SERVICE RESILIENCE AND SOFTWARE RISK

NOVEMBER 2023

bcs The Chartered Institute for IT
IT Leaders Forum

bci Leading the way to resilience

CONTENTS

WHY THIS REPORT?

The UK Government Resilience Framework[1] is built around three fundamental principles:

- That we need a **shared understanding** of the risks we face;
- That we must focus on **prevention and preparation**; and
- That resilience requires a **whole of society approach**.

This report identifies the risk from software failure as a hurdle to national resilience; resilience is defined as "action to prevent or mitigate risk". We – people and organisations in the UK - are increasingly dependent on services that are at risk from software failure. This report makes recommendations to prevent software (defined as "the programs and other operating information used by a computer") failures and to mitigate the risk from these software failures to the resilience of service delivery.

There is insufficient **shared understanding** of the actual and potential risk of software failures and their impact. Recent surveys show that the C-Suite are overwhelmingly unaware of the risks to their business and reputation from service outages due to software failure. Shared understanding is needed before most organisations will adopt adequate policies, budget, and processes to prevent software failures and be able to mitigate their consequences. With software, preparation means having recovery procedures in place before failure occurs. Implementing adequate prevention and recovery processes will require investment in skills and knowledge at operational levels.

Much software in use today is old – up to 40 years (legacy) – with new components supplied by the global industry. There is evidence that digital systems are increasingly liable to service outages due to failures in hardware, software, user errors, cyber-attacks among other causes, and that these outages are increasing in scale and duration as well as becoming less predictable in timing. In thinking about **prevention and preparation** (for recovery), a service resilience (impact focused) approach is more effective than attempting to improve software component design or purchase.

The cost to the economy of service outages due to software failures is at least that of road accidents and increasing. Outages due to cyber-attacks and interest in AI have raised the level of interest in the role of software risk in service resilience. Failures in infrastructure services

have a particularly important effect on the rest of the economy: the regulatory regimes of infrastructure sectors in the UK have recently been oriented towards keeping consumer costs down rather than continuity of service: "keeping the lights on".

Impacts on users, the economy and society, are not collected or collated despite their significance[2]: **a whole of society approach** is needed.

WHAT CAN BE DONE?

A RoundTable (see Acknowledgement for participants) shared their expertise to agree a set of recommendations.

A first step in **prevention and preparation** is to improve our measurement of the cost of service outages arising from software failures.

Recommendation: Metrics

The public sector should take the lead in gathering and sharing this data, taking **a whole of society approach.**

Recommendation: Public Sector Leadership

Financial services authorities have defined a set of processes to increase service resilience which can be applied to other sectors. Infrastructure is particularly vulnerable and outages here have an effect across the UK economy and society.

