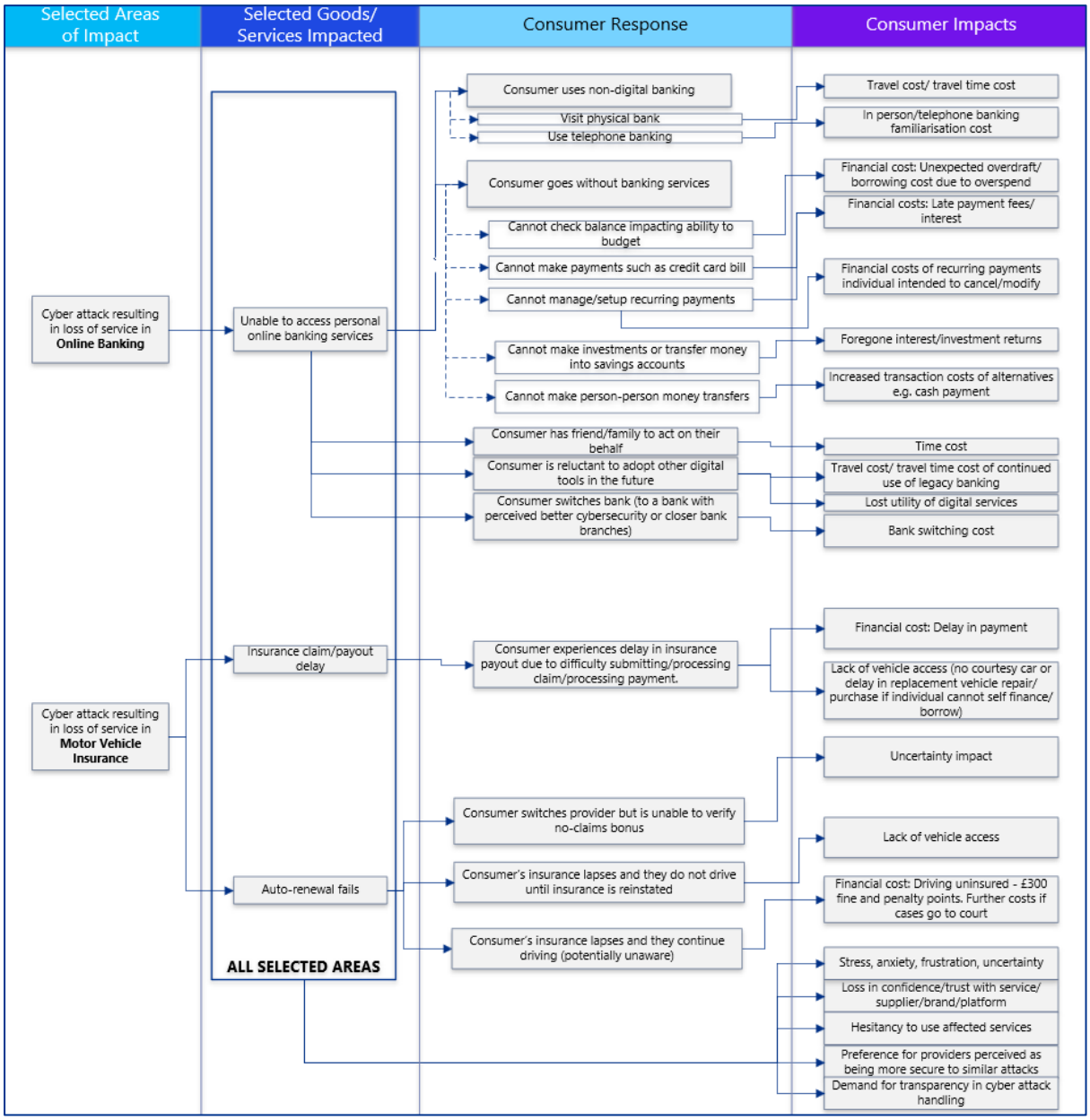
Set out below are the more detailed impact maps developed for each of the sectors within scope of the study and an explanation of each. While the impact maps show the generally expected consumer response and impacts based on the findings from the literature review and stakeholder input, it should be noted that the consumer response, and scale and type of impacts, may vary across different consumer groups.

3.3 Sector specific consumer impacts

3.3.1 Financial services – online banking and motor vehicle insurance

The impact map below shows the potential impacts on consumers from a successful cyber attack in the financial services sector. The scope of the analysis for this sector, as agreed with DSIT and the project Steering Group, is the impacts on consumers of cyber attacks on either online banking or motor vehicle insurance. Consumer impacts from cyber attacks on the financial services sector affecting the provision of other goods and services is not within the agreed scope of the study.

Figure 2: Financial Services impact map



As shown in the impact map presented above, if there is a successful cyber attack on online banking services it would be expected to result in consumers being unable to access their personal online banking and unable to use the associated banking services including:

- checking balances;
- making payments e.g. to other people or businesses or paying bills;
- making investments;
- transferring money to other accounts such as savings account; and
- managing/ setting up recurring payments e.g. standing orders and direct debits.

In response to being unable to access online banking services, consumers may do nothing and therefore go without these banking services until the business attacked takes action to respond to the cyber attack such that online banking services resume. Alternatively, consumers may 'do something' such as using non-digital banking services (for example, either visiting a bank branch or using telephone banking) to access the banking services they would have used online, asking a friend/

family to carry out a financial transaction on their behalf, or potentially switching to the banking services of an alternative provider (i.e. another bank).

Consumers who go without banking services for the duration of the cyber attack may face financial harm, such as from incurring late payment fees from not being able to make payments, or forgone interest from not being able to transfer money into savings accounts. Consumers may also forgo the benefit they may have realised from making a purchase or transaction if they are unable to do this. Consumers who 'do something' will face switching costs including, for example, travel costs, time costs, and familiarisation costs.

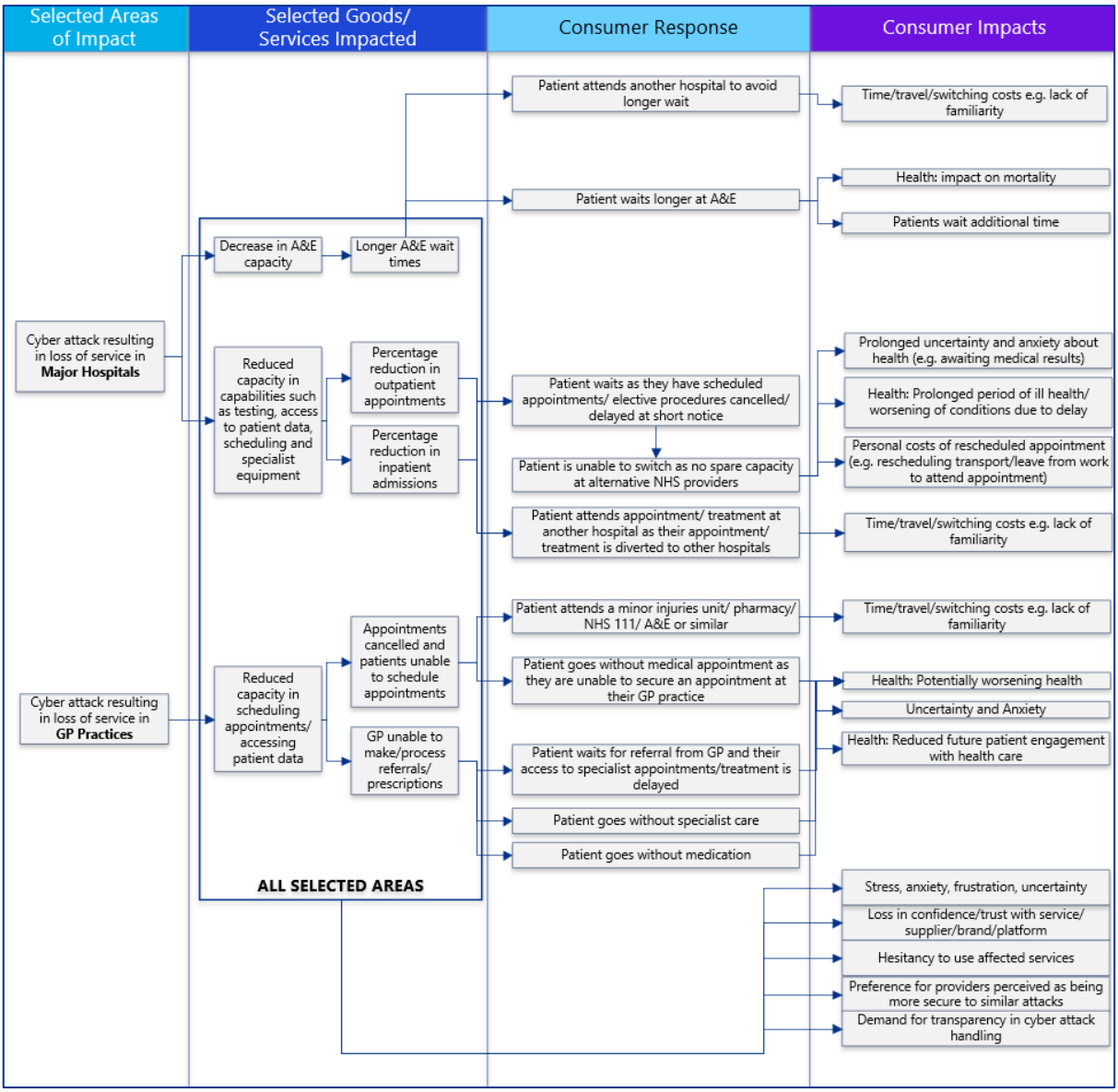
If there is a successful cyber attack on motor vehicle insurance services, this could result in disruption to insurance claims processing and insurance auto-renewals. Consumers may therefore face delays and difficulties when making insurance claims and in receiving payouts, and/ or experience lapses in their motor vehicle insurance if auto-renewals fail.

As a result of delays in processing claims and receiving payouts, consumers may face financial costs and may have no access to a vehicle if they are not given a courtesy car and cannot finance the necessary vehicle repairs. If consumer's insurance auto-renewal fails then consumers may stop driving until their insurance is reinstated and may therefore have no access to a vehicle, or consumers may potentially continue driving without insurance and therefore face the potential consequences if they are caught driving uninsured (including a fine and penalty points), and/ or the consequences if they have an accident when uninsured.

3.3.2 Health care – GP practices and major hospitals

The impact map below details the potential impacts on the users of health care from a successful cyber attack on the health care sector. The scope of the analysis for this sector, as agreed with DSIT and the project Steering Group, is the impacts on consumers of cyber attacks on either major hospitals or GP practices. Consumer impacts from cyber attacks on the health care sector affecting the provision of other services is not within the agreed scope of the study.

Figure 3: Health care impact map



Major hospitals

As shown in the impact map above, a cyber attack affecting major hospitals may reduce the capacity of hospitals, resulting in longer wait times at A&E departments and disruptions to the provision of elective services, both inpatient and outpatient appointments, admissions, surgeries and procedures, as seen in the case study examples described in the literature review.

In response to increased wait times at A&E departments, where it is a viable alternative option, individuals may choose to travel further to attend A&E services at an alternative hospital or if they opt to still attend the impacted hospital, for example if they are unaware of the cyber attack or attending another hospital is not possible for them, they may face the increased wait times and delays to their treatment.

Different consumers are likely to respond differently depending on a number of factors including their health condition and location. For example, the literature review highlighted the difference in journey times between patients in rural and urban areas to reach unaffected hospitals. Previous analyses of the impacts of hospital cyber attacks have not found an overall impact on the mortality of patients admitted through A&E despite observing increased wait times (Ghafur et al. 2019). Studies found that

the impact of hospital cyber attacks on A&E wait times was mitigated in part by the diversion of patients to other hospitals (Ghafur et al. 2019, Neprash et al. 2024). Potential negative health impacts may be mitigated by prioritising and diverting patients depending on how urgently they need to be seen. Some studies suggest that the impact on those who wait additional time at the impacted hospital is primarily a time impact, although this will depend on how urgently patients need to be seen and their specific health condition. Those who divert to other hospitals may also face increased travel costs.

As a result of disruptions to elective outpatient and inpatient admissions/ appointments, patients may have scheduled elective appointments and procedures delayed or, if feasible, be diverted to other hospitals for treatment. Patients whose appointments and procedures are cancelled and delayed may face costs including health impacts and other personal costs. Health impacts may include a prolonged period of ill health, a worsening of current conditions or worsened outcomes due to a delay in diagnosis and the initiation of treatment (e.g. delays in cancer diagnosis), wellbeing impacts due to prolonged periods of uncertainty and anxiety (e.g. due to awaiting medical results or a long awaited surgery). Other personal costs may include those associated with rescheduling the required time off from work or childcare associated with attending hospital. Patients who are diverted to other hospitals may face time and travel costs as well as familiarisation costs associated with attending an unfamiliar hospital.

GP practices

A successful cyber attack on GP practices may result in a reduction in the ability of the practice to schedule appointments, access patient data and other computer systems. This may result in the cancellation of existing appointments, reduced availability of GP appointments, the inability for GPs to make or process referrals to specialist care and the inability of GPs to issue prescriptions.

In response to appointment cancellation and a reduced availability of GP appointments, some patients may access the services they require from an alternative source of health care provision such as a minor injuries unit, pharmacy, NHS 111 or A&E. In these cases, the cost to consumers (the patients) may include time, travel, and familiarisation costs associated with accessing this alternative provision. In addition, patients may realise different health outcomes as the service provided and the care patients receive from these alternative sources of health care is unlikely to be identical to that which they would have from the GP. There will also be knock-on impacts to these alternative sources of health care provision, which may affect the existing patients of these services e.g. waiting times.

Alternatively, some patients may go without care or wait and face a delay until a GP appointment is available. This may be because the alternative primary care providers are not suitable or accessible, or because the patient is unaware of, or unwilling to utilise, the available alternative provision. In this case the patient may experience similar costs to those with cancelled/ delayed major hospital appointments; namely, psychological impacts due to prolonged uncertainty and anxiety, and health impacts of prolonged ill health and delayed diagnosis and treatment. In addition, the experience of increased difficulty in accessing primary care services through their GP practice may reduce the patient's future engagement with healthcare services with consequent health and wellbeing effects.

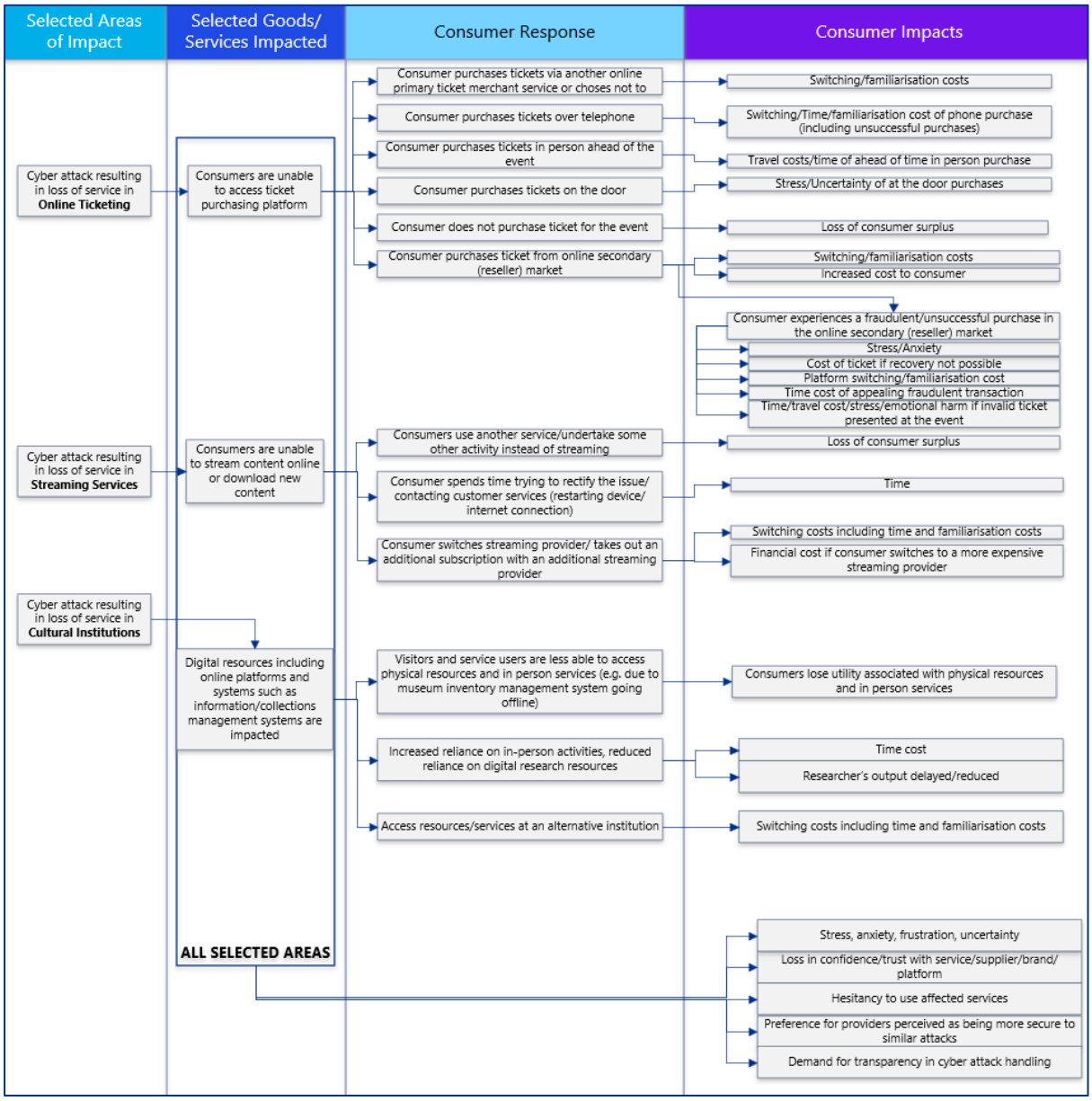
A GP's inability to make and process referrals may result in patients having to wait longer after having made a referral request (either in a GP appointment or by phone) for the GP to process the referral and subsequently be seen by the relevant specialist. These delays may result in patients experiencing impacts similar to those with cancelled/ delayed major hospital appointments. In addition, the difficulty and delay experienced by patients may lead to patients disengaging with health care, potentially with subsequent negative health impacts.

Disruption to GP's ability to issue prescriptions may result in patients having to wait longer to obtain prescriptions and in turn longer to obtain the prescription medication required. This may have health and wellbeing impacts with the extent depending on how long patients have to wait, whether it is for repeat or one-off prescriptions, the medical condition the prescription medication is for, and whether non-prescription medication could provide an alternative in the short term.

3.3.3 Creative industries and arts – online ticketing, streaming services and cultural institutions

The impact map below details the potential consumer impacts of successful cyber attacks in the creative industries and arts sector. The scope of the analysis for this sector, as agreed with DSIT and the project Steering Group, is the impacts on consumers of cyber attacks on either online ticketing, streaming services and cultural institutions. Consumer impacts from cyber attacks on the creative industries and arts sector affecting the provision of other goods and services is not within the agreed scope of the study.

Figure 4: Creative industries and arts impact map



Online ticketing

Online ticketing services include websites and apps that facilitate the search and purchase of tickets, and also provide access to previously purchased tickets for consumers. For the purpose of this study, as agreed with DSIT, the focus of the analysis is on the purchase of tickets on online ticketing platforms for live events such as the theatre and live music.

A cyber attack on an online ticketing platform may result in consumers being temporarily unable to purchase tickets from that platform. The nature of the ticket market affects the range of potential consumer responses. If consumers cannot purchase tickets from one online primary ticket merchant, in some cases tickets for the same event may also be available from other online primary ticket merchants while in other cases tickets may be exclusively sold by one online primary ticket merchant. In addition to the primary ticket sellers, there are offline channels and secondary (reseller) ticket markets.

If the consumer is able to purchase tickets from an alternative primary ticket seller (such as ATG Tickets, See Tickets or Ticketmaster[108]), they may respond to a cyber attack on one online ticketing services provider by purchasing tickets through an alternative provider. In this case, the switching consumer may experience a switching cost associated with the time required to familiarise themself with the unfamiliar platform or undertake activity such as creating a new account with the ticket seller.

The consumer may alternatively choose to purchase tickets through the secondary market,[109] (ticket resellers such as Seatwave and Viagogo[110]) if tickets are available, although this may come at an increased financial cost and the risk of a fraudulent or unsuccessful purchase.[111]

The consumer may alternatively respond by purchasing tickets through offline channels where these are available such as over the phone (if this service is unaffected by the cyber attack), at the box office (ahead of the event) or on the door. Switching to phone purchases of tickets may be associated with a familiarisation and time cost, and users unfamiliar with the venue may find it difficult to make a properly informed choice on seating. Travelling to the box office ahead of the event has a time and travel cost to the consumer with a further cost to the consumer if they are unable to ascertain if tickets are available before they arrive at the box office. On the door purchases are also associated with a cost to the consumer due to uncertainty that suitable tickets will be available for purchase.

Some consumers may respond by choosing to not purchase tickets for the event they would have if the cyber attack had not affected their ability to purchase tickets, forgoing the consumer benefit associated with the transaction.

Streaming services

Online streaming services include platforms that deliver content, such as films, music and games, online in real time, without consumers needing to download the content in advance. Examples include Netflix, Spotify, and YouTube Gaming. For the purpose of this study, as agreed with DSIT, the focus of the analysis is online video streaming.

A successful cyber attack on a provider of streaming services may result in the unavailability of a service for consumers. In response, the consumer may opt to go without access to that streaming service for the period of the outage or if the consumer wishes to continue to access online streaming services they may potentially switch to an alternative streaming service they already have access to or subscribe to a new streaming service they do not currently use. In addition, the consumer may spend time contacting customer services and/ or attempt to rectify the loss of provision of services themselves (e.g. by restarting devices or their Wi-Fi router) ahead of knowing it is a cyber attack affecting the provision of all services from the provider.

If a consumer goes without the services of the streaming provider for a period (undertaking some other activity), they forgo the benefit they derive from the access to the service for that period. Even if a consumer would not have used the streaming service during the affected period, there is an option value that the consumer loses during this period. The option value is the value people place on having

[108] ASTA | Buying Guide
[109] Secondary ticket websites that are operated by primary ticket sellers may be unavailable in the event of a successful cyber attack on a primary ticket seller. For example, GET ME IN! and Seatwave are both owned by Ticketmaster (source ASTA | Buying Guide).
[110] ASTA | Buying Guide
[111] CMA demands StubHub fix concerns or face court action - GOV.UK

the option to use the service over a period even if they do not plan on using it; this can be seen as a form of insurance.[112]

If the consumer switches/ takes out a new subscription with an alternative streaming provider they aren't already subscribed to, they face time costs associated with switching including the time taken to sign up with the alternative provider as well as the time taken to familiarise themselves with the new service. In addition, there may be a further financial cost, if the consumer switches to a more expensive streaming provider and/ or takes out an additional subscription.

If the consumer switches to a streaming provider they already have access to, then they may forgo some consumer benefit from not being able to access their preferred streaming service and having to use an alternative.

Cultural institutions

Successful cyber attacks on cultural institutions such as museums and libraries, may lead to the degradation of both online and in-person services. Online services including websites and digital catalogues may be unavailable or be provided with limited functionality. In-person services may be impacted through disruption to ticketing (with consumers being unable to purchase/ book tickets or experiencing entry delays without online tickets), through digitally enhanced experiences such as museum companion apps,[113] and through management systems that may impact the ability of staff to locate items within the institution's collection among other critical functions.[114]

If consumers can no longer access online services and resources of cultural institutions, some may respond by visiting the institution in-person in order to maintain access to the services and resources. Switching from digital access to in-person access may result in these consumers facing time and travel costs and a potential decrease in the output of researchers.

Consumers who continue to visit a cultural institution where the in-person services have been negatively impacted may experience reduced utility, learning or enjoyment of their visit. If the benefit they derive from their visit is less than what they expected, or what they realised on a previous visit, this may in turn impact consumers' future propensity to visit the cultural institution.

Some consumers of the digital and in-person services of an affected institution may respond by switching to an alternative cultural institution, for example visiting an alternative library to access a resource instead of their usual library or going to a different museum if the one that they planned to visit has been affected. These consumers may face switching and familiarisation costs including increased travel time/ costs, time to sign up as a guest user of a different library, time taken to research alternative museums for a day trip as well as the loss of benefits if the alternative service provider is less well suited to their needs.

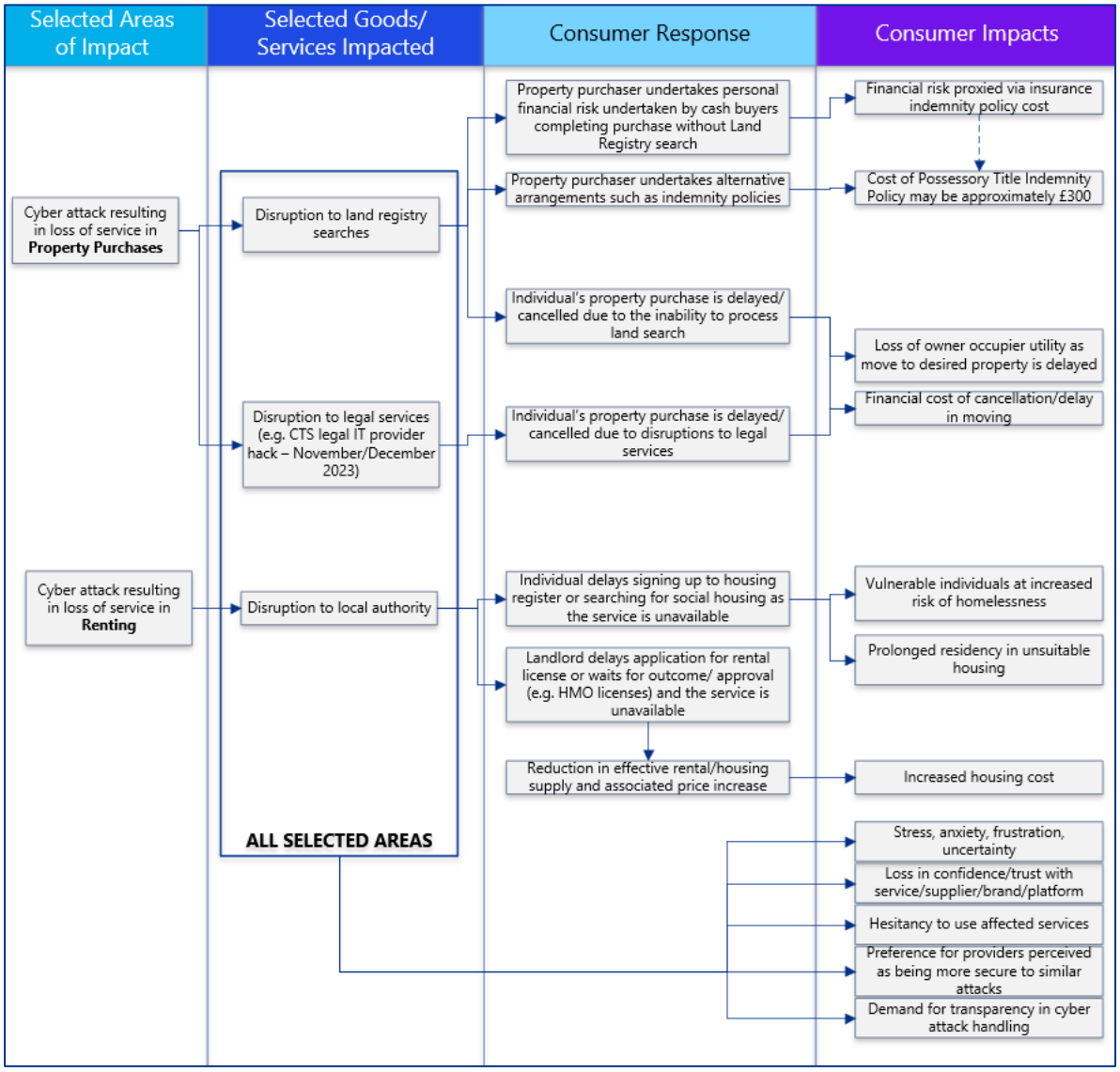
Finally, some consumers may respond to the incident by going without the services previously on offer or waiting until service has been restored. Where the consumer is able to wait, there may still be some cost to the individual such as the time taken to reschedule a visit, or due to a time preference for visiting sooner. Where an individual simply goes without the services the consumer cost can be seen as a loss of the consumer benefit of accessing the institution's services. These differential impacts are highlighted through the impacts of the ransomware attack on the British Library in October 2023, where scholars with access to alternative catalogues or resources could redirect their efforts, while others reliant on specific services experienced prolonged setbacks.

[112] Department for Environment, Food & Rural Affairs (2023). Enabling a Natural Capital Approach (ENCA): Guidance - GOV.UK. Section 2.4 Option Value
[113] For example, the British Museum's audio app. Audio app | British Museum
[114] As was the case during the Gallery Systems ransomware attack. Software Used by Hundreds of Museums Taken Down by Ransomware Attack

3.3.4 Real estate and renting – property purchases and renting

The impact map below details the potential consumer impacts of successful cyber attacks in the real estate and renting sector. The scope of the analysis for this sector, as agreed with DSIT and the project Steering Group, is the impacts on consumers of cyber attacks affecting either property purchases or renting. Consumer impacts from cyber attacks on the real estate and renting sector affecting the provision of other goods is not within the agreed scope of the study.

Figure 5: Real estate and renting impact map



Property purchases

Land registry searches are commonly undertaken before completing property purchases in the UK for various reasons including foremost to confirm property ownership therefore protecting purchasers from fraud, and to clarify property boundaries to prevent disputes. Legal services also play a critical role in property purchases, acting on behalf of buyers and sellers to make sure legal and regulatory requirements are met. Therefore, as shown in the above impact map, a cyber attack that causes disruptions to Land Registry searches or legal services may impact individuals' ability to complete property purchases.

As a result of a cyber attack affecting land registry searches or legal services, the property purchase process may be delayed and in some cases it may prevent property purchases completing altogether, with this likely depending on the stage the property purchase is at when the cyber attack, and hence the service disruption, occurs. If property purchases are delayed, consumers (i.e. the property purchasers) may face personal and financial costs such as those associated with reorganising the move, accommodation and storage during the delay period, and a delay to the utility they realise from the move. If the property purchase cannot complete and/ or falls through as a result of the delay (e.g. if the purchase is in a chain), consumers may face costs such as foregone legal/ conveyancing fees and moving costs and a loss of the utility that they would have realised from the purchase.[115] In both cases, consumers may also face wellbeing impacts, such as stress and frustration.

In the case of a purchaser being unable to confirm ownership through a Land Registry search, they may choose to continue with the purchase either by personally taking on the risk (if it is a cash purchase) or by purchasing indemnity insurance.[116] Continuing with the purchase as planned is associated with financial costs, either that associated with purchasing insurance, or the equivalent financial cost of 'self-insuring' by taking on the risk without insurance.

Renting

The impact map and analysis is focused on the impact on renters affected by a cyber attack on a local authority (LA) given the role of LAs in social housing and private rental and the evidence available e.g. from the Hackney Council ransomware attack in October 2020. LAs play a key role in rental housing provision in the UK, particularly through managing social housing provision, maintaining housing registers and issuing licences to landlords, such as mandatory House in Multiple Occupation (HMO) licenses which are required for 'house shares' and selective licensing where required.[117] If there was a cyber attack on a LA that affected the provision of such services, this could impact consumers who rent or access social housing through the affected LA.

In the event of a cyber attack on a LA, prospective renters in the social housing market may be temporarily unable to sign up to the housing register or to search for available social housing. These prospective renters may have to wait until service is restored in order to access housing services or seek alternative arrangements. This could potentially lead vulnerable individuals to face an increased risk of homelessness or experience prolonged residency in unsuitable housing. Such cyber attacks can also erode consumer confidence in local government services.

