HM Treasury

The Value of Resilience

Cyber Resilience in Financial Services

July 2026

HM Treasury

The Value of Resilience

Cyber Resilience in Financial Services

July 2026

This publication is available at: www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at public.enquiries@hmtreasury.gov.uk.

ISBN: 978-1-918417-61-6 PU: 3653

Contents

Ministerial Foreword

The UK has one of the most innovative, dynamic and trusted financial sectors in the world. Digital transformation has delivered real benefits for consumers and businesses, supporting productivity, inclusion and growth across the economy. As digital technologies become ever more central to how financial services are delivered, maintaining strong cyber and operational resilience is increasingly important to sustaining these gains.

This report brings together new and established evidence on the value of resilience in a digital financial system. It shows clearly that resilience is no longer just about preventing disruption or meeting minimum requirements. When done well, it underpins confidence, supports innovation and enables firms to operate and invest with greater certainty in an increasingly complex environment.

The government is committed to a regulatory framework that is proportionate, outcomes-focused and supportive of growth. Working closely with regulators, industry and the National Cyber Security Centre, we are ensuring that expectations around operational and cyber resilience remain clear, risk-based and aligned with the realities of modern financial services. Our approach is designed to provide confidence and consistency while allowing firms the flexibility to innovate and compete.

Artificial intelligence (AI) continues to evolve, with frontier AI models representing an advancement in capability and potential implications for cybersecurity and operational resilience. These developments may influence the nature and delivery of cyber risks, including through increased speed and scale, particularly where such technologies are used maliciously.

Within this context, firms themselves play a central role. Evidence in this report indicates that organisations that invest effectively in resilience are better placed to recover quickly from disruption, maintain trust and sustain performance. Strong resilience also enables firms to modernise systems, adopt new technologies, and deepen digital capabilities without disruption undermining delivery. In doing so, it supports more informed decision-making at board level, sharper prioritisation of investment, and stronger accountability across the organisation.

Importantly, the report shows that resilience delivers value well beyond risk reduction alone. Firms with more mature resilience capabilities tend to perform better over time, sustaining growth and profitability through periods of stress and change. By improving preparedness for severe but plausible disruption, resilience enables firms to operate with confidence in an environment where volatility and external shocks are an enduring feature.

I welcome this report as a timely and constructive contribution to the evidence base on cyber resilience in financial services. It reinforces a positive message: resilience is a strategic capability that supports innovation, competitiveness and long-term value creation. By embedding resilience at the heart of business strategy, firms can help protect customers, strengthen market confidence and support the UK's position as a leading global financial centre.

Rachel Blake

Economic Secretary to the Treasury

About this report

This report sets out new and existing evidence on the economic and financial value of operational resilience, with a particular focus on cyber disruption in financial services. It explores how resilience affects financial performance, recovery from disruption and longer-term growth, and how these impacts are felt both within financial services and more widely across the economy.

The report has been developed with analytical support from Accenture, KPMG Cyber Risk Insights (CRI), FreedomPay, Retail Economics, Resilience, and the Association of British Insurers, whose contributions provided data, modelling and sector insight to inform the findings. External research is used to contextualise the findings within the broader industry landscape.

Executive Summary

Cyber risk has intensified and represents a growing material challenge for organisations and markets. Evidence from UK surveys, National Cyber Security Centre (NCSC) incident data and sector-level breach research indicates that cyber attacks are becoming more severe, with incidents leading to more significant consequences. At the same time, increasing reliance on third-party suppliers, including cloud service providers and digital infrastructure, can contribute to both the scale and complexity of disruption when cyber attacks occur. The Bank of England's 2026 H1 Systemic Risk Survey found that 82% of UK banks, insurers and asset managers surveyed cited cyber attacks as a top-five risk to the financial system,[1] up ten percentage points from 2024.[2]

In 2024–25, the number of highly significant incidents reported increased by 50% year on year, with nearly half of all incidents meeting the NCSC threshold for national significance.[3] Loss modelling by KPMG Cyber Risk Insights (CRI) indicates that ransomware losses are highly skewed, with a small number of severe incidents accounting for a disproportionate share of total financial losses. For mid-sized financial firms, plausible worst-case losses (1-in-100) exceed £230 million, and for large firms, approach £466 million. The modelling also shows that in many years firms may experience no material losses, while a small number of scenarios drive very large impacts. In this context, average cost estimates provide only a partial view of exposure, as they do not capture the concentration of losses in more severe scenarios. These trends underline the importance of resilience planning that considers high-impact disruption alongside day-to-day incident activity.

The financial consequences of cyber disruption have become more severe over time. Earlier studies, reflecting a different stage of digital dependence, often found that cyber incidents had limited or short-lived effects on firm performance. More recent evidence indicates that impacts are now larger and more persistent. Companies that have recently experienced a major cyber incident underperform the market by around 5% on average for a year or more,[4] and major incidents are associated with an average 9% decline in shareholder value in the year following the event.[5] These impacts reflect not only direct recovery costs, but wider effects on trust, reputation and investor confidence, particularly where important business services are disrupted.

---

[1] Systemic Risk Survey Results - 2026 H1 | Bank of England

[2] Systemic Risk Survey Results - 2024 H1 | Bank of England

[3] NCSC Annual Review 2025

[4] The Sustained Negative Impacts of Cyber Incidents on Shareholder Value

[5] Build a Plan to Address the Perils of Reputational Risk

Against this backdrop, resilience should be seen not merely as a protective function, but as a foundational enabler of growth and performance. Organisations with stronger resilience can recover faster from disruption, protect customer trust and sustain operational momentum. Evidence indicates that more resilient firms outperform peers across a range of outcomes, including revenue growth, profitability, technical debt reduction and customer trust. Analysis by Accenture found that among firms in the highest resilience quartile, 60% record profit gains following a severe shock, compared with 21% among the least resilient.[6] Highly resilient companies grow revenues 6 percentage points faster than their peers and have profit margins that are 8 percentage points higher than the median company in their industry over a three-year horizon.[7]

Resilience supports growth by reducing uncertainty, improving execution across complex systems, and sustaining confidence among customers and investors. As digital technologies continue to evolve, including developments in AI, these trends may shape the scale and delivery of cyber risks over time, for example through increased speed and automation. Within this context, resilience plays an important role in enabling organisations to manage disruption and sustain performance. Evidence suggests that organisations with stronger resilience capabilities are generally better placed to recover from disruption, maintain trust and support ongoing performance. They are also better positioned to modernise systems, adopt new technologies and pursue digital transformation without disruption undermining delivery. In this way, resilience can support growth as well as risk management, functioning not only as a protective capability but as a foundation for sustained performance in an increasingly digital environment.