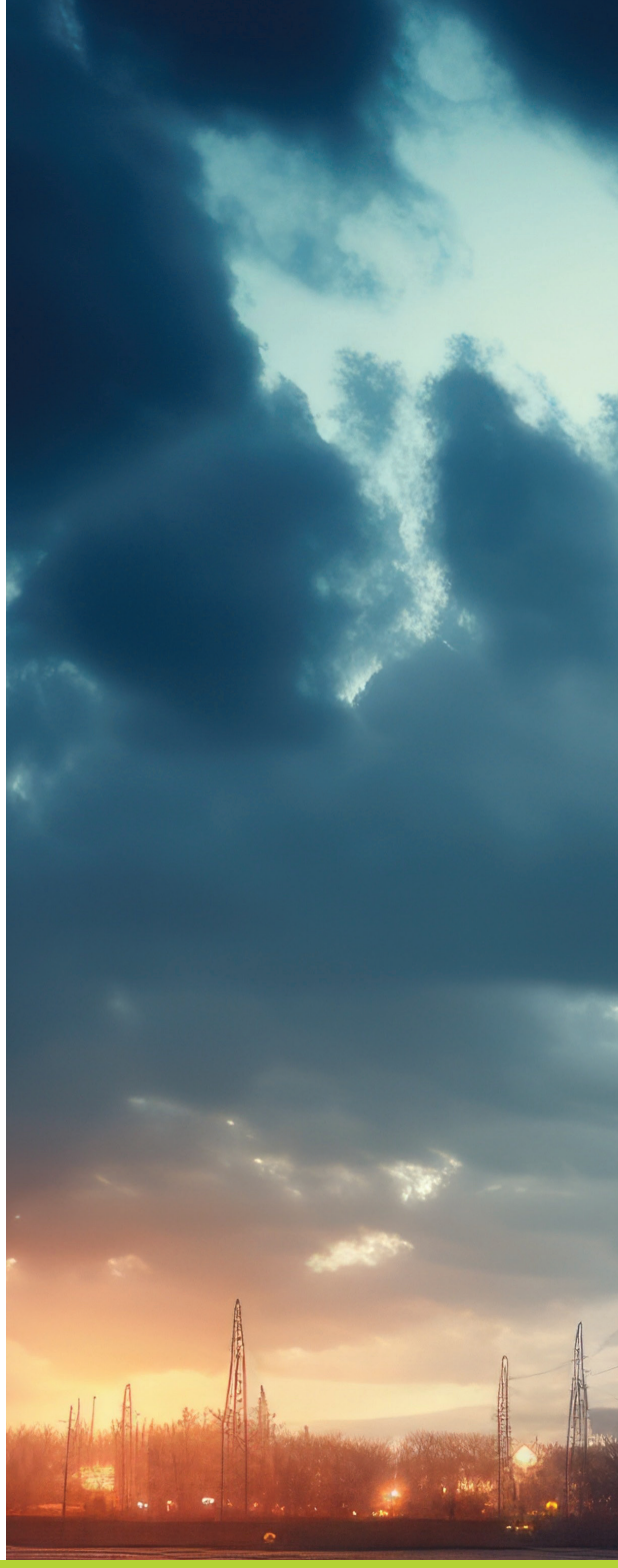
Recommendation: Infrastructure

Organisations in the public and private sectors can take measures to reduce service outages and increase resilience.

Recommendation: Measurement and Mitigation in Organisations

Shared understanding of the economic and societal impact of software failures, and their impact on services, should be part of management education. IT and risk professionals should develop and promote education, training and testing for service resilience in 24/7 operational conditions.

Recommendation: Education and Training



WHAT HAPPENED AT NATS[3]

Around 2,000 flights at airports across the UK were cancelled when NATS' system for automatically processing flight plans failed on August 28th, 2023. NATS has said the problem was caused by a flight plan featuring two waypoints – which use letters and numbers to represent locations – with identical names. Giving evidence to the Commons' Transport Select Committee, Ryanair boss Mr O'Leary said: "Why did they collapse their system? We have written confirmation from other ATC (providers). (They) said they routinely and regularly receive flight plans that have duplicate waypoints in them. So this is not something complicated. NATS not just collapsed the main system. They collapsed your backup system. All your engineers were sitting at home watching morning television instead of being where they're supposed to be."

Mr O'Leary said the cost to Ryanair of paying for meals, drinks and hotel rooms for affected passengers was £15 million.

(We add, the cost to affected passengers was likely to be considerably more).

RECOMMENDATIONS

In this section 'we' refers to the BCS Service Resilience Working Group taking account of views from the RoundTable.

METRICS

(See "What would increase confidence in service resilience?")

Service outages due to software failures reduce society's productivity, security, health, and welfare[4]. Taking action to reduce these consequences requires shared understanding. This depends on two factors. The first is a common language for classifying the type of impact – the consequence - of service outages. The second is a better knowledge of the magnitude of the incidence and impact of software failures.

We recommend the adoption of the Network and Information Systems (NIS) framework[5] for classifying and measuring the impact of service outages following software failures. This framework focuses on four measures: availability (lost user hours); loss of integrity, authenticity or confidentiality of data stored or transmitted; risk to public safety, public security, or of loss of life; material (financial) damage to users. While adoption of this framework does not indicate strategies for prevention or preparation, it does improve shared understanding and provides a quality benchmark for data collection.

PUBLIC SECTOR LEADERSHIP

(See "What would increase confidence in service resilience?")

The government is in a unique position to improve national resilience of services using software across the UK by classifying and measuring its own performance, and by sharing this data across society. This transparency would show leadership and promote the use of digital methods to increase efficiency.

We recommend that the government should:

- Take a lead in publishing data on service outages of government services due to software failures, using the NIS framework.

- Set up either a government or a non-profit organisation tasked with collecting, collating, and publishing data about software failures and related service outages across all sectors.

- Consider a backstop for re-insurance against the impact of catastrophic outages. (see "What are the hurdles to software resilience and what works in improving it?")

INFRASTRUCTURE

(See "What are the hurdles and what works in improving service resilience?")

We are highlighting a new risk resulting from the increasing dependency of Industry 4.0 (and digitalisation in general) on infrastructure systems. The obligation to provide essential services is embedded into laws and regulations because social well-being and economic health depend on it. But many infrastructure organisations do not yet appreciate the potential scale and impact of this risk, so they are not prepared for the consequences resulting from software failures. Infrastructure failures have knock-on effects on the economy and society, and infrastructure organisations are particularly liable to service outages due to software failures.

