The Economy Research

THE ECONOMY / RESEARCH PAPER SERIES

NOVEMBER 2026

Financing Resilience When Cyber Catastrophe Cannot Be Priced Reliably

Transmission, Loss Allocation and Recovery Investment under Shared Digital Dependence

The Economy Research Editorial
The Economy Research

RESEARCH PAPER

economy.ac/research

About the paper

This paper examines how shared digital-service failures propagate through payments, production, customers and confidence, and how firms can finance resilience when the probability of a cyber catastrophe cannot be reliably estimated.

Reading the evidence

Published incidents are considered alongside conditional payment-network stress tests. Simulated intervention results rest on stated assumptions, and no modelled outcome is a forecast.

Author

The Economy Research Editorial
The Economy Research

71 Lower Baggot Street
Dublin 2
Co. Dublin, D02 P593, Ireland

Publication

The Economy Research
November 2026
economy.ac/research

Originally published
Not specified in supplied manuscript
The Economy Research Editorial
Read the original paper

Contents

Abstract 1

1 Introduction - The Need to Finance Resilience 1

2 Transmission throughout the Economy 2

3 Distribution of Losses between Affected Parties 5

4 Number of Providers versus Independent Sources of Disruption 6

5 Relative Benefits of Improved Recovery and Prevention 9

6 Scope for Insurance and Other Risk-Sharing 11

7 Conclusion 15

References 16

Eight figures and two tables accompany the analysis. The reference list identifies the works cited in the manuscript.

Abstract

In July 2024, CrowdStrike caused around 8.5m Windows machines to fail. A number of large hospital, banking and air transport groups failed together, although they were independent businesses protected by different insurers. Aggregate direct impact to these firms in the Fortune 500 was in the order of USD 5.4bn, with only c. 10-20% covered by insurance. This paper considers the financing of resilience where the probability of failure cannot be reliably estimated. In particular, the paper follows the propagation of disruption through available funds, goods and services supplied, consumers and broader trust. It draws on recent examples including the CrowdStrike incident, Change Healthcare and the Eurosystem T2 outage in February 2025. An accounting treatment distinguishes the depletion of assets and forgone income from payments by insurers, third-party claims or government support, all of which merely redistribute rather than reduce the original loss. The number of suppliers is misleading, given the near two-thirds share of the global cloud market by just three companies, and the commonality of their service providers. Building on a companion stress test of a payment network, investment in recovery will typically cost less than additional preventive measures, unless prevention is highly effective and repair already fast. With an exogenous measure of the economic cost of delaying a payment by one day, this can be quantified in monetary terms. Remaining gaps in coverage will depend on the terms and scope of commercial and state-provided solutions.

1 Introduction - The Need to Finance Resilience

On 19 July 2024 at 04:09 UTC, CrowdStrike pushed an update to the Falcon agent running on Windows. Virtually all machines receiving and reading the update shut down key functions and continued to do so on reboot and further attempts. Around 8.5 million machines were so affected, representing under 1 percent of all Windows machines.[1] The sequence of errors leading to this was apparently quite ordinary: an erroneous definition specifying 21 parameters for some data; code elsewhere supplying 20; validation performed against the definition and not against expected inputs to the code; and reading beyond the end of an array.[2] There was therefore no malicious activity. Nevertheless, many hospitals, banks, air carriers and others were severely disrupted in key operations, all dependent on the relevant functions, with presumably different management, security arrangements, risk management and insurance. Their only obvious common feature was the installation of the Falcon agent, configured to accept and act on pushed updates.

Parametrix, an insurer of business interruption from loss or damage to cloud services, believed around 125 Fortune 500 companies suffered disruption, with aggregate losses, excluding losses to Microsoft, of USD 5.4 billion, and that perhaps only 10 to 20 percent would be recovered under insurance.[3] Delta's cancellations over about five days exceeded 7,000 flights; it expected lost revenue of about USD 380 million, principally in refunds and goodwill payments to customers, plus around USD 170 million of other operating costs, partly offset by savings on around USD 50 million of fuel.[4] Other major U.S. air carriers, including Southwest and Alaska, which did not use CrowdStrike software, had relatively few cancellations, but Delta, including associated regional carriers, accounted for more than 60 percent of cancelled flights globally

on the following Monday.[5] Delta brought an action against CrowdStrike. CrowdStrike has indicated through counsel that it would be liable for no more than a few million dollars under the applicable contracts; in May 2025, a court allowed some but not all of Delta's various claims, including gross negligence and unauthorised access to computers, to proceed.[6] Nothing public suggests the proportion, if any, of Delta's losses for which CrowdStrike will ultimately be held liable.

Many features of the issue considered in this paper can be seen in this single example. Each organization will wish to make some provision for resilience against such events. The frequency of occurrence is not susceptible to reliable estimation from available information and the level of loss to any organization will be largely a function of its success and speed in restoring operations and of various prior risk-sharing arrangements. It is therefore appropriate that Klein and Singhal have called on regulators of financial markets and institutions to consider how resilient their key systems are, given the increased capabilities available to malevolent agents from AI.[7]

The associated SIAI paper considered what could be learned about possible systemic catastrophes in payment systems, by reference to a stress test of a notional group of 40 banks, conditional on the compromise of information allowing access to those systems operated by one common provider.[8] Its main results are briefly recalled below, in three paragraphs, but the main concern here is with the provision of finance for resilience. Sections 2 to 4 describe possible routes by which disruption may spread throughout the economy, the various types of losses suffered by different parties and the significance of the number of providers compared with the number of independent sources of disruption. Section 5 considers the relative merits of further prevention versus recovery, expressing these in monetary terms conditional on knowledge of one unknown parameter. Section 6 considers the scope for sharing risks under insurance and other public arrangements.

2 Transmission throughout the Economy

There will be at least four effects, each involving flows of funds. First, businesses continuing normally may fail to receive funds due to the lack of operation of other businesses' systems responsible for making payments to them. Second, there will be lost production. Third, there will be losses to customers. Fourth, there may be loss of confidence in the continuing provision of particular services, lasting some months. Each type of effect will fall initially on different businesses, so this is an important consideration in deciding which businesses should make what provision for resilience.

