Availability: the challenge for IT professionals

Report from a RoundTable

Held at BCS London on 9th January 2025

Contents

Authors: Gill Ringland, Ed Steinmueller, Paul Reason.

Table Facilitators: Andy Fenton, Chris Fowler, Paul Reason, Gill Ringland, Ed Steinmueller.

Insights from Professor Alan Brown, Professor Michael Mainelli.

January 2025

Summary

The **#Crowdstrike** outage last year showed yet again how dependent we are on IT systems. Millions of Windows systems crashed, disrupting critical services and business operations globally.

The BCS IT Leaders Forum (ITLF) held a RoundTable on 9th January at the BCS, The Chartered Institute for IT offices, on *Availability: the challenge for IT Professionals*. The RoundTable discussed what could reduce the impact of IT failures on users, the economy and society; and the challenge for IT professionals.

The RoundTable also marked the launch of Gill Ringland and Ed Steinmueller's book, *Resilience of Services: Reducing the Impact of IT Failures***,** based upon and extending the work of the BCS ITLF Service Resilience Working Group. The book is available on Kindle or book form at Amazon, and for order at https://londonpublishingpartnership.co.uk/books/resilience-of-services-reducing-the-impact-of-it-failures/

Key takeaways:

- IT is a utility; users expect utilities to work.
- IT is built on software which is inherently fallible.
- Safety by design is necessary but will not meet the need – legacy systems and system procurement from external vendors are dominant features of today's IT world.
- Cultural change - firms must understand the reputational and financial risks of service failures and plan to reduce their impact on users.
- Transparent and open reporting is a must - along with a system for sharing information so lessons can be learned.
- Organisations need to have access to highly skilled tech professionals.
- The importance of developing frameworks to understand the economic cost of outages – to combine assurance with insurance.

Next actions

The report makes a number of recommendations. ITLF will be working with appropriate partners to progress these over the next months. We actively seek input of ideas and data, and offers of help: the authors' emails are:
gillringland@gmail.com, w.e.steinmueller@sussex.ac.uk, paul@reason.me.uk.

Background

IT is a utility; users expect utilities to work

The RoundTable shared the knowledge that most of our business and personal activities depend on services which include digital systems, that **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 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].

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 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. We discuss measurement systems and the recognition of Important Business Services, in the next section.

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

The operational environment

It is worth describing a "typical" operational environment:

- 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.

Organisations need IT Professionals to have new capabilities

This means that a new set of capabilities are needed to maintain services to users, e.g.

- Testing new components to anticipate and avoid failures in a 24/7 system;
- Ability to work effectively with legal/commercial to ensure adequate protection for the organisation's service commitments;
- Systems thinking eg compartmentalisation to localise failures, focus on important services and the impact of failures on users.

Organisations need to ensure that they manage their risk

IT is the bedrock of the services supplied by most organisations. IT is built on software which is inherently fallible. ***Organisations are mostly unaware of the extent – duration or business impact – of potential failures[2].***

This report includes references (see Appendix 3) to a framework and to a set of processes which can create shared awareness of risk across organisations and within the organisation.

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

Measuring and communicating risk

Firms must understand the reputational and financial risks of IT failures and plan to reduce their impact on users.

The RoundTable considered a framework for measurement, the NIS Framework, which defines user impact. It also considered a set of processes and language for describing Important Business Services and Impact Tolerances. A key step in both is defining the external customers who would be affected by outage of these services.

Transparent and open reporting is a must - along with a system for sharing information so lessons can be learned.

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, and this hinders the ***prevention and preparation*** for a resilient society.

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 at a cost of £1.7-£2.3 billion. There is no central portal where these figures are collated and/or are accessible to businesses and the wider society.

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". The BCS Policy Brief[3] recommends that 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.

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

Skills and capabilities of organisations and their IT professionals

Achieving service resilience involves IT but not only IT

The skills and capabilities 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 need to be visible. Some very basic managerial tools such as RACI[4] provide a means for 'getting started' in assuring availability.