Despite these advantages, preparedness remains limited. Only 10% of organisations report being prepared for AI-augmented cyber threats and 77% lack essential data and AI security practices.[8] More resilient organisations are better positioned to modernise, scale AI and pursue digital transformation without disruption derailing delivery. In this context, resilience can function as a prerequisite for digital growth rather than a constraint on it.

The central conclusion of this report is that operational resilience and resilient organisational cultures can support growth not by eliminating risk, but by reducing uncertainty, limiting disruption and enabling organisations to invest, innovate and scale with confidence.

---

[6] Resilience Redefined: From Readiness to Reinvention | Accenture

[7] How to Grow Your Return on Business Resilience | Accenture

[8] Accenture's State of Cybersecurity Resilience 2025

Introduction

Financial services are increasingly dependent on digital infrastructure, interconnected systems and third-party providers. While this transformation has delivered significant gains in efficiency, innovation and access, it has also fundamentally altered the nature of operational risk. Cyber disruption is no longer a peripheral technical issue; it is a core strategic risk with the potential to affect firm performance and wider economic activity.

The frequency, scale and complexity of cyber incidents are increasing. Attacks are becoming more sophisticated, supply chains more interconnected, and critical services more reliant on shared technologies and providers. Recent high-profile incidents affecting major UK firms, including Marks & Spencer and Jaguar Land Rover, illustrate how cyber disruption can lead to operational downtime, customer impact and wider commercial consequences, including reputational damage and impacts on shareholder value. As a result, when disruption occurs, its impacts can be more severe, more difficult to contain, and more costly to recover from. These impacts extend beyond immediate remediation costs to include lost revenue, operational downtime, reputational damage and, in some cases, sustained effects on firm value and market confidence. More information on current and emerging threats can be found via the National Cyber Security Centre's reports and advisories.

Cyber resilience is a foundational component of financial stability. It refers to the ability of an organisation to maintain the delivery of its key functions and services and ensure the protection of its data, despite cybersecurity events.[9] Nonetheless, resilience is often viewed primarily through a compliance or cost lens, rather than as a broader strategic capability. This perspective can make it harder to reflect the full range of potential losses, particularly those associated with less frequent but more severe events that may affect business continuity and financial performance. It can also understate the role resilience plays in enabling firms to innovate, adopt new technologies and operate with confidence in a more uncertain environment.

Against this backdrop, HM Treasury has undertaken this work to strengthen the evidence base on the value of resilience to private sector entities and to promote more informed firm-level decision-making. This report examines the economic and financial value of cyber resilience in the UK financial sector, helping organisations to better understand the financial implications of cyber disruption, the role resilience plays in shaping outcomes, and how investment in resilience can be considered alongside wider strategic and commercial priorities. It sets out how cyber

[9] Government Cyber Security Strategy 2022–2030

disruption translates into financial impact, how resilience can alter both the likelihood and severity of these outcomes, and how stronger resilience capabilities can support not only risk reduction but also sustained growth and performance.

Chapter 1

Rethinking How Resilience Is Viewed

1.1 Resilience is still often framed as a compliance obligation and cost, rather than as a source of growth.[10] Evidence suggests that resilience can support growth, but it is rarely articulated in those terms.

1.2 Accenture analysed earnings call transcripts from 1,954 global companies between 2020 and 2025. The study examined how companies discuss resilience, whether it is linked to growth, and whether that linkage is sustained over time as part of organisational culture. Companies were classified as 'consistent' if they referenced growth-related resilience in more than half of the quarters in which they reported. The analysis also identifies broader patterns in how resilience is discussed and whether it is positioned as a driver of business performance.

Figure 1

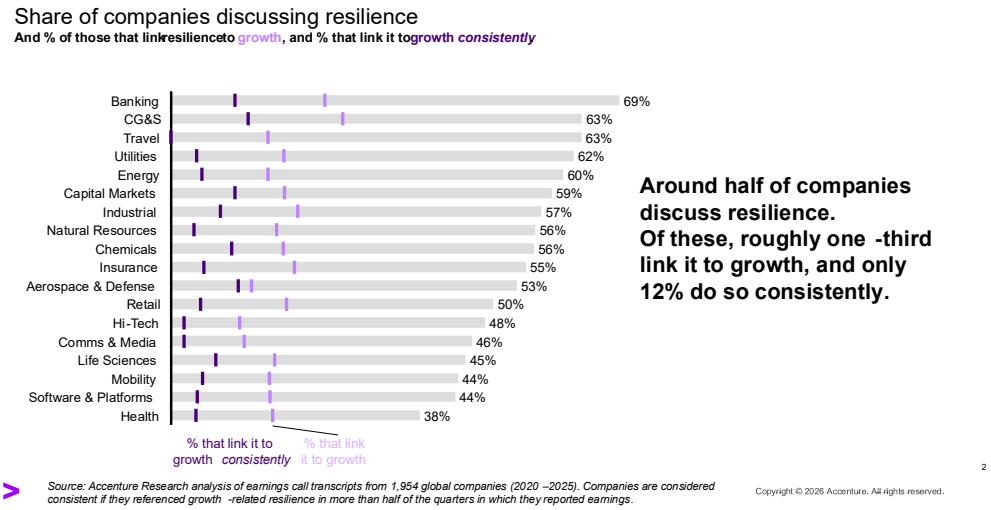

Figure 1: Share of companies discussing resilience in earnings calls, and the share of those companies that link resilience to growth or do so consistently over time (Source: Accenture, 2020–2025).