In February 2024, there was a successful attack on Change Healthcare, and its parent, UnitedHealth, shut down affected systems on 21 February. It provided loans, free of interest and other advances to many businesses. These totalled some USD 3.9 billion by the end of March, increasing to more than USD 9 billion by the end of June.[9] Many physicians, pharmacists, hospitals and other medical businesses, with no problem in their own systems, were unable to receive payment for claims submitted. The Centers for Medicare and Medicaid Services made accelerated payments of more than USD 2.55 billion to more than 4,200 hospitals and other providers of Part A services and advances of around USD 717 million to Part B providers, having recovered more than 96 percent of the total by the date of announcing closure of the

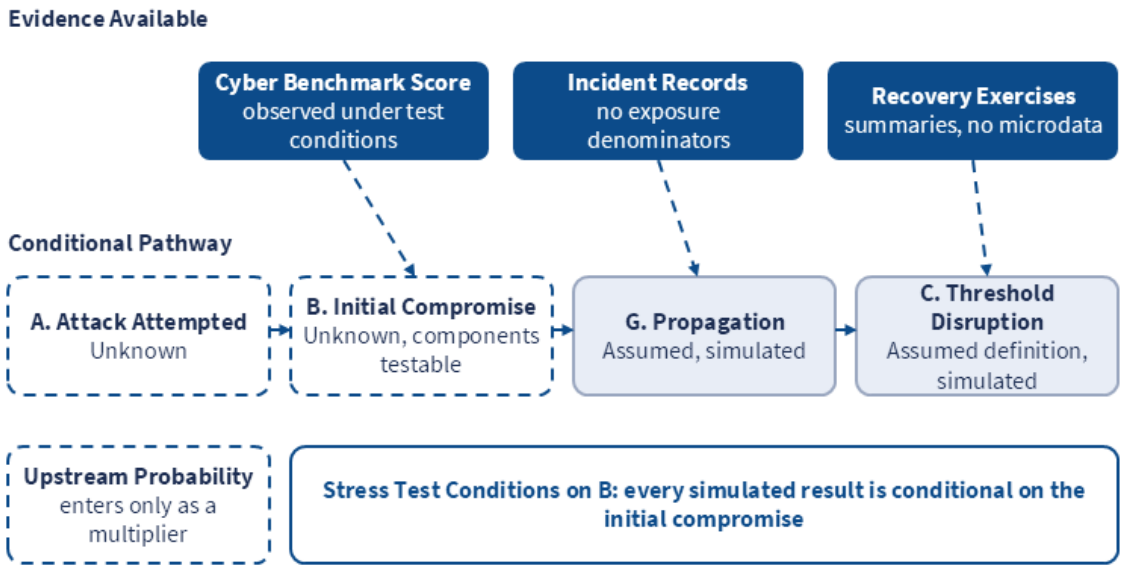
scheme in June 2024.[10] In each case the effect was to bring forward receipt of funds, alleviating a temporary shortage of liquidity, without replacing any lost assets.

There will be a similar effect, but on a much greater scale and for a shorter period, from disruption to major payment systems. T2 and T2S, the Eurosystem's payment and securities settlement systems respectively, were unavailable for about 10 and 8 hours on 27 February 2025, following a defective hardware component.[11] ESMA subsequently communicated that competent authorities would not seek to impose penalties for settlement failures on 27 February and 28 February, so avoiding substantial flows of funds between participants as penalties for failed settlements, due purely to failure of the common public facility.[12]

The results of the stress test described in the companion paper instead reflect an attack rather than inadvertent error, but have a similar implication for liquidity.[13] Assuming 30 percent of all banks are dependent on a single provider whose relevant data is compromised, 43.2 percent of all iterations exceeded the pre-defined threshold to be considered a catastrophe. Average loss over one week was 0.79 days' worth of timely payments, of which 0.25 was suffered by banks themselves unaffected but losing liquidity to other banks unable to meet timely payment obligations. Halving the time to restore operation would be expected to reduce this lost timely-payment capacity by 56 percent, with alternative routes to achieve settlement reducing it by 46 percent, segmentation of the network by 32 percent and restrictions on propagation by 27 percent. These are, of course, all illustrative, conditional on successful compromise of data at one provider. No inference can be drawn about the likelihood of occurrence.

Figure 1. Evidence reaches only the start of the pathway, while propagation and disruption rest on assumptions.

Evidential status of each link from cyber capability to payment-system disruption



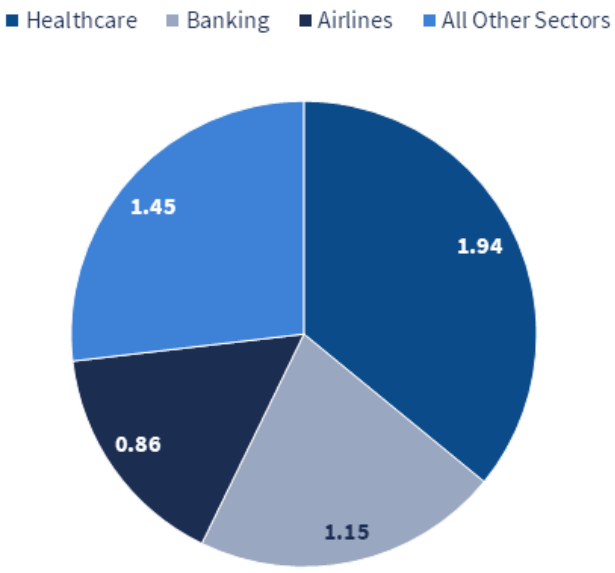
Note: Dashed borders mark unidentified links; dashed arrows show evidence that informs only part of a link. Every simulated result is conditional on the initial compromise.

Source: SIAI Research Editorial (2026) [AI and Cyber-Security] Measuring Catastrophic Risk under Uncertainty: Conditional Pathways, Payment-Network Stress Tests and Minimax Regret. SIAI Research working paper. Swiss Institute of Artificial Intelligence.

The extent of production loss will depend on the proportion of processes requiring real-time input from the disrupted systems, which will vary widely across businesses, as illustrated in the spread of estimated losses to Fortune 500 companies from the CrowdStrike event. Healthcare and banking sectors accounted for 57 percent of total losses, but only about 20 percent of total revenues. All 6 air carriers in the Fortune 500 suffered about USD 143 million each, but 130 manufacturing companies with total revenues of USD 3.4 trillion were estimated to lose only USD 36 million between them.[14] It may be possible to continue considerable production for at least a day or more with failure of planning and scheduling systems; an air carrier is likely to face considerable difficulty scheduling personnel and equipment to meet its next departures. The duration of serious dependency would be a major factor in total losses.

Figure 2. Healthcare and banking accounted for more than half of the Fortune 500 loss from the CrowdStrike outage.

Estimated direct losses of Fortune 500 companies by sector, July 2024 outage, USD billions



Note: Excludes Microsoft. All other sectors, manufacturing included, are the remainder of the estimated USD 5.4 billion total.

Source: Parametrix (2024) CrowdStrike to Cost Fortune 500 $5.4 Billion; Insured Loss Range of $540 Million to $1.08 Billion. Press release, 24 July.

Some customer losses will be transferred to the failed business, as in Delta's case, through rebooking, refunds and goodwill payments. CrowdStrike provided "commitment packages", comprising discounts and other favourable terms, to customers and estimated the effect on subscription revenues over the next 6 months at around USD 60 million.[15] It would be difficult to determine whether these amounts represented appropriate compensation, which might not be due under contract terms, or rather inducements to continue to purchase its products.