The RoundTable found that a systematic approach to skills involves assessing the need - fundamentals, knowledge and expertise. This will help in identifying gaps and disconnects within an organisation. The gaps and disconnects may be bridged by either development of internal capability or by externally procured capabilities. There is no magic bullet that will assure that the necessary skills are available.

Improving internal capacity involves a process of upgrading of learning and skills to gain 'soft' skills, address competencies, and provide mentorship. This often benefits from the use of external standards and qualifications. The characteristics of people to deliver availability management are not easily inferred from a CV or specific qualifications. The role involves values about doing the right thing rather than performing to nominal goals; and an ability to move between larger system perspectives and details of implementation. ***Availability management has become a critical and demanding role.***

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, it becomes easier to enlist the support of management and board level decision makers for investment in service resilience.*** The RoundTable members agreed that IT Leaders could be talking to their boards with a *Cost/time to fail* graph: this shows that greater investment in service resilience buys a lowering of the risk of service failure, but that the risk can never go to zero. This visibility of the organisation's calibration of risk could reduce insurance premiums and could in the future be a requirement to obtain any insurance at all.

Organisations also need to promote the culture of 'safe spaces' for people to openly discuss service resilience and its value to the organisation. This involves more open discussion of failures and outages and the early signs indicating instability or risk. One model may be to

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

draw on some of the practices common in health and safety where there is a positive obligation to call out issues.

Organisations need to establish a 'What If?' approach to planning for future potential scenarios to ensure they have adequate protections in place (similar to futurist approaches but with more concrete scenarios). One way forward is to define and conduct 'pre-mortem' examinations of large-scale failure to address managing organisational risks.

The needs for resilience are increasing everywhere, but in some sectors more rapidly and extensively than in others. This suggests establishing norms on a sector-by-sector basis. This could reset expectations regarding skills and behaviours, and the possibilities for publicity/transparency on failures and their impact.

Economic impact

IT as a utility

IT is now a utility- we expect it to work (like water). Users sue utilities if they fail to deliver their services, and organisations are able to insure against the costs incurred in settling claims.

However, for failures of an IT utility, there is no recognised set of metrics. We need to improve the economic analysis of outcomes (e.g. adopt common methodologies and frameworks) to be able to apply insurance thinking – translating risk into the trade-off between the costs of prevention and the costs of insurance against failures.

At present insurance coverage for software failure and service outages is uneven and often specialised to risks like cyber-attacks. These may be classified as state sponsored or criminal – only the second is covered.

Efficiency vs resilience

The prevailing culture is for organisations to be driven to be efficient. This precludes building in redundancy of staff or processes; and puts pressure to reduce costs e.g. by neglecting anticipatory planning. Further, the assumption among most senior managers is that "it [IT failure] will not happen on my watch".

A further complication is that the consequences of outages are often borne immediately and directly by service users who have little or no recourse to recompense from the service provider. Ultimately, these users may seek other services, but they are unlikely to do so immediately. As a result, a service provider focussed on short term profitability performance sees little value in incurring the costs of building resilience.

Organisations will increasingly need to insure against claims for non-delivery. Insurance allows organisations to balance efficiency against contingency. Claims could come as fines from a regulator or from organisations or, in some jurisdictions, 'class action' claims.

Measuring impact

A starting point for disentangling these issues is the NIS framework which describes four aspects of cost/impact to users. These are cost of "lost user hours", cost of data breaches, cost of damage to life or health, and significant financial impact to users. This is used by the ICO to regulate RDSPs, but it is not a widely used framework for costing the economic impact of service failures.

The development and ***wide use of a methodology for better analysis of cost/impact would allow senior managers to make decisions about the acceptable costs of any disruption, and to insure against it.*** Initiatives are needed to get endorsement and promote such a methodology.

Discussion at the RoundTable

Even with improvements in economic analysis there are a series of practical questions that flowed from the RoundTable discussion. These included:

- Important Business Services were seen to be effective in regulated sectors – what are the incentives if no regulator – in some sectors where uptime is revenue earning, down time is not, this provides incentive.