1.3 Only around half of companies reference resilience at all within their earnings transcripts; of those, roughly one third link it to growth, and only around 12% do so consistently. Financial services has some of the highest rates of resilience discussion, with Banking (69%), Capital

[10] Integrated operational resilience: Your competitive edge | KPMG UK

Markets (59%) and Insurance (55%), likely reflecting regulatory expectations, risk management culture and post-crisis scrutiny. However, even in these sectors, only 30% to 35% of references connect resilience to growth.

1.4 A similar pattern is also reflected in further sector-level evidence. The Retail Economics and FreedomPay Business Resilience Survey 2026, conducted on behalf of HM Treasury, provides an illustration from the retail and hospitality sectors. Although these findings relate to only two sectors, both are highly dependent on payments, digital infrastructure and continuous service provision, and are therefore particularly exposed to operational disruption. Based on responses from 101 UK senior leaders in consumer-facing businesses with annual turnover of £6 million or more,[11] the survey shows that nearly two thirds (64%) of senior decision makers agree that resilience investment reduces risk but delivers limited additional business benefits. Almost half (45%) said that executives do not fully appreciate the value of resilience investments, while 48% believe that executives in their industry think too much is already being spent on resilience. These findings suggest that resilience investment is often viewed primarily as a preventative measure rather than as a broader source of operational or commercial value. Taken together, this suggests that while resilience is recognised as strategically important, its full economic value is not yet clearly understood or articulated.

1.5 The same analysis reveals a similar tension in leaders' expectations about future risk. While four in five of the UK senior leaders surveyed (81%) believe their organisation's investment in operational resilience is broadly sufficient, larger firms nevertheless report shortfalls in the level of investment being made. In parallel, nearly two thirds (60%) expect the frequency of operational disruptions to increase over the next three years. Expectations around recovery are less stark but remain challenging, with a net 9% anticipating longer recovery times. This points to a confidence gap risk: organisations feel broadly prepared today, even as they anticipate a more disruptive and, for some, harder-to-recover operating environment ahead.

[11] All data sourced from the Retail Economics / FreedomPay Business Resilience Survey 2026, conducted on behalf of HM Treasury. Fieldwork conducted 20–26 March 2026. Base: 101 UK senior leaders in consumer-facing businesses (retail and hospitality) with £6m+ turnover. Respondents sit on, or contribute to, risk or audit committees, or hold direct responsibility for risk management within their organisation.

Chapter 2

The Financial Impact of Cyber Disruptions

2.1 Cybersecurity budgets are often determined by technical teams and reviewed by boards as a line item within IT spend.[12] The evidence in this report suggests that this framing may understate the wider financial and strategic impacts of cyber disruption. Losses extend beyond technology functions, affecting profit and loss and, in some cases, firm value. This indicates that cyber resilience has important financial and strategic implications for boards and executives, alongside its technical dimensions.

2.2 This distinction has become increasingly important as the nature of cyber risk and its economic impact has changed materially over time. Historically, cyber incidents were typically treated as operational or technical failures, with costs concentrated on remediation, system repair and limited service disruption. As digital systems have become central to business models, supply chains and customer interaction, the financial consequences of cyber incidents have broadened significantly. Supply chains and dependencies on third-party providers have emerged as significant attack surfaces and transmission channels. Adversaries can exploit vulnerabilities in smaller vendors or service providers to gain access to larger institutions, while disruptions can propagate widely when critical inputs are difficult to substitute.

2.3 Earlier empirical studies generally found that cyber incidents led to limited or short-lived share price impacts, with effects often small and largely reversed within weeks or months, except in the most severe data breaches.[13] More recent evidence shows a different pattern. Studies of public companies have found that firms experiencing major cyber incidents underperform the market by around 5% on average for a year or more,[14] and that major incidents are associated with an average 9% decline in shareholder value relative to the market in the year following the event, over and above general market movements.[15] Companies that

---

[12] Cybersecurity Budgets: Spend More or Spend Better? | Alvarez & Marsal | Management Consulting | Professional Services

[13] What is the Impact of Successful Cyberattacks on Target Firms?

[14] The Sustained Negative Impacts of Cyber Incidents on Shareholder Value

[15] Build a Plan to Address the Perils of Reputational Risk Based on an event-study analysis of 47 prominent cyber incidents involving publicly listed companies globally, measuring cumulative abnormal shareholder returns over the 12 months following each event relative to broader market performance.

fared worse realised an average decline of 21% in shareholder value.[16] As a result, costs increasingly arise not only from direct response and recovery activity, but from wider effects on trust, reputation and firm value. This shift reflects growing digital dependence and a change in investor behaviour, with cyber incidents increasingly interpreted as signals of weaknesses in governance, operational resilience and management rather than isolated technical failures.

2.4 This shift in framing matters because the cyber threat environment is changing. NCSC incident management analysis points to not only a rising volume of attacks, but also a rising severity of incidents. In 2024–25, 'nationally significant' incidents represented 48% (204) of all incidents, a significant increase from the previous year (89). A nationally significant incident covers incidents in the upper three categories in the NCSC and UK law enforcement categorisation model. Among those incidents, 4% (18) were categorised as highly significant in nature. This marks a 50% increase in highly significant incidents, continuing a rise seen for the third consecutive year.[17]