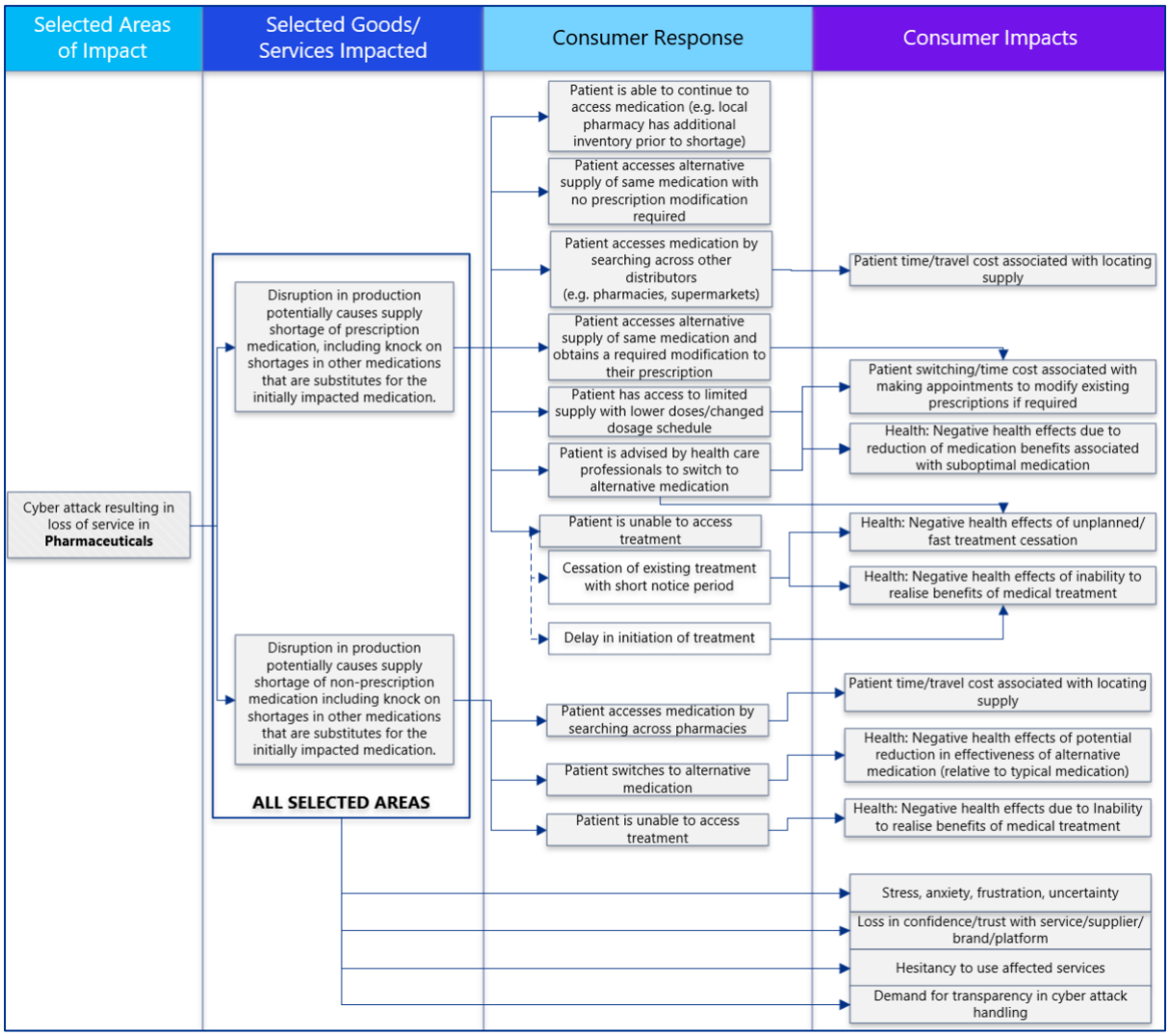
Delays in landlord license approvals such as HMO licenses may reduce the effective housing supply with resulting increases in housing costs for prospective renters. In addition, HMOs serve to make sure privately rented accommodation is safe and well-managed. Hence delays to such licences may jeopardise this.

3.3.5 Manufacturing – pharmaceutical manufacturing

The impact map below details the potential impacts on consumers of a successful cyber attack in the manufacturing sector. The scope of the analysis for this sector, as agreed with DSIT and the project Steering Group, is the impacts on patients of cyber attacks on UK manufacturers of prescription and non-prescription medication. Consumer impacts from cyber attacks on the manufacturing sector affecting the provision of other goods is not within the agreed scope of the study.

[115] Hackney cyber-attack causes collapse of property purchases - BBC News
[116] Hackney's property market 'on pause' following Town Hall cyber attack – Hackney Citizen
[117] House in multiple occupation licence - GOV.UK

Figure 6: Manufacturing impact map



Cyber attacks on pharmaceutical manufacturers have the potential to cause supply issues for specific medicine(s). These supply issues are likely to be lagged due to production timelines and manufacturers and wholesalers holding stocks. Patients also may respond differently depending on medicine(s) impacted and length of supply issue. For example, patients could be advised not to switch medication if there are very temporary supply shortages and/ or the medication is not critical to their health.

The impact of a supply issue as a result of a cyber attack on prescription medication is considered separately to the impact on non-prescription medication in terms of the potential consumer response and impacts. While it is assumed that there is a patient impact for the purpose of this analysis, it is recognised that disruptions may not result in either supply issues and/ or patient impact. In addition, it is recognised that the health impact ultimately depends on the specific medicine because of its criticality for the treatment it is being used for, the volume impacted, and the availability of suitable alternatives, rather than whether it is prescription or non-prescription.

Assuming a cyber attack affecting pharmaceutical manufacturers impacts the availability of medication in community settings, the loss of availability of a **non-prescription medication** could result in the following scenarios:

- Patient continues to access the medication with additional effort (e.g. searching across pharmacies to access available remaining supplies)
- Patient could be unable to access supply of the medication, resulting in a break in their medication until provision is restored

- Patient is able to switch to an alternative medication on advice from healthcare professional.

The loss of availability of **prescription only medication** could result in the following scenarios:

- Patient continues to access the medication which could be for several reasons including: they have sufficient supply to last until the resolution of the issue, pharmacies/ wholesalers have stock remaining or they continue to receive the same medicine but in an alternative brand, form or strength e.g. a 10mg tablet to a dose of 2x5mg tablets
- Patient could be unable to access supplies of the medication, resulting in a break in their medication
- Patient is able to switch to an alternative medication on advice from healthcare professional.

In the event of a supply issue, there are national, regional and local management, and escalation processes and communication routes.[118] Therefore, the patient responses outlined in the impact map and described below assume that national shortage management mitigations are used. National shortage management tools always aim to mitigate supply issues as much as possible in order to prevent impact to patients.

The impacts on patients are described for non-prescription and prescription medication together below, split by various patient outcomes in terms of accessing their medication.

Patient is unable to access the medication:

A patient may face negative health impacts from being unable to access their medication, either through not having it or the uncertainty of the situation. These health impacts may be amplified for a number of reasons such as the duration of the issue, the type of medication and clinical condition being treated and if the patient is on a medication which should not be stopped abruptly.[119] There could also be additional impacts on health services e.g. due to an increase in appointments.

Patient continues to access the medication:

Patients may be able to continue to access the medication however face additional costs, such as time associated with contacting different pharmacies to find available supply, and travel costs as the pharmacy that has stock may be further away.

In cases where alternative brands or different strengths/ formulations of the same medication are available, a new prescription may be required.[120] This may result in a time cost to the patient associated with obtaining new prescriptions and potentially additional travel costs to the patient if this requires a GP appointment.

Patient is able to switch to an alternative medication:

In cases where a suitable clinical alternative medication is available, the patient will require a new prescription via their GP unless the pharmacy is able to issue through the provision of serious shortage protocols. This could be associated with time costs as well as potential negative health consequences of switching medication (e.g. the patient not responding well to the new medication).

[118] NHS England » A guide to the systems and processes for managing medicines supply issues in England
[119] For example, the Royal College of Psychiatrists state that 'suddenly' stopping antidepressant treatment 'can lead to you developing withdrawal symptoms and increase the chance of you becoming unwell again.' Further recommending to stop antidepressants by 'tapering' over a period of 'a few weeks or months.' Stopping antidepressants
[120] Section 4.1.3 Managing shortages in primary care in Royal Pharmaceutical Society (2024). Medicines Shortages: Solutions for empty shelves

4 Estimated costs to consumers from cyber attacks

4.1 Overview of the approach to valuing consumer impacts

This section sets out the detailed methodologies developed and used to monetise the impacts on consumers of cyber attacks on the specific goods and services within the scope of this study.

For each of the goods and services within scope of this study the following is described:

- The methodology used to monetise the impacts on consumers and the data sources.
- The estimated consumer impact per cyber attack (i.e. the unit value) and the annual consumer impact (i.e. the annual value), which is estimated using data on the estimated frequency of cyber attacks in the relevant sector.
- The limitations of the methodologies used.

The methodologies have been developed in line with HMT Green Book guidance. They utilise available secondary data, as well as primary data collected through the consumer survey carried out as part of this study.

4.2 Valuation methodologies and results

4.2.1 Financial services

4.2.1.1 Online banking

Introduction to the valuation of consumer impacts from cyber attacks on online banking

The potential impacts on consumers from a successful cyber attack on online banking are set out in section 3.3.1. In this section the methodology used to monetise the impacts identified are set out, and the quantified impacts are presented.

As set out in the financial services impact map (see section 3.3.1), consumers may respond in a variety of ways to not being able to access their online banking services as a result of a cyber attack. Broadly, consumers may:

- 'do nothing' and therefore go without the online banking service until the service resumes; or
- 'do something' such as using non-digital banking services, asking a friend/ family member to carry out a financial transaction on their behalf, or potentially switching to the banking services of an alternative unaffected provider.

The associated consumer impacts would also vary. For consumers who go without online banking services, impacts may include financial costs, and for consumers who 'do something', impacts may include travel costs, familiarisation costs, and time costs.

The quantification of the impact on consumers from being unable to access online banking services as a result of a cyber attack uses stated preference techniques in line with HMT Green Book guidance on the valuation of costs and benefits where there is no market price. A consumer survey was designed to elicit consumer willingness to pay (WTP) to avoid a loss of access to online banking services and consumer willingness to accept (WTA) compensation for a loss of access. WTP and WTA are methods used to estimate how much consumers value a good or service. WTP reflects the maximum amount a consumer will pay for something, and WTA reflects the minimum amount a consumer will accept in compensation for a loss. The consumer survey was designed in line with HMT Green Book supplementary guidance on stated preference techniques.[121] The consumer survey

[121] Economic_valuation_with_stated_preference_techniques.pdf

achieved 1,000 completed survey responses and the data was weighted to be representative of the UK population.

In relation to online banking services the consumer survey covered:

- Respondents use of online banking services.
- What respondents would do in the event of being unable to access online banking services, and the associated travel, time, familiarisation and wellbeing impacts associated with this.
- What respondents would be WTP to avoid a loss of access to online banking services and how much they would be WTA in compensation for a loss of access.

Two approaches to elicit the WTP to avoid a loss of access to online banking services and WTA compensation for a loss of access were used in the consumer survey. Firstly, using a double-bounded dichotomous choice approach where respondents were asked whether or not they would be WTP/ WTA a stated amount, and were then asked to say yes or no to higher/ lower amounts, and secondly using an open-ended elicitation approach where respondents were asked their WTP/ WTA in an open question. Under the double-bounded dichotomous choice approach, respondents were asked if they would be WTP or WTA amounts ranging from £7 to £27. The starting values were determined based on a review of monthly current account fees across a range of banks.[122]

The scenario described to respondents was where the loss of access to their main online banking service was expected to last for three days and this would happen at a random time. It may be at a time when access to online banking services is not required, or when there is a greater need for access, such as when setting up a new recurring payment or before making a large purchase. The three day duration was based on information from the 2024 Cyber Security Breaches Survey (CSBS)[123] and the Lloyds Bank DoS attack which disrupted service provision for three days.[124]

The data from the survey responses to the WTP/ WTA questions were then used to value the impact on consumers from being unable to access banking services as a result of a cyber attack, as described below. This involved cleaning the data to remove protest responses, and invalid responses,[125] in order to increase the reliability of the findings. Modelling was then undertaken to derive the WTP/ WTA values (see Appendix 1 for more detail).

Methodology for the valuation of the impact on consumers who are unable to access online banking services as a result of a cyber attack

In order to estimate the impact on consumers from a cyber attack resulting in the loss of access to online banking services in the scenario detailed above, the monetised impact per consumer was multiplied by the number of consumers impacted. Each of these components are considered in turn below.

[122] Monthly current account fees were taken from banks own websites. Halifax: £0 to £19, Santander: £0 to £5, Monzo £3 to £17 and Lloyds £0 to £22.50. Information correct as at 9th January.
[123] Cyber security breaches survey 2024 - GOV.UK. In response to the survey question that asked about the duration to restoration of ransomware and DOS incidents in the finance/ insurance sector, 1 respondent said 'no time at all', 1 respondent said 'less than a day' and 1 respondent said 'between a day and under a week.'
[124] Lloyds cyber-attack details emerge - BBC News
[125] Protest and invalid responses were identified through the application of a set of rules. A response was deemed invalid if the self-reported maximum WTP/ minimum WTA value was inconsistent with the dichotomous choice answered provided. A response was deemed invalid or a protest response if the self-reported minimum WTA was very high (above £100 for online banking). A response was deemed invalid where the respondent had answered 'yes, yes' or 'no, no' for the WTP dichotomous choice questions and indicated that one of the reasons for the answer was that they did not believe that the cyber-attack would actually happen. A WTP value was deemed a protest response if the respondent answered 'no, no' to the dichotomous choice and indicated that they shouldn't have to pay as a reason whilst not indicating any of the following reasons: that they do not value the service sufficiently, that they could not afford to pay more or that not having access to the service for the duration was not an issue. In addition, where the respondent had provided a free-text 'other' reason, these reasons were manually sorted to identify any protest or invalid responses.

The impact per consumer

The table below sets out the estimated value that consumers would be WTP to avoid loss of access to online banking services and WTA to be compensated for the loss of access, for both the double-bounded dichotomous choice approach and open-ended elicitation approach used in the consumer survey. This is the WTP/ WTA across all consumers, regardless of how they respond to the loss of access to online banking services (i.e. whether they would 'do nothing' and wait until the service resumes, as well as those who would 'do something' as an alternative). When answering questions about what respondents are WTP/ WTA they are implicitly considering what they would do in the event of being unable to access online banking services.

Table 10: WTP and WTA amounts for loss of access to online banking services

Weighted median values	WTP (£)	WTA (£)
Estimate from double-bounded dichotomous choice approach	4.34	15.14
Estimate from open-ended elicitation approach	0.00	15.00

Source: Consumer survey, 2025. KPMG analysis.

As shown in the table above, the estimated WTP and WTA values derived from the survey data, varied from a WTP of £0 to a WTA of £15.14. For the purpose of estimating the potential impact on consumers from a cyber attack resulting in the loss of access to online banking services, the range from a WTP of £4.34 to a WTA of £15.14 is used. The WTA values under both approaches were higher than the WTP values. This is common with stated preference techniques as consumers tend to value losses more than gains, and so are willing to pay less than they are willing to accept. In addition, WTP is affected by consumers' incomes while there is no constraint on compensation. The results show that under the open-ended elicitation approach the median WTP was £0. This often arises where consumers don't believe they should need to pay for something (see reasons below).

There were also some differences between the WTA under the open-ended elicitation approach[126] between demographic groups, including the following groups which had a higher WTA compared to all respondents:

- For respondents aged 66+ the median WTA was £20
- For respondents with a self-reported disability the median WTA was £19
- For female respondents the median WTA was £19.50

In line with best practice, survey respondents were asked why they would not be willing to pay more than the amount they stated when asked about their willingness to pay to avoid the loss of access to online banking services and why they would not be willing to accept less to compensate them for the loss of access than the amount they stated.

As shown in the table below, the most frequently reported reasons for not being willing to pay more than the amount respondents stated was because respondents did not think they should have to pay to avoid the loss (cited by 50% of respondents) and because losing access for three days wouldn't be a problem for them (cited by 36% of respondents). Those who selected the 'other' category were presented with a free-text input to provide further detail on their reasoning. Almost all of those who provided an 'other reason went on to express a protest response or rejection of the premise of the question and were excluded. Most of these reasons can be categorised as those criticising banks (i.e. complaining about the closure of branches), stating that they should not have to pay for this (either as they already pay or that this is a basic service requirement), or questioning the idea of paying to prevent a hack (e.g. complaining that it is wrong to pay cyber criminals a ransom or disagreeing with the notion that they could pay more in order to receive protection from a cyber-attack).

[126] The nature of double-bounded dichotomous choice method involves aggregating responses in order to estimate the average WTA/ WTP values. This aggregation can obscure individual demographic differences and due to the reduced statistical power when estimating double-bounded dichotomous choice WTA/ WTP values for subgroups it is not possible to reliably estimate and report these figures.

Table 11: Reasons for respondents not being willing to pay more to avoid a loss of access to online banking services

Consumer response	Percentage
I don't value it sufficiently	14
I could not afford it	26
I should not have to pay to avoid this	50
Losing access to my main online banking service/ banking app for 3 days would not be a problem for me	36
I am already paying for this service through bank charges	24
I don't believe this will happen	3
I don't feel confident stating a value/ I need more information	22
Don't know	5
Other	0

Source: Consumer survey, 2025. KPMG analysis.
Note: Total sums to more than 100% because respondents could select multiple options.

As shown in the table below, the most frequently reported reasons for not being willing to accept less in compensation than the amount respondents stated was because respondents would not be satisfied by less (cited by 35% of respondents) and because they did not think it would be a fair amount (cited by 31% of respondents). Of those who selected the other category, most of the subsequent reasons provided can be categorised into the following categories: referencing the inconvenience or time cost to the individual, that they would not need compensation for loss of banking services given the length of the outage, questioning the applicability of compensation or stating that the bank would not be at fault (these were counted as invalid), direct reference to the account fees that they pay, criticisms of banks (these were counted as invalid) and a small number suggesting that they were concerned about their bank accounts being compromised (these were counted as invalid).

Table 12: Reasons for respondents not being willing to accept less in compensation for a loss of access to online banking services

Consumer response	Percentage
It wouldn't be a fair amount	31
It wouldn't cover the cost of what I would do instead	18
I wouldn't be satisfied by less	35
Don't know	7
Other	10

Source: Consumer survey, 2025. KPMG analysis.
Note: May not sum to 100% due to rounding.

The number of consumers impacted

To estimate the number of consumers potentially impacted by a cyber attack, data on bank market shares by volume of main Personal Current Accounts (PCAs) is used from the CMA Retail Banking Market Investigation in 2016.[127] This is set out in the table below.

[127] Retail banking market investigation final report, table 5.1.

Table 13: GB market shares by volume of main PCAs, 2015

Bank	Market share (%)
Barclays	10-20
Clydesdale	0-5
Co-op Bank	0-5
Danske	0-5
HSBCG	10-20
LBG	20-30
Metro	0-5
Nationwide	5-10
RBSG	10-20
Santander	10-20
TSB	0-5

Source: CMA (2016), Retail Banking Market Investigation Final Report

The consumer survey commissioned as part of this study indicates 94% of adults in the UK[128] use online banking services/ apps, with 76% of respondents using these services either daily or several times a week.[129] Therefore, it is estimated that the number of UK adults using online banking services is approximately 51 million (i.e. 94% of the estimated 54 million individuals aged over 16 in the UK).[130]

Taking the market shares by volume of PCAs together with the number of UK adults using online banking services, the number of consumers who may be impacted by a cyber attack resulting in the loss of access to online banking services for the customers of one major bank is estimated. The estimated number of impacted consumers is therefore estimated to range from 1.3 million (i.e. 2.5%[131] of 51 million) to 15 million (i.e. 30%[132] of 51 million).

Taking the estimated impact per consumer and the number of customers impacted, the estimated impact on consumers per cyber attack is estimated to range from approximately £5.5m (£4.34*1.3 million) to £231m (£15.14*15 million) depending on the market share of the bank affected.

Variation in the impact on consumers who are unable to access online banking services as a result of a cyber attack

It may be expected that the impact of a cyber attack resulting in the loss of access to online banking services would vary across consumers depending on their response to this loss of access. The table below shows the results from the consumer survey in terms of what respondents said they would do instead of using online banking. As can be seen, 20% of respondents said they would do nothing and wait until the service resumes, while the next most frequently reported response was visiting a bank branch (17%) and using a cash machine (14%). Only 2% of respondents said they would switch banking services to another provider which is consistent with the low level of switching seen in the banking sector generally. In 2015, the CMA estimated that the annual rate of switching personal current accounts was 3%[133] and pay.uk data shows there were 1.17 million personal current account switches in 2024.[134]

[128] The survey data was weighted to be representative of the UK population.
[129] Frequency of use varies by consumer groups with 98% of consumers with an income of £100k or more, and 83% of 35 to 44 year olds, more using online banking service daily or several times a week.
[130] Population estimates for the UK, England and Wales, Scotland and Northern Ireland - Office for National Statistics
[131] This is based on the mid-point of the market share where the market share is 0 to 5%.
[132] This is based on the maximum of the market share where the market share is 20 to 30%.
[133] Quantitative analysis of searching and switching in personal current accounts
[134] Current Account Switch Service statistics - Pay.UK

Table 14: Consumer responses to loss of access to online banking services

Consumer response	Percentage
Wait until banking service/ banking app is available again	20
Visit a bank branch	17
Use a cash machine	14
Use telephone banking services	5
Ask a friend/ family member to take an action on your behalf	2
Switch banking services to another provider	2
Other	2
Don't know	11

Source: Consumer survey, 2025. KPMG analysis.

The consumer survey suggests that the response of consumers varies by key characteristics. In particular:

- Consumers who missed a payment for any essential bills[135] in the last six months were less likely than all respondents to do nothing and wait until the online banking service resumes (15% of respondents who had missed a payment vs. 20% of all respondents).
- Consumers aged 66+ were more likely to use a cash machine than all consumers (19% of 66+ year olds vs. 14% of all respondents).

The consumer survey also asked questions to understand the costs associated with how consumers would respond to a loss of access to online banking services, including travel, time, familiarisation and stress/ anxiety impacts.

Travel: Consumers who said they would respond to a loss of access to online banking services by visiting a bank branch or using a cash machine, were asked about the travel time associated with doing this. The most frequently reported one-way journey time was six to 15 minutes reported by 38% of consumers who would visit a bank branch or use a cash machine, followed by 16 to 30 minutes for 29% of consumers.

Time: In terms of the additional time taken to pursue their alternative action in the event of a loss of access to online banking services, respondents most frequently reported that it would take an additional six to 15 minutes (24% of respondents), followed by 16 to 30 minutes (reported by 21% of respondents), compared to using online banking services.

The additional time reported varied depending on the action taken by consumers. Switching bank, and asking a friend/ family member to take an action on your behalf was associated with more time:

- Of the respondents who said they would switch bank, 19% reported this would take more than 1 hour longer than using online banking services.
- Of the respondents who said they would ask a friend/ family member to take an action on their behalf, 13% reported this would take more than 1 hour longer than using online banking services.

Familiarisation: To understand whether consumers would incur a familiarisation cost in relation to the action they would take as a result of not being able to access online banking services, the survey asked whether they had taken this action in the last 12 months. The idea being that if a consumer had taken this action in the last 12 months then they would be unlikely to incur a familiarisation cost. The survey found that 53% of respondents had taken this action in the last 12 months, while 47% had not. Hence suggesting that just under half of consumers would incur some level of a familiarisation cost. It is possible that even for consumers that had not taken this action recently, they would be unlikely to incur a familiarisation cost in addition to the additional time reported, such as for those who would use a cash machine or ask a friend/ family member to take an action on their behalf.

[135] i.e. rent/ mortgage, utilities, internet/ phone, council tax

Stress and anxiety: The survey also asked respondents about the extent to which they would feel stressed and anxious about having to pursue an alternative action in the event of not being able to access online banking services. While 20% of respondents said they would not feel at all stressed, 18% said they would feel very stressed. This was higher among consumers who had missed a payment for any essential bills in the last six months, at 26%.

The extent to which survey respondents reported they would feel stressed and anxious about having to pursue an alternative action varied by the action taken by consumers. Notably, more respondents who said they would ask a friend/ family member to take an action on their behalf, or who would switch bank, reported that they would feel very stressed about having to do this.

- Of the respondents who said they would switch bank, 33% reported they would feel very stressed, 48% said they would feel slightly stressed, 14% said they would feel not very stressed, and 5% said not at all stressed.
- Of the respondents who said they would ask a friend/ family member to take an action on their behalf, 22% reported they would feel very stressed 41% said they would feel slightly stressed, 33% said they would feel not very stressed, and 4% said not at all stressed.

Estimated frequency of cyber attacks and associated impacts

The frequency of successful cyber attacks was estimated using data from the annual Cyber Security Breaches Survey (CSBS),[136] combining data from the years 2019 to 2024.

In order to understand the annual occurrence of ransomware attacks, responses to the following question were analysed, 'Have any of the following happened to your organisation in the last 12 months, or not?: Your organisation's devices being targeted with ransomware.' It is noted that this question does not isolate only those cyber attacks that had a material impact, and will include responses relating to both 'successful' and 'unsuccessful' cyber attacks. Survey data relating to ransomware attacks was the focus of the analysis given these attacks have the ability to generate the consumer impacts which this study aims to capture, namely disruptions to the provision of and consumer access to services.

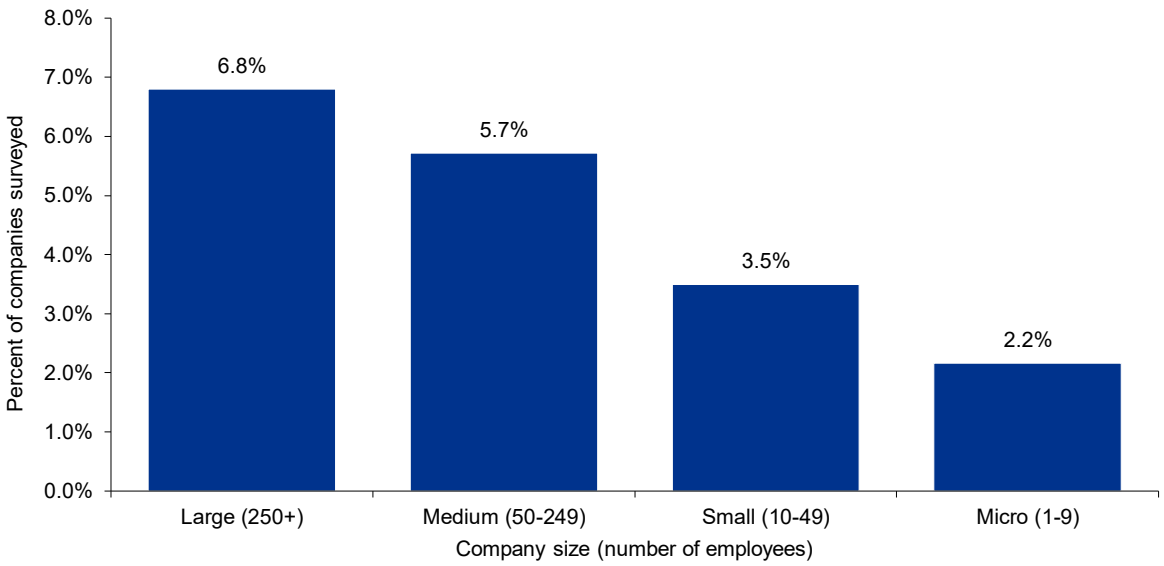
Focusing on private sector companies,[137] it can be seen that larger companies were more likely to report in the survey that they had been the target of a ransomware attack in the 12 months prior (see Figure 9). Due to the relatively small number of firms surveyed who did report being a ransomware target, analysis of the CSBS is on unweighted data. As large companies (such as major banks and insurers) and their consumers are the focus of the analysis, the estimated frequency of successful cyber attacks is informed by survey responses from large companies (as defined in the CSBS as those with 250 or more employees).

The percentage of large companies reporting being a target of ransomware attacks in the survey varied over the years included in the analysis (see Figure 8), with the highest rate in 2020 when 11.6% of large companies surveyed reported being the target of ransomware in the previous 12 months and the lowest rate of 3.8% was in 2022.

[136] Department for Science, Innovation and Technology and the Home Office (2024) Cyber security breaches survey 2024 - GOV.UK

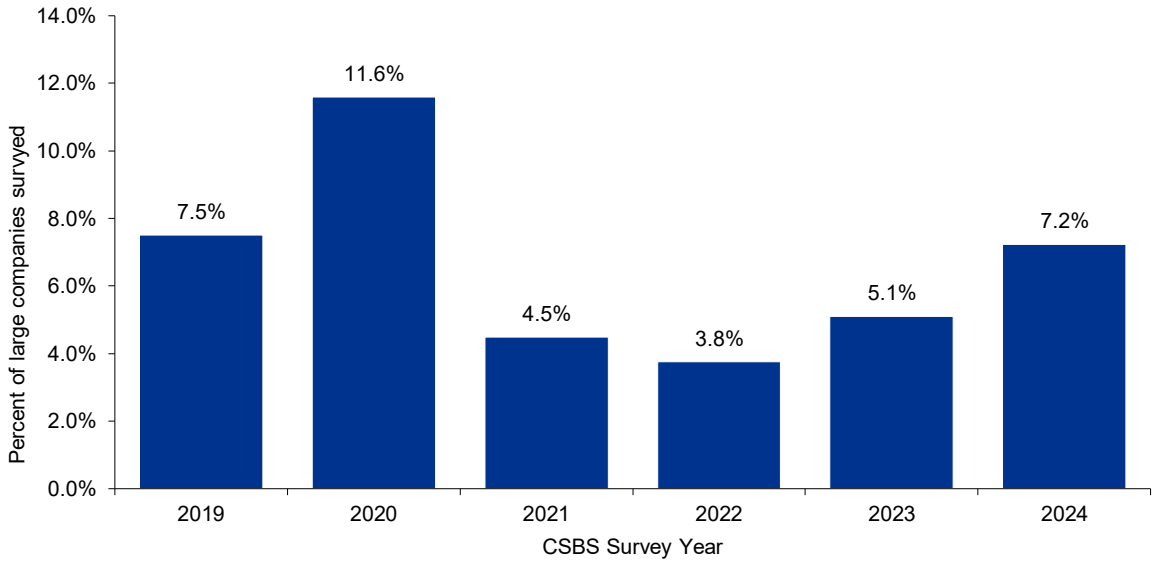
[137] CSBS samples three groups of organisations, private sector companies, charities and state education institutions. In the 2024 survey, data on the size of the organisation was only available for private sector companies. As such, the analysis focuses on the survey results for private sector companies. In addition, in earlier years of the survey, the state education sector was not consistently split out from the other groups, and as such all surveyed companies identified as either state education institutions or classified as within the education sector have been grouped together across all years and split out from the charity and private sector companies groups.

Figure 7: Companies experiencing being targeted with ransomware in the 12 months prior to being surveyed: private sector companies, 2019 – 2024



Source: CSBS, KPMG Analysis

Figure 8: Large companies experiencing being targeted with ransomware in the 12 months prior to being surveyed: private sector companies with 250 or more employees, 2019 – 2024



Source: CSBS Data, KPMG analysis

The low number of reported ransomware attacks in the survey data is a source of the high annual variation in the estimated proportion of companies targeted. As can be seen in Table 15, the low rate of ransomware targeting reported in 2022 coincided with only five companies reporting experiencing a targeting incident in the last 12 months, and a relatively small overall sample of large companies in that year's CSBS. As a result, the frequency of ransomware attacks is taken from the combined sample of all years 2019 to 2024, which is 6.8%.