- In the public sector there is no link between uptime and revenue, or ease of use and revenue. What incentives apply in the public sector?

- How can a vendor insure their software? For example, should a storage provider in the cloud be insured against the likelihood of storage availability issues affecting emergency service response? Consensus was that this should be the service owner that insures for this outcome.

- Assurance vs Insurance – It is more valuable to prevent my house from burning down than to be recompensed via insurance. How do we factor the assurance that something won't fail and the value of the reduced likelihood of failure into the service delivery ecosystem? How far can the cost of insurance feed into the investment calculation?

Recommendations

The following recommendations are based on discussions at the event, were formulated after the event, and reviewed by RoundTable participants. ITLF will be working with appropriate partners to progress actions in line with these recommendations.

Promoting Awareness of Risks and Their Costs

IT is a utility, and users expect utilities to be available. But IT is implemented in software, and software is inherently fallible. Organisations need to plan for the risk of failure of IT based services.

- We need to improve the economic analysis of outcomes (e.g. to adopt common methodologies and frameworks).
- Transparent and open reporting provides basis for more comprehensive insurance coverage.
- Insurance impels organisations to make a clearer assessment of the costs of prevention measured against the cost of insurance.

Recommendation 1: Develop and promote economic analysis supporting development of insurance for service failure risks.

Accompanying the risks of failure is responsibility – the need for visibility of ownership (e.g. using a RACI matrix) of service resilience risks and not just IT team. There is sometimes a lack of understanding that boards should own the risk and a reluctance to do so – it's an 'IT' problem.

Recommendation 2: Engage with practitioners who use RACI for assigning responsibility for Availability.

The need for measurement, management and understanding of risks to service resilience spans individual organisations. Building a common language for assessing the consequences of service failure such as the NIS Framework, and hence the value of prevention and mitigation, is an urgent task. The financial service approach of identifying important business services, setting failure tolerances, and investing in prevention and mitigation to stay within these tolerances is a workable approach that addresses the lack of cultural appreciation for service resilience.

Recommendation 3: Publicise the NIS Framework and the FS process using IBS and Impact Tolerance.

Promoting safe spaces for people to be open about service resilience is necessary to make the value of resilience visible. There is a 'getting started' issue in building transparency that presents an opportunity for public sector leadership.

> Recommendation 4: Work with government to support Transparency in the public sector. Ideally this would be followed by broader transparency initiatives in regulated sectors and the economy as a whole.

Need for highly skilled tech professionals

There is a clear need for credentialing, mentoring standards regarding skills in availability engineering and resilience management that suggests several very specific recommendations.

> Recommendation 5: Discuss with appropriate Universities eg Newcastle University re computer science training on resilience.

> Recommendation 6: Review ITIL 4 and recommend updates if necessary.

> Recommendation 7: Work with SFIA framework to ensure it represents the need for Availability and recommend updates as needed.

> Recommendation 8: Develop mentoring related to Availability, for BCS members and others.

Engagement across and outside the organisation

Bridging the silos of development, operations, and user adoption/use of systems vitally important to building resilience. Scenario-based (or pre-mortem) analysis of not only recovery but restoration is essential for setting priorities in resilience investment, analysing the potential for failure before it happens, and what can go wrong.

> Recommendation 9: Organise/publicise events that develop and apply resilience management methods such as case studies or simulations

Raising the perceived value of resilience capability can make an important contribution to societal improvement. We need to make practices such as business continuity planning an attractive proposition to our best people and to signal its value to boards, IT teams, and society as a whole.

> Recommendation 10: Organise/publicise a prize related to making resilience work, possibly joint with IRM[5] and/or BCI[6].

[5] https://www.theirm.org/what-we-do/about-us/
[6] https://www.thebci.org/

In addition, there are relevant recommendations from the recent BCS response to government on Cyber Security.

All organisations should:

> Enforce a ‘secure and resilient by design’ culture for all critical and important IT systems
>
> Enforce strong cyber governance, including continuous monitoring/assurance of third parties, especially in government and Critical National Infrastructure supply chains.

