ITLF Service Resilience Paper 3

Availability: the NIS Framework

This brief contains extracts from *Resilience of Services*[1] and builds on the work of the BCS IT Leaders Forum Service Resilience Working Group[2]. It provides an introduction to the NIS Framework and potential uses.

- IT is a utility and expected to be available 24/7: regulators and others are concerned to measure the impact of service outages on users.
- The UK's Network and Information Systems Regulations 2018[3] (the NIS regulations) require publication of data on service outages and data breaches for "relevant digital service providers", covering user hours lost, the volume loss of data integrity, the threat to health or life, and financial damage to users.
- We refer to the set of four metrics above as the NIS framework: this can provide a basis for sharing information and identifying causes of service outages and data breaches, leading to remediation, in sectors broader than "digital service providers".

Background

IT is a utility; users expect utilities to work

Most of our business and personal activities depend on services which include digital systems. IT is now a utility. Society does not expect utilities to fail: people expect their services to be available 24/7.

IT is built on software which is inherently fallible

However, digital systems, and hence user services, are based on software. This is a problem, because *software, unlike other widely used products, fails unpredictably*. This is because it is complex, it is subject to rapid change, and it is made up of many inter-dependent components from a multiplicity of sources. Services seem to be subject to increasing numbers and severity of outages. These

[1] https://londonpublishingpartnership.co.uk/books/resilience-of-services-reducing-the-impact-of-it-failures/

[2] https://www.bcs.org/media/3j1n1mhc/service-resilience-and-software-risk-2023.pdf

[3] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

affect increasing numbers of people and wider aspects of life as our dependence on digital systems increases. Software is the elephant in the room[4].

Software failures leading to service outages can arise from inherent software flaws, user error, cyber-attacks, or new vulnerabilities resulting from emerging technologies like Artificial Intelligence algorithms. Access to services may be blocked. Data may be lost, corrupted, or looted. A service outage may be ephemeral and affect only a small number of people – so ignored or attributed to random events like cosmic rays. It may also be long-lasting, affecting millions of people and lead to major damage to life and/or health.

Safety by design is necessary but will not meet the need

Legacy systems and systems procured from external vendors are dominant in UK organisations. Software has a long shelf life – many components still in use were designed for the conditions of the 70's. This means that organisations need a "whole systems" approach - based on the capability of the end-to-end system to deliver services to users.

The operational environment

Today, a "typical" operational environment includes:

- 24/7 operation of services to users;
- Multiplicity of external suppliers (several 100's of software vendors alone);
- Complex supply chains covering many jurisdictions for services and for software components.

Achieving service resilience involves IT but not only IT

The skills and capabilities needed to achieve more resilient services are often broadly dispersed within organisations. Often, the gaps in knowledge and practice are only recognised after an outage.

The first steps in building a more resilient organisation are about visibility of issues and responsibilities. Some very basic managerial tools such as RACI[5] provide a means for 'getting started' in assuring availability. *Availability management has become a critical and demanding role.*

[4] https://nationalpreparednesscommission.uk/publications/elephant-in-the-room/ and https://nationalpreparednesscommission.uk/publications/the-elephant-in-the-room-one-year-on/

[5] The RACI framework is based on assigning Responsibility and Accountability with Consultation and the Informing of stakeholders.

Organisational capabilities

Organisations can build partnership and consensus by developing 'translators' and attention to achieving a common language for discussing performance, between technical and non-technical people. *With a common language to measure the impact of digital systems failures it is easier to invest appropriately in service resilience.*

Metrics for user impact

User impact as a common language

As IT becomes recognised as a utility, availability – the ability to deliver 24/7 – will become of public interest. In the same way that rail transport publishes data on the cost of delays and cancellations to consumers, and organisations are mandated to report Health and Safety breaches, organisations will be judged on their service delivery, including those based on digital systems.

User impact as an organisational metric

One of the hurdles to improving availability within organisations is the complexity of the IT delivery supply chain and the lack of a common language for discussing performance, between technical and non-technical people. The introduction of user impact measures, visible across the organisation, allows the technical team to focus on priorities.

Organisations implementing the four steps of the FS Process[6] to improve resilience define Impact Tolerances for Important Business Services. An impact tolerance is defined as 'the maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption The use of user impact metrics to measure disruption focuses attention on the purposes of the business.

User impact as a metric for sharing data within a sector or publicising to the public

Organisations are sensitive to the potential reputational damage they might incur from visibility of service outages. This creates a barrier to the sharing of information about failures and their causes. Market incentives are inadequate – revealing the extent and impact of failures and their sources could make rivals

[6] https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-sop

more competitive. Government could take a lead by publishing data on service outages in the public sector[7]. This would contribute to detoxifying software failure. The lead from government could also include the support of a government or not-for-profit sector organisation, tasked with collecting, collating, and publishing data about service outages across all sectors.

The absence of data on service outages hinders systematic learning about sources of failure and preventing and preparing for their impact. It makes it more difficult to offer insurance and increases the insurance premiums charged for business continuity and related types of insurance. It fosters complacency - "software failures are like the weather – difficult to predict and impossible to control".

User impact data using the four metrics below could facilitate sharing of data.

Four metrics for user impact

One published framework for capturing and sharing information on the impact of data breaches and service outages is shown below.

Four metrics for user impact

Parameter	Metric
Availability	Your service was unavailable for a number of affected users for a duration of 60 minutes (lost user hours).
Integrity, authenticity or confidentiality	The incident resulted in a loss of integrity, authenticity or confidentiality of the data your service stores or transmits, or the related services you offer or make available via your systems.
Risk	The incident created a risk to public safety, to public security or of loss of life.
Material damage	The incident caused material damage to at least one user.

Impact on UK Economy

There is no publicly available data on the impact of digital systems failures on the UK economy.

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

Some published estimates of the cost impact of failures have been based on the cost of restitution to the supplier organisation[8] and applying this metric suggests a cost to the UK economy (2022 figures) as about £12 billion.

What is missing from this is that an important share of costs to the economy are external to the company that directly experiences the service outage. Here "lost user hours" provides an estimating basis by considering the value of time lost to the users during a service outage. The scale of these costs can be estimated based on assumptions on the aggregated amount of lost time and the average 'opportunity cost' of this lost time.

For the UK population, their use of the internet, and the assumed value of a lost user hour, the range of lost opportunity cost is between £4 billion and £35 billion, to be added to the £12 billion internal cost.

These numbers constitute a significant percentage of UK total GDP, ranging from 0.5-2%. In effect these losses can be understood as a drag on national income and productivity that is similar in proportion to the difference between positive growth and recession in recent years.

The NIS Framework

The four metrics discussed above are defined for network and information systems, i.e. any systems that process 'digital data' for operation, use, protection and maintenance purposes, by the UK regulator, the ICO[9].

Definition of NIS (network and information systems)

Network and information systems play a vital role in the economy and wider society, and the NIS regulation aims to address the threats posed to them from a range of areas. The regulation requires these systems to have sufficient security to prevent any action that compromises either the data they store, or any related services they provide. Although it primarily concerns cybersecurity, it also covers other causes of software failure and physical and environmental factors.

The NIS regulations are enforced by sector-specific 'competent authorities. The regulations in the UK apply to two groups of organizations: 'operators of essential services' (OESs) and 'relevant digital service providers' (RDSPs)[10].

[8] See *Resilience of Services,* as footnote 1, Appendix 1
[9] https://ico.org.uk/
[10] https://ico.org.uk/for-organisations/the-guide-to-nis/key-concepts-and-definitions/

The Information Commissioner's Office is the competent authority for RDSPs in the UK, with a range of powers to enforce the NIS regulations, including issuing fines of up to £17 million in the most serious cases.

OESs are organizations that operate services deemed critical to the economy and wider society. These services include communications, energy, health, transport and water. NIS is regulated in the UK by sector-specific 'competent authorities' for OESs.

Reporting thresholds

The UK RDSP regulator requires reporting if certain thresholds are exceeded:

- Availability: more than 750,000 lost user hours.
- Data compromised: the loss affected more than 15,000 users in the UK.
- Risk: No regulatory threshold
- Material damage: The damage to at least one user exceeded £850,000.

In other sectors the regulator could set different reporting thresholds.

Reporting thresholds as set by the regulator may also be higher than are needed to drive performance in the organisation. For instance, in thinking about critical national infrastructure[11], it is clear that detecting failures, at the level required for reporting alone, is insufficient to improve resilience.

For further information on the NIS Framework

Our book *Resilience of Services* (as above) contains further useful discussion and references.

Gill Ringland, Ed Steinmueller

[11] https://www.ncsc.gov.uk/collection/annual-review-2023/resilience/