Table 15: CSBS data (2019-2024): Experience as a ransomware target by large companies

Survey year	No. large companies surveyed (250+ employees)	No. targeted by ransomware in the last 12 months	% targeted by ransomware in the last 12 months
2019	200	15	7.5%
2020	207	24	11.6%
2021	201	9	4.5%
2022	133	5	3.8%
2023	196	10	5.1%
2024	166	12	7.2%

Source: CSBS Data, KPMG analysis

To understand the frequency of incidents, the rate of conversion from targeting incidents to disruptive cyber attacks is applied to the 6.8% annual targeting rate. CSBS data was used to identify this conversion rate, filtering the dataset to only include companies who had reported being targets of ransomware attacks. Those companies experiencing a 'successful' cyber attack causing disruption to consumers were identified if they had experienced disruption as a result of a ransomware attack and had not indicated that the time until normal service was restored was 'no time at all.' Over the six years of CSBS survey data analysed, the conversion rate from ransomware targeting to ransomware related disruptive cyber attacks was 36% for large private sector companies (see Table 16). The ransomware conversion rate was similar for medium sized companies (34.6%), and the ransomware conversation rates for small and micro companies were similar to each other although around 10 percentage points lower than the rates seen for large and medium sized companies.

Table 16: CSBS data (2019-2024): Ransomware conversion rates in private sector companies

Company size (number of employees)	No. targeted by ransomware in the last 12 months	No. disrupted by ransomware in the last 12 months	Ransomware conversion rate (%)
Large (250+)	75	27	36.0%
Medium (50-249)	58	27	34.6%
Small (10-24)	69	18	26.1%
Micro (1-9)	112	28	25.0%

Source: CSBS Data, KPMG analysis

Combining the targeting rate of 6.8% with the ransomware conversion rate for large companies of 36.0%, the rate of successful ransomware attacks is estimated at **2.45% per company per year**, or approximately one in forty companies. Applying this rate to the relevant set of companies for online banking this equates to an expected 0.27 cyber attacks per year across the 11 major providers of Personal Current accounts (see Table 13). This equates to approximately one successful cyber attack every four years. The estimated consumer impact and frequency are shown in Table 17.

Table 17: Estimated consumer impact of a cyber attack resulting in a loss of access to online banking services and estimated frequency of relevant cyber attacks

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Years per incident (approx.)
	Low	High		
Online Banking	£5.5m	£231m	0.27 per year	Once every four years

Note: Where the estimated annual frequency of cyber attacks is not a whole number, DSIT requested that the annual consumer impact was not monetised.

Limitations of the approach to valuing the impact on consumers who are unable to access online banking services as a result of a cyber attack

There are a number of important limitations of the approach to valuing the impact on consumers from a loss of access to online banking services as a result of a cyber attack:

- **Bias:** A number of factors may lead to respondents not stating their true WTP/ WTA. In particular, because the scenario is hypothetical and there are no real financial consequences of the amounts stated. In addition, respondents may deliberately over or under state WTP/ WTA in order to try to influence how they think the values will be used. Furthermore, misunderstanding the concepts and/ or the scenario may bias the results.
- **Context:** The WTP/ WTA values relate to the specific scenario described to respondents (see description above). Therefore, this may not be representative of the impact of all cyber attacks affecting access to online banking. For example, it is likely to depend on the duration of the disruption and the timing of the impact.
- **Anchoring effect:** A limitation of the double-bounded dichotomous choice approach is the so called 'anchoring effect' whereby respondents WTP and WTA are influenced in some way by the value first presented to them. To mitigate against this anchoring effect, respondents were also asked to self-report their WTP and WTA through the open-ended elicitation approach. However, as this question was asked after the questions for the double-bounded dichotomous choice approach, the stated values may still influence the self-reported values.
- **Number of consumers impacted:** While an attempt has been made to estimate the number of consumers potentially affected by a cyber attack resulting in the loss of access to online banking services, there is considerable uncertainty around this. Data from the CMA Retail Banking Market Investigation in 2016 is used which is old, due to a lack of reliable, more recent data, and the market may have changed since. In addition, the number of consumers impacted depends on the size of the impacted provider but also the degree to which consumers have multiple bank accounts that could be used instead. It is estimated that 22% of customers have more than one PCA with different banks, and a further 9% have more than one PCA with the same as well as with a different bank.[138]
- **Limitations of sample:** The survey was conducted online and therefore excludes people without online access. Therefore, it may be that the percentage of respondents who reported to use online banking may be overestimated.

4.2.1.2 Motor vehicle insurance

Introduction to the valuation of consumer impacts from cyber attacks on the motor vehicle insurance sector

The potential impacts on consumers from a cyber attack on motor vehicle insurance providers are set out in section 3.3.1. In the section below, the methodology for monetising the financial impact that would arise due to delays in insurance claims/ payouts is set out and the consumer impact is quantified.

The methodology focuses on assessing the monetary value of delays in insurance payments through the application of a rate of interest to the claim/ payout in order to estimate the opportunity cost of not having the payment earlier due to delays in processing claims. Non-financial impacts, such as the lack of access to a courtesy car and the stress, anxiety, and frustration associated with delays to claims/ payouts are not captured in this methodology (see limitations for further details).

Methodology for the valuation of consumer impacts from cyber attacks on motor vehicle insurance sector

To estimate the financial impacts on consumers of delayed payment as a result of a cyber attack on a motor vehicle insurance provider, the following approach is taken:

- **Motor vehicle insurance payments per provider:** Total annual payments to consumers per insurance provider is estimated by applying an estimated share of motor vehicle insurance payouts per provider to the total claim payouts of the motor vehicle insurance market;
- **Payments during the period impacted by the cyber attack:** The value of payments impacted during the period over which insurance payments are delayed is estimated based on an estimate of the typical duration of disruption and the share of annual payments for the period of disruption; and

[138] Retail banking final report - Appendices 1.1 to 6.9, A6.1-15, CMA, 2016.

- **Opportunity cost of payment delays:** A rate of interest is then applied to calculate the monetary value of delayed payments.

Each of these steps are described in further detail below. Please note that figures have been rounded for ease of presentation. As a result, some figures may not sum due to rounding.

Motor vehicle insurance payments per provider

The annual value of motor vehicle insurance payments in 2024 was £11.7 billion according to the Association of British Insurers (ABI).[139]

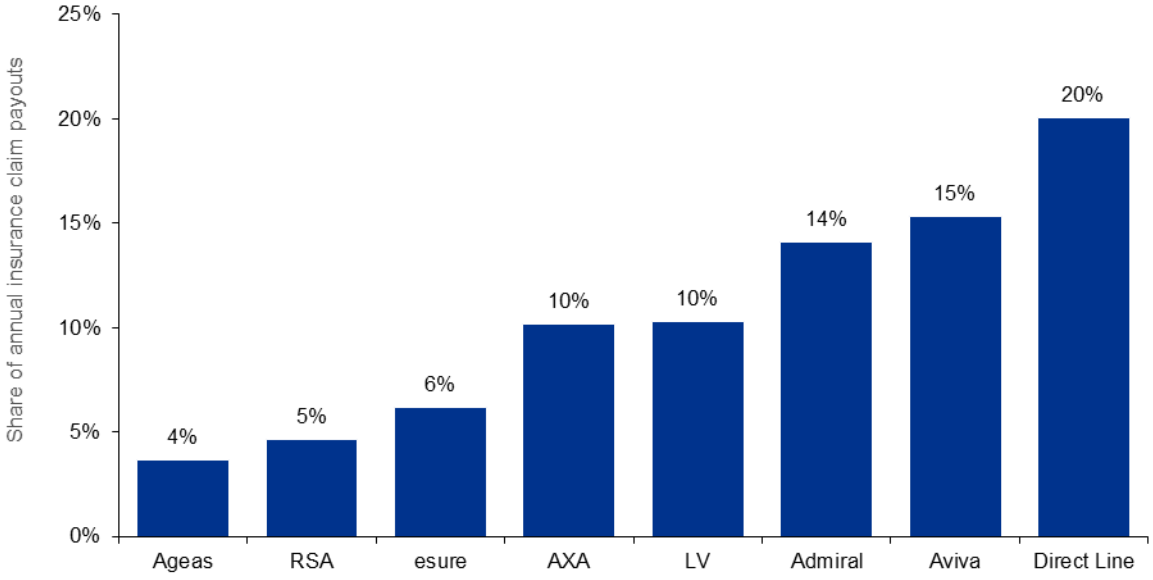
There is a lack of publicly available data on the current market share of providers of motor insurance. A 2013 report by the Competition Commission,[140] shows that the majority of the private motor vehicle market was comprised of the following ten largest insurers:

- Admiral Group plc (Admiral)
- Ageas NV/SA (Ageas)
- Aviva plc (Aviva)
- Axa Insurance UK plc (AXA)
- CIS General Insurance Limited (Royal London)[141,142]
- Direct Line Insurance Group plc (Direct Line)
- esure Insurance Limited (esure)
- Liverpool Victoria Insurance Company Limited (LV)
- Royal & Sun Alliance Insurance plc (RSA)
- Zurich Insurance plc (Zurich)[143]

Two of these insurers, Royal London and Zurich, are no longer active in the UK motor vehicle insurance market. Data on motor vehicle insurance claims incurred from the 2023 SFCR (Solvency and Financial Conditions Report) regulatory filings for the eight firms still active in the market were combined with the ABI's reported £9.9 billion of payments by motor vehicle insurers in the same year[144] to estimate these firms' share of UK motor vehicle insurance payouts.

[139] The Association of British Insurers (2025) Motor claims hit record £11.7 billion in 2024 | ABI
[140] Competition Commission (2013) Private Motor Insurance - Background to private motor insurance (insurers, brokers and price comparison websites)
[141] Looking for Co-operative Insurance Society (CIS)? - Royal London
[142] Royal London is not presently active in the motor vehicle insurance market.
[143] Zurich is not presently active in the motor vehicle insurance market.
[144] The Association of British Insurers (2024) Motor insurers pay out record amounts to help keep motorists mobile | ABI

Figure 9: Estimated share of UK motor vehicle insurance payouts (by value), 2023



Source: Company SFCR filings, The Association of British Insurers, KPMG analysis.

The eight companies accounted for an estimated 84% of motor vehicle insurance payouts in 2023, averaging 11% per firm with a range of 4% to 20%. It should be noted that these figures may not reflect firms market share of premiums. The difference in the share of the market in terms of claim payouts, means that any successful cyber attack affecting larger firms could result in substantially larger consumer impacts than if a smaller firm was affected. Due to the large variation in payout share impacts are presented as a range, from 4% to 20%.

Applying the share of payouts per firm to the £11.5 billion 2024 motor vehicle insurance payout figure results in the following estimated payout per provider:

- Low: £0.5 billion per year for a firm accounting for 4% of payouts.
- High: £2.3 billion per year for a firm accounting for 20% payouts.
- Average: £1.3 billion per year for a firm account for 11% of payouts.

Payments during the period impacted by cyber attacks

The duration of the cyber attack is a key variable in estimating the extent of the impacts on consumers.

As mentioned in the literature review (see section 2.3.1), a high profile ransomware attack on a large US health insurance provider, Change Healthcare, was associated with a system outage of over one month and some providers were still short of expected revenue three months later.[145,146] However, due to the large size of the attack, and complexities of the health insurance sector, such impacts are unlikely to be typical of a cyber attack in the insurance sector more broadly or on motor insurance providers specifically. Therefore, data from the Cyber Security Breaches Survey (CSBS) [147] was used to estimate the typical time until resolution for a ransomware attack. While the data used is not specific to the insurance sector, it was considered to be more representative of the duration of a

[145] On February 21st 2024 Change healthcare discovered a ransomware breach and went offline to mitigate damage and some small providers were still short expected Medicare revenue for the period at the end of June. Source: Fliegelman and Stemp (2024) The Cyberattack on Change Healthcare: Lessons For Financial Stability. Office of Financial Resilience - Brief Series

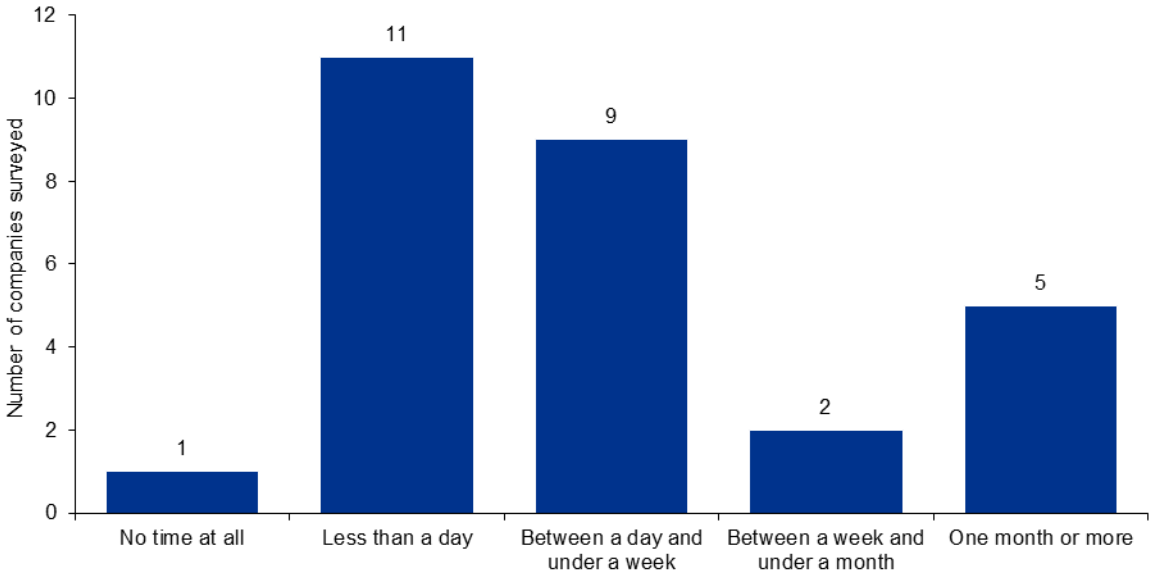
[146] 'March 27, 2024, 5 a.m. cst. Medical claims are flowing through Change Healthcare's network.' - UnitedHealth Group, Information on the Change Healthcare Cyber Response

[147] Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport (2024) Cyber Security Breaches Survey - GOV.UK

typical cyber attack affecting motor vehicle providers than the duration of the Change Healthcare cyber attack.

The CSBS is an annual survey of UK businesses, collecting data on how UK businesses and charities approach, respond to, and experience cyber security issues. Due to the relatively low frequency of ransomware attacks (as a percentage of sampled firms) data from 2019 to 2024 was used to estimate the typical duration. In order to capture a relevant sample, survey results were filtered to only include private sector firms (excluding education) with a headcount of at least 250. The resulting sample of firms reporting time until restoration following a ransomware attack was 28.

Figure 10: Time until restoration following a ransomware attack, CSBS 2019-2024



Source: CSBS, 2019-2024

Taking the midpoint number of weekdays for each of the time categories,[148] the average duration until restoration was 11 days.

The value of the delayed payments for the 11 day period is calculated by dividing the annual payouts per insurance firm by 365 (to estimate a daily value) and then multiplying by 11 (to scale up to the 11 days of disruption). The resulting range of values of the payments that are delayed are:

- Low: £14m for a firm accounting for 4% of payouts
- High: £71m for a firm accounting for 20% of payouts
- Average: £39m for a firm accounting for 11% of payouts

Opportunity cost of payment delays

To estimate the opportunity cost of not having the payment earlier, a daily interest rate is applied to the value of delayed payments associated with a cyber attack. As payments are paid in nominal terms, with no inflation adjustment made for payment delays, nominal interest rates are used.

Due to differences in the financial circumstances of customers affected, results are presented across the full range of interest rates. If an individual was required to finance in the interim (for example to

[148] No time at all – 0 days, less than a day – 0.5 days, between a day and a week – 4 days, between a week and a month – 18.5 days, One month or more – 45 days (one month 30 days and two months 60 days – capped at two months to avoid extreme values dominating the subsequent estimated average duration).

pay for a courtesy, repairs, or to purchase a replacement vehicle) ability to self-finance may lead to different costs of the delay:

- Individuals who can self-finance through cash savings or deposits may face a relatively low cost due to foregone interest on instant cash deposits.
- Individuals with assets and a good credit record may be able to access secured loans at a rate of interest lower than those on credit cards or overdrafts.
- Some individuals may need to resort to higher interest rate options such as credit cards or overdrafts.

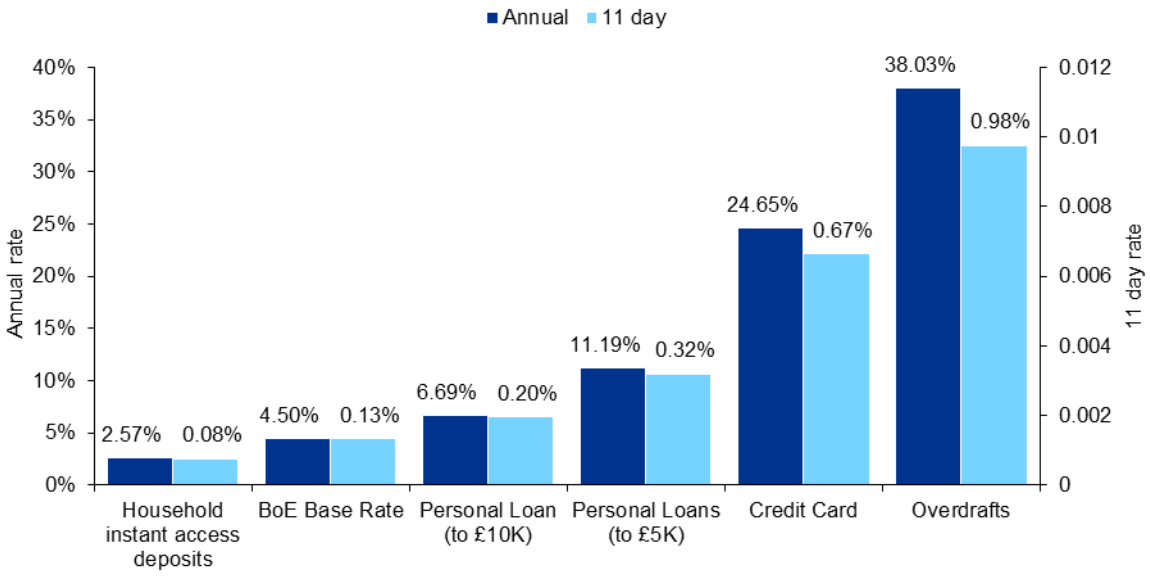
The 11 day interest rate was calculated as follows:

$$1 + r_{11} = (1 + r_{annual})^{11/365} \quad \text{where } r = \text{interest rate}$$

The above formula calculated the effective 11-day interest rate given an annual interest rate and assuming that interest is compounded daily. This is the foregone interest for the 11 day period of payment processing delay due to the cyber attack.

Consistent with the estimate for payments during the impacted period, the 11 day duration was used to estimate the interest associated with the delay period. A range of annual and 11 day interest rates are presented in Figure 11.

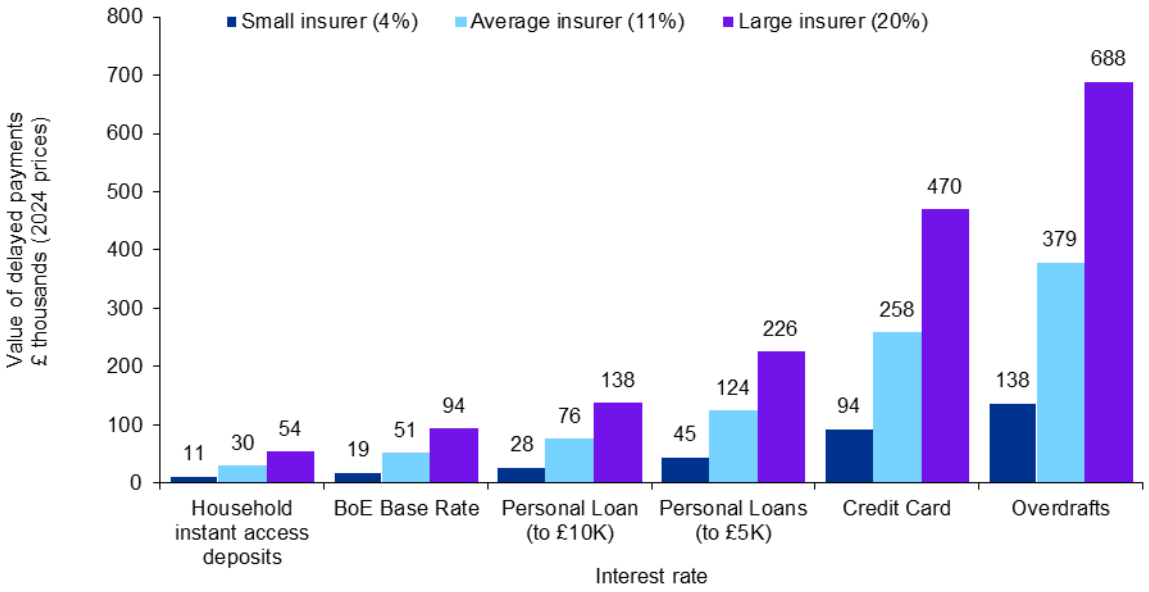
Figure 11: Annual and 11 day interest rates, February 2025



Source: BoE base rate as set on the 6th February 2025 Monetary Policy Committee Bank Rate publication, Other rates were sourced from the 28th February 2025 data in B0E (2025) Quoted Rates.

The 11 day interest rates shown in Figure 11 are applied to the insurance payouts for the relevant period (low £14m, high £71m, average £39m), with the resulting values ranging from £11,000 per cyber attack (for a small insurance firm and the lowest rate of interest) to £688,000 per cyber attack (for a large insurance firm and the highest rate of interest). These results are shown in Figure 12.

Figure 12: Consumer value of 11 day delay in motor vehicle insurance claim payments, by interest rate and insurer size: Small insurer (4% payment share), Average insurer (11%), and Large insurer (20%)



Source: BoE data, KPMG analysis

Estimated frequency of cyber attacks and associated impacts

The frequency of successful ransomware attacks affecting motor vehicle insurance providers was estimated using data from the CSBS (for details of the analysis, see annual impacts in section 4.2.1.1 Online banking). The rate was estimated at **2.45% per company per year**, or approximately one in forty companies. Applying this rate to the relevant set of companies for motor vehicle insurance provision equates to an expected 0.20 cyber attacks per year across the eight major providers, or one successful cyber attack every five years (see Figure 9). The estimated consumer impact and frequency are shown in Table 18.

Table 18: Estimated consumer impact of a cyber attack resulting in disruption to a motor vehicle insurance provider and estimated frequency of relevant cyber attacks

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Years per incident (approx.)
	Low	High		
Motor Vehicle Insurance	£0.011m	£0.688m	0.20 per year	Once every five years

Note: Where the estimated annual frequency of cyber attacks is not a whole number, DSIT requested that the annual consumer impact was not monetised.

Limitations of the approach to the valuation of consumer impacts from cyber attacks on motor vehicle insurance sector

The following limitations of the methodology used to value the impact on consumers from cyber attacks on motor vehicle insurance should be noted:

- **The interest rate:** The potential impact on consumers varies depending on the appropriate interest rate to use. As explained above, individuals who can self-finance any costs incurred during the period payments are impacted, may face lower costs, compared to individuals who have to use high interest rate options.
- **Non-monetised impacts:** As set out in the impact map in section 3.3.1, other consumer impacts associated with a cyber attack affecting motor vehicle insurance providers, include a lack of access to a courtesy car and the associated stress, anxiety and frustration associated with delayed payments and the disruption caused by the cyber attack more broadly. However,

these impacts are not quantified due to a lack of robust data and evidence on which to base any modelling. In line with Government Better Regulation guidance, the impacts associated with penalties incurred from potentially being caught driving without insurance are not included in the analysis.[149]

4.2.2 Health care

Introduction to the valuation of consumer impacts from cyber attacks on GP practices and major hospitals

The potential impacts on the users of health care from a successful cyber attack on either major hospitals or GP practices are set out in section 3.3.2. In this section the methodology used to monetise the impacts identified is detailed, and the quantified impacts are presented.

The detailed methodology for quantifying the following impacts is each described in the sections below:

- The health impact on patients of disrupted appointments and procedures at hospitals and GP surgeries; and
- The impact on consumers of longer wait times at A&E departments.

It should be noted that the impacts quantified are for consumers who do not switch hospitals or seek alternatives to GP health care, either because they are unable to or choose not to (see limitations of the approach for further details about consumers who switch). As set out in the health care impact map (see section 3.3.2), the consumer impacts for patients who do not switch include the health impacts of cancelled and delayed GP and hospital appointments and the time cost of longer wait times at A&E. These are the specific areas of focus for the quantification of consumer impacts as these can be robustly quantified.

The health impacts are measured in QALYs (Quality Adjusted Life Years), which is a commonly used measure to assess health impacts of policy interventions, as it captures both the level of health and longevity of life. The value of time, which captures the opportunity cost of waiting for consumers, i.e. the value of the next best alternative use of consumers' time, is used to measure the time cost of longer A&E wait times. This is a commonly used approach to assessing the impact of transport policy interventions, and the same methodology is applied here to quantify the time cost of additional A&E waiting time.

The detailed methodology for quantifying the following impacts is each described in detail below:

- The health impact on patients of disrupted appointments and procedures at hospitals and GP surgeries; and
- The impact on consumers of longer wait times at A&E departments.

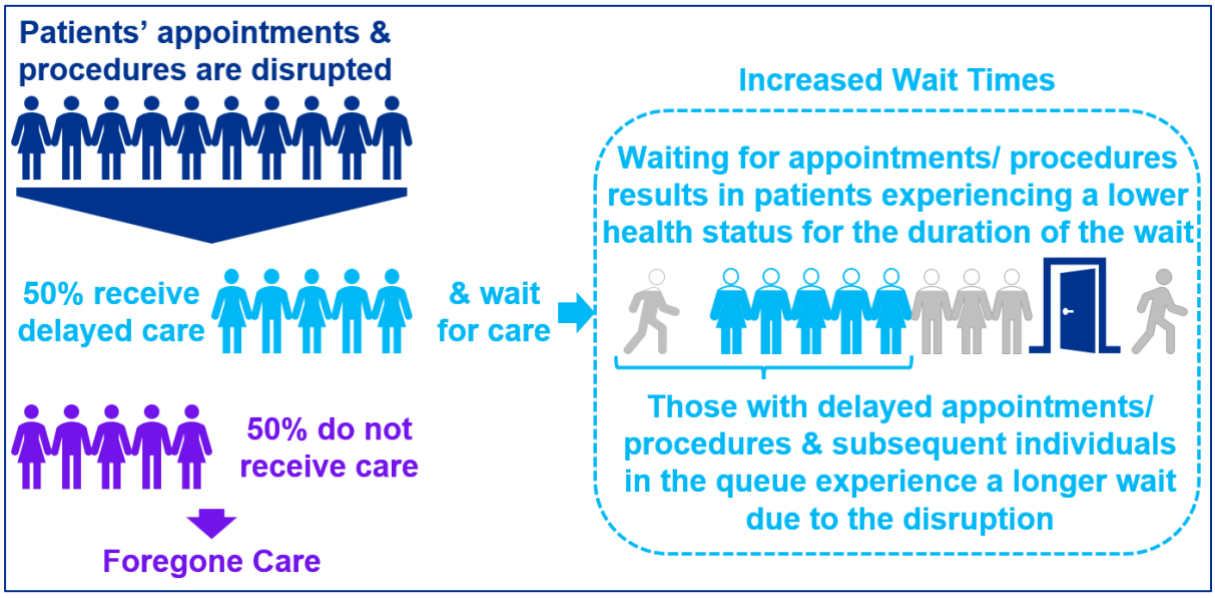
Methodology for the valuation of the health impact on patients of disrupted appointments and procedures at hospitals and GP surgeries

The methodology used to estimate the QALY impact on patients of cancelled appointments and procedures at hospitals and GP surgeries is based on a methodology used to estimate the impact of cancelled care as a result of the Covid-19 pandemic.[150] This methodology was provided by the Department of Health and Social Care (DHSC), and an earlier version of this methodology is included in a 2020 paper co-authored by several government departments.[151] An overview of this methodology is presented in Figure 13. The limitations associated with the methodology should be noted when

[149] Better regulation framework guidance 2023
[150] Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity. Shared by DHSC via email.
[151] Methodology applied for category C: 'Health impacts from changes to health and social care made in order to respond to COVID-19' in Department of Health and Social Care, Office for National Statistics, Government Actuary's Department and Home Office (2020) Direct and Indirect Impacts of COVID-19 on Excess Deaths and Morbidity: November 2020 Update.

considering the findings (see limitations below), resulting in a high level of uncertainty around the estimated impacts.

Figure 13: Patient health impacts of disrupted health care



Source: Adapted from the methodology in Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity.

The health impacts of disrupted health care are estimated using the following steps:

- Of the appointments and procedures impacted by a successful cyber attack, it is assumed that 50% of patients do not receive care at any point (i.e. they drop out of the system for the disrupted appointment/ procedure). The remaining 50% of patients receive care at a later date (the bounce back assumption explained below).[152]
- **For the 50% of patients who do not receive care** the health impact is estimated by converting the financial cost to the NHS of the care they no longer receive, to a QALY amount. This is done by dividing the typical financial cost to the NHS of the foregone hospital and GP care by the estimated marginal NHS cost of a QALY[153] (central estimate £15,000[154]).
- **The 50% of patients who receive delayed care** increases NHS waiting times across all patients. For patients experiencing a delay to elective care, this results in negative health impacts due to the longer time patients are at the lower pre-treatment health state (as their health state increases after treatment). The time spent by patients at the pre-treatment health state is converted into a QALY impact using the approach detailed further below. For patients experiencing a delay to non-elective care and GP appointments there is assumed to be no change in health status pre and post treatment, and hence no health impact from delayed care for these patients.[155] The cumulative additional amount of time waited by patients on the

[152] This assumption is sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity. This in turn is based on the NHS delivery plan for tackling the COVID-19 backlog of elective care.
[153] This is the amount of additional NHS spend to provide an additional QALY.
[154] This value is sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity. This in turn is based on research undertaken by the University of York into the estimation of the National Institute for Health and Care Excellence (NICE) cost-effectiveness threshold.
[155] This assumption is sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity. This in turn is based on research undertaken by the University of York, Accounting for the quality of NHS output (2018) and research into the health effects of people required to wait for admission to receive elective surgery to a New Zealand regional hospital from 1999.

NHS waiting list is estimated over time using a straight line 10% reduction in the waiting list per year, with the waiting list reducing to zero after 10 years.[156]

The resulting QALY impacts are subsequently monetised using the £70,000 (2020/21 prices) monetary value of a QALY from the HM Treasury Green Book.[157]

Number of disrupted appointments and procedures:

The number of disrupted appointments and procedures depends on a number of factors including the size of the hospital that is affected by a cyber attack, the duration of a cyber attack and the timing of attack (i.e. the time of year and day of week).

As there is a need to estimate a quantified figure for the consumer impact for this analysis, the number of disrupted appointments due a cyber attack in a major hospital was estimated using data on the impact of the Synnovis cyber attack on planned care and outpatient appointments at Guy's and St Thomas' NHS Foundation Trust and King's College Hospital NHS Foundation Trust.[158] This has been used given the availability of data for this cyber attack.

These figures were then scaled based on the median number of appointments across NHS hospitals in the year to March 2024.[159] This resulted in an estimated:

- 438 disrupted elective appointments and procedures per cyber attack (0.77% of annual total elective appointments and procedures); and
- 4,705 disrupted non-elective appointments and procedures per cyber attack (7.4% of annual total non-elective appointments and procedures).

To estimate the reduction in GP appointments, data from NHS England on the number of attended appointments on Friday July 19th 2024 (during the CrowdStrike cyber incident) was compared against that during other Fridays in July 2024, as a proxy for the percent reduction that may be expected during a successful cyber attack.[160] Although the 2024 CrowdStrike incident was not a cyber attack it was identified as a relevant proxy for the following reasons:

- It captures the impacts of GPs losing access to digital systems; and
- Due to its widespread nature, the resulting impact on GP service provision can be detected through readily available nationally aggregated statistics.