Government should:

> Introduce a Cybersecurity Code of Practice with mandatory breach reporting and quarterly reporting on risk (including third party risk) rather than, as currently, a voluntary code.
>
> Require Boards to include a member who will be held accountable for their company's cyber security throughout its life cycle.

Appendix 1: The Brief

Our economy and society are increasingly dependent on digital systems.

- IT Leaders are assumed to be responsible for **availability** of digital systems in the new operational paradigm in which these systems
    - Must operate 24/7.
    - Require proactive management of complex hardware and software supply chains.
    - Are ever more complex and interdependent, ensuring that failures will occur.
- Software underpinning digital systems
    - Fails.
    - Fails in unpredictable ways, not just due to user error or cyber- attack.
    - Includes many legacy elements – some embedded components are 50 years old.
- Boards need to be aware of the financial and reputational risk from service outages and data breaches that accompany digital systems failure.
    - A process and language for this is the definition of Important Business Services (IBS) and the setting of tolerances for duration and scope of failures that that the organisation can accept.
    - A framework for measuring the impact of failures is the Network and Information Systems (NIS) framework: it measures lost user hours, lost data integrity, damage to life of health, and financial impact of outages or data breaches on users.
- New skills are needed to deliver measurable availability in the new operational paradigm.

Invitation

We will explore these issues in an event: "Availability: the challenge for IT professionals". This will bring together CIOs and other experts to discuss how to meet the new Availability challenge in terms of leadership, skill and methods. It will be held at BCS, 25 Copthall Avenue, London EC2R 7BP from 4-6pm on 9th January, by invitation. The agenda includes short briefings, discussion in groups and feedback, and refreshments. The aim is to create a network of people committed to improving the Availability of digital system.

Copies of the book *Resilience of Services: reducing the impact of IT failures* will be given to all participants. ***Please RSVP to gillringland@gmail.com if you would like a place, as space at the venue is limited.***

Appendix 2: Participants: alphabetic order without titles:

Alan Brown
Alan Farrell
Andy Fenton
Bob Compton
Chris Fowler
Claire Penketh
Dai David
Daljit Rehal
David Geere
David Harding
David Knott
Dominic Aslan
Ed Steinmueller
Fred Tear
Giles Lindsay
Gill Ringland
Holly Porter
Indrajit Sugunasingha
James Davenport
Jeff Parker
Joe Little
John Morton
Jon Hammant
Jonathan Leeson
Katie Barnes
Michael Crooymans
Michael Mainelli
Neil Bourke
Neville De Mendonca
Nick Drouet
Paul Reason
Paul Williams
Peter Smith
Randolph Kent
Richard Corbridge
Roger Maull
Sat Gainda
Steve Sands
Sue Milton
William Hooper

Appendix 3: Measurement and reduction of the impact of failures on users: two management tools

NIS Framework – measurement

The NIS framework[7] measures the 'consequences' of outages and provides a set of metrics for the consequences to service users. See table below for the thresholds set by the ICO for Registered Data Service Providers.

Parameter	Threshold
Availability	*Your service was unavailable for more than 750,000 user-hours.* The term "user hour" refers to the number of affected users in the UK for a duration of 60 minutes.
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. *The loss affected more than 15,000 users in the UK.*
Risk	The incident created a risk to public safety, public security, or of loss of life.
Material damage	The incident caused material damage to at least one user in the UK, *and the damage to that user exceeded £850,000.*

Approach based on regulations for FS[8]

- Financial service (FS) regulations aim to improve the resilience of the FS industry by defining Important Business Services and acceptable outcomes – Impact Tolerances
- The definition of Important Business Services provides a shared language for managers and IT Professionals to agree priorities
- The process to achieve acceptable outcomes or consequences – the Impact Tolerances - is generic and a useful template for all sectors.

[7] https://ico.org.uk/for-organisations/the-guide-to-nis/what-is-nis/
[8] https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience