Transparency – Software is the Elephant in the Room

This Policy Brief is based on the results from a two-year project by the BCS, The Chartered Institute for IT specialist group, the IT Leaders Forum, supported by the Business Continuity Institute and the National Preparedness Commission. The purpose of the project was to assess the risk to the UK economy and society from software failure and to make recommendations on the reduction of this risk. This Policy Brief is accompanied by a Technical Annex which provides access to the reports, blogs, and webinars on the topic, plus some links to other relevant sources.

Most of our business and personal activities depend on services which include digital systems. These 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 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 affect increasing numbers of people and wider aspects of life as our dependence on digital systems increases. Software is the elephant in the room.[1]

Service outages due to software failures are a risk to prosperity, productivity, security, health, and welfare. This is not adequately recognised in **shared societal understanding** of the consequences of digitisation[2], and hinders the **prevention and preparation** for a resilient society.

Software accidents leading to failure and service outages can arise from inherent software flaws, user error, cyber-attacks, or new vulnerabilities resulting from emerging technologies like Artificial Intelligence algorithms. Software failures are disruptive. 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.

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 CrowdStrike outage has, so far, been quantified by independent consultants[3] at a cost of £1.7-£2.3 billion. There is no central government portal where these figures are collated and are accessible to businesses and the wider society.

One earlier in 2022 estimate[4] , by the BCS IT Leaders Forum, suggested £12 billion per annum was a conservative estimate of the costs of software failure to the UK economy.

Shared understanding

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 more competitive. Government could take a lead by publishing data on service outages in the public sector. 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.

[1] » Lord Harris – Why Software is the Elephant in the Room (pictfor.org.uk)

[2] NPC_BCS_Software-Risk_-the-Elephant-in-the-Room_Dec-2022-Upload.pdf (nationalpreparednesscommission.uk)

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

[4] itlf-software-risk-resilience.pdf (bcs.org)

Prevention and preparation

The IT industry is working on a number of approaches to the reduction of software failures. These include using AI to increase the capability of software testing and to improve measures internal to service delivery organisations such as Mean Time to Repair. These approaches can be informed and focused to improve their impact on users by increasing the transparency of data on service outages.

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".

Who meets the cost of service outages? Direct costs are incurred by the organisation responsible for the service, and indirectly by their users.

Attempts by the service delivery organisation to recoup the costs they have incurred are often limited to disputes between them and their suppliers of software and digital service. These may be difficult to resolve due to the complex supply chain, lack of knowledge of responsible actors, and the web of inter-dependencies. For the many services that we rely upon such as financial, logistics, scheduling, ecommerce etc. services, there is little precedent for re-imbursing users for their costs of service outages. An exception is the backstop scheme set up for re-insurance to deal with catastrophic impacts of terrorist attacks.[5]

Our conclusions are that:

- Service outages of digital systems represent a cost to the economy through lost user hours, loss of access to data, damage to health and life, and financial damage which is largely hidden and is the elephant in the room.
- Data on service outages would provide a focus for work by the IT industry on addressing software failures.
- Market forces cannot provide this data.

Therefore, we recommend:

- The government should create a central point responsible for collating incident reports, similar to the Mandatory Occurrence Reporting system operated by the UK Civil Aviation Authority since 1976. Government departments could take the lead in publishing failure data on their own services, using a framework based on the RDSPs proposed by the NIS directive 2018[6] . This framework could cover aspects like availability, integrity, authenticity, confidentiality, risk, and material damage to users.

- We also recommend that boards of organisations that provide UK Critical National Infrastructure (CNI) services should have an accountable company board member for cyber and software resilience. Improved trust should be established to enable more effective sharing with private sector organisations that provide or support UK CNI services.

[5] Insurers in talks on adding state-backed cyber to UK reinsurance scheme (ft.com)
[6] The NIS Regulations 2018 - GOV.UK (www.gov.uk)