3 Distribution of Losses between Affected Parties

Many different figures may be quoted for total losses suffered, each appropriate to one aspect. The costs of investigating, responding to and remedying the failure will fall on one or more businesses; there will be lost revenues, there may be significant payments under insurance policies and other risk-sharing agreements and public funds may be advanced and penalties waived. Any sum combining two or more of these would double count some elements and omit others. Various possible elements and some rules of aggregation are set out in Table 1.

Table 1. Categories of Loss after a Shared-Provider Failure

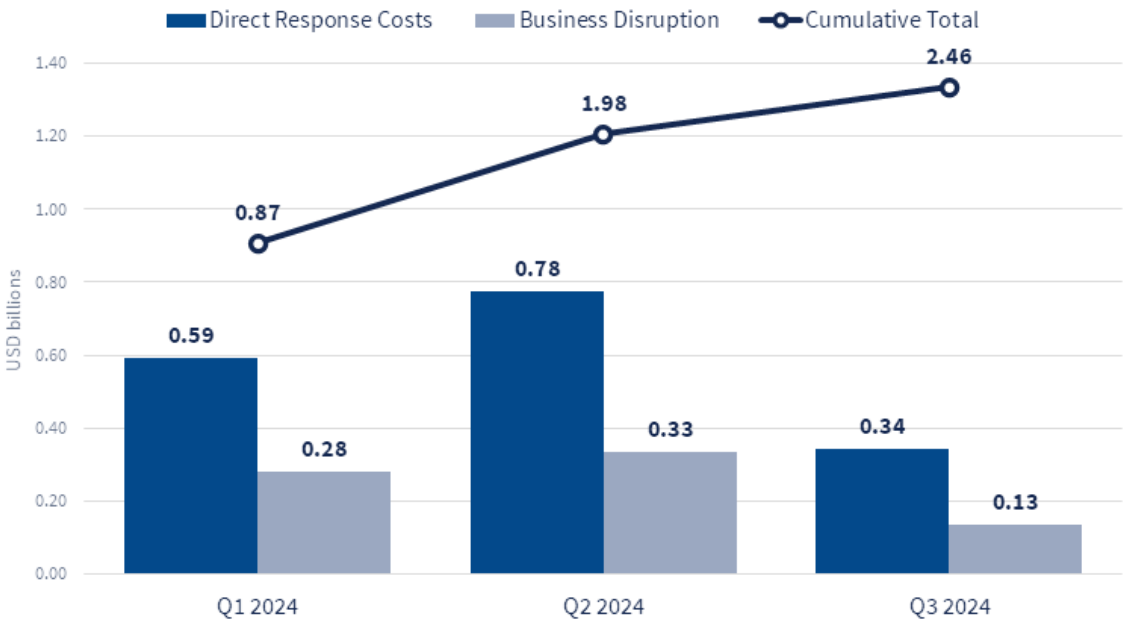
Category	Description	Illustrative example	Should not aggregate with
Loss of resources	Direct costs incurred responding to and recovering from event	USD 2.2 billion incurred by United-Health in 2024, including funding cost of interest-free loans	Amounts loaned, since only funding cost is lost
Lost production and sales	Value of net production lost as a result	Delta's lost revenue, net of saved fuel cost; Parametrix's estimate for all affected businesses	Additional sales to competi-tors; sales deferred
Payments by others to compensate	Under insurance and liability; service credits	Insured losses in consequence of CrowdStrike event; "commitment packages"	Any other category of loss, be-ing merely transfer of burden
Public funds advanced, penalties waived, con-tingent liability	Public liquidity, waived penalties and contingent backstops	Advances to clients of Change Health-care; waiver of penalties due follow-ing T2 failure	Gross advances, since rele-vant amounts would be net unrecovered and contingent amounts at risk

Source: UnitedHealth Group (2025); Delta Air Lines (2024); Parametrix (2024); CrowdStrike (2024b); Centers for Medicare & Medicaid Services (2024); European Securities and Markets Authority (2025)

Total losses are thus represented by the first 2 rows of Table 1. Row 3 identifies how the losses will be shared and row 4 shows public funds advanced and contingent liabilities assumed, but these give rise to losses only if unrecovered. As shown by its published results, a business may incur very substantial costs in rows 1 and 2. In the first three quarters of 2024, UnitedHealth reported costs of responding to the event of USD 593 million, 776 million and 341 million and lost revenues of USD 279 million and, for the 9 months, 747 million. Full-year amounts were USD 2.2 billion and 867 million, respectively.[16] It would be expected that, as owner of the failed operation and part of a group including one of the major payers of medical expenses under insurance contracts, it would wish to minimise disruption to its clients and would have ample resources to make advances. It is doubtful whether the owner of any other business providing similar services, although possibly similarly important, would wish or be able to make such advances, with the result that much greater disruption would be experienced by its clients and others.

Figure 3. Change Healthcare cost UnitedHealth nearly USD 2.5 billion in the first nine months of 2024.

Direct response costs and business disruption by quarter, with the cumulative total of both, USD billions, 2024



Note: Second-quarter business disruption is the nine-month total less the first and third quarters.

Source: UnitedHealth Group (2024a, 2024b, 2024c) Form 10-Q for the quarterly periods ended 31 March, 30 June and 30 September 2024. Minnetonka, MN: UnitedHealth Group.

CrowdStrike, at the other extreme, expects to be liable to its customers for very small amounts only, a few million dollars, on the terms of their contracts, for the successful prosecution of sufficiently serious allegations. Only a modest proportion of its customers' losses is expected to be insured, reflecting large deductibles and modest maximum cover relative to likely losses, according to Parametrix.

It would be very unusual for information sufficient to complete all rows of Table 1 for all parties affected to be available. The first published reports by financial institutions to their supervisory authorities of major ICT incidents under DORA, covering 2025 and all types of incidents, showed no estimate of either direct or indirect losses in about 40 percent of cases, the omission of the relevant field altogether in 15 percent and recovery of no amount by insurance, indemnity or other means in about 66 percent.[17] There is no apparent requirement for any subsequent report identifying the ultimate sources of funds meeting losses.

