ITLF Availability/Service Resilience Paper 11

Treat IT resilience like we treat safety

Input in relation to the
Cyber Security and Resilience Draft Bill

Summary

The proposals outlined in the Cyber Security and Resilience Bill[1] are welcome and timely. The wider scope of the framework for reporting of the impact of cyber incidents to include Critical National Infrastructure[2] is a major step forward.

Our comments below are based on the knowledge that measures to anticipate, contain and recover from IT failures are similar for failures due to cyber-attacks and other sources of risk[3] . We also highlight the systemic risk to resilience from commonly used 3rd party software and services.

We[4] suggest that UK resilience could be further increased by:

1. Visibility of data on the impacts on users of all digital incidents, using existing frameworks – in the same way that the Information Commissioner's Office publishes information on fines[5];
2. Visibility of all digital incidents over a well-defined threshold – whether caused by cyber-attack or other types of IT failure, based on existing schemes, across all CNI sectors;

[1] https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement/cyber-security-and-resilience-bill-policy-statement

[2] There are 14 Critical National Infrastructure (CNI) sectors: Chemicals, Civil Nuclear, Communications, Data Centres, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water, https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure

[3] See Resilience of Services: reducing the impact of IT failures, https://londonpublishingpartnership.co.uk/books/resilience-of-services-reducing-the-impact-of-it-failures/

[4] "we" refers, in this text and others in the series of ITLF Availability Papers, to the Availability/Service Resilience Working Group of the IT Leaders Forum of the BCS – the Chartered Institute for IT, with insights from our extended network see https://www.bcs.org/membership-and-registrations/member-communities/bcs-it-leaders-forum/papers/ .

[5] https://ico.org.uk/for-organisations/the-guide-to-nis/incident-reporting/

3. Government support for information sharing on vulnerabilities and root causes (particularly related to 3rd party software and services), as well as impacts, across all CNI sectors, for instance based on the CISP[6] platform.

It may seem as though we are proposing more regulation at a time when government is rolling back regulation. However, the measures proposed emphasise the role of visibility of information, across organisations. This information is often in the public domain, but anecdotally and partially presented in news media.

Increased visibility in a structured manner is key to understanding the current status of services to users and to measuring progress made in improving resilience. Increased visibility would allow government, society and organisations and their technicians to share understanding, and to prioritise actions, to improve societal resilience and economic productivity.

Existing systems and new software

Recording and sharing data on software failures and their root causes can provide valuable insights—and is essential to improving current operational systems. But this is only part of the picture. Resilience will be improved through good practice in how software is built, tested, and deployed. Data will allow this good practice to be focused on improvement of services important to users.

Designing new software for failure helps mitigate the impact of individual component failures. However, organisations are dependent on existing systems while new software and systems are mostly developed outside the UK.

In operational systems, tools are available to scan and assess software quality, security, efficiency, and composition, while also enabling automated testing, enforcing compliance policies. Techniques allow teams to simulate stress conditions, uncover vulnerabilities, and implement compensating behaviours that maintain system stability under adverse scenarios. Application performance monitoring, combined with AI, can proactively detect and reduce failures. In practice, adoption of these tools and techniques is limited by cost, time, and resource constraints specific to the required service levels and by constraints due to the inherent complexity of legacy systems.

[6] CISP is a platform for cyber security professionals in the UK to collaborate on cyber threat information in a secure and confidential environment. It is managed by the NCSC and membership is free. CISP stands for Connect Inform Share Protect. About CISP - NCSC.GOV.UK

Background: UK Government policy statement

"The digital revolution is transforming our Critical National Infrastructure and our essential public services. It offers an extraordinary opportunity – to make our people and our country better off. However, it may also bring new and dangerous vulnerabilities. …

Our legislative proposals reflect the insights we have gathered from our international partners, including valuable lessons from the European Union on the implementation of its NIS2 regime. They are also informed by consultations conducted by the previous Government in 2022 and 2023.

However, it is vital that we also recognise the unique threats that the UK faces now and the threats that we cannot yet predict in the decades to come. At the same time, we must ensure that regulation works for businesses and investors, today and tomorrow."[7]

Cyber Security and Resilience Bill measures as announced in the King's Speech 2024 included:

1. Bringing more entities into scope of the regulatory framework
2. Empowering regulators and enhancing oversight
3. Ensuring the regulatory framework can keep pace with the ever-changing cyber landscape.

Three additional areas for consideration are outlined in the next three sections.

1. Visibility of data on impacts of incidents.
2. Visibility of all incidents - IT failures not just cyber-related.
3. Why information sharing.