This was then applied to the average number of appointments per practice per working weekday over the 12 month period ending November 2024. This resulted in an estimated reduction of 79 appointments (38%) per day per cyber attack on a GP practice. With an assumed three day duration. The duration is informed by the chronology of the 2017 WannaCry ransomware cyber attack on the NHS. The alert was raised on Friday the 12th May, with the securing of the emergency care pathway completing on the Sunday 14th May and primary care assured to be operationally stable by the morning of Monday 15th May.[161]

The bounce back assumption:

[156] This assumption is sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity. This in turn is based on The NHS Plan (2000) and The NHS Improvement Plan (2004) which aimed to reduce waiting times.
[157] Section 9.3 Life and health in HMT (2022) The Green Book.
[158] NHS England (2024) Synnovis Ransomware Cyber-Attack: Weekly Data. Note: the weekly data spans the time-period 3rd June to 22nd September 2024 (inclusive).
[159] Median NHS hospital with over 10,000 non-elective and elective recorded episodes respectively, compared against the combined total for Guy's and St Thomas' NHS Foundation Trust and King's College Hospital NHS Foundation Trust. Source: NHS Digital (2024) Hospital Episode Statistics Monthly Activity Report, October 2024: Open Data. Available at: Provisional Monthly Hospital Episode Statistics for Admitted Patient Care, Outpatient and Accident and Emergency data, April 2024 - October 2024 - NHS England Digital
[160] NHS Digital (2024) Appointments in General Practice – July 2024 Summary.
[161] William Smart - Chief Information Officer for Health and Social Care (2018) Lessons learned review of the WannaCry Ransomware Cyber Attack.

Of the disrupted appointments and procedures (categorised into elective and other) as a result of a cyber attack, a 'bounce back' assumption of 50%[162] is used. It is assumed that 50% of the disrupted appointments and procedures are **delayed** and the remaining 50% result in **foregone care** (with the patient never receiving the disrupted care).

Foregone care: Health impacts for patients who do not receive disrupted health care (appointments and procedures)

The impact of disrupted care for those patients who do not go onto receive this care at a later date is estimated by converting the cost of the disrupted appointment/ procedure[163] into a QALY figure per appointment/ procedure. This conversion is done using an estimate of the marginal cost of a QALY to the NHS (i.e. the amount of additional NHS spend required to provide an additional QALY). The resulting QALY per appointment/ procedure is shown in Table 19 alongside the associated monetised patient value based on the Green Book value of a QALY.

Table 19: Patient loss per forgone appointment/ procedure

	QALYs	Patient Value (£ 2020/21 prices)
Elective hospital	0.120	8,432
Non-elective hospital	0.0118	826
GP appointment	0.00245	171

Note: QALY values have been presented to 3 significant figures, while consumer values are rounded to the nearest whole £.

As shown in Table 20, applying the patient QALY loss per forgone appointment/ procedure to 50% of the estimated number of disrupted appointments and procedures results in the following consumer impacts for the forgone care group, i.e. the patients who never receive the disrupted health care:

- £3.8m (2020/21 prices)[164] (54 QALYs) of lost patient value per successful cyber attack on a hospital (which results in delays or cancellations); and
- £20,309 (2020/21 prices) (0.3 QALYs) of lost patient value per successful cyber attack on a single (average) GP practice (which results in delays or cancellations).

Table 20: Monetised value of the health impacts for foregone health care per cyber attack

	Appointments	QALYs	Patient Value (£ 2020/21 prices)
Cyber attack on major **hospital**			
Elective hospital	219	26	1,846,525
Non-elective hospital	2,352.5	28	1,943,780
Total	2,572.5	54	3,790,305
Cyber attack **on GP practice**			
GP appointments	118.5	0.3	20,309

Note: Totals may not sum due to rounding.

Delayed care: Health impacts for patients who experience delayed health care (appointments and procedures)

For the patients whose appointments and procedures are delayed (i.e. the delayed care patient group), the knock-on impacts of cancellations are converted to an increase in wait times across all patients on the waiting list (and those who subsequently join). It is assumed that the waiting list

[162] 50% bounce back assumption is sourced from Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity.
[163] As sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity
[164] On DHSC advice, this figure was not uplifted to reflect any increase in value since 2020/21.

reduces by 10% per year such that the increase in the waiting list length is cleared after 10 years.[165] This is used to estimate the multi-year impact of increased wait times.

The additional time waited until treatment is converted to QALY impacts for patients using the difference between the patient's health state before treatment and after treatment[166] (see Table 21). To estimate the QALY impact, the percentage point change in health status is multiplied by the duration of the delay for health care (in years) and the number of patients affected.

For example, being at a health status that is 10 percentage points lower while awaiting healthcare for one patient over half a year is the equivalent of -0.05 QALYs ($-0.10 \times 1 \times \frac{1}{2} = -0.05$ QALYs), while 12 patients for a period of 1 month at the same lower health status is the equivalent of 0.1 QALYS ($-0.10 \times 12 \times \frac{1}{12} = -0.1$ QALYs). The resulting QALY impacts are monetised using the Green Book WTP value of £70,000 per QALY (2020/21 prices).

Table 21: Patient health status before and after treatment

	Elective Care	Non-Elective Care and GP Appointments
Pre-treatment health status	50%	75%
Post-treatment health status	60%	75%
Change in health status	10 percentage points (20%)	null

Note: Health status is measured on a percent scale with 100% representing perfect health.
Source: Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity.

It is assumed that there is no health impact from delayed non-elective hospital care and from GP care, therefore the estimation of the health impact of delayed care is only undertaken for elective hospital care. The yearly progression of this delay and associated patient impacts are shown in Table 22.

Table 22: Additional individuals on waitlist and associated health impacts (QALY and monetised) due to delayed elective hospital care per cyber attack

Year	Estimated Additional Individuals on Waitlist			Value of Lower QoL* During Wait		
	Start of year	End of year	Average	QALYs	£	£ **NPV**
0	219	197	208	21	1,456,350	1,456,350
1	197	175	186	19	1,303,050	1,283,793
2	175	153	164	16	1,149,750	1,116,018
3	153	131	142	14	996,450	952,922
4	131	101	120	12	843,150	794,403
5	110	88	99	10	689,850	640,360
6	88	66	77	8	536,550	490,698
7	66	44	55	5	383,250	345,319
8	44	22	33	3	229,950	204,129
9	22	null	11	1	76,650	67,037
10	null	null	null	null	null	null
Total:				110	7,665,000	7,351,029

*Quality of life
Notes: Calculations and averages may not sum due to rounding.

[165] This assumption is sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity. This in turn is based on The NHS Plan (2000) and The NHS Improvement Plan (2004) which aimed to reduce waiting times.
[166] The health status before and after treatment is sourced from the Department of Health and Social Care (2022) Indirect effects of COVID-19 on health – estimating the health impacts of the backlogs created by lost activity. This in turn is based on research undertaken by the University of York, Accounting for the quality of NHS output (2018) and research into the health effects of people required to wait for admission to receive elective surgery to a New Zealand regional hospital from 1999.

In line with HMT Green Book guidance for health impacts, net present values (NPV) are calculated with a 1.5% annual discount rate.
£ figures are presented in 2020/21 prices.

Combining the impacts for patients associated with foregone care and delayed care provides an estimate of the total consumer (patient) impact of a cyber attack on a major hospital or GP practice. The results are shown in Table 23 below:

Table 23: Consumer value of disrupted health care per cyber attack

	Appointments	QALYs	Patient Value (£ 2020/21 prices)	Patient Value NPV (£ 2020/21 prices)
Cyber attack on major hospital				
Elective hospital	438	136	9,511,525	9,197,554
Non-elective hospital	4,705	28	1,943,780	1,943,780
Total	**5,143**	**164**	**11,455,305**	**11,141,334**
Cyber attack on GP practice				
GP appointments	**237**	**0.3**	**20,309**	**20,309**

Note: Totals may not sum due to rounding.

Methodology for the valuation of the impact on consumers of longer wait times at A&E departments

The consumer impact of additional wait time in A&E is estimated and monetised using three key inputs:

- Additional wait time per patient: An estimated average 19 minute additional wait time per patient, sourced from Wretborn et al. (2019).[167]
- A&E patients per day: The number of patients per day is taken from hospital A&E activity data for the year 2023-24.[168] The median number of A&E patients across 183 hospitals was 125,960 per year, equating to an average of 344.15 patients per day.
- Duration of disruption: The cyber attack is assumed to lead to increased delays at A&E over a two day period. While this duration would be dependent on the type of cyber attack and its severity, for the purposes of the analysis two days is assumed based on evidence from Wretborn et al. (2019).
- Value of time: The value of time is assumed to be £7.20 per hour (2024 prices) based on the value in the DfT Tag Data Book.[169]

Taking the above assumptions, it is estimated that patients in A&E would experience a total of 218 hours of wait time, with a monetised impact for patients of £1,569 (2024 prices), per cyber attack on a major hospital.

In the literature, it is seen that while there is a decrease in the number of patients attending an A&E department impacted by a cyber attack, there is no overall decrease in the number of A&E attendances due to the displacement of A&E attendees to other hospitals.[170] As such, it could be assumed that the marginal A&E attendee choosing between an affected A&E department and

[167] Jens Wretborn, Ulf Ekelund, and Daniel B Wilhelms (2019) Emergency Department Workload and Crowding During a Major Electronic Health Record Breakdown. Front. Public Health.
[168] NHS Digital (2024) Hospital Accident and Emergency Activity, 2023-24.
[169] DFT (2024) Tag Data Book, November 2024, Table A1.3.2
[170] During the 2017 WannaCry attack on the National Health Service it was found that while the 1% reduction in emergency attendances and A&E attendances at impacted trusts (relative to the previous week) 'was not clinically significant' and 'unlikely to be related with the WannaCry attack', the hospitals within those trusts that had been directly impacted by ransomware had 'significantly fewer emergency and elective admissions' demonstrating displacement and diversion of emergency provision to other hospitals. Source Ghafur et al (2019) A retrospective impact analysis of the WannaCry cyberattack on the NHS.

diversion to an alternative A&E department would face switching costs equal to the additional wait time.

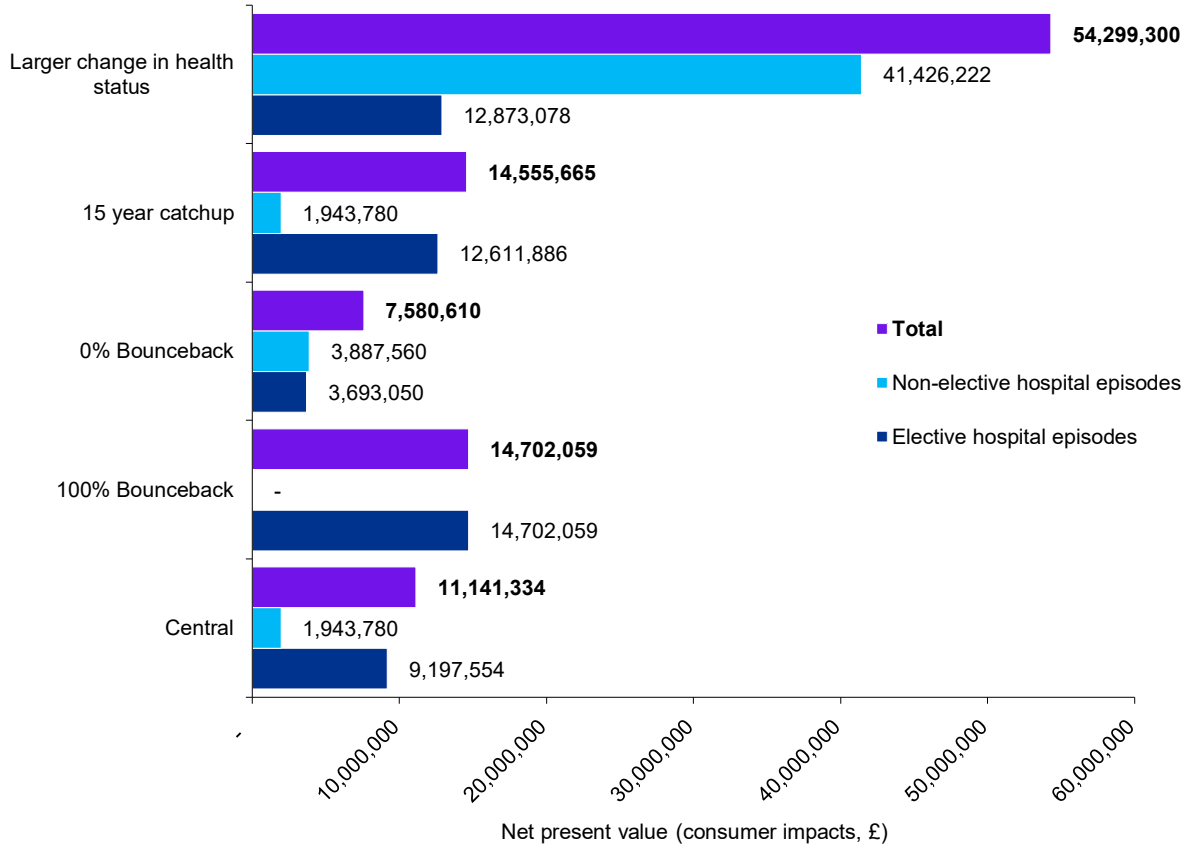
Sensitivity analysis

The analysis of the health care sector involves several key assumptions within the model that are important in driving the results. To understand the robustness of the findings with regards to changes in the assumptions the following sensitivity analysis analyses how the assumptions impact the results.

The results are shown across the following assumption variations:

- **Central**: these are the results shown in the main analysis and are shown here for comparison.
- **100% bounceback**: the bounceback assumption is increased from 50% (central assumption) to 100%, such that all patients are assumed to join the waitlist and receive delayed care.
- **0% bounceback**: the bounceback assumption is decreased from 50% (central assumption) to 0%, such that all patients are assumed to forgo care and therefore none join the waitlist.
- **15 year catchup**: the waitlist clears after 15 years rather than the 10 years (central assumption).
- **Larger change in health status**: the health status reduction during wait is assumed to be 15pp (percentage points) for elective patients and 5pp for non-elective patients (as opposed to 10pp and 0pp in the central assumptions).

Figure 14: Hospital elective and non-elective sensitivities: consumer impacts, net present values per cyber attack



As can be seen in Figure 14, the results are most sensitive to changes in assumptions around the change in health status, with the total hospital elective and non-elective impacts being approximately 400% larger under this variation than in the main analysis. Notably the non-elective consumer impacts are larger than the elective consumer impacts (a reversal of the main analysis), highlighting the potential for the large number of non-elective patients impacted to experience substantial impacts if delays for this patient group cause worse health outcomes.

Estimated frequency of cyber attacks and associated impacts

The annual impact is estimated by applying the frequency of successful cyber attacks causing impacts on consumers to the estimate of impacts per incident. The rate of relevant cyber attacks for major hospitals is estimated using the observed frequency over the 2024 calendar year. Due to the high-profile nature of these attacks on hospitals it has been possible to identify individual attacks as reported in the media. Three relevant cyber attacks were identified:[171]

- King's College Hospital NHS Foundation and Guy's and St Thomas' NHS Foundation Trust[172]
- Wirral University Teaching Hospital[173]
- Adler Hey Children's NHS Foundation Trust, Liverpool Heart and Chest Hospital and Royal Liverpool University Hospital[174]

[171] These were identified though a web search of the BBC website using the keywords 'cyber', 'incident', 'hospital' and 'NHS'. Search results were limited by date range from 1st January to the 31st December 2024.
[172] BBC News (2024) Cyber attack on hospitals impacts 1,130 operations in London - BBC News
[173] BBC News (2024) Major incident declared at Arrowe Park Hospital over cyber issue - BBC News
[174] BBC News (2024) Merseyside: Three more hospitals hit by cyber attack - BBC News

In addition to the three listed above, there was a cyber attack on NHS Dumfries & Galloway in March 2024,[175] although the health board indicated that there was no impact of the attack on hospital services.[176]

Due to the relatively low number of high-profile cyber attacks on GP surgeries and their smaller size and non-standard business nature, data from the charities and education section of the CSBS sample was gathered. The targeting rate was 2.5% (6,217 surveyed, 158 targeted with ransomware) and the conversion rate (percent of targeted companies that went on to also experience ransomware associated disruption) was 19.0% (158 targeted, 30 experiencing disruption). The resulting successful attack per GP practice per year is therefore estimated at 0.475%. Applying the 0.475% rate per year to the 7,791 general practices in the UK[177] results in an estimated 37.0 cyber attacks impacting patients at GP practices per year.

The estimated consumer impact of a cyber attack on major hospitals and GP practices, and the estimated frequency of attacks, are presented in Table 24.

Table 24: Estimated consumer impact of a cyber attack affecting major hospitals and GP Practices and estimated frequency of relevant cyber attacks

Service	Consumer impact per successful cyber attack (2024 prices)	Estimated frequency (approx.)	Annual consumer impact
Major Hospitals	£11.141m	3 per year	£33.424m
GP Practices	£0.020m	37 per year	£0.740m

Limitations of the approach

The following limitations of the methodology used to value the impact on consumers (patients) from cyber attacks on major hospitals and GP practices should be noted:

- **Scope of the analysis:** The analysis quantifies the impact on consumers who do not switch in the event of a cyber attack on a major hospital or GP practice. However, as set out in the impact map (see section 3.3.2) patients may go to another hospital to avoid longer A&E wait times, patients may be diverted to other hospitals for appointments/ procedures, and patients may seek alternative sources of health care if they are unable to access GP appointments. If patients were to do this, they would face the associated switching costs. This may include time costs, travel costs, familiarisation costs, and health costs if there were differences in health care received. Due to a lack of available data and evidence these switching costs for such patients are not estimated.
- **Assumptions:** The quantified impacts are highly dependent on the assumptions used in the analysis, and are based on limited evidence. As demonstrated in the sensitivity analysis, the estimated impacts vary with changes to individual assumptions, notably the assumed change in hand also depend on the combination of assumptions used. While the assumptions used in the analysis have been sourced primarily from the methodology used by DHSC to estimate the impact of cancelled care as a result of the Covid-19 pandemic, and are based on the best available evidence, future analysis should consider if these assumptions remain appropriate.

[175] BBC News (2024) NHS Dumfries and Galloway fears hackers have stolen patient data - BBC News
[176] 'No data on our systems was deleted or altered as a result of the cyber attack, and services have continued to run as normal. No patient appointments or operations have had to be cancelled or rescheduled.' NHS Dumfries & Galloway Health Board (2024) Update: 21.05.24 Cyber Attack – NHS Dumfries & Galloway
[177] 6,221 General Practices in England in February 2025 – NHS England (2025) General Practice Workforce, 28 February 2025 - NHS England Digital.
371 General Practices in Wales in September 2024 – Stats Wales (2025) Number of active general practices by practice size and local health board.
887 General Practices in Scotland in January 2025 – Public Health Scotland (2025) General practice list size and demographics information - Publications - Public Health Scotland.
312 General Practices in Northern Ireland on the 31st March 2024 – NISRA and HSC Business Services Organisation (2024) General Medical Services Statistics - Business Services Organisation (BSO) Website

- **Potential for underestimated impacts:** The quantified impacts on consumers may be underestimated for a number of reasons including:
  - There are other costs that consumers who experience delayed health care may face that are not included in the quantified analysis. For example, as set out in the impact map (see section 3.3.2) patients may face personal costs from having appointments rescheduled, such as rearranging transport/ leave from work.
  - If a patient is in pain or discomfort while having to wait longer at A&E to be seen, a higher value of time may be appropriate than the standard value of time used in this analysis given the negative impacts on health and wellbeing. As such, the impacts on consumers of longer wait times at A&E may be underestimated.
  - If a patient attends A&E with another individual (such as a family member) there would also be a time cost to that individual associated with having to wait longer. This cost has not been included in this analysis due to the focus on direct consumer impacts.
  - There may be further time costs, such as those experienced by patients at nearby A&E departments, who experience longer waits due to the knock-on effects of displaced A&E patients who would otherwise have attended the A&E department affected by the cyber attack.
- **Evidence on the frequency of successful cyber attacks at GP practices:** This frequency is estimated based on the charities and education portion of the CSBS survey and may not accurately reflect the actual frequency of such incidents at GP practices. Due to the limited availability of data specific to GP practices, data from the charities and education sector was used. As such there is increased uncertainty on the estimated frequency of such incidents and the resulting annual impacts (as shown in Table 24).
- **Evidence on the frequency of successful cyber attacks on major hospitals:** The frequency estimated is based on the observed frequency during the calendar year 2024. This may not be representative of a typical year, and caution should be used when interpreting the frequency and associated annual consumer impacts.

4.2.3 Creative industries and arts

Introduction to the valuation of consumer impacts from cyber attacks resulting in the loss of access to online ticketing, streaming services and cultural institutions

The potential impacts on consumers from a successful cyber attack on online ticketing, streaming services and cultural institutions are set out in section 3.3.3. In this section, the methodology used to monetise the impacts identified is set out, and the quantified impacts are presented.

As set out in the creative industries and arts impact map, consumers may respond in a variety of ways to not being able to access online ticketing, streaming services and cultural institutions services as a result of a cyber attack, with the associated consumer impacts also varying depending on the action taken.

The quantification of the impact on consumers from being unable to access these services as a result of a cyber attack uses stated preference techniques in line with HMT Green Book guidance on the valuation of costs and benefits where there is no market price. For online ticketing and streaming services, the consumer survey conducted as part of this study is used to elicit consumer WTP to avoid a loss of access to these services and consumer WTA compensation for a loss of access to these services. For cultural institution existing WTP and WTA studies are used. For the purpose of this analysis, when modelling the impact on consumers of cyber attacks on cultural institutions the focus is on museums and libraries.

WTP and WTA are methods used to estimate how much consumers value a good or service. WTP reflects the maximum amount a consumer will pay for something, and WTA reflects the minimum amount a consumer will accept in compensation for a loss. The consumer survey was designed in line with HMT Green Book supplementary guidance on stated preference techniques.[178] The consumer

[178] Economic_valuation_with_stated_preference_techniques.pdf

survey achieved 1,000 completed survey responses and the data was weighted to be representative of the UK population.

In relation to online ticketing and streaming services the consumer survey covered:

- Respondents use of online ticketing and online video streaming services.[179]
- What respondents would do in the event of being unable to access online ticketing services and online video streaming services, and the associated travel, time, familiarisation and wellbeing impacts associated with this.
- What respondents would be WTP to avoid a loss of access to online ticketing and online video streaming services and what they would be WTA in compensation for a loss of access.

Similar to the approach taken to valuing the impact on consumers of a loss of access to online banking services, two approaches to elicit the WTP to avoid a loss of access to online ticketing and online video streaming services, and WTA compensation for a loss of access to these services were used in the consumer survey. First, using a double-bounded dichotomous choice approach where respondents were asked whether or not they would be WTP/ WTA a stated amount, and were then asked to say yes or no to higher/ lower amounts, and second using an open-ended elicitation approach where respondents were asked their WTP/ WTA in an open question.

Under the double-bounded dichotomous choice approach, respondents were asked if they would be WTP or WTA amounts ranging from £1 to £19 for online ticketing services, and amounts ranging from £1 to £9 for online video streaming services in the scenarios of loss of access detailed below. The starting values for online ticketing services were based on the various fees (such as booking, processing and e-ticket fees) associated with using these services.[180] The starting values for online video streaming services were determined based on a review of monthly prices for streaming services.[181]

The scenarios described to respondents were as follows:

- For online ticketing services, the loss of access was expected to last for one day at a time of attempting to purchase tickets for an event.
- For online video streaming services, the loss of access was expected to last for one day, and respondents were asked to consider their average use of the online video streaming service they primarily use.

These scenarios were determined considering the findings in the 2024 Cyber Security Breaches Survey (CSBS) on the duration taken for the restoration of services following ransomware and DoS incidents in the entertainment sector,[182] as well as expert input from academic advisers.

The data from the survey was then used to monetise the impact on consumers from being unable to access online ticketing and online streaming services as a result of a cyber attack, as described below. This involved cleaning the data to remove protest responses,[183] and invalid responses (e.g.

[179] The consumer survey specifically referenced online video streaming services, as it was considered necessary to refer to a specific type of streaming service within the consumer survey as the WTP/ WTA may vary across different streaming services, such as music and video streaming services.
[180] Which? calls for crackdown on sneaky gig ticket fees as new laws set to come into force - Which? Policy and insight
[181] Monthly prices were taken from streaming services own websites. Netflix: £4.99 to £17.99, Disney+: £4.99 to £12.99, Amazon Prime Video: £8.99, Apply TV+: £8.99 and BBC £0. Information correct as at 9th January.
[182] Cyber security breaches survey 2024 - GOV.UK. In response to the survey question that asked about the duration to restoration of ransomware and DOS incidents in the entertainment sector, 2 respondents said 'no time at all', 2 respondents said 'between a day and under a week', and 1 respondent said 'still not back to normal'.
[183] Protest and invalid responses were identified through the application of a set of rules. A response was deemed invalid if the self-reported maximum WTP/ minimum WTA value was inconsistent with the dichotomous choice answered provided. A response was deemed invalid or a protest response if the self-reported minimum WTA was very high (above £50 for ticketing and streaming). A response was deemed invalid where the respondent had answered 'yes, yes' or 'no, no' for the WTP dichotomous choice questions and indicated that one of the reasons for the answer was that they did not believe that the cyber-attack would actually happen. A WTP

where the value of responses was inconsistent between the two approaches used), in order to increase the reliability of the findings. Modelling was then undertaken to derive the WTP/ WTA values (see Appendix 1 for more detail).

Methodology for the valuation of the impact on consumers who are unable to access online ticketing, streaming services, and cultural institutions as a result of cyber attack

In order to estimate the impact on consumers from a cyber attack resulting in the loss of access to online ticketing, streaming services and cultural institutions, the monetised impact per consumer is multiplied by the number of consumers impacted. Each of these components are considered in turn below.

The impact per consumer: online ticketing and streaming services

The table below sets out the estimated value that consumers would be WTP to avoid the loss of access to online ticketing and streaming services, and WTA to be compensated for the loss of access to these services, for both the double-bounded dichotomous choice approach and open-ended elicitation approach used in the consumer survey. This is the WTP/ WTA across all consumers, regardless of how they respond to the loss of access to these services (i.e. whether they would 'do nothing' and wait until the service resumes, as well as those who would 'do something' as an alternative). When answering questions about what respondents are WTP/ WTA they are implicitly considering what they would do in the event of being unable to access these services from the impacted provider.

Table 25: WTP and WTA amounts for loss of access to online ticketing and streaming services

Weighted median values	Online ticketing		Streaming services	
	WTP (£)	WTA (£)	WTP (£)	WTA (£)
Estimate from double-bounded dichotomous choice approach	0.48	5.81	0.59	2.99
Estimate from open-ended elicitation approach	0.00	10.00	0.00	5.00

Source: Consumer survey, 2025. KPMG analysis.

As shown in the table above the estimated WTP and WTA values derived from the survey data, varied from a WTP of £0 to a WTA of £10.00 for online ticketing services, and from a WTP of £0 to a WTA of £5.00 for streaming services. For the purpose of estimating the potential impact on consumers from a cyber attack resulting in the loss of access to these services, the range from a WTP of £0.48 to a WTA of £10.00 is used for online ticketing services, and the range from a WTP of £0.59 to a WTA of £5.00 is used for streaming services. The WTA values under both approaches were higher than the WTP values for both services. As explained in relation to the online banking analysis, this is common with stated preference techniques because:

- consumers tend to value losses more than gains so are willing to pay less than they are willing to accept; and
- WTP is affected by consumers' incomes (i.e. their ability to pay) while there is no constraint on compensation.

The results also show that under the open-ended elicitation approach the median WTP was £0 for both services. This often arises where consumers don't believe they should need to pay for something (see reasons in Table 26 below).

value was deemed a protest response if the respondent answered 'no, no' to the dichotomous choice and indicated that they shouldn't have to pay as a reason whilst not indicating any of the following reasons: that they do not value the service sufficiently, that they could not afford to pay more or that not having access to the service for the duration was not an issue. In addition, where the respondent had provided a free-text 'other' reason, these reasons were manually sorted to identify any protest or invalid responses.

Another noticeable finding is the rounded values resulting from the open-ended elicitation approach. This may occur because:

- respondents are uncertain about their valuation which leads to a tendency to provide an approximate rounded value rather than a precise value; and
- the round number bias which is the tendency for people to prefer round numbers over others because they are easier to understand, process and communicate.

In line with best practice, survey respondents were asked why they would not be willing to pay more than the amount they stated when asked about their WTP to avoid the loss of access to online ticketing and online video streaming services and why they would not be willing to accept less to compensate them for the loss of access than the amount they stated.

As shown in the table below, the most frequently reported reasons for not being willing to pay more than the amount respondents stated for each of these services was because respondents did not think that losing access for one day to these services would be a problem for them (cited by 45% of respondents in relation to online ticketing services and by 57% of respondents in relation to streaming services). Of those who selected 'other', the majority self reported that the maximum they would be willing to pay was zero. Across ticketing and streaming, a large proportion of those selecting the 'other' reason went on to indicate that the reason was because the ticketing provider should not charge a fee –indicating a protest response – and a small number in both cases questioned the validity of the hypothetical and challenged if they could pay to avoid the outage – indicating an invalid response. A small number of individuals also went on to indicate that they would be able to use an alternative (such as live television or an alternative ticketing channel).

Table 26: Reasons for respondents not being willing to pay more to avoid a loss of access to online ticketing and streaming services

Consumer response	Online ticketing percentage	Streaming services percentage
I don't value it sufficiently	32	29
I could not afford it	14	9
I should not have to pay to avoid this	38	45
Losing access to the online ticketing/ video streaming service I primarily use for 1 day would not be a problem for me	45	57
I would be able to use an alternative online ticketing platform	21	N/A
I am already paying for this service through ticket charges/ streaming subscription	28	44
I don't believe this will happen	3	3
I don't feel confident stating a value/ I need more information	13	8
Don't know	4	5
Other	3	1

Note: Total for each service may sum to more than 100% because respondents could select multiple options.
Source: Consumer survey, 2025. KPMG analysis.

As shown in the table below, the most frequently reported reasons for not being willing to accept less in compensation than the amount respondents stated for each of these services was because respondents would not be satisfied by less (cited by 34% of respondents in relation to online ticketing services and by 36% of respondents in relation to streaming services). Of those who selected the 'other' category of reasons, a range of subsequent reasons were provided. In the online video streaming section of the survey, the 'other' reasons provided generally fell into two categories, with some referencing the monthly subscriptions they paid while others emphasised the fact that a one day outage would not be a significant inconvenience to them. In the online ticketing section of the survey, the 'other' reasons were mostly on the theme of not requiring or expecting any kind of compensation for this, with many mentioning that they would be able to access tickets through an alternative provider or channel. A small number of individuals mentioned missing a popular booking, but as the website would be down for all individuals competing to purchase the popular booking these responses were counted as invalid.

Table 27: Reasons for respondents not being willing to accept less in compensation for a loss of access to online ticketing and streaming services

Consumer response	Online ticketing percentage	Streaming services percentage
It wouldn't be a fair amount	24	30
It wouldn't cover the cost of what I would do instead	18	10
I wouldn't be satisfied by less	34	36
Don't know	11	11
Other	14	13

Note: Percentages for each service may not sum to 100% due to rounding.
Source: Consumer survey, 2025. KPMG analysis.

It may be expected that the impact of a cyber attack resulting in the loss of access to online ticketing and streaming services, would vary across consumers depending on their response to this loss of access. The tables below show the results from the consumer survey in terms of what respondents said they would do instead of using online ticketing and online video streaming services.

Table 28: Consumer responses to loss of access to online ticketing services

Consumer response	Percentage
Wait until online ticketing service is available again	32
Use another online ticketing platform	40
Use telephone ticketing services	16
Visit a ticket office	9
Purchase tickets on the door	2
Other	1
Don't know	0

Source: Consumer survey, 2025. KPMG analysis.