4 Number of Providers versus Independent Sources of Disruption

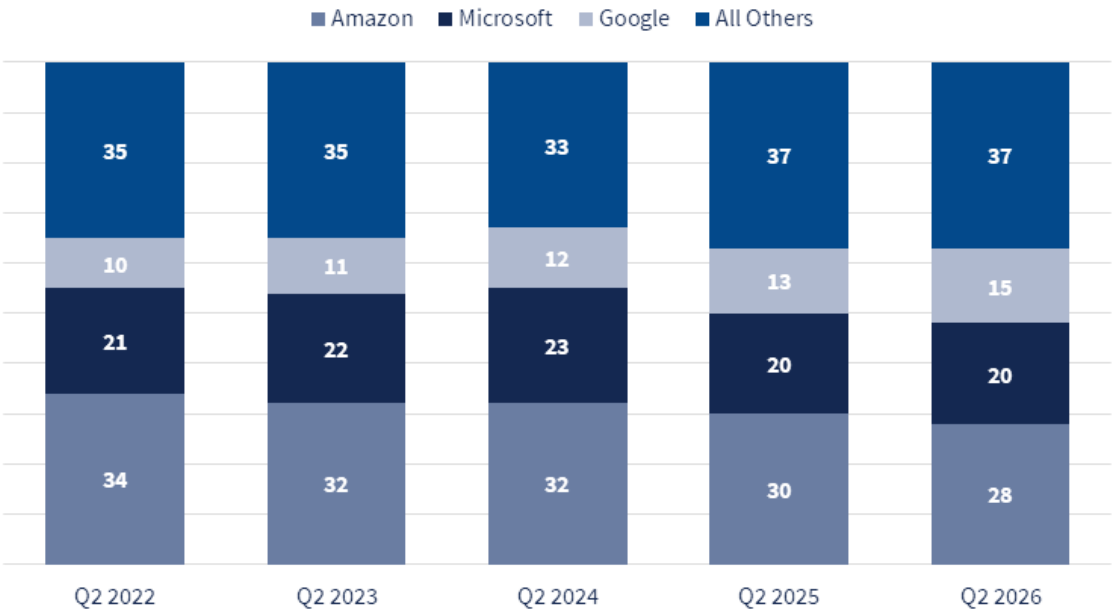
A business may purchase its payroll processing, CRM and other data processing from several unrelated providers. However, they may all use the same cloud service provider in one region, rely on one other provider for authentication, use the same provider of virus protection and other agents installed locally and so on. It may therefore have little redundancy if any one of these fails. The number of external suppliers of various processes is unlikely to be a good

indication of the number of separate events any one of which could seriously disrupt operations. There will be many levels and types of providers of infrastructure, for example cloud regions, authentication, locally installed software, content delivery and various network services, none of which may be identified to the business in its suppliers' contracts.

As indicated below, there does not appear to be any significant reduction of concentration as the total market has expanded. According to Synergy Research, the top 3 providers, Amazon, Microsoft and Google, accounted for 65 percent of total global revenue on cloud infrastructure in Q2 2022, when total expenditure per quarter was about USD 55 billion. In Q2 2026 they accounted for 63 percent of the much larger total, around USD 143 billion.[18] Amazon declined from 34 percent of the market to 28 percent and Google increased from 10 to 15 percent. All other providers combined have varied between 33 and 37 percent.

Figure 4. The three largest cloud providers held close to two-thirds of the market which nearly tripled.

Shares of worldwide cloud infrastructure service revenue in the second quarter of each year, percent



Note: Covers IaaS, PaaS and hosted private cloud services.

Source: Synergy Research Group (2022, 2023, 2024, 2025, 2026) Quarterly cloud infrastructure services market releases, second quarter of each year. Reno, NV: Synergy Research Group.

With such a concentration of the provision of basic infrastructure, failure in one cloud region may readily have a widespread impact on many supposedly independent suppliers to any business. The failure of part of Amazon's US-EAST-1 region on 19 October 2025 is an example. A "race condition" apparently lying dormant in certain automatic processes relating to DNS entries for DynamoDB resulted at that time in no entry at all at the relevant regional address, spreading over subsequent hours to other instances and load balancers. Various customers experienced effects at three separate times from 11:48 pm, 19 October to 2:20 pm the following afternoon, all Pacific time.[19] Many businesses were affected whose contracts were with other providers of applications or other functions using DynamoDB. Various functions relating to worldwide services were dependent on facilities in US-EAST-1, such as some updates to users' authorisations.

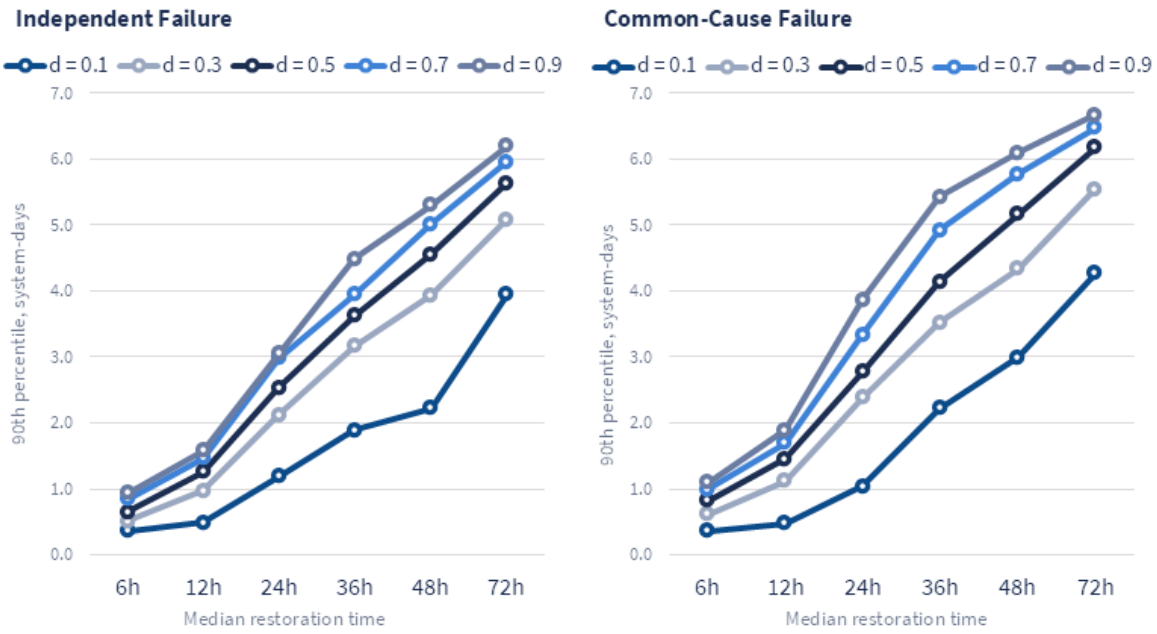
The supervisory authorities' report on incidents during 2025 indicated that 29 percent were due to failures at third parties and drew attention to the possibility that one event might lead to many major incident reports from various smaller institutions within a group, dependent on common major providers.[20] In an earlier exercise to map dependencies, the authorities identified around 15,000 providers of various aspects of ICT to the approximately 1,600 financial institutions sampled.[21] In November 2025 they designated 19 providers to be considered critical and so subject to direct supervision, including major cloud service providers, data centres, telecoms and FinTech.[22] The UK has introduced similar provisions, to apply from 1 January 2025 to providers so designated by HM Treasury.[23]

Such measures at the provider level may reduce the chance of failure and improve response to any failure, but cannot remove the problem of common failure of all dependent clients. Böhme and Kataria distinguish between correlation in failures of systems within one business and across businesses and argue that the latter will be relevant to difficulties of insuring, as determining the number of insured businesses simultaneously claiming.[24] Obvious reliance on another provider may remove dependency on one provider, but not on the common facilities used. Although the authorities may be able, from information provided, to identify providers and the facilities used by each financial institution, there seems to be little information available to individual institutions about further levels of dependency on their providers.