Figure 2

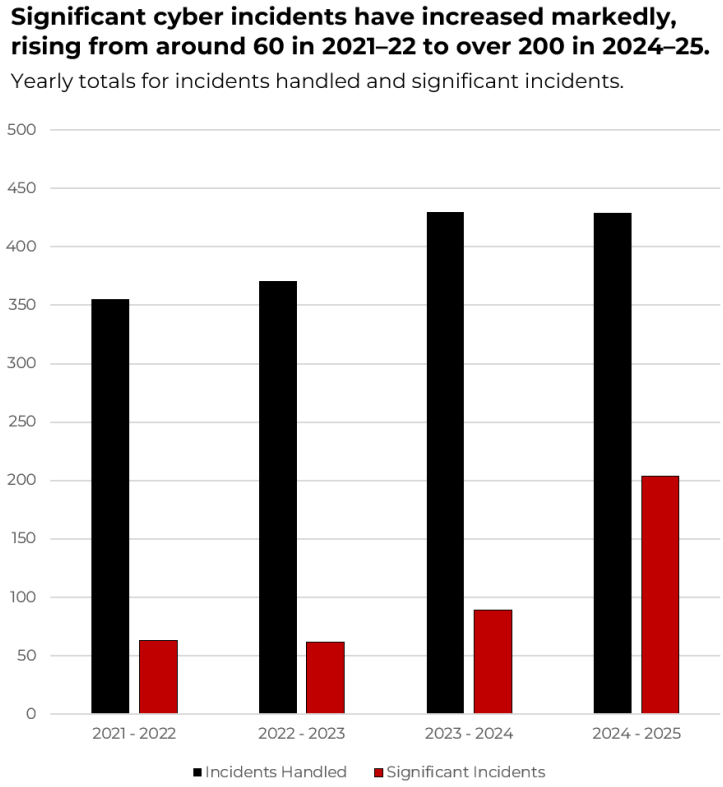

Figure 2: Incidents handled by the NCSC Incident Management team and associated severity categories. (Source: National Cyber Security Centre (NCSC) Annual Reviews, 2022–2025).

[16] Build a Plan to Address the Perils of Reputational Risk

[17] NCSC Annual Review 2025

2.5 Ransomware provides a clear illustration of how this risk materialises financially for financial organisations. The share of global financial institutions reporting ransomware attacks rose sharply from 35% in 2021 to 65% in 2024.[18] Over the same period, the mean global recovery cost for financial firms, excluding ransom payments, increased to £2.04 million in 2024, up from £1.76 million the previous year.[19] This escalation is reflected in wider indicators of harm: National Crime Agency reporting showed that identified incidents of ransomware impacting UK victims doubled between 2022 and 2023,[20] and ransomware incidents reported to the Information Commissioner's Office reached their highest level since 2019 in 2023.[21]

2.6 Looking beyond point estimates, loss modelling developed by KPMG CRI, drawing on global incident data, highlights why ransomware risk is difficult to assess using averages alone. Table 1[22] presents three measures of ransomware exposure for financial services firms of different sizes. The average figure provides an indication of expected loss over time, while the midpoint (P50) shows that in many modelled years there may be no material ransomware loss. The upper-end estimate (P99) illustrates what a more severe but still plausible year can look like, with only 1% of outcomes exceeding this level.

2.7 The results show that ransomware risk is driven less by frequent moderate losses and more by less frequent events with materially larger consequences. This pattern is evident across firm sizes: for mid-sized financial firms, plausible worst-case losses exceed £230 million, and for large firms approach £466 million, indicating that risk becomes financially significant well before the largest end of the market.

2.8 These findings highlight the limitations of relying on average losses alone for management decision-making. Much of the risk sits in the gap between typical outcomes and the severe end of the loss distribution, where impacts become harder to absorb and more likely to affect financial performance. This reinforces the importance of resilience

---

18 Global financial ransomware attack rate 2024| Statista

19 https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-financial-services-2024 Dollar figures have been converted to sterling using an illustrative USD–GBP exchange rate (approximately 0.79), broadly consistent with recent multi-year averages.

20 [ARCHIVED CONTENT] NSA 2024 - Overview of SOC - National Crime Agency

21 https://ico.org.uk/action-weve-taken/data-security-incident-trends/

22 This analysis is based on the KPMG Cyber Risk Insights (CRI) Industry Insights Database, which is informed by over 150,000 cyber loss events between 2008 and 2025. The database covers 20 industries, including finance, public sector, retail, healthcare, manufacturing, utilities, transportation, energy, and a range of service industries, and is based on global incident data. Data is strongest for the highly regulated sectors like healthcare and finance, due to their strict public disclosure laws, and for geographies with more mature public disclosure regimes. Financial services industry data was used to derive Loss Event Frequency (LEF) and Loss Magnitude (LM) assumptions, which were modelled using CRI's Ransomware scenario model to estimate Annualised Loss Expectancy, including the average, 50th percentile (P50), and 99th percentile (P99) estimates.

planning that considers low-frequency, high-impact disruption alongside day-to-day incident activity.

Table 1

Size (Revenue)	Average	Midpoint (P50)	99th Percentile (P99)
Small (<£1B)	£1.5M	£0	£35M
Mid (£1B–<£10B)	£9.8M	£0	£232M
Large (£10B–£100B)	£22.3M	£0	£466M

Table 1: Annualised ransomware loss exposure analysis for different sizes of financial services institutions (Source: KPMG Cyber Risk Insights (CRI) Industry Insights Database).

2.9 The value impact can extend beyond immediate direct costs. Cyber incidents can undermine investor confidence where they expose broader weaknesses in governance, controls, or operational resilience, linking cyber risk directly to corporate valuation and brand credibility.[23] In practice, the most significant costs often arise when disruption affects an important business service rather than a contained technical system.

2.10 This risk is increasingly recognised at the system level. The Bank of England's 2026 H1 Systemic Risk Survey found that 82% of UK banks, insurers and asset managers cited cyber attacks as a top-five risk to the financial system,[24] up ten percentage points from 2024.[25] Firm-level analysis reinforces the scale of exposure: a meaningful share of large financial institutions face a roughly 10% annual probability of losing 10% or more of annual profit to a single cyber event, with some facing exposure of 20% or more.[26]

2.11 Across the wider economy, cyber and operational losses are not evenly distributed across firms or incidents. Most operational disruptions result in limited financial impact, while a small number account for a disproportionate share of total losses.

2.12 Figure 3 illustrates this distribution across sectors in the UK, showing the estimated financial impact of a single operational disruption as a percentage of the previous year's turnover. The analysis draws on a sample of disruption events across a range of sectors, including government, manufacturing, professional services, retail, transport, healthcare and financial services. The dataset combines publicly reported incidents with insurance-based loss data. Most disruptions in the sample are linked to cyber incidents, particularly

[23] Kamiya et al, 2019

[24] Systemic Risk Survey Results - 2026 H1 | Bank of England

[25] Systemic Risk Survey Results - 2024 H1 | Bank of England

[26] Cyber Risk and Financial Resilience in the S&P 500 Report | Kovrr

ransomware attacks, credential theft and other forms of cyber-enabled fraud. These incidents typically result in operational disruption, including downtime, revenue loss and remediation costs.