The survey results show that in the event of a loss of access to online ticketing services 32% of respondents said they would wait until the online ticketing service is available again, but most respondents said they would use other ticketing services, with 40% of respondents saying they would use another online ticketing platform and a further 16% saying they would use telephone ticketing services.

The consumer survey suggests that the response of consumers varies by key characteristics. In particular:

- Consumers aged 66+ were more likely to say they would use telephone ticketing services (27%) or visit a ticket office (14%).
- Consumers with a household income under £35k and consumers aged 66+ were less likely to say they would use another online ticketing platform (32% and 15% respectively).

Table 29: Consumer responses to loss of access to online video streaming services

Consumer response	Percentage
Wait until online video streaming service is available again	16
Watch TV broadcasts (e.g. BBC)	31
Use another online video streaming service you already subscribe to	28
Undertake an alternative activity (e.g. a hobby)	19
Subscribe to an alternative streaming service you don't currently have	2
Other	2
Don't know	11

Source: Consumer survey, 2025. KPMG analysis.

As shown in the table above, the most frequently reported response to a loss of access to online video streaming services was to watch TV broadcasts (by 31% of respondents), followed by using another online video streaming service they are already subscribed to (by 28% of respondents).[184]

The consumer survey suggests that the response of consumers varies by key characteristics. In particular:

- Consumers with a household income of £100k or more, were more likely to say they would undertake an alternative activity (27%).
- Consumers aged 55 to 64 and 66+ were more likely to say they would watch TV broadcasts (50% of consumers aged 55 to 64 and 53% of consumers aged 66+).

The consumer survey also asked questions to understand the costs associated with how consumers would respond to a loss of access to online ticketing and streaming services, including travel, time, familiarisation and stress/ anxiety impacts. These findings are not used in the modelling to estimate the impact on consumers from cyber attacks, as survey respondents implicitly take these costs into account when providing WTP/ WTA values. However, they provide an indication of the prevalence of these costs. The findings for online ticketing services and online video streaming services are set out below.

Online ticketing

Travel: Consumers who said they would respond to a loss of access to online ticketing services by visiting a ticket office were asked about the associated travel time. The most frequently reported one-way journey time was six to 15 minutes, reported by 26% of respondents, followed by 16 to 30 minutes, reported by 25% of respondents.

Time: In terms of the additional time taken to pursue the alternative action in the event of a loss of access to the online ticketing services they primarily use, the most frequently reported response was not any longer by 21% of respondents, followed by five minutes or less by 18% of respondents.

However, the additional time reported varied depending on the action respondents said they would take:

- Of the respondents who said they would use telephone ticketing services, the most frequently reported response given by 22% of respondents was that it would take 31 to 59 minutes longer than using the online ticketing service they primarily use.
- Of the respondents who said they would visit a ticket office, the most frequently reported response given by 30% of respondents was that it would take 16 to 30 minutes longer than using the online ticketing service they primarily use.

Familiarisation: To understand whether consumers would incur a familiarisation cost in relation to the action they would take as a result of not being able to access online ticketing services, the survey asked whether they had taken this action in the last 12 months. This was asked on the basis that if a consumer had taken this action in the last 12 months then they would be unlikely to incur a familiarisation cost. The survey found that 71% of consumers had not taken this action in the last 12 months, suggesting most consumers would likely incur a familiarisation cost. This was higher among consumers aged 55 to 64 at 84% and those aged 66+ at 80% suggesting they would be more likely to incur a familiarisation cost.

Stress and anxiety: The survey also asked respondents about the extent to which they would feel stressed and anxious about having to pursue an alternative action in the event of not being able to access the online ticketing service they primarily use. 51% of respondents said they would not feel at all or not very stressed or anxious, while 47% of respondents said they would feel slightly (36%) or

[184] According to the consumer survey 63% of respondents had subscriptions to two or more online video streaming services.

very stressed (11%). These results did not show much variation depending on the action respondents said they would take.

Online video streaming services

Time: In terms of the additional time taken to pursue the alternative action instead of using the online video streaming service primarily used, over half (54%) of respondents said it would not take any longer, and a further 12% of respondents said it would take five minutes longer or less. However, for respondents who said they would subscribe to an alternative streaming service they don't currently have, the expected additional time was longer. Of the respondents who said they would do this, 27% said it was one to two hours longer, and a further 13% said 31 to 59 minutes longer than using the online video streaming service primarily used.

Familiarisation: To understand whether consumers would incur a familiarisation cost in relation to the action they would take as a result of not being able to access online video streaming services, the survey asked whether they had taken this action in the last 12 months. The survey found that 67% of consumers had taken this action in the last 12 months, suggesting most consumers would be unlikely to incur a familiarisation cost. This was higher, at 75%, among consumers with a health condition which they consider impacts or limits their daily activities or work.[185]

Stress and anxiety: The survey also asked respondents about the extent to which they would feel stressed and anxious about having to pursue an alternative action in the event of not being able to access the online video streaming service they primarily use. While most respondents (77%) said they would not feel at all or not very stressed/ anxious, 22% of respondents said they would feel slightly (18%) or very stressed or anxious (5%).[186] This was noticeably higher among consumers aged 25 to 34 at 27%.

Respondents who said they would subscribe to an alternative streaming service or wait until the online video streaming service is available again reported to feel more stressed and anxious.

- Of the respondents who said they would subscribe to an alternative streaming service, 47% of respondents said they would feel slightly (40%) or very stressed/ anxious (7%).
- Of the respondents who said they would wait until online video streaming service is available again, 34% of respondents said they would feel slightly (26%) or very stressed/ anxious (8%).

Impact per consumer: cultural institutions - museums and galleries

The impact on consumers from a cyber attack resulting in the loss of access to the services provided by cultural institutions was assessed through the existing literature, taking the values from previous WTP studies on the value of relevant services to visitors.

The DCMS commissioned Culture and Heritage Capital Evidence Bank[187] was searched to identify relevant values for the digital provision of services by museums and galleries. No relevant studies focusing on the digital provision by museums were identified.[188]

The value of museum online offerings was estimated at £3.90 per month (2021/22 prices, £4.47, 2024 prices)[189] per attendee in a 2023 report by Simetrica Jacobs and Creative Industries Policy Evidence Centre for The Department for Culture Media and Sport and Arts Council England.[190] This study

[185] Health conditions related to hearing, eyesight, mobility, dexterity, breathing, mental abilities, speech, social behaviour, mental health and other illnesses/ conditions.
[186] Does not sum due to rounding.
[187] Simetrica-Jacobs (2022) Rapid Evidence Assessment: Culture and Heritage Valuation Studies - GOV.UK
[188] The evidence bank was searched for mentions of the words 'online', 'web' and 'digital.' The results for this search did not identify any relevant studies.
[189] CPIH adjusted
[190] Table 4.22 WTP a monthly household subscription fee for Digital Offer if Covid-19 had not happened Simetrica Jacobs and Creative Industries Policy Evidence Centre (2023) Measuring the economic value of museums and galleries digital offers: an exploratory use of contingent valuation techniques - GOV.UK

surveyed individuals about four different museums across England,[191] asking for their WTP for access to digital content. The pooled average value across the four museums included in the study is £3.90 per month, while the average WTP value across each individual site ranged from £1.70 to £5.20 per month (2021/22 prices).[192]

As the value was based on hypothetical monthly subscription cost, this value is not converted to an annual value in order to reflect the usage of the website during the month that the visit occurs in order to compliment the visitor experience. The £4.47 value (2024 prices) per visitor is therefore applied to the typical number of UK visitors to a museum over the impacted period.

Impact per consumer: libraries

The DCMS commissioned Culture and Heritage Capital Evidence Bank[193] was searched to identify relevant values for library services. The evidence bank was filtered using the following criteria:

- Valuation Method: Stated Preference: Contingent Valuation
- Cultural or Heritage Asset Type: Library
- User groups: Library users
- Country: United Kingdom
- Overall quality rating: Medium or High (scale = Low, Medium, High) as judged in the 2022 Rapid Evidence Assessment.

The resulting three papers and their associated contingent valuations are shown in Table 30.

Table 30: Library user WTP/ WTA studies in the 2022 DCMS commissioned Culture and Heritage Valuation Studies Rapid Evidence Assessment (REA)

Title	REA Quality Rating	Midpoint value (if based on range)	Annual value (2024 prices)
Jura Consultants (2005) Bolton's Museum, Library and Archive Services; An Economic Valuation.	Empirical Design: Medium Method/Dataset: Low Sample Size: Medium Overall: Medium	£3.63 (WTP) £4.83 (WTA) Monthly, 2005 prices See note	£67.49 (WTP) £97.01 (WTA
C Pung, T Elwes, P Marks (2004) Measuring the Economic Impact of the British Library.	Empirical Design: Medium Method/Dataset: Medium Sample Size: Medium Overall: Medium	£116.00 (WTP) £273.00 (WTA) Monthly, 2003 prices	£2,411.95 (WTP) £5,676.41 (WTA)
D Fujiwara, R Lawton, S Mourato (2019) More than a good book: contingent valuation of public library services in England.	Empirical Design: Medium Method/Dataset: High Sample Size: High Overall: High	£19.51 (WTP) Annual, 2014 prices	£26.03 (WTP)

Source: Simetrica-Jacobs (2022) Rapid Evidence Assessment: Culture and Heritage Valuation Studies - GOV.UK
Jura Consultants (2005) Bolton's Museum, Library and Archive Services; An Economic Valuation. Available at: https://webarchive.nationalarchives.gov.uk/ukgwa/20120215214224/http:/research.mla.gov.uk/evidence/documents/bolton_main.pdf
Note: The values from the Jura Consultants paper presented in the table above were sourced directly from the paper.
Monthly values were annualised by multiplying the monthly value by 12. Adjustment to 2024 prices was undertaken using the ONS CPIH price index.

Of the three papers identified, only the £19.51 annual WTP value from D Fujiwara, R Lawton and S Mourato (2019) was considered to be appropriate for application. The Jura Consultants (2005) paper

[191] Derby Museum and Art Gallery, Bristol Museum and Art Gallery, Foundling Museum and Great North Museum.
[192] The survey was run from October 2021 to March 2022.Survey participants were asked questions to determine if their WTP was affected by the COVID-19 pandemic. The results used in this analysis are those that are adjusted for COVID-19.
[193] Simetrica-Jacobs (2022) Rapid Evidence Assessment: Culture and Heritage Valuation Studies - GOV.UK

has a low quality score for method/ dataset as it was an open ended contingent valuation study where respondents were not asked if they found the scenario realistic, and the reported values per user appeared to high. The 2004 study of the British Library was for users of British Library's reading rooms and as such they do not reflect typical library usage. Rather, it may reflect a smaller group of individuals using the facilities of a research library including the use of regular work or study space.

The results of the Fujiwara et al (2019) paper were previously included in a 2015 WTP study commissioned by Arts Council England.[194] The WTP value for those who had used public libraries in the past year was £19.51 per year (2014 price, £26.03 2024 prices)[195] with the survey framing this as a hypothetical increase in annual council tax payments. Due to the council tax payment vehicle, this value is per household, rather than per individual user. Given the digitisation of library inventory management and substantial provision of digital services it was assumed that the full WTP value is 'at-risk' for the period of the cyber attack.

The number of consumers impacted: online ticketing

To estimate the number of consumers potentially affected by a cyber attack resulting in the loss of access to online ticketing services, the percentage of event tickets purchased using Ticketmaster vs. other providers, and the number of tickets sold is used. The CMA found that Ticketmaster's share of the UK market for the primary retailing of live music tickets[196] in 2008 was between 40% and 50%, and no other provider had a market share above 5%.[197] This is supported by more recent data which shows that 60% of event ticket purchasers in the UK use Ticketmaster.[198]

The consumer survey commissioned as part of this study indicates approximately 50% of adults in the UK use online ticketing services.[199] Therefore, it is estimated that the number of UK adults using online ticketing services is approximately 27 million (i.e. 50% of the estimated 54 million people aged over 16 in the UK).[200]

Taking the estimated market share of the largest and smallest online ticketing services providers together with the number of UK adults using online ticketing services, the number of consumers who may be impacted by a cyber attack resulting in the loss of access to online ticketing services is estimated. The number of impacted consumers is therefore estimated to range from 1.3 million[201] (i.e. 5% of 27 million) to 16 million (i.e. 60% of 27 million).

Taking the estimated impact per consumer and the number of customers impacted, the estimated impact on consumers per cyber attack is estimated to range from approximately £0.6m (£0.48*1.3 million) to £161m (£10*16 million) depending on the market share of the online ticketing service affected. The lower bound of this range is calculated based on the smallest number of consumers potentially impacted and the lowest positive WTP value, while the higher bound of this range is calculated based on the largest number of consumers potentially impacts and the highest WTA value.

The number of consumers impacted: streaming services

To estimate the number of consumers potentially impacted by a cyber attack on streaming services, data on the percentage of households with subscriptions to streaming services was used from the

[194] Fujiwara, Lawton and Mourato (2015) The health and wellbeing benefits of public libraries. Report for Arts Council England. The health and wellbeing benefits of public libraries.pdf
[195] CPIH adjusted
[196] The market share of Ticketmaster for the primary retailing of live music tickets is used as a proxy for the event ticket market.
[197] A report on the completed merger between Ticketmaster Entertainment, Inc and Live Nation, Inc
[198] ticketmaster brand profile UK 2022 | Statista
[199] The survey data was weighted to be representative of the UK population.
[200] Population estimates for the UK, England and Wales, Scotland and Northern Ireland - Office for National Statistics
[201] This may be an overestimate given no other provider had more than a 5% market share, and this assumes a 5% market share.

Ofcom Media Nations 2023 report.[202] The table below shows the percentage of households subscribed across major streaming services in the UK. From this, the number of consumers potentially impacted by a cyber attack resulting in the loss of access to streaming services was derived based on the 28.4 million households in the UK, and assuming 2.36 people per household.[203,204]

Figure 15: Estimated number of subscribers by streaming service

Streaming service	Percentage of households subscribed (m)	Estimated number of households subscribed (m)	Estimated number of consumers subscribed (m)
Netflix	59	16.8	39.5
Amazon Prime	45	12.8	30.2
Disney+	25	7.1	16.8
Apple TV+	7	2.0	4.7
NOW	7	2.0	4.7
Others	9	2.6	6.0

Source: Media Nations: UK 2023, Ofcom. KPMG analysis. https://www.finder.com/uk/stats-facts/tv-streaming-statistics

Therefore, the number of consumers who may be impacted by a cyber attack resulting in the loss of access to online video streaming services is estimated to range from 4.7 million to 39.5 million, depending on the size of the streaming service affected.

Taking the estimated impact per consumer and the number of customers impacted, the estimated impact on consumers per cyber attack resulting in the loss of access to streaming services is estimated to range from £2.8m (£0.59*4.7 million) to £197m (£5.00*39.5 million). The lower bound of this range is calculated based on the smallest number of consumers potentially impacted and the lowest positive WTP value, while the higher bound of this range is calculated based on the largest number of consumers potentially impacted and the highest WTA value.

The number of consumers impacted: cultural institutions

To estimate the number of consumers impacted by a cyber attack on cultural institutions, data from museums and galleries with over 1 million annual visitors was collected from a range of sources to cover the four nations. The analysis focused on museums with over 1 million visitors as larger institutions are more likely to be targets for cyber attacks. Visitor figures were grouped at the museum group level,[205] under the assumption that museum groups share digital systems and cyber attack impacts would cause disruption at a group level.

The data sources for visitor numbers were:

- **England**: DCMS data on the number of visits to DCMS-sponsored museums and galleries for the period January 2024 – December 2024.[206]
- **Northern Ireland**: Northern Irish museums were not included as data for 2023/24 reported fewer than 1 million visitors across National Museum NI's four sites.[207]

[202] Media Nations: UK 2023, Ofcom
[203] Families and households in the UK - Office for National Statistics
[204] Households are subscribed to multiple streaming services. Therefore the estimated number of households subscribed may not reflect the number of households for which that streaming service is their main streaming service i.e. the streaming service they primarily use.
[205] For example, the Science Museum Group operates several museums across different sites. Attendance figures are therefore taken at the aggregate level (summing attendance across all sites) to reflect the potential for a cyber attack on the museum group to impact all sites.
[206] DCMS (2025) Museums and galleries monthly visits - GOV.UK
[207] National Museums NI (2024) Annual Review 2023-24

- **Scotland:** Association of Scottish Visitor Attractions (AVSA) data on 2024 attendance to free admission attractions was used.[208]
- **Wales:** Visitor numbers to the Museum Wales group for the 12 months to March 2024 was used.[209]

To estimate the number of UK consumers potentially impacted by a cyber attack on a museum/ gallery, data from DCMS-sponsored museum and galleries KPIs[210] on attendance by overseas and total visitors was combined with 2024 attendance data. This suggests that approximately 65% of museum attendees were UK visitors.

Table 31: Estimated annual domestic visitors, museums and galleries 2024

	Domestic (UK) visitors (millions)
England	
British Museum	2.92
Imperial War Museum Group	1.42
National Gallery	1.84
Natural History Museum Group	4.23
Royal Museums Greenwich	1.22
National Museums Liverpool	2.04
Science Museum Group	3.42
National Portrait Gallery	0.91
Royal Armouries Group	1.89
Tate Group	4.17
V&A Group	2.69
Scotland	
National Museum of Scotland	1.51
National Galleries Scotland: National	1.31
Riverside Museum	0.83
Wales	
Museum Wales	1.02

Source: DCMS, AVSA, Museum Wales, KPMG analysis
Note: Northern Irish museums were not included as the 2023/24 data for the National Museum NI indicated annual visitor numbers below 1 million per year. See main text for detail.

Across the 18 museums and museum groups identified, there was an average domestic attendance of **2.01 million annual visitors per museum** (or museum group).

As with the motor insurance impacts, there is an assumed 11 day disruption (based on the typical duration until restoration following a ransomware attack across large companies in the CSBS, see section 4.2.1.2) with an associated 61 thousand visitors impacted.[211]

Taking the estimated impact per consumer and the number of customers impacted, the estimated impact on consumers per cyber attack resulting in the loss of access to museums is estimated at c. £271,000 per cyber attack. This is estimated by applying the £4.47 value to the visitor number (61 thousand).[212]

The number of consumers impacted: libraries

[208] AVSA (2025) Heritage Sites and Film Locations Enjoy Surge in Visitor Numbers
[209] Museum Wales (2024) https://museum.wales/visitor_figures/april-2023-march-2024/
[210] DCMS (2024) DCMS-sponsored museums and galleries annual performance indicators - GOV.UK
[211] (2.01 million visitors / 365 days) * 11 days = 61 thousand visitors during 11 day cyber attack induced disruption period. Rounded results of calculation on unrounded visitor numbers.
[212] Calculated on unrounded figures.

To estimate the number of library users that may be impacted as a result of a cyber attack, the average number of households per local authority (LA) was estimated, based on a total of 28.4 million UK households[213] and 382 local authorities (LAs) across the four nations (317 English LAs,[214] 11 Northern Irish Councils,[215] 32 Scottish LAs[216] and 22 Welsh UAs[217]). This gives an average number of households per LA of c. 74,000.

Data from the Participation Survey[218] on the use of libraries was used to estimate the percentage of households that are users of libraries. It was reported that 30% of adults used libraries (either online or physically) in the period May 2023 to March 2024. Applying this percentage to the average number of households per LA, results in an estimated 22,000 library user households per LA.

Converting the annual WTP value to an 11 day value (based on typical duration until restoration following a ransomware attack across large companies in the CSBS, see section 4.2.1.2) the value per household of the lost library services is estimated at £0.78 per household.[219] Applying this figure to the number of library user households per LA equates to a consumer impact of £17,000 per successful cyber attack on a library service.[220]

Estimated frequency of cyber attacks and associated impacts

The frequency of successful ransomware attacks affecting video streaming, online ticketing, museums and galleries, and libraries, was estimated using data from the CSBS (for details of the analysis, see annual impacts in section 4.2.1.1 Online banking). The rate was estimated at **2.45% per company per year**, or approximately one in forty companies. Applying this rate to the relevant sets of companies this equates to an expected:

- 0.12 incidents per year for streaming service providers (given the five main video streaming services), or approximately one successful cyber attack every eight years.
- 0.37 incidents per year for museums (given the 15 museum groups identified), or approximately one successful cyber attack every three years.
- 0.22 incidents per years for ticketing providers (given the one ticketing provider with 60% market share are eight ticketing providers with approximately 5% market share), or approximately one successful cyber attack every four to five years.

As local libraries are provided by local authorities, the rate of successful cyber attacks per local authority is used to estimate the annual impacts of successful cyber attacks impacting consumer access to local library provision. Due to the relatively low number of high-profile cyber attacks on LAs and their non-business nature, data from the charities and education section of the CSBS sample was gathered, the targeting rate was 2.5% (6,217 surveyed, 158 targeted with ransomware) and the conversion rate was 19.0% (158 targeted, 30 experiencing disruption). The resulting successful attack per LA per year is therefore estimated at 0.475%. Applying this rate to the 382 local authorities, this equates to an estimated 1.8 cyber incidents per year impacting local libraries in the UK, or approximately one successful cyber attack every seven months.

The estimated consumer impact per cyber attack and the estimated frequency of cyber attacks for each service considered in the creative industries and arts sector are presented in Table 32 below.

[213] ONS (2024) Families and households in the UK - Office for National Statistics
[214] DLUHC (2023) Local government structure and elections - GOV.UK
[215] nidirect Local councils in Northern Ireland | nidirect
[216] mygov.scot Organisations - mygov.scot
[217] Law Wales (2021) Local government bodies | Law Wales
[218] DCMS, Arts Council England and DSIT (2025) Headline findings for the Participation Survey (May 2023 to March 2024) - GOV.UK
[219] (£26.03/365 days)*11days = £0.78 per library user household per 11 day cyber attack induced disruption. Rounded to the nearest thousand.
[220] Calculated using unrounded figures.

Table 32: Estimated consumer impact of a cyber attack affecting services in the creative industries and arts, and estimated frequency of relevant cyber attacks

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Years/ months per incident (approx.)
	Low	High		
Video Streaming	£2.8m	£197m	0.12 per year	Once every eight years
Online Ticketing	£0.6m	£161m	0.22 per year	Once every four to five years
Museums & Galleries	£0.271m		0.37 per year	Once every three years
Local Libraries	£0.017m		1.8 per year	Once every seven months

Note: Where the estimated annual frequency of cyber attacks is not a whole number, DSIT requested that the annual consumer impact was not monetised.

Limitations of the approach to valuing the impact on consumers who are unable to access online ticketing, video streaming services, and cultural institutions as a result of cyber attack

- **Online ticketing and video streaming services:** There are a number of important limitations of the approach to valuing the impact on consumers from a loss of access to online ticketing and online video streaming services as a result of a cyber attack, some of which are similar to those described in referred to online banking:
  - **Bias:** A number of factors may lead to respondents not stating their true WTP/ WTA. In particular, because the scenarios described are hypothetical and there are no real financial consequences to the amounts stated. In addition, respondents may deliberately over or under state WTP/ WTA in order to try to influence how they think the values will be used. Furthermore, misunderstanding the concepts and/ or the scenario may bias the results.
  - **Context:** The WTP/ WTA values relate to the specific scenario described to respondents (see descriptions above). Therefore this may not be representative of the impact of all cyber attacks affecting access to online ticketing and online video streaming services. For example, it is likely to depend on the duration of the disruption, while in the consumer survey the scenario described for these services specified the disruption lasting for one day.
  - **Anchoring effect:** A limitation of the double-bounded dichotomous choice approach is the so called 'anchoring effect' whereby respondents' WTP and WTA are influenced in some way by the value first presented to them. To mitigate against this anchoring effect, respondents were also asked to self-report their WTP and WTA through the open-ended elicitation approach. However, as this question was asked after the questions for the double-bounded dichotomous choice approach, the stated values may still influence the self-reported values.
  - **Number of consumers impacted:** While an attempt has been made to estimate the number of consumers potentially affected by a cyber attack resulting in the loss of access to online ticketing and online video streaming services, there is considerable uncertainty around this. For example, for online video streaming services, the number of consumers impacted depends on the number of households subscribed but also whether the impacted service is that which they primarily use, and the extent to which they have multiple subscriptions to other streaming services.
- **Cultural institutions and libraries:** There are several important limitations to the scope and approach of the analysis. The following key limitations have been identified:
  - **Museums and galleries included:** The analysis of museums and galleries only includes large public museums and galleries (with over 1 million annual visitors), and due to the limitations of the sources used to develop this list, may not be comprehensive. The was on larger museums given the materiality of impact (due to the higher number of customers) and the perception that larger organisations may be more attractive targets for cyber criminals. Due to the UK consumer focus of this report, international visitors to museums and galleries were not included in the estimation of consumer impacts.

- **Museum and gallery in person provision:** For the museum and galleries analysis, only the value of the website to visitors was considered. Due to lack of available data, and the nature of the evidence available, the estimation of impacts was focused on the availability of the website to those who also visit in-person. As such the analysis does not capture the impact on non in-person visitors who only visit the website, any resulting reductions in in-person visitor numbers or the direct impact on the in-person provision of museum and gallery services. As such, the impacts presented may reflect an underestimate of the full consumer impact.
- **Local authority provision of library services:** The analysis of libraries only includes those provided by LAs, and therefore other libraries (such as the British Library and other research libraries) were not included in the scope of the analysis. In addition, there is an underlying assumption that library services are provided at the LA level, although some LAs may share digital and physical resources when delivering library services, such as the Libraries Consortium.[221] If the successful cyber attack impacted service provision across multiple LAs (due to shared systems) the resulting consumer impacts per cyber attack would be larger. Shared systems may also be associated with a higher standard of cyber security and an associated reduced frequency of successful attacks.
- **Library service provision:** For the library analysis, it was assumed that due to the nature of libraries, both digital and in-person service provision would be impacted. In cases where libraries are able to continue to provide library services throughout the period of disruption due to a cyber attack (i.e. by setting up a temporary record keeping system for loans and returns) much of the impact may be mitigated. In addition, the use of libraries as a public space could continue through the cyber attack. This use case was associated with lower individual willingness to pay in the study that was used as the source of the consumer value of library services, so the resulting effect on the consumer value estimates are likely limited.[222]

4.2.4 Real estate and renting

Introduction to the valuation of consumer impacts from cyber attacks affecting home purchases

The potential impacts on consumers from a successful cyber attack affecting property purchases or renting are set out in section 3.3.4. In this section the methodology used to monetise the impacts on consumers who have home purchases disrupted is detailed, and the quantified impacts are presented.

In order to estimate the impact on consumers from a cyber attack affecting home purchases, the monetised impact per consumer was multiplied by the number of transactions impacted.

Methodology for the valuation of real estate and renting impacts on consumers who have home purchases disrupted by a cyber attack

Share of purchases cancelled/ delayed

In order to estimate the share of purchases delayed or cancelled by a successful cyber attack, purchasing volume data from HM Land Registry's UK House Price Index (UKHPI) was analysed. As described in the literature review (see section 2.3.1), Hackney Council was affected by a ransomware attack in October 2020 which rendered its property transaction systems inaccessible for months, therefore impacting the volume of property purchases in the area. By comparing the number of house purchases between Hackney and the surrounding areas over time, the share of property purchases

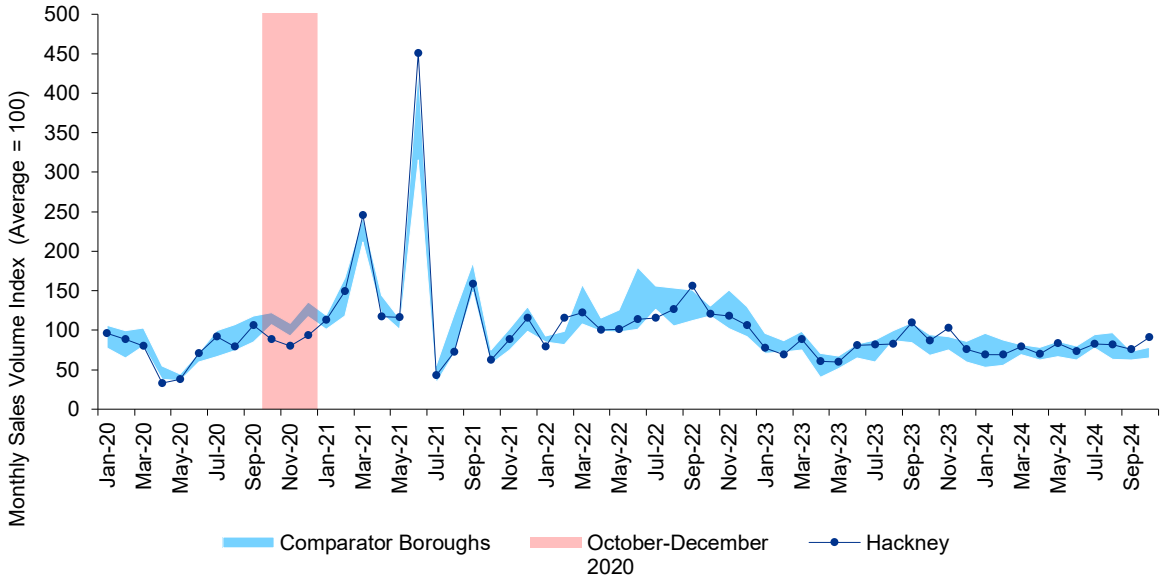
[221] The Libraries Consortium The Libraries Consortium History
[222] Fujiwara, Lawton and Mourato (2015) The health and wellbeing benefits of public libraries. Report for Arts Council England. The health and wellbeing benefits of public libraries.pdf

affected by a cyber attack is estimated, given the neighbouring areas are generally comparable in terms of house purchase activity (see Figure 16).[223]

The reduction in the number of completions is estimated by comparing data from the London Borough of Hackney with the neighbouring boroughs of Haringey, Waltham Forest, Newham and Tower Hamlets. At the time of the analysis the latest available data was for the month of October 2024. In order to capture the period of the Hackney Council cyber attack (commencing October 2020[224]) data from January 2020 onwards was collected. To allow for comparison across the boroughs, the monthly volume of completions for each borough was indexed against the average monthly volume over the full period January 2020 to October 2024 (see Figure 16).

The shading in Figure 16 shows the range of values for the selected neighbouring boroughs, with the values for Hackney closely following that seen by the four selected neighbouring boroughs. The indexed value typically remained within the range of values across the selected comparators over the time period analysed.

Figure 16: Monthly sales volume of all property types: Hackney and neighbouring boroughs (January 2020 to October 2024)



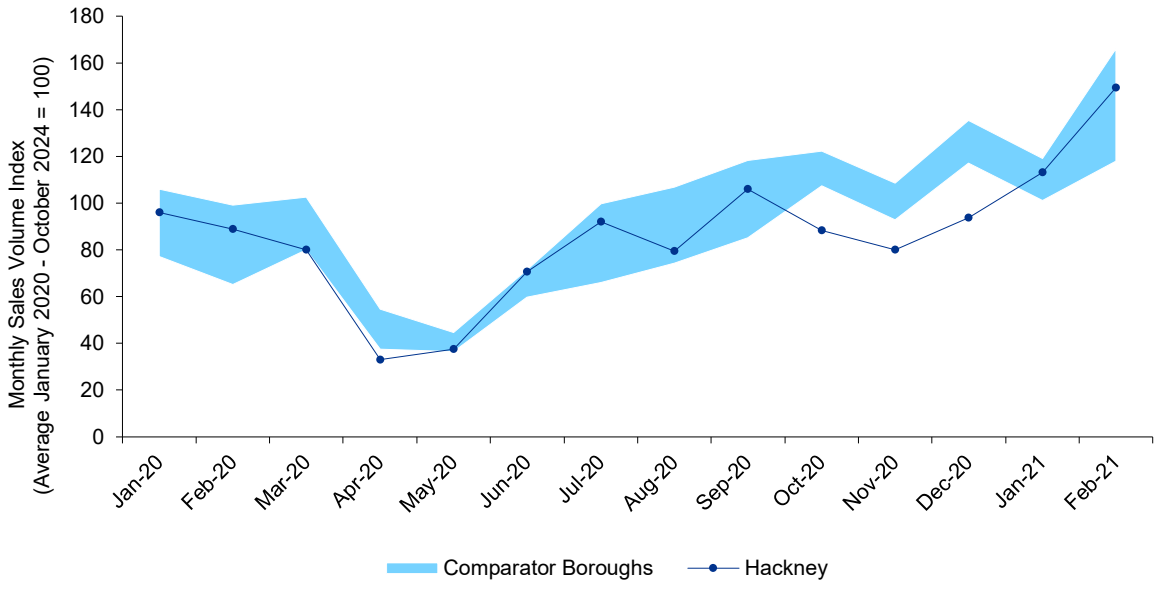
Source: Land Registry UKHPI, KPMG Analysis

During the initial three months after the Hackney Council cyber attack (October to December 2020, see shaded area in Figure 16) the index of sales volume in Hackney fell below that of the lowest of the comparators and remained below the comparators for the following two months (see Figure 17).