Results from the model described in the companion paper indicate the importance of correlation.[25] With an assumed constant expected number of initially affected banks, failures due to one common source gave lower average losses in 29 out of 32 cases compared with independent failures of the same total expected number of banks, but a higher 99th percentile in 27 cases. Intuitively, there is a limit to losses approaching total failure, but all affected banks will be severely affected simultaneously. Speed of recovery was a more important determinant of the extent of losses. Assuming 30 percent dependence on one provider and a common cause of disruption, increasing median time to restore operations from 6 to 72 hours increased average losses about tenfold, compared with an increase of about fivefold from increasing dependency from 10 to 90 percent, allowing 24 hours for restoration; with 72 hours, the 90th percentile was close to complete loss over a week.

Figure 5. Slow restoration raises tail losses more than high dependence and most under correlated failure.

90th percentile of lost payment capacity by median restoration time and share of participants relying on the shared provider, system-days



Note: Model simulation under stated assumptions. Results are conditional on the initial compromise; lines show the share d of participants relying on the shared provider.

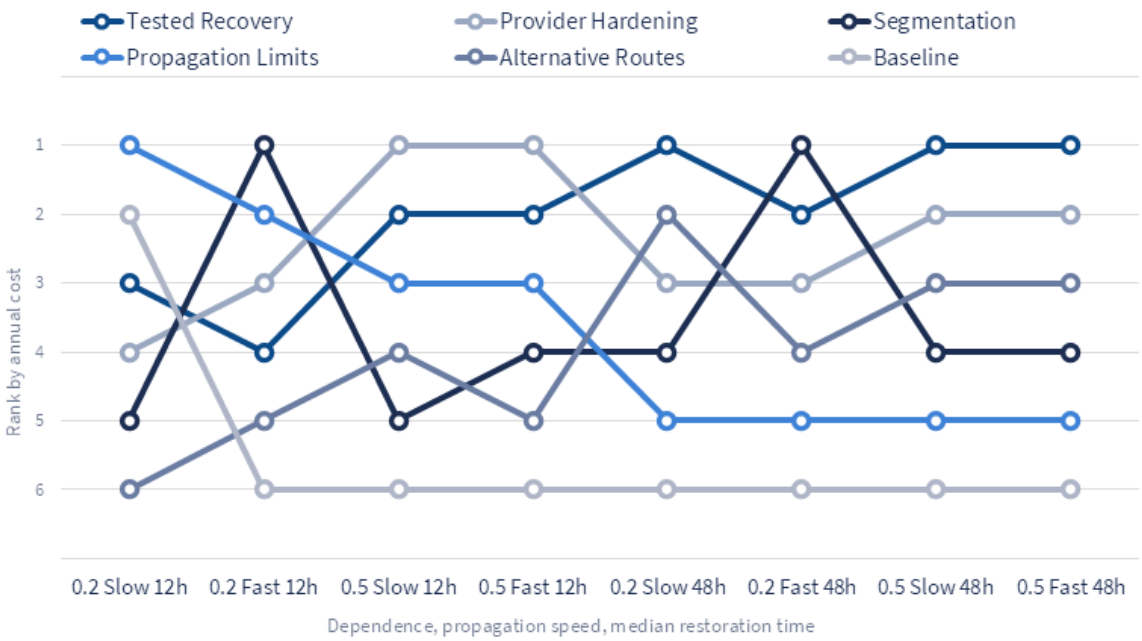
Source: SIAI Research Editorial (2026) [AI and Cyber-Security] Measuring Catastrophic Risk under Uncertainty: Conditional Pathways, Payment-Network Stress Tests and Minimax Regret. SIAI Research working paper. Swiss Institute of Artificial Intelligence.

5 Relative Benefits of Improved Recovery and Prevention

Further prevention at the provider level would benefit all users of the provider, but the provider would be unlikely to benefit directly to any significant extent, if liable for only small amounts in the event of failure. Improvements in the ability of individual clients to recover operations would benefit mainly themselves and in the case of a bank would extend to others with which it trades and would otherwise have suffered loss of liquidity. The companion paper compared the effects of various measures in this respect, over 64 variations in parameters defining structure of the system, assuming 4 alternative values of annual probability of successful attack resulting in compromise of data.[26] Assuming loss measured by expected value, minimal maximum regret was achieved by improving tested recovery times; at the 90th percentile of the distribution of losses, by alternative means of settling; and by improved security at the provider, assuming a constant additional loss on each occurrence exceeding a catastrophe threshold. If provider action reduced probability by 20 percent, tested recovery would always be less costly; if reducing probability by 50 percent, it would be preferable in 72 percent of cases, assuming 10 percent probability per annum, the median break-even probabilities for tested recovery and segmentation being 1.6 and 3.7 percent respectively.

Figure 6. Tested recovery is cheapest in three of four slow-restoration scenarios and no intervention leads everywhere.

Rank of each intervention by annual cost across eight uncertainty scenarios, upstream probability 0.1 a year; rank 1 is cheapest



Note: Model simulation under stated assumptions. Results are conditional on the initial compromise; scenario labels give dependence, propagation speed and median restoration time.

Source: SIAI Research Editorial (2026) [AI and Cyber-Security] Measuring Catastrophic Risk under Uncertainty: Conditional Pathways, Payment-Network Stress Tests and Minimax Regret. SIAI Research working paper. Swiss Institute of Artificial Intelligence.

These conclusions are expressed in terms of on-time payment value. Amounts could be derived if the following were known: the value settled on a typical day; the relevant costs of each type of measure; and the cost of one day's delay per unit of amount payable. If V denotes the value normally settled on a day, p the cost of delay of one day per unit of value, π the probability of successful compromise per year and ΔL the expected reduction in loss measured in days' value of payment on time, the cost per annum C of any such measure would be justified if no greater than π ΔL p V. Table 2 shows $\pi \Delta L$ under central assumptions in the companion paper for various measures, that is, the expected reduction per annum expressed as a proportion of value settled on one day.