2.13 The distribution is highly skewed. For the majority of firms, disruption costs fall within a relatively modest range, typically between 0.2% and 4.6% of annual turnover, reaching around 16% in the most severe incidents. The results therefore highlight a key feature of operational risk: average impacts are not representative of overall risk exposure. While typical disruptions can be manageable, tail events can dominate total losses and can threaten business continuity.

Figure 3

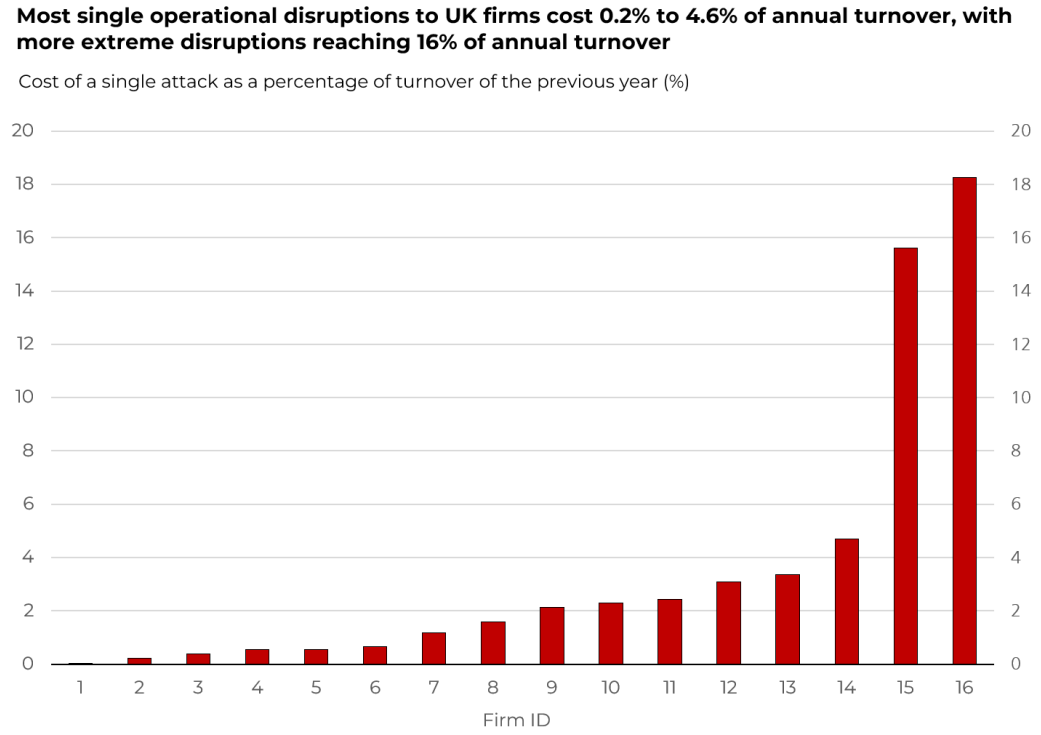

Figure 3: Operational Disruptions as a percentage of annual turnover (Source: ABI Member Firms and Open Source).

Chapter 3

How Resilience Reduces the Likelihood and Impact of Cyber Disruption

3.1 Strong resilience affects outcomes through two main mechanisms. First, it reduces the likelihood of disruptive events, and limits their escalation into more severe incidents, by strengthening detection, containment, escalation, and operational response. Second, it reduces the scale of loss when events do occur, through faster restoration, effective recovery planning, service prioritisation, and the use of fallback arrangements.

3.2 Figure 4[27] illustrates how stronger resilience can change the financial profile of ransomware risk exposure, using data from KPMG's global CRI Industry Insights Database. In this analysis, increased resilience does not refer to a single control or cultural attribute. It refers to the combined effect of capabilities that improve prevention and detection, constrain the spread, accelerate restoration, and preserve critical value during disruption. The graph compares two views of the same ransomware scenario. The first reflects the current loss profile. The second shows an illustrative stronger resilience scenario in which detection and prevention are stronger, spread is better contained, recovery is more effective, and more critical service value is preserved during disruption. The result is fewer severe outcomes and a smaller upper tail of loss.

3.3 The modelling indicates that increased resilience affects the loss distribution in two principal ways. First, it reduces the likelihood that disruptive events escalate into severe outcomes. Second, it reduces the scale of losses when disruption does occur. This pattern is consistent with complementary analysis by Aon, which highlights substantial variation in firm outcomes following major cyber incidents. Not all companies experienced a decline in shareholder value following a cyber incident. In

[27] The illustrative Loss Exceedance Curve (LEC) was developed by applying representative Loss Event Frequency (LEF) and Loss Magnitude (LM) data for a large (£10B - £100B revenue) financial services organisation. The LEF and LM were used as inputs to the KPMG CRI Ransomware scenario model to generate a LEC. A resilience-adjusted scenario was then modelled through expert judgement-based reductions to LEF and LM assumptions to assess the change in the loss distribution.

a subset of cases, effective response and recovery were associated with better reputational outcomes and stronger investor confidence. Aon identified 17 of the 47 companies examined as having successfully navigated major cyber incidents, with these firms achieving an average increase in shareholder value of around 18% above market trends.[28] In these cases, timely and well-executed responses helped limit operational and reputational impacts and manage external perceptions during and after the incident.