[223] Data from 2010 was also collected to assess whether the house purchasing quantities in Hackney closely followed those in the comparator boroughs. This was found to be the case. While there were some short periods of divergence between sales quantities in Hackney and the comparator boroughs, these were explained by a large spike in the sale of new-build housing. No such large spikes in the sale of new build housing were present in Hackney around the of the cyber attack.

[224] Hackney Council (2020) Serious cyberattack on Council systems: statement

Figure 17: Monthly sales volumes of all property types: Hackney and neighbouring boroughs (January 2020 to February 2021)



Source: Land Registry UKHPI, KPMG Analysis

Using the conservative assumption, that sales volumes in Hackney would be equal to the bottom of the range in the neighbouring comparator boroughs if not for the cyber attack, the reduction in volumes is estimated as:

- 18% in October 2020;
- 14% in November 2020; and
- 20% in December 2020.

Over the three-month period the reduction in volumes was estimated at 17%.

Total volume of sales per local authority

In order to analyse the volume of sales per local authority (LA), Land Registry UKHPI data from the last available 12 months (November 2023 to October 2024) was captured for all London Boroughs, English Unitary Authorities, English Metropolitan and Non-Metropolitan Districts, Northern Irish Local Government Districts, Scottish Council Areas and Welsh Unitary Authorities.

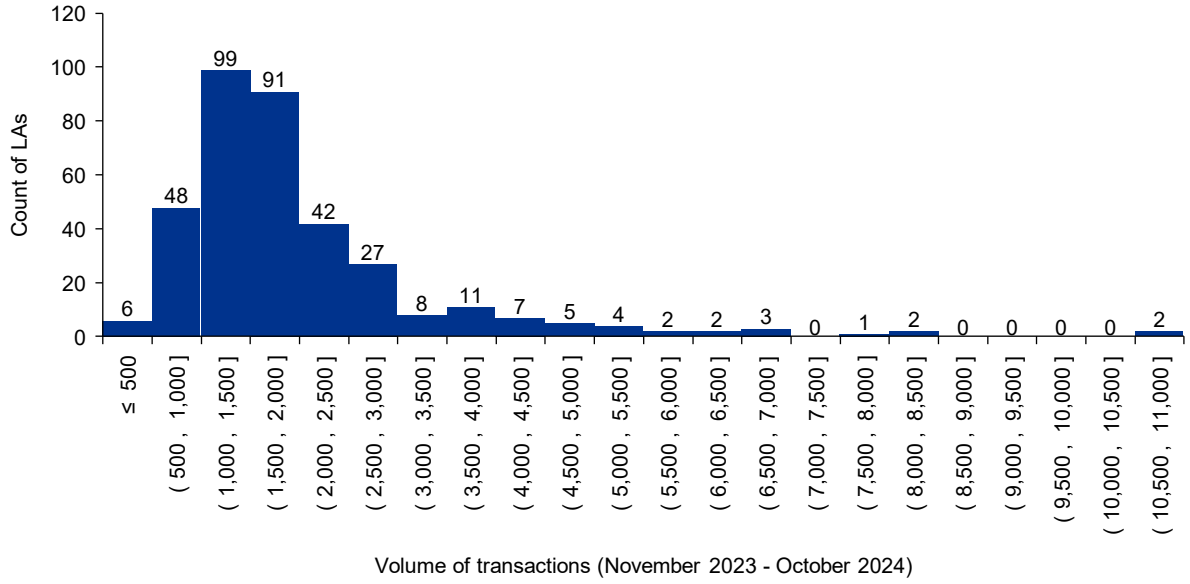
The number of transactions over the 12-month period ranged from 148 in the City of London, to 10,953 in the City of Edinburgh. The distribution of sales volumes is skewed, with a large right-hand tail (see Figure 18). Across all 360 LAs included in the 12-month period November 2023 to October 2024:

- The mean volume of transactions per LA was 2,006.
- The median volume of transactions per LA was 1,621; and
- The inter quartile range[225] of transactions per LA was 1,220 to 2,205.

Hackney Council, the target of a previously successful cyber attack was associated with 1,729 over the 12-month period, an amount slightly higher than the median LA.

[225] The inter quartile range is a measure of the dispersion of data. It is the difference between the upper quartile and lower quartile.

Figure 18: Distribution of transaction volumes across UK local authorities



Source: Land Registry UKHPI Data, KPMG Analysis

Consumer impact per cyber attack

The following two impacts are monetised per cyber-attack:

- Moving delays and cancellation: assumed as £500 - £1,000 per transaction delayed/ cancelled.[226]
- Indemnity insurance: assumed as £300 - £500 per transaction continued without possessory title.[227]

Assuming the median LA transaction volume of 1,621, a 3-month duration for the impact on the real estate market of a successful cyber attack (as seen in the analysis of the Hackney Council volumes) and 17% reduction in sales, it is estimated there would be:

- Approximately 69 delayed/ cancelled transactions, with an associated cost ranging from £34,446 to £68,893.
- Approximately 336 transactions potentially at risk due to possessory title uncertainty, with an associated cost ranging from £100,907 to £168,179.
- Total impacts per successful cyber attack across these two impact areas in range of £135,354 to £237,071.

Estimated frequency of cyber attacks and associated impacts

The frequency of successful cyber attacks affecting property purchase transactions was estimated using data from the CSBS.[228] The analysis of CSBS data aggregated survey responses from the years 2019 to 2024 due to the relatively low frequency of ransomware incidents. Details of the analysis of the CSBS survey can be found in in section 4.2.1.1.

Due to the relatively low number of high-profile cyber attacks on LAs and their non-business nature, data from the charities and education section of the CSBS sample was analysed. The targeting rate was 2.5% (6,217 surveyed, 158 targeted with ransomware) and the conversion rate (percent of targeted companies that went on to also experience ransomware associated disruption) was 19.0%

[226] Homeowners Alliance Moving Day Delays - 115,000 Delayed Moves; Cost To Homeowners £15 Million - HomeOwners Alliance
[227] Bollanack & Bishop Solicitors Can You Sell Land With Possessory Title? | Property Lawyers
[228] Department for Science, Innovation and Technology and the Home Office (2024) Cyber Security Breaches Survey 2024 - GOV.UK

(158 targeted, 30 experiencing disruption). The resulting successful attack per LA per year is therefore estimated at 0.475%. Applying the 0.475% rate per year to the 360 LAs results in an estimated 1.71 incidents per year, or approximately one attack every seven months.

The estimated consumer impact per cyber attack and the estimated frequency of cyber attacks affecting property purchases due to an attack on a LA, are presented in

Table 33.

Table 33: Estimated consumer impact of a cyber attack affecting property purchases and estimated frequency of relevant cyber attacks

Service	Consumer impact per successful cyber attack		Estimated annual frequency (approx.)	Months per incident (approx.)
	Low	High		
Land Registry Searches (Local Authorities)	£0.135m	£0.237m	1.71 per year	Once every seven months

Note: Where the estimated annual frequency of cyber attacks is not a whole number, DSIT requested that the annual consumer impact was not monetised.

Limitations of the approach to the valuation of consumer impacts who have home purchases disrupted by a cyber attack

The following limitations of the methodology used to value the impact on consumers from disruptions to home purchases resulting from cyber attacks should be noted:

- **Scope of the analysis:** The analysis quantifies the impact on consumers who experience disruptions to property purchases. However, this excludes a range of identified impacts including the loss of utility from delayed property purchases and wellbeing impacts due to a lack of available evidence and not being able to include additional questions within the consumer survey to gather the information required due to the need to keep the survey short. In addition, as set out in the impact map (see section 3.3.4), cyber attacks may also disrupt rentals through delays in being able to sign up to the housing register and being unable to search for social housing.
- **Representativeness and quality of data:** The analysis is highly assumption driven with the results being sensitive the assumptions used. In particular, the estimated number of consumers impacted is derived from evidence from a single cyber attacks on a single LA. Additionally, the estimated costs of disruption (moving costs and indemnity insurance) are from single sources and would be expected to vary depending on a range of factors including, geography and size of property purchase.
- **Number of consumers impacted:** While an attempt has been made to estimate the number of consumers potentially affected by property purchases delays from a cyber attack, there is considerable uncertainty around this. The number of consumers impacted depends on the duration of the disruption and the size of the LA affected.

Collectively these limitations mean the results may be over or under estimated and modelling would be needed to value the impacts of specific cyber attack scenarios, and results are indicative only.

4.2.5 Manufacturing

Introduction to the valuation of consumer impacts from cyber attacks on pharmaceutical manufacturing

DSIT and DHSC agreed that estimated values of the potential impacts on patients of a successful cyber attack on UK manufacturers of prescription and non-prescription medication should not be included in this study. This decision was taken for a number of reasons including:

- The variation in the potential patient impacts by medicine, length of issue and prescribing indication.

- The existence of national shortage management process and the tools available at a national and local level may lead to mitigation of the issue. However, the tools and options used to mitigate a supply issue will vary depending on what's needed to mitigate impacts to patients. For example, the type of medication impacted and availability of suitable alternatives, and so not all issues require the same mitigations.
- The sensitivities around monetising patient impacts in a published report given the inherent uncertainties around the assumptions that would need to be made in the analysis.

The following section therefore details a methodology for the estimation of patient impacts, that could be used in the future, without providing quantified estimates of potential impacts.

The potential impacts on patients from a successful cyber attack on UK manufacturers of prescription or non-prescription medication are set out in section 3.3.5. This section sets out the methodology that could be used to monetise the health impacts on patients who cannot switch to alternative medication and are unable to access supply of the affected medication. As detailed in the impact map, it may be that patients can continue to access the affected medication or are able to switch to an alternative. The methodologies to calculate the impact on these patients are not considered in this study due to the variability in patient responses, and uncertainty of associated health impacts of switching to alternative medications (see limitations for more detail).

The methodology set out below is described in relation to prescribed medication given the greater availability of data on dispensing of NHS prescription medication. However, the same approach could be adapted for non-prescription medications subject to the availability of input data for the analysis.

Proposed methodology for the valuation of health impacts on consumers who are unable to access medication impacted by a cyber attack

The methodology described has been developed with DHSC's supply and resilience colleagues.

The health impacts on patients of cyber attacks on UK pharmaceutical manufacturers resulting in patients being unable to access a specific medicine for a period of time can be estimated using QALYs. This can be done by combining the patient impact and the number of days the patient is without the medication.

$$\text{QALY impact of disruption} = \text{QALYs per patient day} \times \text{Patient days of disruption}$$

QALYs per patient day

The impact on a patient per day of no medication can be estimated by the difference in Quality of Life (QoL) between those with and without access to the affected medication.

The QALYs per patient day can be estimated as follows:

$$\text{QALYs per patient day} = {}^{(\text{QoL}_{\text{without medication}} - \text{QoL}_{\text{with medication}})}/_{365}$$

Patient QoL for each state may be estimated using various tools, such as the EuroQol 5 Dimensions 5 Levels (EQ-5D-5L) value set.[229] The EQ-5D-5L is a descriptive system that measures patient wellbeing using 5 levels of severity, across the five dimensions of mobility, ability to self-care, ability to carry out usual activities, pain/ discomfort and anxiety/ depression.[230] The resulting 5-digit code can then be converted to a QoL estimate.

[229] Devlin et al. (2016) Valuing health-related quality of life: An EQ-5D-5L value set for England.
[230] EuroQol Research Foundation, EQ-5D-5L.

Patient days of disruption

Patient days of disruption refers to the number of days of disruption multiplied by the number of patients. For example, a disruption to 100 patients for five days would equate to 500 patient days of disruption.

Two possible methods to estimate the number of patient days of disruption have been identified. The ability to use the second of these approaches, depends on whether the number of units of medication disrupted is known. Both methods should give the same figure, with which method to use being based on what data is available.

Method 1: To understand the number of patients and length of time over which patients are impacted, the following information would be required:

- Annual quantity produced of the medication. Alternatively, the annual quantity used (usage/ demand) may be used as a proxy for the quantity produced.
- Typical daily dosage (i.e. quantity used by each patient per day).
- Duration of disruption to the medicine manufacturer. This is a proxy for the average duration of health impacts.

Using the above information, the impact in patient days could be estimated as follows:

$$\text{Patient days of disruption} = \frac{\text{Annual Quantity}}{\text{Daily Dosage}} \times \frac{\text{Days of manufacturing disruption}}{365}$$

If a manufacturer operates on a five day a week schedule, the calculation may be modified to reflect that.[231] It would also be necessary to check that the Days of manufacturing disruption figure reflects the number of working days of disruption.

Further adjustment may need to be made if the impacted supplier is not the sole supplier of the medication. In such cases, the number of patient days of disruption should be adjusted for the market share of the supplier. This is needed because the impact of a cyber attack affecting the provision of medication from one supplier is mitigated by the availability of the medication through another supplier and this therefore needs to be taken into account in the analysis.

Method 2: If the number of units of medication disrupted is known, the extent of patient disruption can be estimated as follows:

$$\text{Patient days of disruption} = \frac{\text{Quanity of disrupted medication}}{\text{Daily Dosage}}$$

In the case that the number of units of medication disrupted is known, no further adjustment for market share is needed.

QALY impact of disruption

The QALY impact of disruption is then estimated by combining the results of the previous calculations:

$$\text{QALY impact of disruption} = \text{QALYs per patient day} \times \text{Patient days of disruption}$$

This may then be monetised using the Green Book £70,000 (2020/21 prices) per QALY figure. This puts a monetary value on the impact of not having a specific medication for a given period of time. If

[231] 52 weeks* 5 working days a week = 260 weekdays per year. 260 weekdays per year – 8 bank holidays = 252 working weekdays per year.

considering the lack of supply of a number of medicines, the QALY impact of disruption should be calculated separately and then summed up.

Limitations of the approach

The following limitations should be noted:

- **Scope of proposed methodology:** The proposed methodology only considers the health impacts on patients who are unable to switch to alternative medication. As set out in the manufacturing impact map (see 3.3.5), patients may continue to access the affected medication or may be able to switch to an alternative medication in the event of a cyber attack. However, methodologies to estimate the associated impacts for these patients are not considered.
- **Patients who continue to access the affected medication:** There is significant uncertainty and variability around consumer responses to shortages of medication, and a lack of evidence about the potential costs involved in the additional effort consumers may need to exert to continue to access the affected medication, such as travel and time costs. Therefore, it is difficult to estimate the time and effort costs for patients in seeking alternative medication. When consumers exert additional effort in order to continue to access the affected medication, although some consumers may mitigate the potential health impact of losing access to a medication, there is no aggregate change in health impacts (rather there are winners and losers among the consumers).
- **Patients who may be able to switch to an alternative medication:** In the case of some medications, provision of an alternative may be feasible with minimal or no difference in health outcomes, but this varies from medication to medication. The inclusion of the health impact for patients who switch to alternative medication should be considered on a case-by-case basis depending on the medication under consideration, the substitutes available and the potential difference in health outcomes. By not including this in the analysis the proposed methodology may overestimate the impact on consumers of a cyber attack affecting the supply of medication.
- **Variation in potential impacts:** There is likely to be significant variation in the scale of the impacts by medication, meaning that considering the impact of one medicine is unlikely to be representative of other medicines.
- **Assumptions:** The quantified impacts will be highly dependent on any assumptions used in the analysis. The estimated impacts will vary with changes to individual assumptions, as well as depending on the combination of assumptions used. Therefore sensitivity analysis should be undertaken.

4.3 Summary of results

The table below summarises the monetised consumer impacts of cyber attacks for each of the services in scope of this study. It includes the consumer impact per cyber attack (i.e. the unit value monetised in 2024 prices) and the estimated annual frequency.

Table 34: Estimated consumer impacts from cyber attacks

Sector	Good/ service	Unit value (i.e. per cyber attack)		Estimated annual frequency (approx.)
		(Low)	(High)	
Financial services	Online banking	£5.5m	£231m	0.27 per year
	Motor vehicle insurance	£0.011m	£0.688m	0.20 per year
Health care	Major hospital	£11.141m		3 per year
	GP practice	£0.020m		37 per year
Creative industries and arts	Online ticketing	£0.6m	£161m	0.22 per year
	Video streaming services	£2.8m	£197m	0.12 per year
	Museums and galleries	£0.271m		0.37 per year
	Local libraries	£0.017m		1.8 per year
Real estate and renting	Property purchases	£0.135m	£0.237m	1.71 per year

Source: KPMG analysis.
Note: Where the estimated annual frequency of cyber attacks is not a whole number, DSIT requested that the annual consumer impact was not monetised.
Note: DSIT and DHSC agreed that estimated values of the potential impacts on patients of a successful cyber attack on UK manufacturers of prescription and non-prescription medication should not be included in this study. See reasons set out in section 4.2.5.

These results are indicative of the potential scale of the impact on consumers from cyber attacks affecting the access to these goods and services. There are a number of important limitations to the methodologies used to estimate these values that should be noted when considering the results presented in the table. The values presented are sensitive to the assumptions used in the analysis and do not necessarily capture all areas of impact. The limitations are specific to the methodologies used for each of the goods and services considered and therefore the key limitations are set out alongside the methodologies in the previous sections.

4.4 Concluding remarks

This study contributes to the evidence base about the impact on consumers of cyber attacks resulting in the loss of access to goods and services. While existing research into the impacts of cyber attacks has generally focused on the impact on businesses, the impact on consumers is less well understood. Therefore, this study aims to help to fill this evidence gap.

This study focuses on five sectors, and specific services within these sectors, as agreed with DSIT at the outset. However, similar approaches could be adopted to value the impact on consumers of cyber attacks resulting in the loss of goods and services in other sectors. Specifically, developing impact maps to identify the impacts on consumers and how consumers may respond, and developing methodologies using primary and secondary data to quantify the impacts identified.

The analysis shows that the impacts on consumers of a successful cyber attack is highly dependent on a range of factors, including the type, scale and duration of a cyber attack, as well as the types of consumers impacted. Therefore, while the analysis and consumer impact estimates produced for this report provides an indication of the potential cost to consumers of a range of attacks, these costs are highly dependent on the specific attack scenario being considered. Furthermore, there are a range of impacts on consumers that are often not valued in the study across the sectors and scenarios considered, including the wellbeing impacts, such as the stress, anxiety and frustration consumers may experience as a result of being unable to access goods and services.[232] Other impacts that are not valued are specific to the sectors and scenarios, such as the personal costs patients may face, such as rearranging transport and time off work, from changes to health care appointments/ procedures. This means that the overall cost to consumers of a successful cyber attacks may be higher, particularly if the duration, severity and frequency of attacks is greater.

As technology advances, it is expected that cyber attacks may become more sophisticated, although so too should defence mechanisms. In turn, the impacts on consumers presented in this study may be expected to change over time. Therefore, future consideration should be given to the continued

[232] This is included in the valuations where a WTA/ WTP approach is used.

validity of the findings presented and as the nature of cyber attacks evolve over time and the sectors and services impacted expand, further analysis will likely be required to provide a fuller assessment of costs to consumers of successful attacks.

Appendix 1 Methodology

This Appendix details the approach to developing the consumer survey and deriving the WTP and WTA estimates.

A1.1 Consumer survey

A1.1.1 Survey development

The consumer survey was designed in line with GSR Professional Guidance[233] for research, as well as with HMT Green Book supplementary guidance on stated preference techniques.

It therefore followed the suggested structure for a typical contingent valuation questionnaire:

- Purpose: The purpose of the survey was explained to respondents so that they understood the context and could participate in an informed manner. This also encouraged participation and cooperation.
- Attitudinal questions: These were used to understand respondent's attitudes towards cyber attacks and the relevant goods/ services.
- Use of the good/ service: Questions were asked to understand if respondents used the goods/ services in question and their frequency of use, to determine the respondent's familiarity with the goods/ services.
- The scenario: The scenario (in this case the various cyber attack scenarios affecting the provision of certain goods/ services) was then explained to respondents. This is essential for the credibility of the survey and eliciting meaningful responses.
- Value elicitation questions: These questions were designed to understand the maximum WTP to avoid the loss of the goods/ services, and the minimum WTA for the loss of the goods/ services. Two approaches were adopted for these questions: an open-ended elicitation approach where respondents were asked their WTP/ WTA in an open question, and a double-bounded dichotomous choice approach. In the double-bounded dichotomous choice approach respondents were asked whether or not they would be WTP/ WTA a stated amount (see detail of these amounts in section A1.1.3), and were then asked to say yes or no to higher/ lower amounts. The dichotomous choice approach has the advantage of encouraging truth telling and helps the respondents with the valuation task. However, there may be anchoring bias, as answers are anchored to the initial amount stated in the question.
- Follow-up questions: Questions were then asked to help understand the reasons behind respondent's answers and to test the validity of responses. This was used to identify invalid and protest responses (see further detail below).

Respondent characteristic data including gender, age band and household income, was also available, but was not collected as part of the survey as it was information already held by YouGov about their online panel.

A1.1.2 Fieldwork

The fieldwork was conducted by YouGov among their online panel of consumers, between Tuesday 21st and Friday 31st January 2025, achieving 1,000 completed survey responses.

WTP and WTA double-bonded dichotomous choice analyses were undertaken to estimate the consumer impact of loss of service for:

- Online banking;
- Online ticketing; and
- Video streaming services

[233] 2021-GSR_Ethics_Guidance_v3.pdf

To avoid confusion, survey participants were either asked WTP or WTA type valuation questions for each of the services, as such the panel was equally split into two samples (a WTP sample and a WTA sample). In order to reduce potential bias due to question ordering, the order of the three service areas (banking, ticketing and streaming) was randomised.

A1.1.3 Survey analysis

WTP and WTA studies are two forms of contingent valuation methodologies. Contingent valuation studies aim to "reveal the monetary tradeoff [sic] each person would make concerning the value of goods or services."[234] In a WTP study, the individual is asked how much they would pay for access to a good or service, conversely in a WTA study, the individual is asked how much they would accept in lieu of the good or service.

A double-bounded dichotomous choice approach is one method of eliciting values in a WTP or WTA study, where survey participants are asked two sequential yes/ no questions to refine the estimate of their value of a good or service.

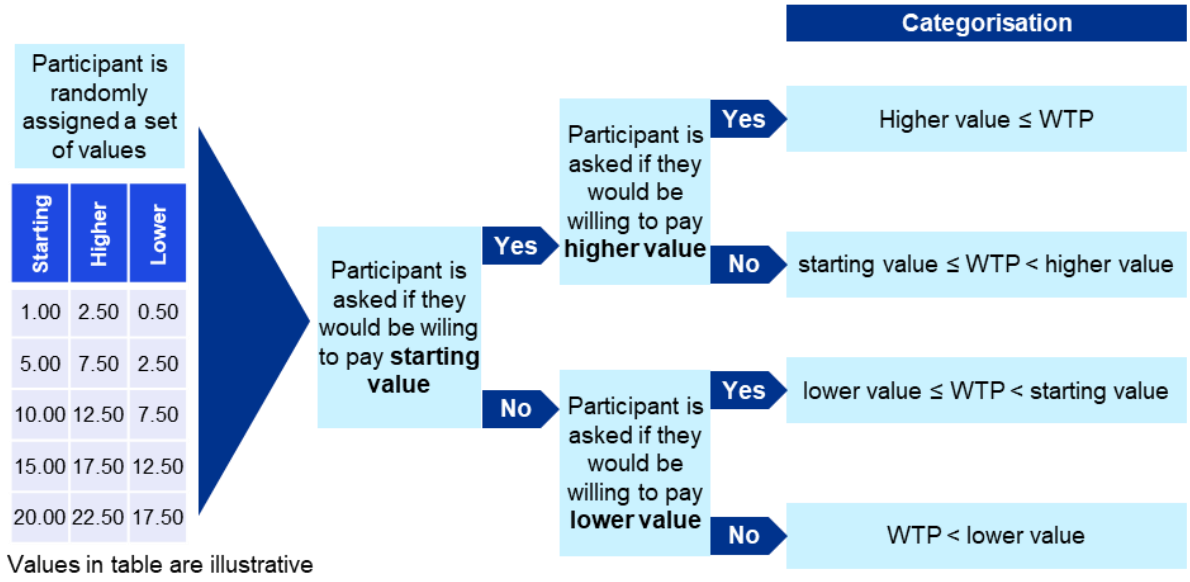
Double-bounded dichotomous choice WTP question ordering:

For the WTP study, the double-bounded dichotomous choice questions were presented as follows (see Figure 19):

- **Random Assignment of WTP Values**: Participants were randomly assigned a set of WTP values, which included a starting value, a higher value, and a lower value.
- **Presentation of First WTP Question**: Each participant was presented with the initial WTP question based on their assigned starting value. They were asked whether they would be willing to pay this amount to avoid the loss of service.
- **Follow-Up WTP Question** (dependant on the participant's response to the first question):
  - If the response was "Yes," they were presented with a follow-up question using the higher WTP value.
  - If the response was "No," they were presented with a follow-up question using the lower WTP value.
- **Categorisation of responses:** Participants could then be categorised based on their responses to the follow-up question:
  - **Higher Value ≤ WTP**: Participants who answered "Yes" to both the starting and higher WTP questions.
  - **Starting Value ≤ WTP < Higher Value**: Participants who answered "Yes" to the starting WTP question but "No" to the higher WTP question.
  - **Lower Value ≤ WTP < Starting Value**: Participants who answered "No" to the starting WTP question but "Yes" to the lower WTP question.
  - **WTP < Lower Value**: Participants who answered "No" to both the starting and lower WTP questions.

[234] Carson, Richard T. (2012) Contingent Valuation: A Practical Alternative When Prices Aren't Available - Journal of Economic Perspectives 26 (4): 27–42.

Figure 19: Survey question flow chart for double-bounded dichotomous choice WTP studies



Source: KPMG analysis

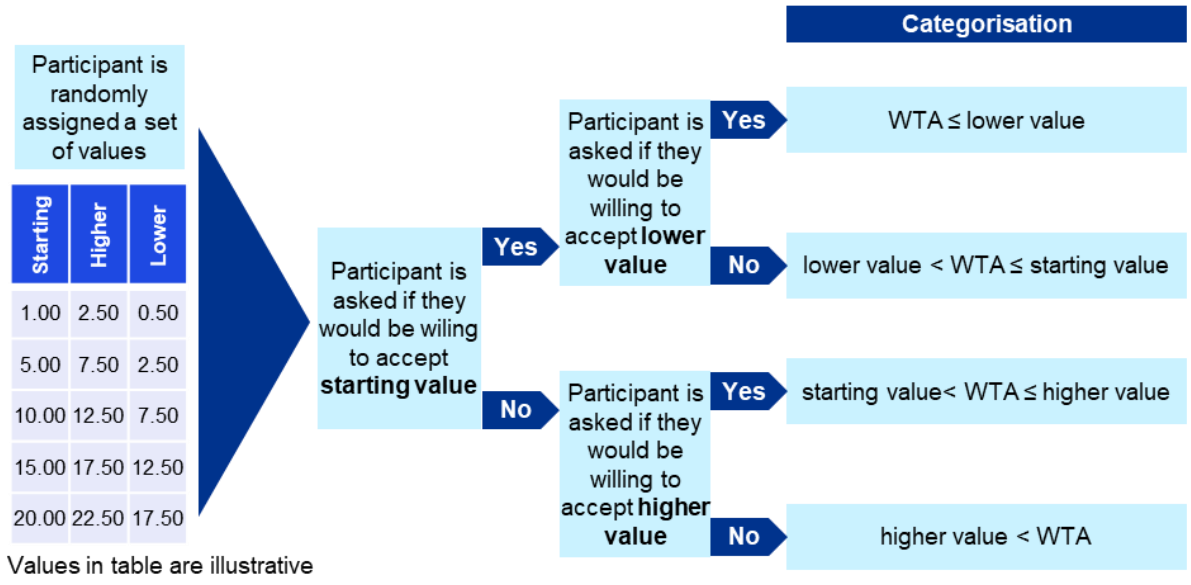
Double-bounded dichotomous choice WTA question ordering:

The presentation and interpretation of double-bounded dichotomous choice questions for the WTA approach is similar to that presented for the WTP approach, with the responses inverted, as it attempts to capture the minimum amount of compensation an individual would require to experience the negative outcome from the cyber attack rather than the amount an individual would be willing to pay to avoid it.

The WTA questions were presented as follows (see Figure 20):

- **Random Assignment of WTA Values**: Participants were randomly assigned a set of WTA values, which included a starting value, a higher value, and a lower value.
- **Presentation of First WTA Question**: Each participant was presented with the initial WTA question based on their assigned starting value. They were asked whether they would be willing to accept this amount as compensation for the loss of service.
- **Follow-Up WTA Question** (dependant on the participant's response to the first question):
  - If the response was "No," they were presented with a follow-up question using the higher WTA value.
  - If the response was "Yes," they were presented with a follow-up question using the lower WTA value.
- **Categorisation of responses:** Participants could then be categorised based on their responses to the follow-up question:
  - **Higher Value < WTA**: Participants who answered "No" to both the starting and higher WTA questions.
  - **Starting Value < WTA ≤ Higher Value**: Participants who answered "No" to the starting WTA question but "Yes" to the higher WTA question.
  - **Lower Value < WTA ≤ Starting Value**: Participants who answered "Yes" to the starting WTA question but "No" to the lower WTA question.
  - **WTP ≤ Lower Value**: Participants who answered "Yes" to both the starting and lower WTA questions.

Figure 20: Survey question flow chart for double-bounded dichotomous choice Willingness to Accept (WTA) studies



Source: KPMG analysis

WTA and WTP values:

Sets of starting, higher and lower values presented to the survey participants were created for each of the three different service areas, with the same sets of values being used for both WTA and WTP questions. The range of values were based on a review of the prices of these services.[235, 236, 237] The resulting values for each of the three service areas are shown in Table 35.

[235] Monthly current account fees were taken from banks own websites. Halifax: £0 to £19, Santander: £0 to £5, Monzo £3 to £17 and Lloyds £0 to £22.50. Information correct as at 9th January.
[236] Monthly prices were taken from streaming services own websites. Netflix: £4.99 to £17.99, Disney+: £4.99 to £12.99, Amazon Prime Video: £8.99, Apply TV+: £8.99 and BBC £0. Information correct as at 9th January.
[237] The starting values for online ticketing were based on the various fees (such as booking, processing and e-ticket fees) associated with using these services. Source: Which? calls for crackdown on sneaky gig ticket fees as new laws set to come into force - Which? Policy and insight

Table 35: Starting, higher, and lower double-bounded dichotomous choice values

Service	Starting Value	Lower Value	Higher Value
Online Banking	£7	£3	£11
	£11	£7	£15
	£15	£11	£19
	£19	£15	£23
	£23	£19	£27
Online Ticketing	£4	£1	£7
	£7	£4	£10
	£10	£7	£13
	£13	£10	£16
	£16	£13	£19
Video Streaming	£1	£0.50	£2
	£2	£1	£3
	£3	£2	£5
	£5	£3	£7
	£7	£5	£9

WTA and WTP follow up questions:

After answering a set of dichotomous choice questions, survey respondents were asked a follow up question to specify their exact minimum WTA or WTP value (i.e. the open-ended elicitation approach). In addition, they were asked to specify reasons for their responses to the survey.