Table 2. Expected Payment Delay Avoided by Each Intervention under Alternative Attack Probabilities

Intervention	Expected reduction per occurrence (days)	Value no longer delayed per year, % of one day's value		
		$\pi = 0.01$	$\pi = 0.03$	$\pi = 0.10$
Tested recovery	0.447	0.45%	1.34%	4.47%
Provider security halving probability	0.397	0.40%	1.19%	3.97%
Alternative settlement	0.368	0.37%	1.10%	3.68%
Segmentation	0.258	0.26%	0.77%	2.58%
Restrictions on propagation	0.217	0.22%	0.65%	2.17%
Provider security reducing probability by 20%	0.159	0.16%	0.48%	1.59%

Note: Model simulation under stated assumptions. Central scenario, conditional on the initial compromise.

Source: SIAI Research Editorial (2026) [AI and Cyber-Security] Measuring Catastrophic Risk under Uncertainty: Conditional Pathways, Payment-Network Stress Tests and Minimax Regret. SIAI Research working paper. Swiss Institute of Artificial Intelligence; SIAI calculations.

The results can therefore be expressed as the value of p required for break-even, given assumptions on other parameters. If the system in question normally settled 1 trillion euro on a day and there was a 3 percent chance of successful compromise each year, tested recovery would result in about 13.4 billion euro a year less expected to be delayed one day. An expenditure of 50 million euro per annum would be justified if one day's delay in receiving any amount cost at least 0.37 percent of its value. This will vary greatly with the purposes of payments, ranging from wages and calls on margin to many others with little urgency. It seems more reasonable to attempt to assess such costs of delay, using experience and data of operators of systems and other participants, than to attempt to estimate probability of attack. The relative benefits of each measure in Table 2 will be unchanged at any value of π, but which is best will depend on costs and on whether losses are assessed on mean, high percentile, or other assumption. Across the companion paper's scenarios, the expected amount recovered on time will vary most widely between cases, principally with speed of restoration of operations. It is consistent with this that most air carriers appeared to recover within a day or so of the CrowdStrike failure, while Delta was disrupted for about five days. It is unclear to what extent individual banks would be expected to provide for speedy recovery of operations, given positive spillovers to other participants.

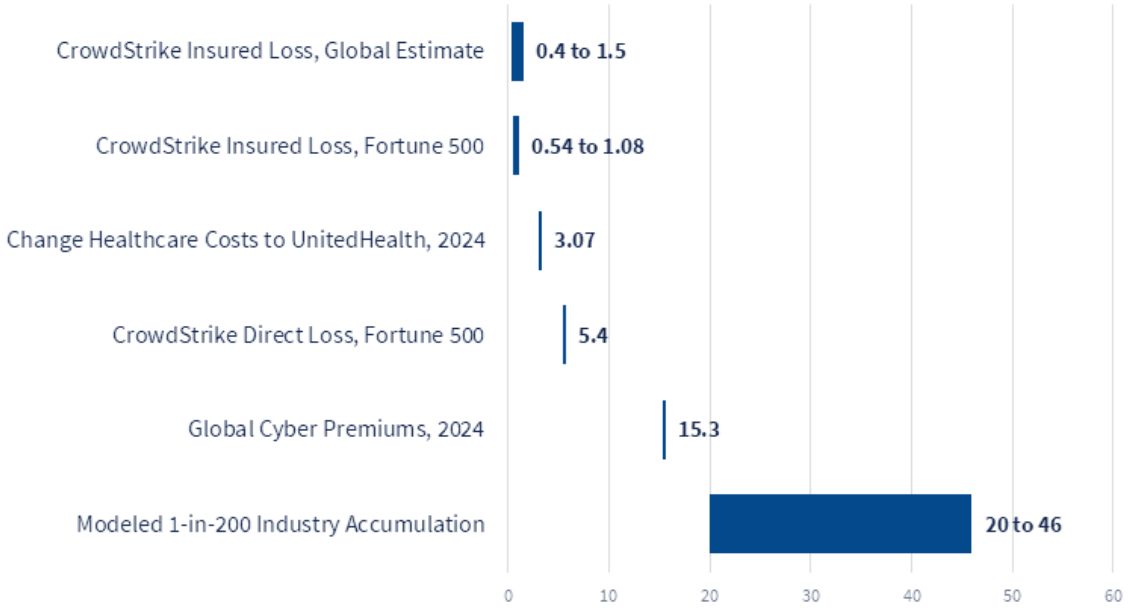
6 Scope for Insurance and Other Risk-Sharing

Insurance is most effective where there is widespread exposure and low probability of simultaneous losses to many insureds. Biener, Eling and Wirfs have argued that these characteristics apply particularly unfavourably to cyber risk, together with lack of information and problems of asymmetric information.[27] Premiums for insurance against catastrophes generally appear to be several times expected losses, reflecting the substantial capital required.[28] There would seem little difficulty in insuring losses from ransomware and other attacks, given wide variation in systems and security measures between companies, at premiums reasonably related to expected losses. However, only a premium or premiums reflecting substantial capital requirements would be appropriate for risks of attack on major shared facilities, if insured at all.

It would appear that losses from the CrowdStrike failure fell well short of the market's annual premium income. CyberCube estimated aggregate insured losses in the stand-alone market between 0.4 and 1.5 billion dollars, implying loss ratios of 3 to 10 percent, on total global premiums of around 15 billion dollars and considered this comparable to losses expected in 1 in 2 to 1 in 6 years.[29] Munich Re estimated 2024 global premiums at 15.3 billion dollars and cited modelled maximum global losses over a very wide range of return periods, up to 1 in 200 years, at 20 to 46 billion dollars.[30] Losses on the largest single event so far have therefore been well below one year's total premiums, although extreme modelled losses would substantially exceed them.

Figure 7. The largest insured cyber loss used a fraction of one year's premiums, while modelled extremes exceed them.

Estimated event losses, annual global cyber premiums and modelled 1-in-200 industry accumulation, USD billions



Note: Bars span published low and high estimates; single values are shown as short bars.