Figure 4

How resilience changes the financial shape of ransomware risk in financial services

Resilience reduces the likelihood and impact of severe disruption

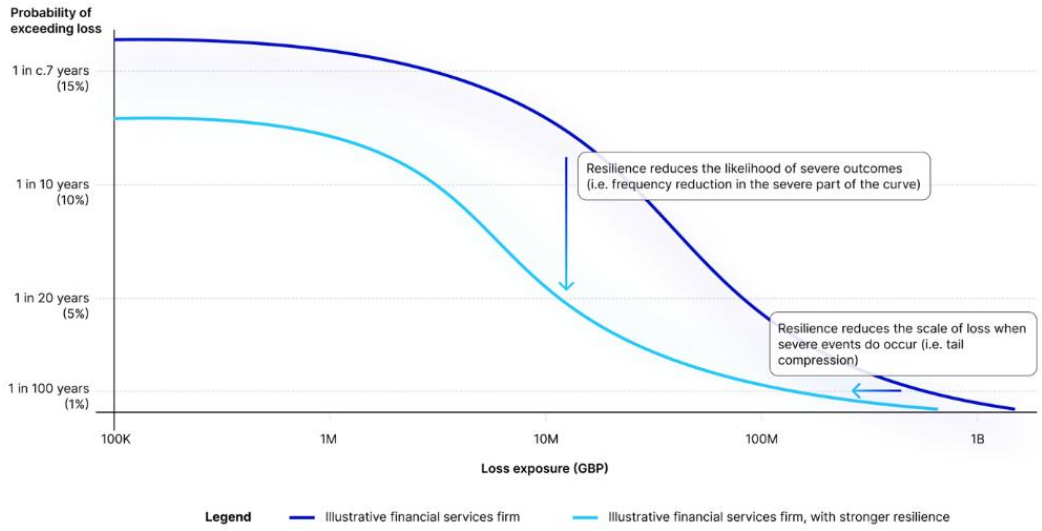

Figure 4: How operational resilience alters the financial risk profile of ransomware in financial services (Source: KPMG's Cyber Risk Insights Widespread Ransomware scenario model).

3.4 Crucially, resilience is not delivered through headline-grabbing innovations in isolation. It emerges from the cumulative effect of consistent, high-quality execution across both foundational security and operational practices, alongside more advanced capabilities. These core controls provide the baseline that enables organisations to absorb disruption, while also amplifying the effectiveness of higher-order defences and preserving value when adverse events occur.

3.5 Evidence from industry reinforces the strategic importance of this baseline. Based on a 2025 survey conducted by Accenture of 2,286 cybersecurity and technology executives at large organisations globally, the research found that only 10% of organisations are prepared to defend against AI-augmented cyber threats, while 77% lack the essential data and AI security practices needed to protect critical business models, data pipelines and cloud infrastructure. That matters because the downside of cyber weakness is no longer confined to

[28] Build a Plan to Address the Perils of Reputational Risk

technical remediation; it increasingly affects the confidence with which organisations can modernise, scale AI and sustain digital growth.

3.6 In the UK context, Cyber Essentials provides a minimum standard for organisations of all sizes, which is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats.[29] NCSC evaluation indicates that basic controls can mitigate the vast majority of common internet-originating vulnerabilities, and NCSC reporting shows that organisations with Cyber Essentials certification are significantly less likely to make a cyber insurance claim.[30] As of October 2025, certification also delivers practical commercial benefits: around 99% of internet-originating vulnerabilities can be mitigated through the assessed controls, Cyber Essentials-certified organisations make around 92% fewer cyber insurance claims, 69% believe that it has increased their market competitiveness and 39% associated it with increased customer trust.[31]

3.7 While Cyber Essentials provides this foundational baseline, organisations still need to make risk-based decisions appropriate to their size, sector and threat exposure. In financial services, for example, more advanced tools such as CBEST are used alongside baseline controls. Faster detection, containment and recovery remain central to limiting both loss severity and outage duration once an incident begins.

3.8 Using KPMG CRI modelling, Figure 5[32] shows how different defensive capabilities contribute to reducing the likelihood of escalation in a ransomware scenario. For example, controls that disrupt initial compromise, such as security training, email filtering and web controls, each contribute around 10–15% reductions in ransomware likelihood.

---

29 Government Cyber Security Strategy 2022–2030

30 NCSC Annual Review 2025

31 It's time to act - NCSC Annual Review 2025

32 The analysis was derived from the KPMG CRI Ransomware scenario model, where attack techniques are linked through AND/OR relationships. Capability contributions were quantified based on their marginal impact on overall scenario success probability.

Figure 5

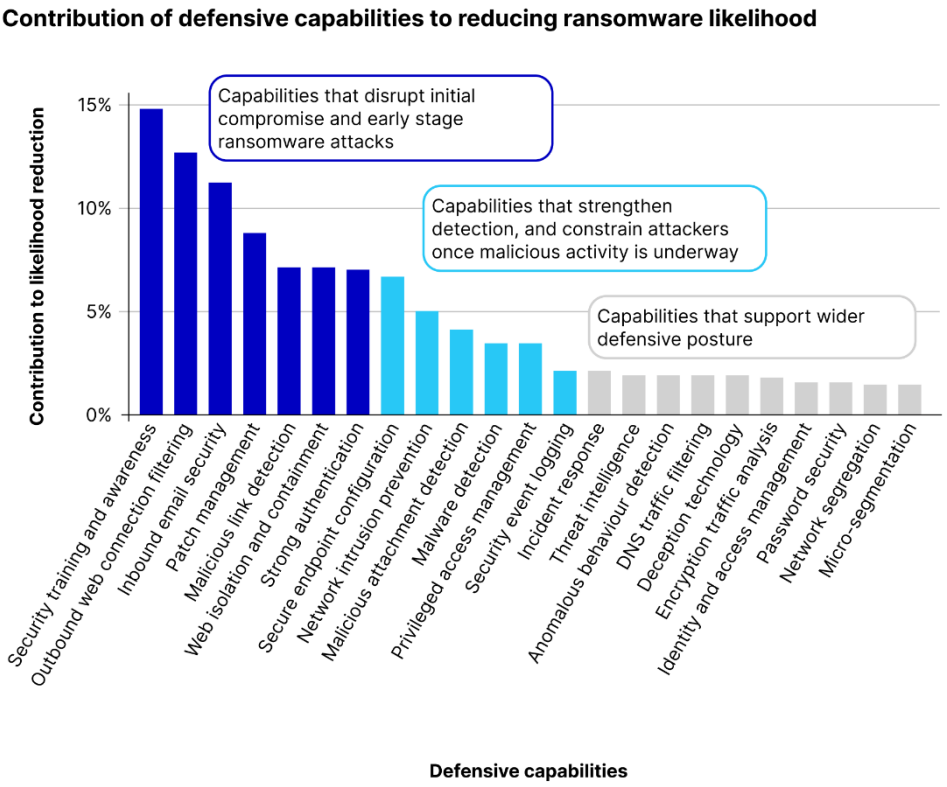

Figure 5: Comparison of likelihood reducing capabilities related to ransomware and their contribution to risk reduction (Source: Analysis of Cyber Risk Insights (CRI) Widespread Ransomware scenario model).

3.9 The CRI analysis shows that a relatively small subset of capabilities contributes a disproportionate share of the reduction in event likelihood. The practical implication is that organisations do not need uniform improvement across every element of the control environment to make meaningful progress. Instead, value comes from understanding where preventive investment delivers the greatest marginal reduction in risk, and how those preventive measures interact with the resilience capabilities required to limit losses from incidents that still occur.

3.10 This evidence supports a more integrated approach to resilience investment. Rather than treating prevention, response, recovery and continuity as separate conversations, firms with the strongest outcomes are those that balance investment across these domains, informed by where capabilities have the greatest impact on likelihood and loss.

Chapter 4

Resilience as a Driver of Growth

4.1 The case for resilience investment is two-sided. Resilience reduces expected loss, but it also supports conditions for growth. Accenture research shows that more resilient organisations outperform peers on revenue growth, profitability, technical debt reduction, visibility across the organisation and customer trust. That matters as large organisations modernise architecture, scale data and AI, deepen ecosystem partnerships and automate more processes. These programmes are more likely to realise full value when the underlying cyber and operational foundations are strong enough to absorb shocks without derailing delivery.

4.2 Highly resilient organisations do not simply report better outcomes; they also operate differently. Compared with less resilient peers, they are materially more likely to assess the security of AI tools before deployment, involve security in procurement, assess supplier maturity, exercise with ecosystem partners and report having the skills needed to meet current cybersecurity objectives.[33] This suggests that resilience maturity is expressed not only in technical controls, but also in stronger operating discipline across transformation, governance and external dependencies.

4.3 Figure 6 captures the core point: the same capabilities that improve cyber outcomes also improve execution, visibility and trust. The chart's central message is that resilience maturity is associated with better business performance, not just better security outcomes. Organisations at the top end of the resilience curve are more likely to reduce technical debt, extract stronger returns from AI, improve visibility across the organisation and sustain customer trust, while being less likely to suffer advanced attacks, making resilience a performance enabler, as much as a protection measure. For example, the analysis shows that reinvention-ready organisations achieve around 1.6 times greater improvements in customer trust compared with baseline peers.

[33] World Economic Forum's Global Cybersecurity Outlook 2026

Figure 6

Accenture: Transformation-ready organisations outperform on business outcomes

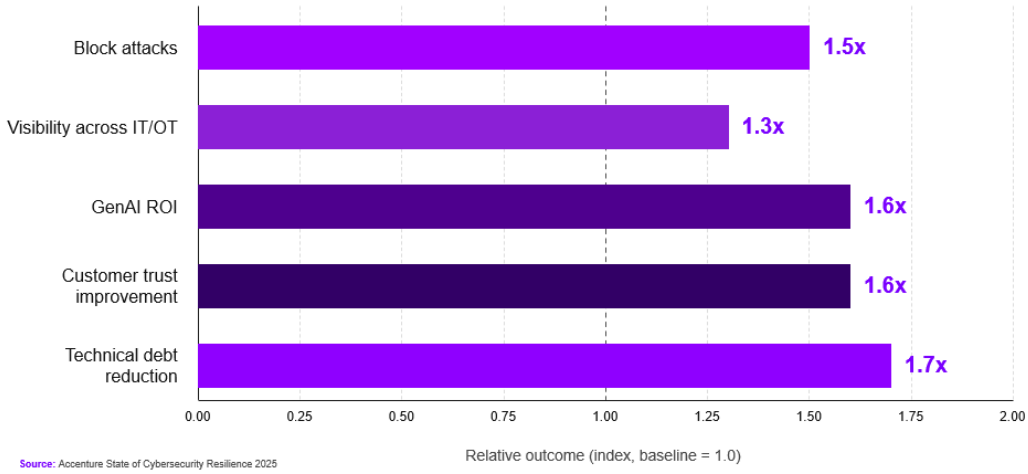

Figure 6: Transformation ready organisations outperform on business outcomes. Index values shown relative to baseline organisations; lower likelihood of advanced attacks is discussed in text because it is directionally inverse.[34] (Source: Accenture).

4.4 Accenture's earlier research points in the same direction. Organisations that align cybersecurity more closely with business objectives are more likely to achieve stronger revenue growth, market share and customer satisfaction outcomes while also reducing breach and incident costs.[35]

4.5 This underscores the importance of senior accountability in embedding resilience as an organisation-wide priority. A cyber-resilient CEO treats cybersecurity as a core business strategy, not just an IT issue, so the company can keep operating, adapting and growing even when cyber attacks happen. In separate CEO research, Accenture found that cyber-resilient CEOs achieved, on average, 16% higher incremental revenue growth, 21% more cost reduction improvements and 19% healthier balance sheet improvements, while facing breach costs around two to three times lower than their peers.[36] The message is consistent: resilience is a multiplier on business execution.

4.6 Accenture's wider resilience research reinforces that relationship. Among firms in the highest resilience quartile, 60% record profit gains following a severe shock, compared with 21% among the least resilient.[37] Highly resilient companies grow revenues 6 percentage points faster than their peers and have profit margins that are 8 percentage points higher than the median company in their industry over a three-year

---

[34] Accenture, State of Cybersecurity Resilience 2025

[35] 2023 Accenture State of Cybersecurity Resilience

[36] Accenture, The Cyber Resilient CEO 2023

[37] Resilience Redefined: From Readiness to Reinvention | Accenture

horizon.[38] This strengthens the case that resilience can influence post-disruption performance as well as pre-disruption preparedness.