We recommend that:

- The remit of regulators in OES's (Operators of Essential Services) should include requiring reporting on digital service outages, using the NIS framework.
- This would enable regulators to address and set standards for service resilience.
- See also the recommendations on "Measurement and Mitigation in Organisations"

MEASUREMENT AND MITIGATION IN ORGANISATIONS

(See "What are the questions that leaders of organisations should be asking about the resilience of the services they deliver?")

We recommend that all organisations that use or supply services involving software (very few do not!) should:

- Think more holistically about the impact of service outages on doing business, delivering on their purpose, or meeting their commitments;
- Identify their critical business services and define tolerances for the failure of these services after software failures in terms of user disruption (e.g. how long access is unavailable, how many users are affected) – the service delivery approach. This requires considering how critical services often depend on suppliers of linked services.
- Develop or adopt means of testing their systems to improve their confidence of being able to stay within failure tolerances and avoid damaging customers or other organisations depending on their systems.
- Design and put in place alternatives or workarounds consistent with the organisation's tolerances of failure. These should include restoration of data generated during the outage; investing in the additional human capacity or skills needed; and implementing robust communication and operational protocols.

EDUCATION AND TRAINING

(See "What would increase confidence in service resilience?")

More IT and Risk professionals need to understand methods for increasing service resilience under 24/7 operational conditions.

We recommend that

- BCS and the Business Continuity Institute (BCI) should promote certification of organisations and professionals in Service Resilience to software failure, e.g.
- Build upon the Cyber Essentials Certification as a possible model;
- Provide templates for Post Graduate University Courses.

Recent surveys find that the C-Suite are overwhelmingly unaware of the risks to their business and reputation from service outages due to software failure. Awareness of the economic and societal impact of software failures and their impact on services, should be part of management education.

We recommend that Government, Boards and C-suite should take steps to improve their confidence in their organisation's service resilience against software failures. This could include:

- Activities to engage the imagination of senior managers about failure possibilities and consequences through simulation games or working through software failure scenarios.
- Dialogue structured around the service delivery approach and leading to action planning to improve resilience to software failures across their supply and demand chains;
- Management education of the next generation of C-Suite to ensure better understanding of the role of resilience in delivering services.

BCS and BCI should engage with Business Schools to develop appropriate management education.

SHARED UNDERSTANDING

BCS and BCI should work with Trade Bodies, Policy Makers and others to advance implementation of the Recommendations.

WHAT HAPPENED AT TSB

TSB[16] has been fined £48.65 million over a botched IT platform migration in 2018 that locked 2 million of its customers out of their accounts. The IT upgrade "immediately experienced technical failures", the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) said, resulting in "significant disruption" to TSB's in-person, online and phone banking services. The regulators found that TSB failed to organise and control the migration adequately and failed to manage operational risks from its IT outsourcing setup.

BACKGROUND

A Pamphleteer published through z/yen in 2020 said "--- software is a problem flying just under the radar, ready to fall into the soup, leaving devastation in its wake. It could crash our planet."[6]

A Working Group[7] of the BCS[8] studied the size and shape of the risk from software to the UK economy. The Group published a report[9] and held a joint RoundTable with the National Preparedness Commission (NPC)[10]. The Working Group on behalf of the BCS answered a call from the Department of Science, Innovation and Technology, the "Call for views on software resilience and security for businesses and organisations." This report was presented internally to BCS audiences, to the Digital Policy Alliance, in webinars[11] [12] and as a basis for published blogs [13] [14].

Members of the Working Group have been active in engaging with and consulting a wide range of professionals, within the IT profession and in related areas: see the list of people consulted at the back of the report. In September 2023, the Group published a report, identifying what could be done to reduce software risk to the resilience of services[15].

This report builds on the September report and RoundTable discussions held on 25th October 2023: the participants are listed at the back of this report. The RoundTable asked and answered three questions:

- What are the hurdles and what works in improving service resilience?
- What are the questions that leaders of organisations should be asking about the resilience of the services they deliver?
- What would increase confidence in service resilience?