[7] https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement/cyber-security-and-resilience-bill-policy-statement

1. *Visibility of data on impacts of incidents*

Service outages due to software failures of all types pose a significant risk to prosperity, productivity, security, health, and welfare. This is not adequately recognised in *shared societal understanding* regarding the consequences of digitisation, and this hinders the *prevention and preparation* for a resilient society. These risks are ever-growing as digital services are expected to be available 24/7 with these services becoming even more central to how we conduct business and live our lives.

No publicly available data

At present, there is no publicly available data in the UK on the incidence, duration, and impact of digital service outages. For instance, the cost to the UK economy of the CrowdStrike outage has, so far, been quantified by independent consultants at £1.7-£2.3 billion.[8] We are unaware of publicly available data in the UK or elsewhere on the incidence, duration, and impact of digital service outages. There is no central portal equivalent to that for Health and Safety[9] or Road Accidents[10]. The UK could take a lead in establishing frameworks for visibility of this information for digital systems.

The lack of data hinders prevention and cure

The absence of data on service outages hinders systematic learning about sources of failure and means for preventing and preparing for their impact. A lack of data fosters complacency - "software failures are like the weather – difficult to predict and impossible to control". A BCS Policy Brief[11] recommends that the government should create a central authority responsible for collating incident reports, as in the Mandatory Occurrence Reporting System operated by the UK Civil Aviation Authority[12].

The lack of data impedes insurance coverage

Insurance coverage for software failure and service outages is uneven and often specialised to risks like cyber-attacks at present, and classified as state

[8] https://www.kovrr.com/reports/the-uk-cost-of-the-crowdstrike-incident

[9] https://www.hse.gov.uk/statistics/

[10] https://www.gov.uk/government/statistics/reported-road-casualties-great-britain-annual-report-2023/reported-road-casualties-great-britain-annual-report-2023#headline-figures

[11] https://www.bcs.org/media/tvudbfex/transparency-software-is-the-elephant-in-the-room-policy-brief-v5.pdf

[12] https://www.caa.co.uk/our-work/make-a-report-or-complaint/report-something/mor/occurrence-reporting/

sponsored or criminal – with only the second being covered. Absence of data is an impediment to efficient functioning of insurance markets. This is of increasing importance as organisations need to insure against claims for non-delivery.

There is a precedent

A precedent has been set for Financial Services firms. The UK Prudential Regulation Authority (PRA) requires these risks to be mitigated through firms' business continuity plans, and scenario testing of these risks – with demonstrably successful stressed exit plans[13]. Similar guidelines have been put in place by the PRA's global counterparts[14], as well as embedded in key international standards like ISO27001[15] and the US Cybersecurity and Infrastructure Security Agency (CISA[16]).

A similar regime across CNI sectors would provide a basis for information sharing on the impacts of IT failures and decrease the risk and impact of failures in services to users.

[13] https://www.bankofengland.co.uk/stress-testing

[14] eg https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[15] See for instance https://www.socotec-certification-international.co.uk/certification-solutions/isoiec-27001

[16] https://www.cisa.gov/

2. *Visibility of all incidents - IT failures*

Recent headlines have reported cyber-attacks which may have been coordinated, and have caused extensive outages across many sectors.

As IT professionals we are concerned that the cyber-attack or threat discussion overshadows a vitally important component of our information infrastructure – the inherent or intrinsic risk of software (and hence system) failure. All software contains errors[17] and the construction of ever larger and more inter-dependent systems based upon software amplifies the potential for catastrophic system failures.

Failures do not require a 'bad actor' (from overseas or at home); many are an unintended consequence of complex software systems. Cyber security and software-based service resilience discussions need to acknowledge and address the intrinsic risks of software.

Much of the data on IT failures appears to be anecdotal and not collated. Systematic data collections with variable scope are addressed in the Treasury Select Committee Report in March 2025, covering over 150 IT failures over two years,[18] and the annual Uptime Institute Reports on data centre outages.[19]

Treasury Select Committee

BBC's Today Programme on 6 March 2025 featured - "Nine major banks and building societies operating in the UK accumulated 803 hours of tech outages in the years 2023 and 2024".[20] The item was based on data supplied by the banks to the UK Treasury Committee, covering over 150 outages.

Why the Nine Banks data is important

Financial Services organisations in the UK are intensive users of digital systems and each of the nine banks reporting data provides services through a complex

[17] The error rate for software has stayed at 25 errors per 1000 lines of code over many years, see https://www.bcs.org/media/9679/itlf-software-risk-resilience.pdf. The line limits for correctness proofs are in the low hundreds, https://www.sciencedirect.com/topics/computer-science/correctness-proofs. So, it is unsafe to assume that software is error free.

[18] https://committees.parliament.uk/committee/158/treasury-committee/news/205611/more-than-one-months-worth-of-it-failures-at-major-banks-and-building-societies-in-the-last-two-years/#:~:text=Nine%20of%20the%20top%20banks,by%20the%20Treasury%20Committee%20shows.