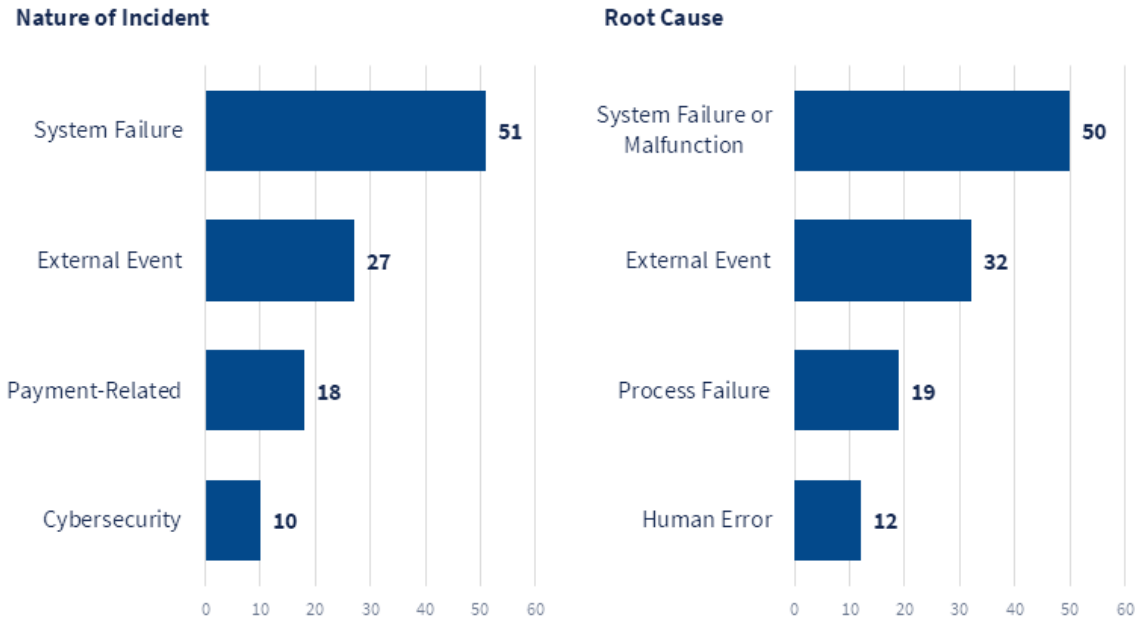
Source: CyberCube (2024) CyberCube Estimates $400mn to $1.5bn Global Insured Losses from the CrowdOut Event; Parametrix (2024) CrowdStrike to Cost Fortune 500 $5.4 Billion; UnitedHealth Group (2025) Form 10-K for the fiscal year ended 31 December 2024; Munich Re (2025) Cyber Insurance: Risks and Trends 2025.

A number of insurers appear to have sought to limit cover, for example by excluding significant state-sponsored attacks. Lloyd's has imposed this as a condition of writing stand-alone policies since March 2023, updating the requirement in May 2024, but recognising that systemic risk may result from other causes.[31] Many insurers apparently exclude losses following failure of major infrastructure and the U.S. Federal Government will share in losses only from attacks certified to be acts of terrorism.[32] This would normally require a violent or threatening act, so excluding the CrowdStrike incident and presumably most incidents identified by supervisory authorities, which indicate around 50 percent of major incidents due to simple system failure, both by nature and as root cause and 10 percent due to cybersecurity incidents.[33] Based on its experience with companies of all sizes, Munich Re sees about 3 times as many events involving malicious acts as otherwise, although the proportion due to other causes is greater for medium and larger companies. It currently estimates premiums in 2025 at almost 15 billion dollars,

below its forecast made a year before, increasing to about 28 billion dollars by 2030.[34] Total premium written directly in the U.S. recovered slightly in 2025, to around 9.46 billion dollars, after falling in 2024, with a higher proportion of 53 percent, compared with 48.7 percent, of premium absorbed in losses.[35]

Figure 8. System failures account for about half of major ICT incidents in EU finance and cyberattacks for a tenth.

Share of 3,383 major ICT-related incidents reported by EU financial entities in 2025, by nature and by root cause, percent



Note: Approximate shares; an incident can carry more than one classification, so shares exceed 100.

Source: European Supervisory Authorities (2026) 2025 Report on Major ICT-Related Incidents. JC 2026 16. Paris: European Supervisory Authorities, 3 June.

There are different considerations for the assumption of risks by public authorities. If the returns to an undertaking were uncorrelated with general economic welfare and widely shared between all taxpayers, Arrow and Lind argued that there would be little cost to the economy of the variability of outcomes.[36] The availability of payment systems is clearly highly correlated with the general state of the economy, so only limited comfort can be derived from this. Nevertheless, it seems that public authorities would inevitably have to meet much of any catastrophic loss, for example by preventing failure of major payment systems, or, as here, by provision of funds to medical providers. Each of these occurred spontaneously following events described above. It would be possible to arrange appropriate facilities in advance, on defined terms. The U.S. GAO in 2022 recommended that various authorities jointly consider provision of insurance cover against catastrophic events, but this apparently had not been undertaken as at May 2025.[37]

Various disclosures could assist in the assessment of risks and appropriate measures. Publication of typical times taken to restore operation of key systems after incidents would provide a guide to a key parameter. Mapping of dependencies between providers and their facilities, as far as information is available to the supervisory authorities, would enable businesses to assess more reliably the independence of various providers. Finally, publication, after about 1

year, of details of the ultimate sources of funds meeting each category of loss in Table 1 would be informative.

7 Conclusion

As shown, the widespread use of common facilities by otherwise unrelated businesses may leave them all similarly affected by one event. Disruption spreads via various channels, with timescales largely reflecting the speed at which businesses restore operations. There are various types of costs and losses incurred, as in Table 1, so various published estimates of losses will differ substantially in what they include. Only the first two rows involve net loss of resources, the rest representing agreement, court decision or public action as to which businesses should meet those losses. In the examples discussed, this has resulted in modest liability of providers, insurance covering a small proportion, 10 to 20 percent, of losses of major companies, substantial assistance from public funds and considerable losses borne by customers. There is no reason to expect any reduction in concentration of provision of key infrastructure and little information on which to base assessment of the number of truly independent sources of disruption.

Within the model considered, it is generally preferable to provide for faster recovery of operations than to further reduce the likelihood of disruption, except if the latter can be substantially reduced and there is already rapid recovery. Given further assumptions, the benefits could readily be expressed in monetary terms dependent on an unknown parameter, the economic cost of delay of one day in receipt of amounts due. There remains the question whether individual companies would rationally provide for as rapid recovery as is desirable from the point of view of spillovers, whether sufficient capital is available to insure against extreme losses and whether insurers will continue to widen exclusions and what further provision public authorities may wish to make. The various considerations discussed in this paper inform each of these questions, without providing answers. In particular, there does not appear to be any current estimate of the key parameter of the cost of delay.

References

[1] Weston, D. (2024) 'Helping our customers through the CrowdStrike outage', Official Microsoft Blog. Redmond, WA: Microsoft, 20 July.

[2] CrowdStrike (2024a) External Technical Root Cause Analysis: Channel File 291. Austin, TX: CrowdStrike, 6 August.

[3] Parametrix (2024) CrowdStrike to Cost Fortune 500 $5.4 Billion; Insured Loss Range of $540 Million to $1.08 Billion. Press release. New York: Parametrix, 24 July.

[4] Delta Air Lines (2024) Form 8-K, Regulation FD Disclosure. Atlanta, GA: Delta Air Lines, 8 August.