The RoundTable also explored the use of an interactive simulation to frame discussions in the C-suite using Crisis Simulation Platform - Conducttr **(www.conducttr.com).**

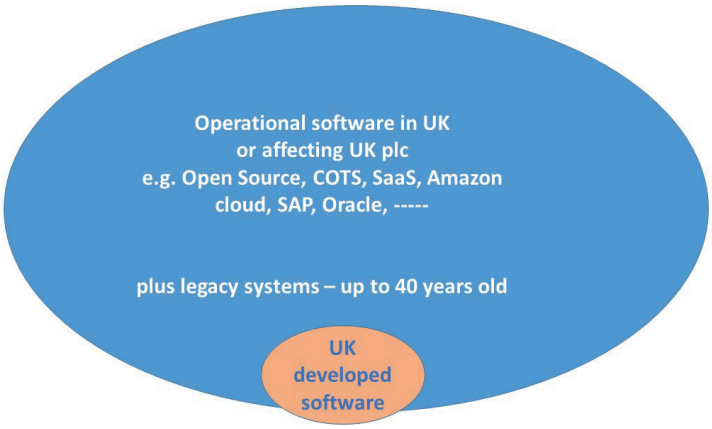
SOFTWARE IN THE UK - THE CONTEXT

Many people – including IT professionals – have not understood the paradigm-shifting changes in software usage and supply over the past few years.

Software failures can result from relatively modest, limited, or non-obvious factors or incidents as well as from cyber-attacks. The resulting service outages can seriously affect many people and stakeholders. There is increased visibility of service outages from cyber-attacks and software "accidents". The consequences of software failures leading to service outages are now potentially huge, both in scale and extent.

Trends contributing to the increase in these risks include the complexity of digital systems and more people using online services, particularly post Covid. The explosion of AI application focuses attention on the quality of the underlying software, and the trust that can be placed in outputs.

Software now consists of loosely and tightly coupled complex



systems which are liable to unpredictable failures. The software components used by most organisations are supplied by a web of organisations from across the globe. Combining old (legacy) and recent technology – which have different reliability characteristics - can result in operational instability.

Neither formal methods for software development nor testing will deliver "zero defect" software in the short to medium term.

A service delivery approach – focussing on consequences -- rather than a software component approach – focussing on standards for software development - is therefore essential to increase service resilience and reduce service outages and their impact on the resilience of the UK.

WHAT ARE THE HURDLES AND WHAT WORKS IN IMPROVING SERVICE RESILIENCE?

One hurdle surfaced by the RoundTable was interview results showing that 90% of CEOs think that everything is fine. This complacency leads to poor risk management – 'the software has not failed before so we can get away with risking it in the future' or 'It never fails on my machine.' This means that many decision makers are not aware of potential impacts, the seriousness of consequences, and the extent and numbers of those potentially affected by service outages arising from software failure. And differences in attitudes to outages and how to deal with them, across sectors and also between organisations in a sector, can be astounding.

Culture and power dynamics were seen as major hurdles, particularly as the business environment changes and dependence on technology increases. There can be reluctance to collect data about operational experiences of using software products or services. There is even more reluctance to share this information. Supplier contracts were also highlighted as a hurdle to resilience. Many organisations do not have the expertise to assess contracts, while global suppliers offer contracts with one-sided terms and limited or no penalties.

In discussing "what works", participants mentioned methodologies successfully used in Critical National Infrastructure. The methods include technologies for testing in a 24/7 environment such as used in emergency services. These are not widely used even though failures in many other sectors - particularly Other Essential Services (OES) - could also cripple the economy.

We highlighted a new risk resulting from the increasing dependency of Industry 4.0 (and digitalisation in general) on infrastructure systems. But infrastructure organisations do not yet appreciate the potential scale and impact of this risk, so they are not prepared for the consequences of software failures. The regulatory regimes of infrastructure sectors in the UK have recently been oriented towards keeping consumer costs down rather than "keeping the lights on". It was thought that the remit of regulators in OES's should include requiring reporting on digital service outages, using the NIS framework. This would enable the regulators to address wider resilience requirements.

We discussed the role of insurance. Currently, the cost of some cyber-attacks is met – but the industry is not yet clear on a way forward. One approach that is being considered is a scheme similar to that employed for terrorist attacks in which the government financially back stops the re-insurance industry for catastrophic failures.

A service delivery approach based on the guidelines from regulators in financial services was highlighted and discussed in the next session.

CULTURE AND POWER DYNAMICS WERE SEEN AS MAJOR HURDLES, PARTICULARLY AS THE BUSINESS ENVIRONMENT CHANGES AND DEPENDENCE ON TECHNOLOGY INCREASES.

WHAT ARE THE QUESTIONS THAT LEADERS OF ORGANISATIONS SHOULD BE ASKING ABOUT THE RESILIENCE OF THE SERVICES THEY DELIVER?

Paul Williams, National Preparedness Commissioner, described the service delivery approach based on the regulatory guidelines for financial services[17]. This is an organisational approach with software as an important part. It is principles and outcomes focussed. It simplifies how you look at the problem.

Which software-dependent services:

- Is the business most financially dependent on?
- Would have the most significant reputational consequences?
- Has the biggest consequences for customers in case of failure?

What are the impact tolerances for each service (e.g. based on the NIS framework) in terms of:

- User hours, data loss/access, damage to life or health, financial impact?

The overall conclusion of the RoundTable was that this approach applies outside financial services because it provides a framework for agreements on priorities between decision makers and other functions including the IT team. Three specific implications of this approach are:

It encourages focus on **organisational needs and differences**. Organisations may have critical services which relate to their business cycle or business model. Examples were tabled of discussions on times of year that services were essential – like tax collection deadlines for accountants or HMRC. Other organisations were focussed on community impact – their reputation with customers was critical and defined their critical services.

THIS MEANS THAT ORGANISATIONS NEED TO DETOXIFY FAILURE SO THAT INFORMATION CAN BE SHARED.

The service delivery approach also encourages conversation across functions in the organisation on **costs and benefits**. In the private sector this could be about the balance of investment versus risk and involve the risk management function. In government, the concept of intolerable harm could be a focus. In regulated sectors, there are statutory objectives. (It was noted that these did not currently adequately focus on resilience i.e., "keeping the lights on").

The RoundTable also concluded that there is **no one-size fits all** implementation of the service delivery approach. Not all organisations need to provide 24/7 resilient services based on software. Examples are games platforms, where users are often co-opted into the development and testing of the game: this approach is not appropriate for services that people rely on and that are integral to many facets of our daily lives.

Across all sectors there is a need to think holistically about the impact of service outages on doing business, the tolerance for failure, and delivering on their purpose or meeting their commitments. In addition to staying within failure tolerances, it is important to have alternatives or workarounds in place, along with restoration of data to include that generated through the outage; investment in the additional human capacity or skills needed; and communications and operational protocols, consistent with defined tolerances for failure.

In tackling "how could the data on failure instances and causes be gathered?" the RoundTable started

with the understanding that software fails. This means that organisations need to detoxify failure so that information can be shared. Overcoming reluctance to sharing this information could involve incentives, e.g. the creation of a 'safe harbour', that would demonstrate the benefits of sharing.

A first step in sharing data is the creation of a shared taxonomy, for instance the NIS framework. Then, to protect sources, data can be anonymised before collation. This would provide a safe haven for sharing information between organisations. There is a precedent in infrastructure stress tests which use firewalls to protect individual organisations. (However, in practice anonymisation removes important context and hence value, so should only be undertaken on the data at the time it is passed to other organisations.)

The RoundTable also discussed what data could lead to improvements in service resilience. Participants agreed that a well maintained body of evidence is central. This should include not only catastrophic failures but also information about minor failures and near misses (canaries in the coal mine) as defined in the ITIL framework[18]. This could be used to analyse patterns, predict future major failure, and identify the areas of the enterprise that could be at risk, e.g. using statistical and AI techniques[19].

Given the discussion earlier on the variation in needs for resilience across organisations and sectors, the RoundTable thought that there are opportunities for Trade Bodies to gather and provide data for their members.

WHAT WOULD INCREASE CONFIDENCE IN SERVICE RESILIENCE?

Professor Liz Varga, National Preparedness Commissioner, led this discussion, which surfaced four themes for enabling the C-suite to have increased confidence in service resilience.

A factor which might give the C-Suite confidence in the resilience of their services was **a widely known and measurable definition of resilience**. The RoundTable proposed the UK Government Resilience Framework definition, "action to prevent or mitigate risk". In measuring resilience, the RoundTable proposed that a community (outward) focus rather than business (inward focus) was important for the economy and society. So, the RoundTable proposes the wider use of the NIS Directive metrics, i.e., availability (lost user hours), data integrity (loss or unauthorised access), risk to life or heath, financial damage to users.

The second was the **collation and publication of public sector data on service outages**. This would have (at least) three effects – the familiarisation of the C-Suite with metrics for service resilience, shared understanding of the challenges and approaches, and legitimisation of transparency – detoxifying failure.

The third theme was the **use of the service delivery approach from financial services guidance**[20]. This could include a structured conversation around priorities and potential impacts:

- How do you protect against intolerable harm? What does intolerable harm look like in this sector?
- Map and understand how their own digital infrastructure (enterprise architecture) works. Test it and then refine it.
- Make it about what the C-suite really cares about. Avoid using jargon which they do not understand.

A fourth theme – complementary to the above - was **engaging the imagination of the C-Suite** about possibilities and consequences of failure through role playing, through simulation, or scenario stories.

For the next generation of C-Suite, management education to ensure better understanding of the role of resilience in delivering services should increase confidence.

The RoundTable had previously discussed the hurdles to sharing data on service outages and software failures. The RoundTable understood the problems in sharing data on service resilience, but was clear that without data, the capability for improvement is limited. The feeling was that government could take one or more roles: publishing public sector data, and/or sponsoring a service to share data across sectors. In particular, the collection of the data necessary to support the detection of patterns of events/minor failures could predict future major failure and the areas at risk.

The RoundTable asked – where could research help? Tabled were: testing methods for 24/7 complex tightly coupled systems; analysis of characteristics of failure modes, precipitating events, causes, accompanying events and aftermaths of software failures; resilience characteristics of open-source software; and how to tackle the problems of accountability.

In thinking about education and training, it was clear that there are **major gaps in awareness of the impact of software failures both within and outside the IT team**.

Board level and senior management education was a key theme in increasing the confidence of the C-suite in service resilience. It was felt

that management education should enable senior managers to have the same confidence to ask questions about service resilience as they do about the financials – both are essential for the health of the organisation.

Education and training of IT professionals in service resilience should take place in the workplace (professional lifelong learning) and in university courses. Certification emerged as a key concept[21]: normally, certification is usually developed against a defined standard. Such a standard is not yet in place for service resilience, though work is under way to define ISO and BSI standards. The RoundTable thought that there is currently enough collective wisdom on resilience to deliver training in pilot mode. It could include elements from existing concrete modules (risk analysis, business continuity management, etc). The fundamentals would apply in many contexts. There could also be sector specific modules/ versions developed with different Trade Bodies.

The RoundTable met at the BCS offices in central London on October 25th 2023.

WHAT HAPPENED AT TRANSPENNINE EXPRESS?

In December 2022, TransPennine Express (TPE)[22] had to cancel dozens of services for a second day running with some linked to an ongoing IT problem.

The operator said a software issue that caused more than 100 cancellations had not yet been resolved.

TPE introduced new timetables earlier in December, which were aimed at solving some problems. TPE said the latest disruption was caused by a software issue "rather than a staffing problem", which led to it advising passengers not to travel. The operator said the issue was affecting rostering and could cause further disruption over the coming days.

TPE was nationalised in May 2023.

LINKS AND REFERENCES

1. THE UK GOVERNMENT RESILIENCE FRAMEWORK (HTML) - GOV.UK

WWW.GOV.UK

2. POST OFFICE: HORIZON SCANDAL VICTIMS OFFERED £600,000 COMPENSATION

BBC NEWS

WWW.BBC.CO.UK/NEWS/BUSINESS-66843548

3. RYANAIR: AIR TRAFFIC CONTROL CHAOS HAPPENED AS NATS 'COLLAPSED THEIR SYSTEM' | THE INDEPENDENT

WWW.INDEPENDENT.CO.UK/BUSINESS/RYANAIR-AIR-TRAFFIC-CONTROL-CHAOS-HAPPENED-AS-NATS-COLLAPSED-THEIR-SYSTEM-B2431669.HTML

4. WHAT IS CUTTING UK PRODUCTIVITY? - LONG FINANCE

WWW.LONGFINANCE.NET/NEWS/PAMPHLETEERS/WHAT-IS-CUTTING-UK-PRODUCTIVITY/

5. THE NIS REGULATIONS 2018 - GOV.UK **(WWW.GOV.UK)** IN IMPLEMENTING THE NIS FRAMEWORK, IT MAY BE NECESSARY TO REVIEW THE PARAMETERS (THRESHOLDS) OF DAMAGE TO BALANCE BENEFITS AND COSTS.