4.7 Furthermore, World Economic Forum (WEF) evidence explores additional reasons for this advantage: highly resilient organisations are more likely to embed security into business processes and ecosystem management: 76% involve the security function in procurement, 74% assess supplier security maturity and 44% simulate cyber incidents or recovery exercises with ecosystem partners, compared with materially lower figures among insufficiently resilient organisations.[39] In practice, that means resilience improves the quality of change, reduces friction in supplier assurance and makes organisations better able to sustain performance through disruption.

Correlation and causation

4.8 It can be argued that the observed relationship between resilience and performance reflects correlation rather than causation. More successful firms may invest more in resilience because higher revenues allow for larger security budgets, while larger or more complex institutions may require more robust controls by necessity. A further explanation may be that a third factor, such as leadership quality, drives both stronger performance and higher resilience maturity.

4.9 People and leadership capability appear to play an important role. The resilience of any organisation is, in part, shaped by the resilience of its individual members. Employees who exhibit strong personal resilience are 1.7 times more likely to contribute to a resilient enterprise.[40] This connection is especially pertinent in the banking sector, where regulation requires firms to detect, respond to and recover from disruptions within defined tolerances.

4.10 Evidence also points to the importance of leadership. Around 67% of employees look to their CEO for guidance on how well the company can endure disruption. Employees who believe their CEO leads with purpose are 1.9 times more likely to be resilient themselves.[41] This people-centred strategy not only enables firms to fulfil regulatory expectations but also enhances their capacity to recover from cyber and other incidents, adapt to changing conditions, and sustain value for customers and stakeholders over the long term.

4.11 The most important cultural lesson from the evidence is that resilience is a shared organisational behaviour, not a specialist function. Many firms still lack the basic cultural infrastructure required for resilience: clear senior accountability, regular staff training, incident

---

38 How to Grow Your Return on Business Resilience | Accenture

39 World Economic Forum, Global Cybersecurity Outlook

40 *Accenture's research, How to Grow Your Return on Business Resilience, 2024*

41 *Accenture's research, How to Grow Your Return on Business Resilience, 2024*

planning, and supply-chain scrutiny. When those conditions are absent, even good technology is less effective because decisions slow down and the organisation cannot execute a coherent response under pressure.[42]

4.12 Recent academic evidence provides stronger support for a causal link between cybersecurity and financial performance. A large multi-country banking study covering the period 2009–2023 finds that the adoption of formal cybersecurity policies is associated with statistically significant improvements in profitability, including returns on assets, equity and tangible equity.[43] The study shows that these gains operate through reduced operational risk and stronger governance and ESG performance. Rather than acting as a cost or constraint, cybersecurity policy can strengthen financial resilience and stakeholder trust in the evolving threat landscape, supporting sustainable profitability and long-term growth.

[42] WEF_Cyber_Resilience_Index_2022.pdf

[43] Cybersecurity policy, ESG and operational risk: A Virtuous relationship to improve banks' performance - ScienceDirect

Conclusion

The evidence presented in this report indicates that cyber risk is becoming more severe and more complex, particularly within increasingly digital and interconnected operating environments. Survey evidence, incident data and sector-level analysis point consistently to rising disruption, higher recovery costs and growing exposure through third-party and platform dependencies. Within financial services, these risks are recognised by senior decision-makers as both a firm-level and sector-level concern.

The findings also highlight how the financial consequences of cyber disruption have changed over time. Cyber incidents are no longer confined to short-lived technical outages. They can generate material profit and loss impacts, affect firm value, and undermine trust where they expose broader weaknesses in governance, controls or operational resilience. Ransomware provides a clear illustration of this shift, with losses increasingly concentrated in high-impact events that are not well captured by average cost estimates alone.

This has implications for how cyber risk and resilience are assessed and managed. The analysis suggests that reliance on averages can understate exposure, particularly for larger and more complex organisations. Consideration of tail risks provides a more informative basis for understanding potential impacts and supporting decision-making.

The report also finds that resilience outcomes are shaped not only by the level of investment but by how effectively capabilities are prioritised and integrated. Strong outcomes are associated with a combination of foundational controls, such as patching and vulnerability management, alongside targeted improvements in detection, response and recovery. These measures reduce the likelihood that incidents escalate and limit the scale and duration of losses when disruption occurs.

Finally, the evidence indicates that resilience is increasingly relevant beyond risk mitigation alone. Organisations with stronger resilience capabilities tend to sustain performance more effectively through disruption and are better positioned to support ongoing transformation, innovation and growth. Collectively, the findings suggest that cyber resilience should be understood as an organisational capability for operating in an environment characterised by persistent external disruption, rather than solely as a response to isolated internal failures.

Annex A

Stakeholder Information

Accenture: Accenture is a global professional services company that helps enterprises reinvent by building their digital core and unleashing the power of AI to create value at speed across the enterprise. Visit their website at accenture.com.

KPMG: KPMG Cyber Risk Insights (CRI) is KPMG's global cyber risk quantification (CRQ) capability and technology platform. CRI combines advanced analytics, threat intelligence, incident data and financial modelling to assess the potential economic impact of cyber and operational disruption. Visit their website at kpmgcri.com.

FreedomPay: FreedomPay's Next Level Commerce™ platform transforms existing payment systems and processes from legacy to leading edge. Visit their website at freedompay.com.

Retail Economics: Retail Economics is an independent economics research consultancy focused on the consumer and retail industry. Visit their website at retaileconomics.co.uk.

ABI: The Association of British Insurers (ABI) is the trade association for the UK's insurance and long-term savings sector. Visit their website at abi.org.uk.

Resilience: Resilience is a cyber risk company that offers risk quantification software, cybersecurity experts, and insurance in connected solutions purpose-built for large and middle-market organisations. Visit their website at cyberresilience.com.

HM Treasury contacts

This document can be downloaded from www.gov.uk.

If you require this information in an alternative format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 5000

Email: public.enquiries@hmtreasury.gov.uk