For the WTA sample, respondents were asked to specify a single main reason from a list, while those in the WTP sample were able to select multiple answers from a list. Where the respondent chose 'other' they were presented with a free-text input field to record their reason.

For all three service types the same follow up question was asked to respondents for the WTA studies:
What is the main reason you would not be willing to accept less than this?

- It wouldn't be a fair amount
- It wouldn't cover the cost of what I would do instead
- I wouldn't be satisfied by less
- Other
- Don't know

For all three service types, respondents were asked the same follow up question for the WTP studies: Why would you not be willing to pay more than this? The options available as answers to the question varied slightly across the three WTP studies, to reflect the different services (see Table 36).

Table 36: Available answer options to WTP follow up question

	Online Banking	Online Ticketing	Video Streaming
I don't value it sufficiently	✓	✓	✓
I could not afford it	✓	✓	✓
I should not have to pay to avoid this	✓	✓	✓
Losing access to my main online banking service/ banking app for 3 days would not be a problem for me	✓	×	×
Losing access to the online ticketing service I primarily use for 1 day would not be a problem for me	×	✓	×
Losing access to the online video streaming service I primarily use for 1 day would not be a problem for me	×	×	✓
I am already paying for this service though bank charges	✓	×	×
I am already paying for this service though ticket charges	×	✓	×
I am already paying for this service through streaming subscription	×	×	✓
I don't believe this will happen	✓	✓	✓
I don't feel confident stating a value/ I need more information	✓	✓	✓
I would be able to use an alternative online ticketing platform	×	✓	×
Other	✓	✓	✓
Don't know	✓	✓	✓

Identification of invalid and protest responses:

Protest and invalid responses were identified through the application of a set of rules:

- A response was deemed invalid if the self-reported maximum WTP/ minimum WTA value was inconsistent with the dichotomous choice answered provided.
- A response was deemed invalid or a protest response if the self-reported minimum WTA was very high (above £100 for online banking, or above £50 for online ticketing and video streaming).
- A response was deemed invalid where the respondent had answered 'Yes, Yes' or 'No, No' (i.e. that they would be WTP the starting and higher value, or would not be WTP either the starting or lower value) for the WTP dichotomous choice questions and indicated that one of the reasons for the answer was that they did not believe that the cyber attack would actually happen.
- A WTP value was deemed a protest response if the respondent answered 'No, No' to the dichotomous choice and indicated that they shouldn't have to pay as a reason whilst not

indicating any of the following reasons: that they do not value the service sufficiently, that they could not afford to pay more, or that not having access to the service for the duration was not an issue.

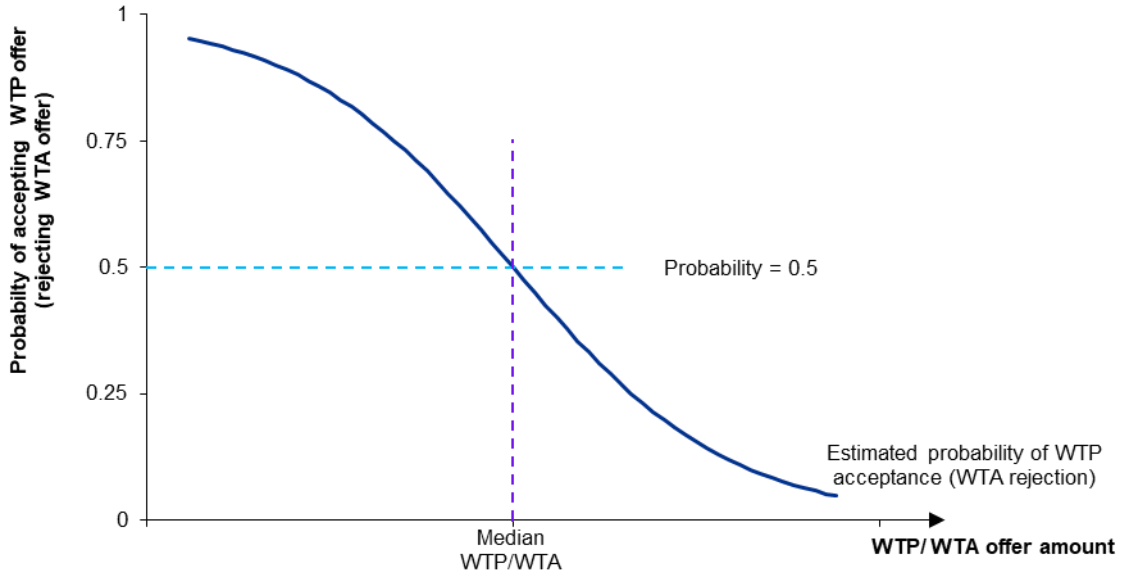
– In addition, where the respondent had provided a free-text 'other' reason, these reasons were manually sorted to identify any protest or invalid responses.

WTP and WTA value estimation:

The double-bounded dichotomous choice estimation was undertaken using the DCchoice package[238,239,240] in the R programming language.[241]

The DCchoice package provides a range of functions for analysing dichotomous choice contingent valuation data including double-bounded dichotomous choice contingent valuation data. To analyse the data the included dbchoice function from the DCchoice package was used, which applied a utility difference approach. A log transformation was applied on the presented WTP/ WTA values (see Table 35), and for the WTA survey responses the responses (acceptance or rejection) were inverted to convert the data into the required WTP format.

Figure 21: Illustrative log-likelihood curve for utility difference WTP/ WTA estimation



Source KPMG analysis
Note This figure is for illustrative purposes only and does not use real data. It is intended to provide a simplified example to assist with understanding of the utility difference method for estimating median WTP/ WTA.

The utility difference approach estimates the probability of accepting/ rejecting an amount presented, and calculates the median WTP/ WTA amount as the offer amount associated with a 50% probability of accepting/ rejecting the offer (see Figure 21). This is estimated econometrically with a number of additional explanatory variables included (in addition to the log transform of the offer amount). The additional explanatory variables included were the gender, age band and household income band of the respondents.

[238] Aizaki H, Nakatani T, Sato K, Fogarty J (2022). R package DCchoice for dichotomous choice contingent valuation: a contribution to open scientific software and its impact. Japanese Journal of Statistics and Data Science. 5:871-884. DOI.
[239] Aizaki H, Nakatani T, Sato K (2014). Stated Preference Methods Using R. CRC Press. DOI.
[240] Tomoaki Nakatani, Hideo Aizaki, Kazuo Sato (2023). DCchoice: An R Package for Analyzing Dichotomous Choice Contingent Valuation Data. R package version 0.2.0.
[241] R Core Team (2023) R: A Language and Environment for Statistical Computing _. R Foundation for Statistical Computing, Vienna, Austria.

In order to extract weighted results and reduce the bias due to the exclusion of protest/ invalid responses, the estimated coefficients generated by the dbchoice function were applied to the explanatory variables of the full WTP and WTA samples. A weighted mean was then taken of the resulting estimated median WTP/ WTA values from the full sample of those who answered a WTP/ WTA question (including those providing protest and invalid responses).

Appendix 2 Literature Review

As part of the research a literature review was undertaken by UCL Consultants Ltd. led by Professor Madeline Carr, and Chloé Colomer, UCL Department of Computer Science. The literature review was designed to:

- identify and summarise the existing evidence on the consumer harms from cyber attacks resulting in the loss of goods and services; and
- gather evidence and insights to inform the development of the impact maps setting out the impacts on consumers from cyber attacks resulting in the loss of goods and services.

A2.1 Context of the literature review

This review aims to synthesise evidence on the economic harms caused by cyber attacks, focusing on consumers experiencing disruptions to goods and services across the UK in the five sectors in scope of this study (financial services, health care, creative industries and arts, manufacturing and real estate and renting). Therefore, the primary overarching research question for this study is: What are the economic impacts of cyber attacks on consumers as a result of the loss of access to goods and services, across different sectors, and how do these impacts vary by sector characteristics?

In addition, the study focuses on the following supplementary research questions:

1. What are the direct economic impacts on consumers when access to goods or services is disrupted by a cyber attack? And how do consumers respond to the loss of goods or services?
2. What differences exist in the economic impacts on consumers across sectors when access to goods and services is disrupted by cyber attacks?
3. What variations exist in these impacts based on consumer characteristics (e.g. income, geographic location, and demographic factors)?
4. What do national security experts say about the potential impacts of AI on the nature and severity of cyber attacks and consumer disruptions?

A2.2 Approach to conducting the literature review

To answer the research questions, a dual approach was adopted to explore the economic impacts of cyber attacks on consumers.

1. A systematic literature search: The first approach involved a systematic literature review, which followed a search protocol outlined below, aiming to gather evidence from peer-reviewed academic sources.
2. A focused search: The second approach focused on a detailed examination of grey literature and news reports. It prioritised the most relevant case studies and policy documents to understand the effects on consumers when they lose access to goods and services (e.g. reports from consumers).

The approach and literature review protocol were agreed with DSIT at the start of the study. Each strategy was designed to complement the other and cover a range of supporting evidence as detailed in Table 37.

Table 37: Literature search protocol

	Systematic literature search	Focused search
Search terms/ case studies analysis	(“cyber incident*” OR “cyber attack*” OR “cyber-attack*” OR “cyberattack*” OR “ransomware” OR “ddos” OR “denial of services” OR “malware”) AND ("consumer impact*" OR "direct consumer loss*" OR "financial harm" OR "financial loss*" OR “access disruption" OR "loss of access to services" OR "service disruption*" OR “consumer reaction*”) AND (“financial service*” OR “bank*” OR “insurance” OR “healthcare” OR “NHS” OR “hospital” OR “manufacturing” OR “critical infrastructures” OR “real estate” OR “renting” OR “streaming” OR “online ticket*” OR “librar*” OR “pharmaceutical*”)	the health care sector will be explored through ransomware attacks on major hospitals and GP practices; the financial services sector will be assessed through the exploration of online banking and motor insurance; for the real estate and renting, it will be focused in considering how cyber attacks may impact property purchases and renting including conveyancing (e.g. cases like the Foxtons breach and Hackney Council sales issues); the creative industries and arts, such as the cyber attack on the British Library (British Library's blog and the British library Annual Report and Accounts 2023/24 included) and streaming platform incidents (e.g. Disney); and manufacturing insights will come from ransomware cases involving US oil companies (e.g. 2021 Colonial pipeline attack), and pharmaceuticals.
Databases	Web of Science, ACM Digital Lib, IEEE Xplore, Scopus, Google Scholar	Nexis (Nexis Uni, regional and international news sources (including The Guardian, NYT, Financial times), legal publications, and specialised collections covering business and industry-specific insights) and Google news
Type of literature included	Academic	Grey (policy, institutional, governmental, thinktank or industrial reports) and news reports.
Total screened (including duplicates)	300+	1,000+
Total included	16 (including the covid sources)	33 (including the covid sources)

The selection process prioritised:

- Topic relevance: with a focus on studies that discussed the direct impacts of cyber attacks on consumers resulting from the loss of access to goods and services.
- Sector relevance: with a focus on studies about the five sectors of interest in this study (financial services, health care, creative industries and arts, manufacturing and real estate and renting).
- Recency: the most recent publications, to ensure the inclusion of recent and contextually relevant findings, only publications from 2019 onwards were considered.
- Language: all sources were limited to English to maintain consistency in interpretation and analysis.
- Quality: for academic literature, only peer-reviewed papers were considered.

Any study focusing solely on indirect impacts, such as organisational financial losses, without addressing consumer consequences were excluded. Publications that fell outside the specified date range or were unrelated to the specific sectors outlined (financial services, health care, creative industries and arts, manufacturing and real estate and renting) in the research focus were also excluded.

Inclusion of covid-19 sources

In the early stages of implementing the systematic search of academic literature, it became clear that most of the existing studies primarily focused on the impacts of cyber attacks on organisations, such

as financial losses and cyber security investments. Overall, it seemed that academic studies failed to directly address how disruptions in accessing goods and services affect consumers during and after a cyber attack. Recognising this gap, the research methodology was amended to expand the searches (with search terms ("covid*" AND ("loss of access to good*" OR "loss of access to service*")) on Google Scholar) to include academic literature and grey literature that were relevant to the COVID-19 pandemic. This decision was based on the assumption that as during the COVID-19 period consumers had lost or reduced access to a range of goods and services this could serve as a useful proxy for understanding the potential consequences of cyber attacks that also result in the loss of access to goods and services on consumers. By drawing parallels to the disruptions experienced by consumers during cyber attacks and the pandemic, insights could be gained into how consumers could be similarly affected by cyber attacks which disrupt access to goods and services.

A2.3 Overview of Key Findings

A2.3.1 Availability of literature

The review included 16 academic sources and 33 grey literature and news reports. The literature seemed to have a strong focus on the financial services and health care sectors, with an emphasis on the cyber attacks targeting companies or institutions in the United States (US). While the review tried to focus on cyber attacks in the UK, the US's status as one of the most frequently targeted countries in terms of cyber incident volume and associated costs could explain why many of the references focused on the US.[242] Alternatively, the prominence of US-focused studies might stem from the country's regulatory environment, which mandates detailed reporting of some cyber incidents. Laws such as HIPAA (Health Insurance Portability and Accountability Act) for the health sector, the Gramm-Leach-Bliley Act for the financial sector, and Securities and Exchange Commission (SEC) regulations for publicly traded companies require firms to disclose cyber attacks. The availability of detailed data on cyber attacks in the US, particularly in the financial services and health care sectors, may explain why the literature disproportionately highlights these industries and this geographic context.

A2.3.2 First-Order economic impacts

The literature review identifies the first-order impacts (i.e. the direct consequences) of cyber attacks on consumers through two distinct yet interconnected dimensions: direct impacts and consumer reactions.

- Direct impacts: The first dimension focuses on what consumers lose access to and the direct impacts that result from it. This includes the immediate consequences of a cyber attack, such as the inability to access goods or services. For instance, consumers may lose access to online banking systems, preventing them from making payments or withdrawing cash. These direct impacts capture the scope and scale of how consumers are affected by the loss of access to goods and services due to a cyber attack.
- Consumer reactions: The second dimension examines how consumers react to the loss of access, focusing on their behavioural responses. When faced with disruptions, consumers may respond by seeking alternatives, such as shifting to offline providers, reducing consumption, or postponing purchases. These responses are shaped by the availability of alternatives, the urgency of consumer needs, and their socioeconomic circumstances, with those in more vulnerable situations often withstanding the disruptions.

By considering both the direct impacts of what is lost and the behavioural responses to these losses, this framework provides an understanding of the first-order impacts of cyber attacks.

Table 38 summarises the direct impacts and consumer responses discussed in the literature for each sector within scope.

[242] 'Cost of a data breach 2024 | IBM'. Accessed: Jan. 07, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach

Table 38 - Summary of direct impacts and consumer responses

Sectors	Direct impacts	Consumer reactions
Health care	Unable to access medical diagnosis, delayed appointments, prescriptions or ambulances.	Seeking alternative in the private health care sector or unaffected areas, waiting for resolution.
Financial services	Inaccessible electronic transfers, direct deposits, no access to online balance inquiries and bill payments.	Cash withdrawals, switching banks and in-person visits.
Real estate and renting	Delays or inaccessible housing registers and allocations, land searches for property purchases delayed, council tax and business rates inaccessible.	Resorting to manual processes or waiting for council systems to be restored, financial losses due to delays.
Creative industries and arts	Inaccessible digital collections, inability to view exhibitions online.	Frustration over delays, seeking alternative platforms where possible, reduced access to cultural resources.
Manufacturing	Supply chain disruptions, production halts, delayed delivery of medications, leakage of personal identifiers data.	Worries about misuse of leaked data, rationing supplies, increased financial and health concerns over shortages.

A2.3.3 Variability in consumer impacts and response

The literature suggests that the impact on consumers of a loss of access to goods or services depends on various factors including the consumer's purpose for using the goods or services, the sector in which the disruption occurs, geographic factors, and the affected consumer group.

The literature review suggests that when consumers lose access to goods or services, the consequences of that loss vary depending on several factors, including the consumer's purpose for using the service and the resources available to them. For instance, the temporary inaccessibility of the British Library's catalogue impacted consumers differently based on their needs. Scholars or students using the catalogue for academic research encountered disruptions to their work and frustration, whereas those using it for leisure may have been annoyed by the inconvenience. Scholars with access to alternative resources through their universities, for example, could redirect their efforts to other catalogues, but this ability would be contingent on the support and resources provided by their institutions.

The specific impacts also depend on the sector the disrupted service belongs to, the needs it addresses, and the scale of the disruption. For example, a study on hospital cyber attacks highlighted how rural and urban patients were affected differently by care disruptions. Patients in rural areas faced travel times averaging 33 minutes to reach unaffected hospitals, compared to just nine minutes for urban patients.[243] These extended travel times delayed access to emergency care, and increased financial and emotional burdens on rural patients and their families.

These disparities are not limited to geographic factors but extend to the type of service disrupted and the consumer group affected. During the Hackney Council cyber attack, residents depending on council services for housing accommodations were impacted differently than individuals attempting to buy or sell property who faced delays of the land search services. These varied impacts demonstrate that the consequences of cyber attacks are multifaceted, influenced by the nature of the service disrupted, and the resources and resilience of the affected consumer groups.

Ultimately, the review found that the impacts of cyber attacks for consumers are shaped by a web of factors:

- what services are disrupted,
- in which sector,

[243] C. C. McGlave, H. Neprash, and S. Nikpay, 'Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients', Oct. 04, 2023, Social Science Research Network, Rochester, NY: 4579292. doi: 10.2139/ssrn.4579292.

- for whose needs,
- at what scale, and
- with which agency consumers can respond (i.e. the ability of consumers to respond).

The variability in consumer impacts is discussed in further detail within the findings presented below on the consumer impacts from cyber attacks in each sector.

A2.4 Sector-specific consumer impacts

The impacts on consumers of cyber attacks resulting in the loss of goods and services vary based on consumer characteristics, the type and scale of the cyber attack, and the targeted sector. The findings are organised by sector, to illustrate what the literature shows in relation to the diverse types of cyber attacks, provide concrete case studies, and present the available evidence of how these incidents affected consumers to answer the research questions.

In the next section, each sector is explored blending academic and grey literature, and news to provide a cross-referenced overview of the findings in the following order:

1. Specifics of the sector explored in the review
2. Types of cyber attacks
3. Impact of disruptions and consumer responses (including differences between consumer groups)

Each section is deepened with one or multiple case studies drawing from academic evidence supported by news and grey literature as set out in the table below.

Table 39: Summary of case studies by sector

Sectors	Case studies
Health care	WannaCry (UK), Change Healthcare (US)
Financial services	Patelco Credit Union (US)
Real estate and renting	Hackney council (UK)
Creative industries and arts	British Library (UK)
Manufacturing	Cencora (US)

A2.4.1 Health care

Hospitals, GP practices and other health care services

The literature review found that the health care sector's reliance on interconnected digital systems makes it vulnerable to cyber attacks. These may include disruptions that could cascade across critical care, diagnostics, and ongoing treatments. Former attacks directly impacted patient outcomes, delayed essential services, and strained public resources.

A recent example of such disturbance is the ransomware attack on Synnovis, a pathology service provider for NHS trusts in London, which disrupted diagnostics and health care delivery. Between the 10 June and 16 June 2024, BBC News reports over 1,294 outpatient appointments and 320 planned operations were postponed at King's College Hospital and Guy's and St Thomas' NHS Foundation Trusts.[244] Patients experienced delays in care, including for routine blood tests relied upon by GP practices, leaving thousands with unresolved conditions for weeks. The attack on a single pathology provider cascaded into widespread delays across hospitals and GP practices. Answering to the BBC, Prof. Sir Stephen Powis, National Medical Director of NHS England, highlighted the cascading and

[244] Cyber attack on hospitals impacts 1,130 operations in London, BBC News. Accessed: Jan. 07, 2025. [Online].

escalating nature of these threats, “We have invested over £350bn centrally in the NHS in cyber security since 2017 and of course we have strict standards that we expect suppliers to the NHS to meet in terms of cyber security - but these threats are increasing all the time”.[245] The Synnovis cyber attack, stresses how interconnected the UK's health care system is, including the NHS and its broader supply chain.

Types of cyber attacks

A range of cyber attacks have been shown to have an impact on the provision of health care services including ransomware attacks, data breaches and attacks targeting sub-contractors, such as pathology services or insurance companies.

Studies have examined ransomware attacks on hospitals, particularly in the US, analysing their impact on patients across different demographics. Neprash et al. (2024) examined ransomware events between 2016 to 2021 using data from the Tracking Healthcare Ransomware Events and Traits database, combined with American Hospital Association surveys and Medicare fee-for-service claims.[246] Their research suggests that ransomware attacks on hospitals disrupt operations in both rural and urban hospitals. While the scale of disruption was similar across these settings, rural patients faced exacerbated challenges. Patients in rural areas had to travel greater distances to access alternative care. In the US, Claire McGlave and her colleagues found that ransomware attacks typically decreased hospital service volume by 17 to 26 percent during the first week of an attack,[247] with recovery taking up to three weeks. The study also reported that among patients already admitted when a ransomware attack begins, in-hospital mortality increases by 35 to 41%.

The literature also discussed data breaches targeting electronic health records and operational systems. Portela et al. (2023), in a case study on medical data breaches from Portugal hospitals, found that such incidents might compromise access to critical patient information and support systems, delaying essential hospital activities.[248] These breaches could not only endanger patient physical and mental health during the attack but also have profound financial and health consequences after the attack for patients and health practitioners. The financial impact of these breaches is further underscored by IBM’s Cost of a Data Breach Report, which ranks health care as the most costly industry for data breaches globally.[249]

Finally, attacks targeting sub-contractors, such as pathology services or insurance companies, further amplify the disruption. In the UK, the Synnovis attack on a pathology service provider for NHS trusts in London, highlighted the cascading impacts such incidents have on consumers and the broader health care system. Similarly, the attack on the health insurance provider Change Healthcare in the US disrupted claims processing and prescription refills.[250] Many patients were unable to refill medications without paying out-of-pocket or faced delays in receiving necessary treatments for weeks.

Impacts on consumers and responses

The impact on consumers of cyber attacks on health care providers varies depending on the scale and duration of the attack, as well as the type of care patients were receiving at the time.

---

[245] Cyber attacks on London’s hospitals continue to disrupt services, BBC News. Accessed: Jan. 07, 2025. [Online].
[246] H. T. Neprash, C. C. McGlave, K. Rydberg, and C. Henning-Smith, ‘What happens to rural hospitals during a ransomware attack? Evidence from Medicare data’, The Journal of Rural Health, vol. 40, no. 4, pp. 728–737, 2024, doi: 10.1111/jrh.12834.
[247] Ibid
[248] D. Portela, D. Nogueira-Leite, R. Almeida, and R. Cruz-Correia, ‘Economic Impact of a Hospital Cyberattack in a National Health System: Descriptive Case Study’, JMIR Formative Research, vol. 7, no. 1, p. e41738, Jun. 2023, doi: 10.2196/41738.
[249] Cost of a data breach 2024 | IBM. Accessed: Jan. 07, 2025. [Online]. Available:
[250] M. Cimons, M. Beard, and T. Amenabar, How a health-care cyberattack may affect your prescription drug access, Washington Post, Mar. 05, 2024. Accessed: Jan. 07, 2025. [Online].

Across reports and studies, patients frequently reported delays in accessing essential services (e.g. surgery, blood tests, prescriptions etc.), often with serious consequences for their health and well-being. In some cases, thousands of appointments were cancelled or postponed, with rescheduling taking weeks. Pathology backlogs heightened risks for chronic patients reliant on routine bloodwork, as delays in monitoring and managing critical conditions left them vulnerable. News articles also discussed the psychological toll of these disruptions, reporting it as distressing for patients, especially those requiring urgent care such as chemotherapy or organ transplants. During the Synnovis cyber attack in the UK, 46 organs were diverted to other NHS Trusts in the second week following the attack, compared to just 18 in the first week.[251]

An analysis by The Royal United Services Institute (RUSI), an independent think tank engaged in cutting-edge research on defence, security and international affairs, also draws attention to indirect effects, such as the strain on administrative and medical staff caused by ransomware disruptions.[252] When patient records and scheduling systems are rendered inaccessible, as occurred during the attack on Advanced, an IT provider for the NHS, staff must revert to manual processes. They note that this increased workload not only delays care but also erodes patient confidence in the health care system's ability to deliver reliable services. Patients' trust in public institutions can suffer long-term damage as a result.

When faced with disruptions caused by cyber attacks, the literature indicates that patients adapted in various ways, though often at personal cost. In the US, some patients sought care from private health care providers to avoid delays, incurring substantial out-of-pocket expenses, while others delayed or entirely avoided treatments, placing their health at further risk.[253] But as face-to-face appointments are still a critical aspect of health care for many patients, disruptions to localised services disproportionately affected those in remote or underserved areas, including limiting their agency to respond to the impact. A study by McGlave et al. (2023) found differences in the impact on patients in rural vs. urban areas, with patients in rural areas having to travel 33 minutes on average to reach unaffected hospitals, compared to just nine minutes for patients in urban areas.[254] These extended travel times not only delayed access to emergency and elective care but also increased the financial and emotional burden on patients and their families.

Case Studies: WannaCry and Change Healthcare Attacks

Case Study: WannaCry attack (UK) – 2017

The WannaCry ransomware attack in May 2017 disrupted health care services across 48 NHS hospital trusts, halting critical systems and leaving patients vulnerable to delayed and cancelled care. Exploiting unpatched Windows systems, the attack encrypted data and halted the operations of services with direct impacts on patients including, the inability to access automated systems crucial to the delivery of diagnostics, treatments, and emergency services.

A white paper from Goswami et al. (2025) discussing the WannaCry incident found it targeted critical medical devices, such as the Bayer Medrad device used for MRI scans.[255] This interruption delayed imaging necessary for accurate diagnoses and treatment planning. The investigation of the WannaCry effects by the National Audit Office established that the WannaCry attack disrupted NHS systems across all of England with at least 80 out of the 236 trusts across the country affected. Between 12 May and 18 May 2017, NHS England estimated the total number of cancelled

[251] Cyber attack on hospitals impacts 1,130 operations in London, BBC News. Accessed: Jan. 07, 2025. [Online].
[252] Beyond the Bottom Line: The Societal Impact of Ransomware. Accessed: Jan. 07, 2025. [Online].
[253] M. Bohannon, Change Healthcare Cyberattack Disrupts Services Nationwide—Here's What To Know, Forbes. Accessed: Jan. 07, 2025. [Online].
[254] Ibid
[255] A. Goswami, A. Baveja, B. Melamed, and F. Roberts, Prevention and Mitigation of Disruptions in Medical Device Supply Chains: A Policy Perspective, Journal of Science Policy & Governance, 2024, Accessed: Jan. 07, 2025. [Online].

appointments as being around 19,494 with 139 urgent cancer referrals cancelled, and ambulances diverted to other hospitals, delaying emergency response times and access to critical care.[256]

More localised and detailed impacts for patients have been reported in NHS England's case study on County Durham and Darlington NHS Foundation Trust (CDDFT) which noted multiple patient-level impacts:[257]

- Ambulance handover systems were disabled, leading to delays in transferring critical information about incoming patients.
- The patient transport service booking portal was not available.
- Transfers of CT and MRI scans were inaccessible, resulting in the manual transfer of images via DVDs, which delayed diagnoses.
- Chemo Care systems were inaccessible forcing chemotherapy orders to be processed manually and faxed, further delaying critical cancer treatments.
- Automated blood test result transfers failed, leaving GPs unable to access their caseloads or process results efficiently.

For patients reliant on timely diagnostic testing or ongoing treatment plans, these delays introduced health risks.

Case Study: Change Healthcare Attack (US) – 2024

The February 2024 ransomware attack on Change Healthcare, a division of the UnitedHealth Group (US health insurer), offers a good proxy to understand the consequences of cyber attacks on health care systems and their patients. The incident, widely regarded as one of the most significant cyber attacks in US health care history, exposed vulnerabilities in the interconnected health care infrastructure. Although the US and UK health care systems differ, particularly in the role of insurance companies (with health insurance being the primary way through which health care is accessed in the US, compared to the UK where health care is primarily accessed through the NHS), the widely documented Change Healthcare attack has been included in the literature review because it provides valuable insights into consumer reactions to disruptions in prescription services and broader health care system shutdowns.

At that time, Change Healthcare processed a third of all US health care claims, handling approximately 15 billion transactions annually. The attack paralysed this clearinghouse, leaving hospitals, medical offices, and pharmacies unable to process claims, verify insurance, or collect payments. Over 77% of respondents to an American Medical Association survey reported ongoing service disruptions more than a month after the attack.[258,259] Key functionalities, including claim submissions, patient eligibility verification, and electronic prescribing, remained impaired, forcing providers to implement time-consuming and costly manual workarounds. For smaller practices, these workarounds were particularly burdensome, as they struggled to allocate already stretched resources to resolve operational delays.

For consumers, the attack disrupted access to essential health care services. Patients faced delays in filling prescriptions, with some paying cash for expensive medications due to the inability to process insurance claims. Others were unable to access pharmaceutical discount coupons or verify insurance coverage for necessary treatments.[260] The AMA survey found that some patients could not access cost and coverage information, while some faced delays in receiving prescriptions. Beyond immediate disruptions, the attack raised concerns about the long-term exposure of patient data. Change

[256] National Audit Office, Investigation: WannaCry Cyber Attack and the NHS. Report by the Comptroller and Auditor General, 2018. Accessed: Jan. 07, 2025. [Online].
[257] N. H. S. England, NHS England » NHS England business continuity management toolkit case study: WannaCry attack. Accessed: Jan. 07, 2025. [Online].
[258] American Medical Association, Change healthcare survey results, 2024. Accessed: Jan. 07, 2025. [Online].
[259] American Medical association, 'Change Healthcare cyberattack impact: Key takeaways from informal AMA follow-up survey', 2024.
[260] K. B. and J. Burns, The impact of the Change Healthcare cyberattack: What to know, Association of Health Care Journalists. Accessed: Jan. 07, 2025. [Online].

Healthcare's systems, which connect patient visits, diagnoses, and treatments to insurers for payment processing, hold sensitive medical histories. Experts warn medical records pose a substantial risk to affected patients, as stolen data can be exploited for scams or sold to other criminal groups.[261]

Both the WannaCry and the Change Healthcare attacks reveal how cyber attacks disrupt critical services, create cascading financial challenges for patients and providers, and amplify systemic vulnerabilities.

A2.4.2 Financial Services

Banks and financial services

The financial sector is one of the most targeted industries for cyber attacks. The scale of cyber risk has grown so much that the International Monetary Fund dedicated the third chapter of its 2024 Global Financial Stability Report to cyber risk. They found nearly one-fifth of all reported cyber incidents target financial firms, with attacks like ransomware nearly doubling since the COVID-19 pandemic.[262] While the average financial loss from such incidents is around $0.5m for the affected organisation, the risk of extreme losses exceeding $2.5bn is rising, particularly due to the financial sector's technological and institutional interconnectedness. Severe incidents could trigger cascading disruptions, undermining confidence in financial systems and destabilising other institutions.

Types of cyber attacks

The attacks discussed in the literature included phishing, ransomware and data breach incidents, and intrusions.

Ransomware attacks have emerged as a critical challenge for the financial services sector, as illustrated by the 2024 (US based) Patelco Credit Union case.[263] This attack shut down online banking for Patelco's members and rendered them unable to access their accounts for activity like viewing their balances, making electronic transfers and scheduling new online bill payments. Queues at branches grew as customers sought limited cash withdrawals, while delayed transactions led to financial anxieties, including the risk of overdraft penalties and missed payments. The NCUA Cybersecurity and Credit Union System Resilience Report highlights another dimension: the role of third-party service providers.[264] A ransomware attack on a third-party provider in 2023 disrupted operations across 60 small credit unions in the US, illustrating how attacks on supply chains amplify vulnerabilities across the entire systems.

In 2021, the Hiscox Cyber Readiness survey of 300 Irish companies found that 43% of Irish firms reported at least one cyber attack, with the financial services sector among the most attractive targets for cyber-attackers as criminals steal sensitive data that can be used to open fake accounts.[265] Successful ransomware attacks often stem from phishing campaigns, with one study finding that 65% of ransomware attacks stemmed from phishing.[266] Beyond immediate financial losses, these attacks result in reputational damage, reduced consumer confidence, and prolonged recovery times for affected institutions.

Data breaches represent another major threat. The IBM Cost of Data Breach Report highlights that financial services face some of the highest costs when breached globally.[267] Such breaches have

[261] Ibid
[262] International Monetary Fund, The Last Mile: Financial Vulnerabilities and Risks, 2024. Accessed: Jan. 08, 2025. [Online].
[263] J. Flores, Massive Patelco cyberattack is still affecting half a million people. Here's how to protect yourself, San Francisco Chronicle. Accessed: Jan. 08, 2025. [Online].
[264] National Credit Union Association, Cybersecurity and Credit Union System Resilience Annual Report to Congress, 2024. Accessed: Jan. 08, 2025. [Online].
[265] Grant Thornton, The economic cost of cybercrime, Ireland, 2021. Accessed: Jan. 08, 2025. [Online].
[266] Ibid
[267] Ibid

exposed sensitive customer information, leading to identity theft and fraud. For instance, during an attack on a global payment system, transactions were delayed, and consumer trust was eroded.

Impacts on consumers and responses

As for all sectors, for consumers, the impacts of cyber attacks targeting financial services vary depending on the type, scale, and duration of the attack. Across studies, customers frequently report challenges such as the inability to access funds, compromised personal information, and loss of trust in digital banking platforms.

As highlighted in the case of the Patelco Credit Union attack in 2024, customers were unable to access basic banking services, including checking account balances, making transfers, and scheduling payments.[268] Many customers faced delays in critical financial obligations, such as paying bills, risking penalties and credit score damage. Withdrawal limits exacerbated the frustration felt by affected members who had to visit branches repeatedly throughout the two-week outage. The impact of data breaches on consumers is also discussed in the literature, with a focus on cybercriminals who may use stolen information to perpetrate identity theft, phishing attacks, and fraudulent activities.[269] Victims of such breaches may experience financial losses and endure lengthy processes to recover their compromised accounts. Incidents like data breaches or ransomware attacks often leave consumers feeling anxious and vulnerable. As Ali et al. (2017) noted, the fear of losing sensitive financial data leads many consumers to reduce their use of online banking services, or abandon them entirely, eroding trust in digital financial platforms.[270] Consumers' trust in financial institutions is further undermined when institutions fail to provide timely responses or transparency about the scope of an attack. The long-term erosion of trust in such cases often leads customers to consider switching to competitors, despite the acknowledgment that no system is completely secure.

In response to cyber attacks on the financial sectors, consumers adopt various response strategies. Some consumers switch to alternative financial institutions, though this process can involve fees, lost access to previous banking tools, and disruptions to automated payments.[271] Others attempt to adapt by using traditional banking methods, such as in-person visits and paper checks, despite the inconvenience.[272]

Case Study: Patelco Credit Union (US) – 2024

The ransomware attack on Patelco Credit Union in June 2024 illustrates the severe disruptions that cyber attacks can cause within the financial sector. Although the US and UK financial systems differ, the Patelco Credit Union attack offers insights into consumer reactions to banking shutdowns. As one of Northern California's largest credit unions, serving 500,000 members and managing nearly $10 billion in assets, Patelco's incident not only highlighted the vulnerabilities of financial institutions but also underscored the cascading effects of such disruptions on consumers and the broader financial system.[273] The attack occurred on June 29, 2024, and forced Patelco to shut down several core systems, including its online banking platform, mobile application, and call centre services. This outage left customers unable to perform essential financial transactions including:[274]

- electronic transfers,

[268] J. Flores, Massive Patelco cyberattack is still affecting half a million people. Here's how to protect yourself, San Francisco Chronicle. Accessed: Jan. 08, 2025. [Online].
[269] L. Ali, F. Ali, P. Surendran, and T. Bindhya, 'The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services', IJEEEE, vol. Volume 7 Number 1, 2017, doi: 10.17706/IJEEEE.
[270] Ibid
[271] L. Ali, F. Ali, P. Surendran, and T. Bindhya, 'The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services', IJEEEE, vol. Volume 7 Number 1, 2017, doi: 10.17706/IJEEEE.
[272] J. Flores, Massive Patelco cyberattack is still affecting half a million people. Here's how to protect yourself, San Francisco Chronicle. Accessed: Jan. 08, 2025. [Online].
[273] More Than a Million People Affected by Patelco Credit Union's Data Breach, cutimes.com. Accessed: Jan. 08, 2025. [Online].
[274] I. Arghire, Patelco Credit Union Scrambling to Restore Systems Following Ransomware Attack, SecurityWeek. Accessed: Jan. 08, 2025. [Online].

- direct deposits,
- balance inquiries, and
- bill payments.

While cash withdrawals at ATMs remained operational, consumers experienced intermittent outages at Patelco ATMs.

The attack caused disruptions to Patelco's customers.[275] Many were unable to meet financial obligations, such as paying bills or initiating transfers, resulting in late fees and overdraft penalties, although the credit union later committed to reimburse these costs. Despite these assurances, the outage created financial anxiety among consumers who relied on Patelco's systems for their day-to-day financial needs. Long lines at Patelco branches started to show as members sought to withdraw cash or inquire about their accounts. Customers reported making multiple trips to physical locations due to the lack of online access. Customers expressed their trust in Patelco was shaken given the uncertainty about how their accounts and financial data had been affected, with some considering switching to other financial institutions.

The Patelco incident exposes systemic vulnerabilities within the financial sector, particularly affecting mid-sized institutions like credit unions.

A2.4.3 Real estate and renting

Local authorities and housing services

In the UK, local authority councils facilitate housing services. They do so by relying on digital platforms for managing housing registers, rental agreements, and service requests. For instance, the ransomware attack on Hackney Council in October 2020 caused long-term disruption, affecting housing benefit claims, council tax payments, and property transactions. The fallout from such attacks illustrates how cyber disruptions within local government services cascade into widespread challenges for consumers, exacerbating housing insecurity.[276,277]

Types of cyber attacks

There was significantly less literature on cyber attacks on the housing sector than on the health and financial services sectors. The literature that does focus on the role of local authorities in housing highlights ransomware attacks, data breaches, or phishing scams.

Ransomware attacks have in some cases, such as on Hackney Council in 2020, rendered local authority property transaction systems inaccessible for months, disrupting essential housing operations.[278] Third-party software exploitation has also been discussed in the literature as doing damages. Some local councils rely on third-party providers for IT systems, making them vulnerable to software supply chain attacks. In 2024, the housing software provider Locata was compromised in a cyber attack, leading to disruptions across Greater Manchester councils, including Manchester, Salford, and Bolton.[279,280] These disruptions affected public-facing websites like Manchester Move and Salford Home Search, which are critical for managing housing applications. In some cases, the disruption also included unauthorised access to sensitive resident data. For instance, the August

[275] C. Castañeda, Patelco Credit Union ransomware attack halts banking services for nearly half a million members - CBS San Francisco. Accessed: Jan. 08, 2025. [Online].
[276] Information Commissioner's Office, Iboh updated reprimand with redactions, 2024. Accessed: Jan. 08, 2025. [Online].
[277] Hackney Council, 'Services available, but not back to normal – devastating impact of cyberattack one year on. Accessed: Jan. 08, 2025. [Online]
[278] Ibid
[279] Greater Manchester cyber scam leaves thousands vulnerable, BBC News. Accessed: Jan. 08, 2025. [Online].
[280] BBC News, Salford housing register still down weeks after cyber attack, Aug. 28, 2024. Accessed: Jan. 08, 2025. [Online].

2024 breach of Salford Home Search compromised personal data of over 5,200 residents, leaving them vulnerable to phishing scams.[281]

Impact on consumers and their reactions

Cyber attacks on local authority housing services directly affect residents, particularly those in vulnerable situations. The impacts include delays in accessing housing, financial losses, and heightened psychological stress.

Residents' dependent on housing registers to secure permanent accommodation faced delays in some cases. In Salford, residents were unable to access housing registers for several weeks,[282] leaving many in temporary housing arrangements. The Information Commissioner's Office report investigating the Hackney Council attack noted that over 280,000 individuals were affected, with delays in benefits and housing waiting lists disproportionately impacting vulnerable residents, such as those in temporary accommodation.[283]

Consumers also faced added costs due to service interruptions. For example, in Hackney, prospective homebuyers could not complete transactions because of delays in land search services, incurring financial losses.[284] As for other sectors, cyber attacks erode consumer confidence in local government services. Hackney Mayor Philip Glanville acknowledged this challenge, noting the need to rebuild public trust in council systems.[285]

In response to these disruptions, consumers employed response strategies such as pursuing private housing options at higher costs or delaying housing applications altogether. However, for vulnerable populations, these alternatives were often unfeasible, exacerbating their housing instability.

Case Study: Hackney Council

The ransomware attack on Hackney Council in October 2020 disrupted key digital systems, forcing Hackney to rely on manual processes for months and leaving residents struggling to access housing services. While the Council prioritised restoring its most urgent services, the fallout from the attack lingered for more than a year, impacting residents and businesses alike.[286] The cyber attack on Hackney Council was covered in the news and investigated by the ICO and therefore offers insights on the impacts for consumers.

Hackney Council fell victim to an attack that encrypted sensitive files and disrupted essential IT systems. The malicious actor was able to access and encrypt the personal data, including special category data, contained within 440,000 individual files across a range of systems, relating to at least 280,000 residents of the London Borough of Hackney and other individuals including staff.[287,288] The attack's severity disrupted digital services used by residents and businesses, including:[289,290]

[281] Greater Manchester cyber scam leaves thousands vulnerable, BBC News. Accessed: Jan. 08, 2025. [Online].
[282] No further detail on the duration of disruption was available.
[283] Ibid
[284] BBC News, Hackney cyber-attack causes collapse of property purchases, BBC, Dec. 12, 2020. Accessed: Jan. 08, 2025. [Online].
[285] Hackney Council, Services available, but not back to normal – devastating impact of cyberattack one year on. Accessed: Jan. 08, 2025. [Online].
[286] Information Commissioner's Office, Iboh updated reprimand with redactions, 2024. Accessed: Jan. 08, 2025. [Online].
[287] Ibid
[288] Hackney Council, Services available, but not back to normal – devastating impact of cyberattack one year on, Accessed: Jan. 08, 2025. [Online].
[289] BBC News, Hackney cyber-attack causes collapse of property purchases, BBC, Dec. 12, 2020. Accessed: Jan. 08, 2025. [Online].
[290] M. Burgess, The Untold Story of a Crippling Ransomware Attack, Wired. Accessed: Jan. 08, 2025. [Online].

- Housing registers and allocations: Residents relying on housing registers faced prolonged delays in securing accommodation. Vulnerable individuals in temporary housing reported hardships.
- Land searches for property purchases: The inability to process land searches disrupted property transactions. Prospective buyers incurred financial losses, including missed opportunities.
- Council tax and business rates: Essential billing systems for council tax and business rates were disrupted, delaying updates and payments.

A year after the attack, Hackney Council had not fully restored its systems, and some services continued to experience delays. On top of that, the pandemic exacerbated the backlogs in critical areas like housing and council tax.

A2.4.4 Creative Industries and Arts

Cultural institutions and digital platforms

The creative industries, which include museums, libraries, performance venues, and digital media platforms (including online ticketing and streaming services), are increasingly reliant on interconnected digital systems for managing collections, delivering services, and engaging audiences through online catalogues. These institutions handle consumer and institutional data while simultaneously facilitating public access to creative and educational resources. Recent incidents, such as the attack on the British Library and the targeting of Ticketmaster expose the vulnerability of the sector to cyber threats.

Types of cyber attacks

While the literature is less abundant than for the health care and financial services sectors, cyber attacks in the creative industries predominantly target systems storing sensitive data, catalogues, and operational tools. Common attack types include ransomware, phishing scams, and breaches through third-party service providers.

The British Library faced a severe ransomware attack in October 2023, which encrypted critical systems and rendered catalogues and special collections inaccessible for months.[291] The literature pointed out that phishing is a major vector in the creative industry. It is an attack vector that is used to gain unauthorised entry to secure systems which can then result in data breaches that jeopardise consumers by exposing them to fraud. An example of this was the 2024 Ticketmaster incident, where hackers accessed sensitive customer information, including encrypted payment details.[292] Literature focusing on creative industries also discussed attacks on third-party software. A notable example was the attack on Gallery Systems in December 2023, where vulnerabilities on a third-party software used by museums and galleries led to disruptions.[293] Institutions such as the Museum of Fine Arts in Boston and the Rubin Museum of Art in New York were unable to display their collections online for a time.[294]

Impacts for consumers and their response

The impact of cyber attacks on consumers and their behaviours in the creative industries varies widely depending on the institution targeted and the services disrupted.

Consumers faced delays to complete shutdowns of services for months in some cases. In the British Library attack, consumers lost access to the main catalogue and special collections for months, disrupting consumers and academic work. While the Library's physical premises remained open,

[291] Museums Association, Cyber security is an urgent priority for the sector, Museums Association. Accessed: Jan. 08, 2025. [Online].
[292] Ticketmaster hack: Customers told to sign up to security service, BBC News. Accessed: Jan. 08, 2025. [Online].
[293] Z. Small, Museum World Hit by Cyberattack on Widely Used Software, The New York Times, Jan. 03, 2024. Accessed: Jan. 08, 2025. [Online].
[294] No further detail on the duration of disruption was available.

research services were severely restricted in the first two months following the attack and remained incomplete in January 2024.[295] Similarly, users of Ticketmaster experienced limited access to event ticketing, while being urged to sign up for identity protection services.[296] These disruptions caused frustration and distress among consumers who rely on these services. Curators and museum staff expressed a sense of helplessness as critical tools remained inaccessible for months following the Gallery Systems attack,[297] while consumers noted the inconvenience of losing access to online collections.

Consumers' ability to adapt to these disruptions varied. For example, the British Library experienced "prolonged outages affecting online catalogues, special collections, and in-person services" following a ransomware attack. Scholars with access to alternative catalogues or resources could redirect their efforts, while others reliant on specific services experienced prolonged setbacks.

Case Study: The British Library

In October 2023, the British Library suffered a ransomware cyber attack. The attack targeted the Library's extensive legacy infrastructure, exfiltrating 600GB of sensitive data and encrypting or destroying critical systems. The attackers released stolen data on the dark web after the Library refused to pay a ransom, further intensifying the challenges.[298] The cyber attack severely disrupted the British Library's services and operations, including:

- Catalogue and collection Access: The main online catalogue became inaccessible, delaying researchers and scholars from accessing resources. A partial version of the catalogue was restored by January 2024.
- Digital collections and research tools: Systems supporting digital collections, e-resources, and databases were offline for months, affecting services such as EthOS (database of UK doctoral research theses) and online journals.
- On-site activities: While the Library's physical premises remained open, many staff were unable to carry out parts of their role or faced increased manual workloads.
- Partnerships: Partnerships (such as with international Foundations) relying on constant access to collections were affected, and digitisation activities were paused, leading to delayed projects and reduced commercial income.
- Public trust and data compromise: Personal and sensitive data of Library users and staff were leaked on the dark web. The Library provided identity protection services to affected individuals.

Consumers faced diverse challenges due to the attack, depending on their reliance on library services:

- Scholars: Lost access to collections and tools, delaying academic work.
- Public and small businesses: Disruption in accessing resources such as the Business and IP Centre.
- Library users: Exposure of personal data led to concerns about privacy and financial fraud.

A2.4.5 Manufacturing

Pharmaceutical and logistics

The manufacturing sector, particularly in pharmaceuticals and logistics, depends on automated systems for production, storage, and distribution. In the pharmaceutical industry, cyber incidents may have cascading effects, disrupting supply chains, halting production lines, and compromising patient

[295] Museums Association, Cyber security is an urgent priority for the sector, Museums Association. Accessed: Jan. 08, 2025. [Online].
[296] Ticketmaster hack: Customers told to sign up to security service, BBC News. Accessed: Jan. 08, 2025. [Online].
[297] Z. Small, Museum World Hit by Cyberattack on Widely Used Software, The New York Times, Jan. 03, 2024. Accessed: Jan. 08, 2025. [Online].
[298] British Library, British library cyber incident review, 2024. Accessed: Jan. 09, 2025. [Online].

care.[299] Automated logistics systems, essential for inventory tracking and order fulfilment, are frequent targets of cyber attacks, with interruptions leading to delays in delivering goods to end-users.

Type of cyber attacks

Cyber attacks targeting the pharmaceutical industry exploit various vulnerabilities, including ransomware, data breaches, and disruptions to automated logistics systems.

A prominent example is the Eisai ransomware attack of 2023, which encrypted critical servers and forced the company to take its logistics systems offline, disrupting operations both domestically in Japan and internationally.[300] Another threat involves data breaches and cyber attacks, as discussed by Schachenhofer et al. (2024), who emphasise the risks these cyber attacks pose to the pharmaceutical sector.[301] Such incidents can expose intellectual property, clinical trial data, and sensitive patient records, endangering patient safety while undermining the competitive advantage, market position, and reputation of affected companies. Additionally, cyber attacks on automated supply chain systems could exacerbate operational vulnerabilities by disrupting production plants, warehouse logistics, and delivery networks. Automated systems for order picking and digital inventory tracking, while critical for efficiency, become vulnerabilities during cyber incidents. For instance, pharmaceutical wholesalers have struggled to maintain inventory control and ensure the timely delivery of medications in the aftermath of such disruptions.[302]

Impact on consumers and their responses

The effects of cyber attacks on the pharmaceutical industry can impact consumers at the end of the supply chain of goods and services. Drug shortages caused by cyber attacks are not immediately recoverable due to regulatory requirements for production and distribution changes. In their study focusing on the pharmaceutical sectors under cyber attack conditions, Schachenhofer et al. (2024) wrote: “For patients, the implications of [drug shortage] can be severe as drug shortages can cause serious harm to the patient's health. They might initiate treatment delays, thereby increasing the period of patient suffering and spurring disease progression.”[303]

Few studies have focused directly on consumer reactions to cyber attacks in the pharmaceutical and wider manufacturing sectors. The literature predominantly examines systemic impacts, such as supply chain disruptions, production halts, and delays in medication availability.

Case Study Cencora 2024

The February 2024 cyber attacks on Cencora Inc. (formerly AmerisourceBergen) exposed the vulnerabilities in the pharmaceutical supply chain. The incident happened in the US, but it was documented sufficiently to help understand the potential impacts of a similar scenario unfolding in the UK.

Cencora is a company partnering with pharmaceutical firms, health care providers, and pharmacies and offers drug distribution, patient support and services, business analytics and technology, and other services. Around 20% of pharmaceutical products sold and distributed in the US are handled by Cencora.[304] The attack targeted Cencora’s network, leading to the exfiltration of both personally

[299] L. Schachenhofer and P. Hirsch, ‘Pharmaceutical Logistics under Cyberattack Conditions’, in Proceedings of the 14th International Defense and Homeland Security Simulation Workshop DHSS, CAL-TEK srl, 2024. doi: 10.46354/i3m.2024.dhss.004.
[300] A. Ribeiro, Ransomware attackers target Japanese pharmaceutical company Eisai, Industrial Cyber. Accessed: Jan. 09, 2025. [Online].
[301] Ibid
[302] M. Crosignani, M. Macchiavelli, and A. F. Silva, ‘Pirates without borders: The propagation of cyberattacks through firms’ supply chains’, Journal of Financial Economics, vol. 147, no. 2, pp. 432–448, Feb. 2023, doi: 10.1016/j.jfineco.2022.12.002.
[303] Ibid
[304] S. Alder, Cencora: Additional Data Exfiltrated in February 2024 Cyberattack, The HIPAA Journal. Accessed: Jan. 07, 2025. [Online].

identifiable information and protected health information. In the process of the Cencora cyber attack, data from at least 27 pharmaceutical and biotechnology companies was compromised, including major names like Pfizer, Johnson & Johnson, Novartis, and AbbVie. Over 250,000 individuals were affected. The breach primarily affected data provided by Cencora's clients for its patient support programs, putting at risk the trust and privacy of both consumers and pharmaceutical companies. While the data breaches in itself did not constitute a loss of service to consumers, part of the service provided to patients is to keep their data safe.

Consumers faced diverse challenges due to the Cencora cyber attack, depending on their reliance on pharmaceutical and patient support services:

- Patients in support programs: The exposure of sensitive data, including health diagnoses and prescription details, raised concerns about privacy and the potential misuse of their information.
- Affected patients: While 24 months of credit monitoring and identity theft protection were offered, fears of identity theft and financial fraud persisted, given the sensitive nature of the compromised data.

A2.5 The role of AI in cyber attacks

The literature on the potential impacts of AI on cyber attacks highlights both opportunities and risks, though much remains speculative because of the nascent stage of this technology's application in malicious activities. As noted by cyber security expert Ben Buchanan, "some of the most potent cyber attacks we have seen– including Stuxnet, the 2016 blackout in Ukraine, and the 2017 attack known as NotPetya that caused at least ten billion dollars in damage – feature some forms of automated propagation and attack capability".[305]

Some experts argue AI could improve cyber security through enhanced predictive analytics, enabling the more accurate and faster identification of threats before they materialise.[306] But it could also be used on the offensive side by attackers. AI-powered attacks are predicted to enhance the scale and sophistication of cyber threats by enabling automated system reconnaissance, generating adaptive malware, and creating highly targeted phishing campaigns.[307,308] These factors mean that AI could make future cyber attacks faster and more likely to be successful.

Despite these concerns, the understanding of the role of AI in cyber attacks remains limited, with current discourse relying heavily on theoretical scenarios and controlled experiments rather than a body of real world case studies. In 2019, in view of the anticipated impact that AI will have in the field of cyber security, researchers at the UK's Alan Turing Institute drafted a socio-technical research roadmap highlighting the range of attack vectors likely to be impacted by AI.[309]

A2.6 Conclusion

This literature has reviewed the economic impacts of cyber attacks on consumers across various sectors. The findings suggest that the impact of cyber attacks on consumers varies depending on several factors, including the nature of the disrupted service, the sector to which it belongs, the needs it fulfils, the scale of the disruption and the agency of consumers to adapt. Most of the evidence in both academic and grey literature focused on the financial services and health care sectors. Across health care, financial services, real estate and renting, creative industries and arts, and

[305] B. Buchanan, 'The Future of AI and Cybersecurity', 2019.
[306] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review, Sep. 01, 2022, Social Science Research Network, Rochester, NY: 4323317. Accessed: Jan. 09, 2025. [Online].
[307] S. M. U. H. Minhaj, 'STUDY OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY AND THE EMERGING THREAT OF AI-DRIVEN CYBER ATTACKS AND CHALLENGE', Jul. 17, 2023, Social Science Research Network, Rochester, NY: 4652028. doi: 10.2139/ssrn.4652028.
[308] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, 'Weaponized AI for cyber attacks', Journal of Information Security and Applications, vol. 57, p. 102722, Mar. 2021, doi: 10.1016/j.jisa.2020.102722.
[309] The Turing Institute, 'AI in Cybersecurity: A socio-Technical Research Roadmap', 2019.

manufacturing, cyber attacks exposed vulnerabilities that affect consumer access to goods and services, often with cascading consequences:

- In health care, cyber attacks have disrupted services like diagnostics, treatments, and routine care, disproportionately affecting vulnerable populations such as rural patients or those relying on time-sensitive medical procedures.
- In financial services, the unavailability of banking systems following cyber attacks leaves consumers unable to access their funds, process payments, or manage their financial commitments, creating psychological and financial distress.
- In the real estate and renting sector, attacks on local government have hindered access to essential housing services or administrative processes impacting consumers by causing delays in accessing housing, financial losses, and heightened psychological stress.
- In the creative industries and arts, cyber attacks have impeded cultural participation and limited consumer access to resources like digital collections.
- In the manufacturing sector, particularly pharmaceuticals, the consequences of cyber attacks on automated supply chains and production systems have included disruption of access to life-saving medications and diagnostic tools, leading to impacts across health care and consumer markets.

Case studies, such as those of WannaCry and the British Library, provide real-world illustrations of how these disruptions unfold, showcasing the vulnerabilities of interconnected systems and the long recovery times required after attacks.

The overarching conclusion is clear: the impact of cyber attacks on consumers depends on a range of factors. The type of service affected plays a big role, as more critical services can lead to more severe consequences. The sector in which the disruption happens influences who is impacted and how they are affected. The specific needs of the consumers relying on the service also shape their experience. The scale of the attack, such as whether it is localised or widespread, further determines the extent of its effects. And finally, how well consumers can respond depends on the resources and alternatives available to them, as well as the support they receive. Together, these factors highlight how varied and complex the impacts of cyber attacks can be for different groups of consumers across different sectors.

A2.7 References for Literature review

[1] ‘Cost of a data breach 2024 | IBM’. Accessed: Jan. 07, 2025. [Online].

[2] C. C. McGlave, H. Neprash, and S. Nikpay, ‘Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients’, Oct. 04, 2023, Social Science Research Network, Rochester, NY: 4579292. doi: 10.2139/ssrn.4579292.

[3] ‘Cyber attack on hospitals impacts 1,130 operations in London’, BBC News. Accessed: Jan. 07, 2025. [Online].

[4] ‘Cyber attacks on London’s hospitals continue to disrupt services’, BBC News. Accessed: Jan. 07, 2025. [Online].

[5] H. T. Neprash, C. C. McGlave, K. Rydberg, and C. Henning-Smith, ‘What happens to rural hospitals during a ransomware attack? Evidence from Medicare data’, The Journal of Rural Health, vol. 40, no. 4, pp. 728–737, 2024, doi: 10.1111/jrh.12834.

[6] D. Portela, D. Nogueira-Leite, R. Almeida, and R. Cruz-Correia, ‘Economic Impact of a Hospital Cyberattack in a National Health System: Descriptive Case Study’, JMIR Formative Research, vol. 7, no. 1, p. e41738, Jun. 2023, doi: 10.2196/41738.

[7] M. Cimons, M. Beard, and T. Amenabar, ‘How a health-care cyberattack may affect your prescription drug access’, Washington Post, Mar. 05, 2024. Accessed: Jan. 07, 2025. [Online].

[8] 'Beyond the Bottom Line: The Societal Impact of Ransomware'. Accessed: Jan. 07, 2025. [Online].

[9] M. Bohannon, 'Change Healthcare Cyberattack Disrupts Services Nationwide—Here's What To Know', Forbes. Accessed: Jan. 07, 2025. [Online].

[10] A. Goswami, A. Baveja, B. Melamed, and F. Roberts, 'Prevention and Mitigation of Disruptions in Medical Device Supply Chains: A Policy Perspective', Journal of Science Policy & Governance, 2024, Accessed: Jan. 07, 2025. [Online].

[11] National Audit Office, 'Investigation: WannaCry Cyber Attack and the NHS. Report by the Comptroller and Auditor General', 2018. Accessed: Jan. 07, 2025. [Online].

[12] N. H. S. England, 'NHS England » NHS England business continuity management toolkit case study: WannaCry attack'. Accessed: Jan. 07, 2025. [Online].

[13] American Medical Association, 'Change healthcare survey results', 2024. Accessed: Jan. 07, 2025. [Online].

[14] American Medical association, 'Change Healthcare cyberattack impact: Key takeaways from informal AMA follow-up survey', 2024.

[15] K. B. and J. Burns, 'The impact of the Change Healthcare cyberattack: What to know', Association of Health Care Journalists. Accessed: Jan. 07, 2025. [Online].

[16] International Monetary Fund, 'The Last Mile: Financial Vulnerabilities and Risks', 2024. Accessed: Jan. 08, 2025. [Online].

[17] J. Flores, 'Massive Patelco cyberattack is still affecting half a million people. Here's how to protect yourself', San Francisco Chronicle. Accessed: Jan. 08, 2025. [Online].

[18] National Credit Union Association, 'Cybersecurity and Credit Union System Resilience Annual Report to Congress', 2024. Accessed: Jan. 08, 2025. [Online].

[19] Grant Thornton, 'The economic cost of cybercrime', Ireland, 2021. Accessed: Jan. 08, 2025. [Online].

[20] L. Ali, F. Ali, P. Surendran, and T. Bindhya, 'The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services', IJEEEE, vol. Volume 7 Number 1, 2017, doi: 10.17706/IJEEEE.

[21] 'More Than a Million People Affected by Patelco Credit Union's Data Breach', cutimes.com. Accessed: Jan. 08, 2025. [Online].

[22] I. Arghire, 'Patelco Credit Union Scrambling to Restore Systems Following Ransomware Attack', SecurityWeek. Accessed: Jan. 08, 2025. [Online].

[23] C. Castañeda, 'Patelco Credit Union ransomware attack halts banking services for nearly half a million members - CBS San Francisco'. Accessed: Jan. 08, 2025. [Online].

[24] Information Commissioner's Office, 'Iboh updated reprimand with redactions', 2024. Accessed: Jan. 08, 2025. [Online].

[25] Hackney Council, 'Services available, but not back to normal – devastating impact of cyberattack one year on', Services available, but not back to normal – devastating impact of cyberattack one year on. Accessed: Jan. 08, 2025. [Online].

[26] 'Greater Manchester cyber scam leaves thousands vulnerable', BBC News. Accessed: Jan. 08, 2025. [Online].

[27] BBC News, 'Salford housing register still down weeks after cyber attack', Aug. 28, 2024. Accessed: Jan. 08, 2025. [Online].

[28] BBC News, 'Hackney cyber-attack causes collapse of property purchases', BBC, Dec. 12, 2020. Accessed: Jan. 08, 2025. [Online].

[29] M. Burgess, 'The Untold Story of a Crippling Ransomware Attack', Wired. Accessed: Jan. 08, 2025. [Online].

[30] Museums Association, 'Cyber security is an urgent priority for the sector', Museums Association. Accessed: Jan. 08, 2025. [Online].

[31] Z. Small, 'Museum World Hit by Cyberattack on Widely Used Software', The New York Times, Jan. 03, 2024. Accessed: Jan. 08, 2025. [Online].

[32] 'Ticketmaster hack: Customers told to sign up to security service', BBC News. Accessed: Jan. 08, 2025. [Online].

[33] British Library, 'British library cyber incident review', 2024. Accessed: Jan. 09, 2025. [Online].

[34] L. Schachenhofer and P. Hirsch, 'Pharmaceutical Logistics under Cyberattack Conditions', in Proceedings of the 14th International Defense and Homeland Security Simulation Workshop DHSS, CAL-TEK srl, 2024. doi: 10.46354/i3m.2024.dhss.004.

[35] A. Ribeiro, 'Ransomware attackers target Japanese pharmaceutical company Eisai', Industrial Cyber. Accessed: Jan. 09, 2025. [Online].

[36] M. Crosignani, M. Macchiavelli, and A. F. Silva, 'Pirates without borders: The propagation of cyberattacks through firms' supply chains', Journal of Financial Economics, vol. 147, no. 2, pp. 432–448, Feb. 2023, doi: 10.1016/j.jfineco.2022.12.002.

[37] S. Alder, 'Cencora: Additional Data Exfiltrated in February 2024 Cyberattack', The HIPAA Journal. Accessed: Jan. 07, 2025. [Online].

[38] B. Buchanan, 'The Future of AI and Cybersecurity', 2019.

[39] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, 'The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review', Sep. 01, 2022, Social Science Research Network, Rochester, NY: 4323317. Accessed: Jan. 09, 2025. [Online].

[40] S. M. U. H. Minhaj, 'STUDY OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY AND THE EMERGING THREAT OF AI-DRIVEN CYBER ATTACKS AND CHALLENGE', Jul. 17, 2023, Social Science Research Network, Rochester, NY: 4652028. doi: 10.2139/ssrn.4652028.

[41] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, 'Weaponized AI for cyber attacks', Journal of Information Security and Applications, vol. 57, p. 102722, Mar. 2021, doi: 10.1016/j.jisa.2020.102722.

www.kpmg.com/uk