6. GLOBAL RISKS – IS SOFTWARE THE VLIEG IN DE SOEP*? - LONG FINANCE

WWW.LONGFINANCE.NET/MEDIA/DOCUMENTS/2023.11.01_-_SERVICE_RESILIENCE_AND_SOFTWARE_RISK.PDF

7. SEE THE LIST OF SERVICE RESILIENCE WORKING GROUP MEMBERS BELOW

8. ESTABLISHED AS THE BRITISH COMPUTER SOCIETY IN 1956.

9. **WWW.BCS.ORG/MEDIA/9679/ITLF-SOFTWARE-RISK-RESILIENCE.PDF**

10. **NATIONALPREPAREDNESSCOMMISSION.UK/WP-CONTENT/UPLOADS/2022/12/NPC_BCS_SOFTWARE-RISK_-THE-ELEPHANT-IN-THE-ROOM_DEC-2022-UPLOAD.PDF**

11. DIGITALISATION, RISK & RESILIENCE - LONG FINANCE

WWW.LONGFINANCE.NET/NEWS/PAMPHLETEERS/DIGITALISATION-RISK-AND-RESILIENCE

12. **FSCLUB.ZYEN.COM/EVENTS/PAST-EVENTS/ARE-YOU-CONFIDENT-OF-YOUR-DELIVERY-OF-SERVICES/**

13. SOFTWARE – THE ELEPHANT IN THE ROOM - LONG FINANCE

WWW.LONGFINANCE.NET/NEWS/PAMPHLETEERS/SOFTWARE-THE-ELEPHANT-IN-THE-ROOM/

14. WHAT IS CUTTING UK PRODUCTIVITY? - LONG FINANCE

WWW.LONGFINANCE.NET/NEWS/PAMPHLETEERS/WHAT-IS-CUTTING-UK-PRODUCTIVITY/

15. ITLF-SERVICE-RESILIENCE.PDF (BCS.ORG)

WWW.BCS.ORG/MEDIA/9679/ITLF-SOFTWARE-RISK-RESILIENCE.PDF

16.BRITISH BANK TSB FINED 48.7 MILLION POUNDS OVER BOTCHED IT MIGRATION | REUTERS

WWW.REUTERS.COM/WORLD/UK/BRITISH-BANK-TSB-FINED-4865-MILLION-POUNDS-OVER-IT-PLATFORM-MIGRATION-FAILURES-2022-12-20

17. OPERATIONAL RESILIENCE IN FINANCIAL SERVICES | NATIONAL PREPAREDNESS COMMISSION

NATIONALPREPAREDNESSCOMMISSION.UK/2021/09/OPERATIONAL-RESILIENCE-IN-FINANCIAL-SERVICES/

18. WHAT IS ITIL? A BEGINNER'S GUIDE TO THE ITIL PROCESS | COURSERA

WWW.COURSERA.ORG/IN/ARTICLES/WHAT-IS-ITIL?

19. MANAGING AGILE BUSINESS TECHNOLOGY – THE BUSINESS AND TECHNOLOGY RELATIONSHIP MODEL IN PRACTICE, DAVID MILLER (SPRINGER, 2022)

20. THE PRUDENTIAL REGULATION AUTHORITY (PRA), FINANCIAL CONDUCT AUTHORITY (FCA) AND THE BANK OF ENGLAND HAVE ISSUED THREE SIMILAR SETS OF REGULATIONS

21. CYBER ESSENTIALS - IASME

IASME.CO.UK/CYBER-ESSENTIALS/

22. TRANSPENNINE EXPRESS LOSES CONTRACT OVER POOR SERVICE - BBC NEWS

WWW.BBC.CO.UK/NEWS/BUSINESS-65555262

ACKNOWLEDGEMENTS

The Service Resilience Working Group Members are all volunteers who give their time on top of often onerous "day jobs". They are amazing:

Katie Barnes, Colin Butcher, Stephen Castell, Andy Ellis, Tom Gilb, Jon Hall, Lucy Hunt, Adeel Javaid, Neville de Mendonca, David Miller, Sue Milton, Jeff Parker, Gill Ringland (co-chair), Adam Leon Smith, Ed Steinmueller (co-chair), Gordon Thompson, Liz Varga, Paul Williams, Yusuf Woozer.

The Service Resilience Working Group has been supported within BCS by the IT Leaders Forum, F-TAG, Specialist Groups in Quality, Information Security and Information Risk Management and Assurance, and by headquarters staff at BCS: thank you all.

People who have contributed through providing references, updates on work elsewhere, access to their networks, etc. were:

Alexander Woods, Anijuli Shere, Arthur Hill, Chelsea Frischknecht, Chris Skinner, Chris Yapp, Christine Ashton, Dalim Basu, David Ferguson, David Thorp, David Tynan, Dean Lonsdale, Emma Wright, Estelle Clark, Gemma Robson, Hank Marquis, Harold St John, James Burns, Joe Little, John McDermid, John Mitchell, Jonathan Pownall, Lisa Emery, Lorna Kirkby, Marguerite Landells, Martyn Thomas, Michael Burgess, Michael Mainelli, Martin Hogg, Natasha McCarthy Patricia Lustig, Paul Bailey, Phil Johnson, Philip Virgo, Philip Wardle, Rachael Elliott, Reza Alawi, Rich Bishop, Richard Chilton, Resham Dillon, Richard Peters, Rob Wirszycz, Sam de Silva, Simon Buckland, Sophie Isaacson, Stephen Mason, Stuart Okin, Terry Downing, Tom Clementi, Tom Sykes, Vince Desmond, William Adams.