[5] Associated Press (2024) 'Most airlines except one are recovering from the CrowdStrike tech outage. The feds have noticed', Associated Press, 22 July.

[6] The Register (2025) 'Judge allows Delta's lawsuit against CrowdStrike to proceed with millions in damages on the line', The Register, 21 May.

[7] Klein, A. and Singhal, A. (2026) 'The financial system needs to be one step ahead on AI', in Brookings Institution, Is the AI existential threat real – and can regulatory action prevent it? Washington, DC: Brookings Institution, 23 September.

[8] SIAI Research Editorial (2026) [AI and Cyber-Security] Measuring catastrophic risk under uncertainty: conditional pathways, payment-network stress tests and minimax regret. SIAI Research working paper, November. Swiss Institute of Artificial Intelligence.

[9] UnitedHealth Group (2024a) Form 10-Q for the quarterly period ended March 31, 2024. Minnetonka, MN: UnitedHealth Group, 16 April; UnitedHealth Group (2024b) Form 10-Q for the quarterly period ended June 30, 2024. Minnetonka, MN: UnitedHealth Group, 16 July.

[10] Centers for Medicare & Medicaid Services (2024) CMS Preparing to Close Program that Addressed Medicare Funding Issues Resulting from Change Healthcare Cyber-Attack. Press release. Baltimore, MD: CMS, 17 June.

[11] European Supervisory Authorities (2026) 2025 Report on Major ICT-Related Incidents. Joint Committee report JC 2026 16. Paris: European Supervisory Authorities, 3 June.

[12] European Securities and Markets Authority (2025) ESMA Clarifies the Treatment of Settlement Fails with Respect to the CSDR Penalty Mechanism. Paris: ESMA, 14 March.

[13] SIAI Research Editorial (2026) [AI and Cyber-Security] Measuring catastrophic risk under uncertainty: conditional pathways, payment-network stress tests and minimax regret. SIAI Research working paper, November. Swiss Institute of Artificial Intelligence.

[14] Parametrix (2024) CrowdStrike to Cost Fortune 500 $5.4 Billion; Insured Loss Range of $540 Million to $1.08 Billion. Press release. New York: Parametrix, 24 July.

[15] CrowdStrike (2024b) CrowdStrike Reports Second Quarter Fiscal Year 2025 Financial Results. Austin, TX: CrowdStrike, 28 August.

[16] UnitedHealth Group (2024c) Form 10-Q for the quarterly period ended September 30, 2024. Minnetonka, MN: UnitedHealth Group, 15 October; UnitedHealth Group (2025) Form 10-K for the fiscal year ended December 31, 2024. Minnetonka, MN: UnitedHealth Group, 27 February.

[17] European Supervisory Authorities (2026) 2025 Report on Major ICT-Related Incidents. Joint Committee report JC 2026 16. Paris: European Supervisory Authorities, 3 June.

[18] Synergy Research Group (2022) Q2 Cloud Market Grows by 29% Despite Strong Currency Headwinds; Amazon Increases its Share. Reno, NV: Synergy Research Group, 28 July; Synergy Research Group (2026) Q2 Cloud Market Passes $143 Billion; Highest Growth Rate in Eight Years. Reno, NV: Synergy Research Group, 30 July.

[19] Amazon Web Services (2025) Summary of the Amazon DynamoDB Service Disruption in the Northern Virginia US-EAST-1 Region. Seattle, WA: AWS, October.

[20] European Supervisory Authorities (2026) 2025 Report on Major ICT-Related Incidents. Joint Committee report JC 2026 16. Paris: European Supervisory Authorities, 3 June.

[21] European Supervisory Authorities (2023) ESAs Report on the Landscape of ICT Third-Party Providers in the EU. ESA 2023 22. Paris: European Supervisory Authorities, 27 September.

[22] European Supervisory Authorities (2025) European Supervisory Authorities Designate Critical ICT Third-Party Providers under the Digital Operational Resilience Act. Press release. Paris: European Supervisory Authorities, 18 November.

[23] Bank of England, Prudential Regulation Authority and Financial Conduct Authority (2024) Operational Resilience: Critical Third Parties to the UK Financial Sector. Policy Statement PRA PS16/24, FCA PS24/16. London: Bank of England, 12 November.

[24] Böhme, R. and Kataria, G. (2006) 'Models and measures for correlation in cyber-insurance', Proceedings of the Fifth Workshop on the Economics of Information Security. Cambridge: University of Cambridge, June.

[25] SIAI Research Editorial (2026) [AI and Cyber-Security] Measuring catastrophic risk under uncertainty: conditional pathways, payment-network stress tests and minimax regret. SIAI Research working paper, November. Swiss Institute of Artificial Intelligence.

[26] SIAI Research Editorial (2026) [AI and Cyber-Security] Measuring catastrophic risk under uncertainty: conditional pathways, payment-network stress tests and minimax regret. SIAI Research working paper, November. Swiss Institute of Artificial Intelligence.

[27] Biener, C., Eling, M. and Wirfs, J.H. (2015) 'Insurability of cyber risk: an empirical analysis', The Geneva Papers on Risk and Insurance: Issues and Practice, 40(1), pp. 131–158.

[28] Froot, K.A. (2001) 'The market for catastrophe risk: a clinical examination', Journal of Financial Economics, 60(2–3), pp. 529–571.

[29] CyberCube (2024) CyberCube Estimates $400mn to $1.5bn Global Insured Losses from the CrowdOut Event. Press release. San Francisco, CA: CyberCube, 25 July.

[30] Munich Re (2025) Cyber Insurance: Risks and Trends 2025. Munich: Munich Reinsurance Company, April.

[31] Lloyd's (2024) State Backed Cyber Attack Wordings. Market Bulletin Y5433. London: Lloyd's, 14 May.

[32] Government Accountability Office (2022) Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks. GAO-22-104256. Washington, DC: GAO, 21 June.

[33] European Supervisory Authorities (2026) 2025 Report on Major ICT-Related Incidents. Joint Committee report JC 2026 16. Paris: European Supervisory Authorities, 3 June.

[34] Munich Re (2026a) Cyber Insurance: Risks and Trends 2026. Munich: Munich Reinsurance Company; Munich Re (2026b) Global Cyber Risk and Insurance Survey 2026. Munich: Munich Reinsurance Company.

[35] National Association of Insurance Commissioners (2026) Report on the Cybersecurity Insurance Market. Kansas City, MO: NAIC, October.

[36] Arrow, K.J. and Lind, R.C. (1970) 'Uncertainty and the evaluation of public investment decisions', American Economic Review, 60(3), pp. 364–378.

[37] Government Accountability Office (2025) Terrorism Risk Insurance Act: Considerations for Reauthorization. GAO-25-108748. Washington, DC: GAO, 23 September.