[19] https://www.networkworld.com/article/2079815/network-connectivity-issues-are-leading-cause-of-it-service-outages.html

[20] https://www.longfinance.net/news/pamphleteers/banking-system-failures/

collection of systems. Some of these systems are 50 years old; others are recently bought in from 3rd parties. The sector is stringently regulated and known for best practice.

The installed base of software is likely to be similar to other suppliers of CNI and so lessons learnt from analysis of the nine major UK Banks data may be useful in CNI sectors.

An analysis of the failures[21] found that fewer than 10 of the 150 outages reported to the Treasury Select Committee were possibly caused by a cyber-attack, each with relatively short outage times. This suggests that:

- Cyber-attacks have been largely prevented by efforts specified by the operational resilience regulatory regime for Financial Services in the UK.[22]
- Measures to anticipate, detect and recover from IT failures are limiting the damage caused by cyber-attacks.

Uptime Institute [23]

Uptime conducts surveys on both IT services-related outages and data centre downtime to determine what factors most impact enterprise networks and data centres. They found that the leading causes of publicly reported IT service outages in data centres are:

• IT (software/configuration)	23%
• Network (software/configuration)	22%
• Power	11%
• Cyberattack/ransomware	11%
• Fiber	10%
• Fire, cooling, other	23%

IT software was the single biggest cause of outage, nearly twice that of cyber-attacks. However, the loss of integrity of individual and organisational data, and the number of users affected, are also important in addition to the numbers of outages, in assessing the impact of outages on the economy and users.

[21] https://www.bcs.org/media/rxdmjr5h/availability-6-report-nine-banks-data-roundtable-220425.pdf

[22] E.g., https://www.fca.org.uk/firms/operational-resilience/insights-observations

[23] Uptime Institute provides data on facility and operations performance to and about data centres globally, https://uptimeinstitute.com/.

3. *Why Information sharing*

Information sharing is beneficial

The case for sharing information on failures is established in most industries, e.g., the chemical industry, aerospace, health. The IT industry is the exception.

Information sharing needs infrastructure support

There are companies in the private sector (Downdetector,[24] Uptime Institute[25]) providing data for their customer base. In the US, the AI Incident database contains over 3,000 examples of – specifically – AI applications that are harmful to the user[26] .

The increasing economic and social impact of IT failures[27] is such that a publicly funded infrastructure for information sharing is timely.

Information sharing benefits from common terminology

Based on the Nine Banks analysis, we identify three aspects where a common vocabulary would be helpful:

- Sharing information on vulnerabilities: the National Cyber Security Centre has published a guide;[28] FIRST has a Common Vulnerability Scoring System[29]; and the CERT Division of the Carnegie Mellon Software Engineering Division collates and publishes reports of vulnerabilities.[30]
- Sharing information on root causes: this might focus initially on 3rd party software and services[31].
- User Impact: The Network and Information Security Directive (NIS2) EU directive provides metrics for user impact through availability, data integrity, risk to health or life, and material damage, with thresholds for reporting incidences to be shared for regulated sectors. [32]

[24] https://downdetector.com/for-business/#historical

[25] As [5] above

[26] https://incidentdatabase.ai/

[27] As [2] above

[28]https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities

[29] FIRST is the global Forum of Incident Response and Security Teams. https://www.first.org/cvss/

[30] https://www.kb.cert.org/vuls/report/

[31] 3rd party software and services include open-source software, Commercial Off The Shelf Software (COTS), Software (or Infrastructure or Platform) as a Service, and Cloud services.

[32] As in https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement - Parliamentary Bill due later this year.

Increasing dependence on 3rd party software and services

The increasing reliance on 3rd party providers across large parts of the economy, including CNI, not only presents cyber security risks but also structural risks to operational continuity. In structural terms, supplier failure (e.g. bankruptcy), political risks, supply chain disruption and transfer of ownership are all challenges for organisations.

The IT supply chain is complex, and common 3rd party services within that supply chain cause a level of systemic risk. So, when thinking about UK resilience, we should also be aware of the potential for systemic failure as a result of concentration risk. For instance, whilst the cloud service providers have a very high level of resilience and availability, the impact of failures in this area could be wider than a single organisation. The recent Software Security Code of Practice[33] provides a framework for tackling this risk.

This commonality of individual software or services from a single supplier, across many organisations and sectors, represents an ongoing threat, and underpins the need for sharing of information on vulnerabilities, and causes of incidents. This would add to the value of tools for stress testing and simulation of attacks, such as the BEST family[34].

[33] https://www.gov.uk/government/publications/software-security-code-of-practice

[34] These include CBEST for financial services, https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide;
GBEST for government, https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/492229876481463 ;
TBEST for telecoms https://www.ofcom.org.uk/internet-based-services/network-security/our-work