RoundTable participants in 2022 and 2023 were:

Adam Leon Smith, Alexander Woods, Alexandra Smyth, Arthur Hill, Azalea Raad, Bill Mitchell, Billy McNeil, Colin Butcher, David Miller, Ed Steinmueller, Gemma Robson, Grace Phillips, Gill Ringland, Iraah Wehner, James Davenport, Jenny McEneaney, Jeremy Brown, John Cully, John Easton, Jon Hall, Jonathan Pownall, Karen Salt, Katie Barnes, Katie Owen, Kieran Matthews, Maria Torres Garcia, Matthew Killick, Mike Turner, Neha Mahendru, Neil Chue Hong, Neville de Mendoza, Patricia Lustig, Paul Marshall, Paul Williams, Paula Kulczyk, Rachael Elliott, Rob Wright, Rony Zaman, Santa-Olalla Belen, Stephen Castell, Stephen Groves, Steve Sands, Steve Watt, Suresh Perinanayagam, Terry Downing, Toby (Lord) Harris, Tracey Lorraine, Tom Venning.

The support of (Lord Mayor) Michael Mainelli throughout, both through personal inputs and through access to his z/yen and Long Finance platforms, has been crucial as we developed our ideas. Also seminal was his introduction to (Lord) Toby Harris, Chairman of the National Preparedness Commission. Toby contributed access to members of his personal network and his time to chair the 2022 RoundTable. His blog for PICTFOR is » Lord Harris – Why Software is the Elephant in the Room (pictfor.org.uk), and two National Preparedness Commissioners, Paul Williams and Liz Varga, have led part of the work during 2023. The Working Group Co-Chairs would also particularly like to thank Katie Barnes, Executive Director of the National Preparedness Commission who has not only put her formidable brain in gear on the topic of service resilience but has also set up many useful contacts for the project – the output is so much better than it could have been without her contributions!

Founded in 1994 with the aim of promoting a more resilient world, the BCI has established itself as the world's leading institute for business continuity and resilience. The BCI has become the membership and certifying organization of choice for business continuity and resilience professionals globally with over 9,000 members in more than 100 countries, working in an estimated 3,000 organizations in the private, public, and third sectors. The vast experience of the Institute's broad membership and partner network is built into its world class education, continuing professional development, and networking activities. Every year, more than 1,500 people choose BCI training, with options ranging from short awareness raising tools to a full academic qualification, available online and in a classroom. The Institute stands for excellence in the resilience profession and its globally recognised Certified grades provide assurance of technical and professional competency. The BCI offers a wide range of resources for professionals seeking to raise their organization's level of resilience and its extensive thought leadership and research programme helps drive the industry forward. With approximately 120 partners worldwide, the BCI Corporate Membership offers organizations the opportunity to work with the BCI in promoting best practice in business continuity and resilience.

The BCI welcomes everyone with an interest in building resilient organizations from newcomers, experienced professionals, and organizations.

Further information about The BCI is available at **www.thebci.org**.

IT Leaders Forum

The principal purposes of The BCS IT Leaders Forum are:

1. To be a leading forum for senior Information Technology managers and leaders, and to represent Senior IT Management within the BCS.
2. To provide those members with opportunities to listen to informed opinion, exchange ideas and discuss common issues relating to innovative application, effective operation and strategic development within their IT environments, and in conjunction with such activities, provide the BCS, Industry, Commerce, Government and business as a whole, with authoritative leadership and direction in all such matters.

BCS, The Chartered Institute for IT, is the professional body for the people who work in tech. Together we're on a mission, set by Royal Charter, to build a safe and bright digital future for everyone in society.

To do it, we need a technology profession that's ethical, accountable, diverse and innovative. So we work with key partners and our global membership community to improve IT education and break down barriers, raise professional and ethical standards across industry, and support digital talent in all its forms.

You may know us as the awarding body for BCS professional certification and digital skills qualifications. We're also a leading assessment organisation for digital apprenticeships, and the regulatory body for Chartered IT Professional (CITP) and Register for IT Technicians (RITTech) registration.

Join us on our mission at **www.bcs.org**.