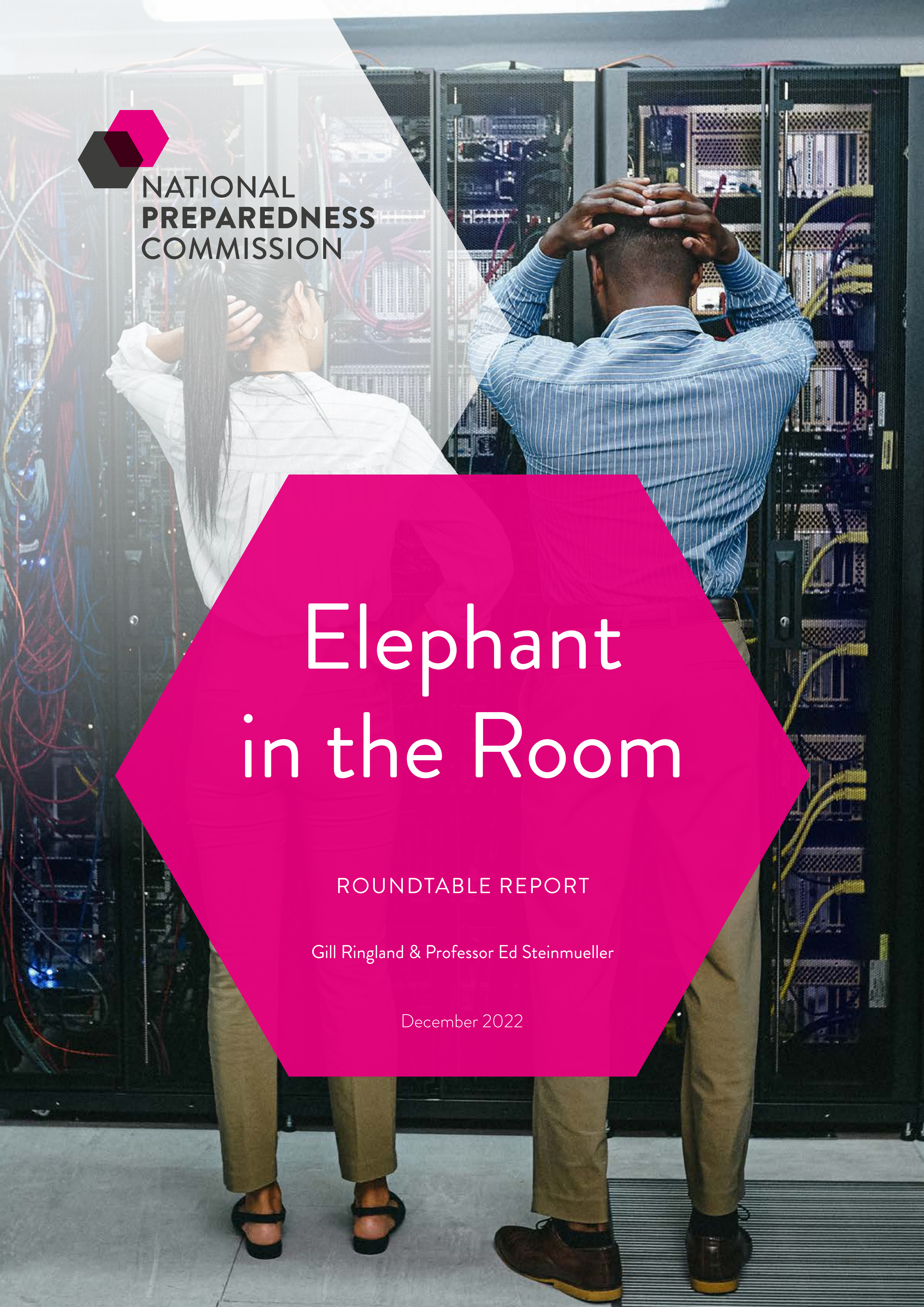
NATIONAL
PREPAREDNESS
COMMISSION



Elephant in the Room

ROUNDTABLE REPORT

Gill Ringland & Professor Ed Steinmueller

December 2022

CONTENTS

EXECUTIVE SUMMARY

People, organisations, the economy and society rely on software-based systems. These systems are vulnerable to both internal defects and external threats. Software defects can cause intermittent failure, malfunction (wrong results or decisions), catastrophic failure and loss of confidential information/privacy - each of which can create a substantial drag on productivity and profit and can, of course, potentially have more serious consequences. Software creation services are largely unregulated.

Software failures are already a significant cost to the UK economy, and the risks of software failure are increasing. At the same time, the scope of the potential impact on the continuity and quality of business services and almost all aspects of day-to-day life is increasing. Technological and human factors both contribute to this trend. Natural Accident Theory predicts that complex and tightly coupled systems, as many software systems are, will intermittently fail.

The National Preparedness Commission and the BCS's IT Leaders Forum (ITLF), a Specialist Group of BCS, held a Roundtable to discuss what could be done to reduce the impact of software failures on the UK's economy and society. The main conclusions were that:

- **More people and organisations need to be AWARE of the actual and potential impact of software failures.**

- **Software is DIFFERENT. It is intangible and obeys different rules from physical systems, creating problems in for example quality control and regulation.**

- **The software element of digital systems failure is a COST TO ECONOMY AND SOCIETY which will only increase as software has become a utility, is in wider usage, and more vulnerable to failure.**

The recommendations arising from these conclusions are:

- **Policy makers should be aware of the consequences of software failures and consider appropriate measures.**

- **As a first step, IT leaders in organisations should work with managers responsible for service delivery to understand the organisation's exposure to software failure.**

- **IT professionals should work with policy makers and standards bodies to explore the implications of the fact that software is different and that not all software failures can be predicted.**

- **IT professionals should create an accessible set of guidelines for organisations to improve the resilience of their digital systems.**

More detailed recommendations arising from the Roundtable cover actions for standards bodies, policy makers, insurers, IT and risk professionals, organisations, professional and business networks and business schools, and government procurement, and can be found in the Conclusions.

BACKGROUND

Recent events – the pandemic, global supply chain disruption, extreme weather – have strained the UK to breaking point. No one can fail to be aware of the consequences of lack of resilience in our economy and society. Digital systems are already a critical part of society and the economy – we all depend on services supplied by digital systems.

The same is true for the vast majority of businesses with the services and products that they provide to their customers and clients being subject to major digital risk. The management of service and product security is, thus, of critical importance.

In August 2022, the IT Leaders' Forum (ITLF), a Specialist Group of BCS[1,] published a policy think piece on *Digitalisation – software risk and resilience*[2]. The purpose was to alert a wider community to the risks from failure of software, in order to engage with partners to reduce these risks and their cost to the economy and society.

Lord Toby Harris, Chair of the National Preparedness Commission[3] (NPC), became aware of this work. It was agreed that the NPC and the BCS's ITLF should jointly organise a Roundtable to take the work forward to a wider audience.

The Roundtable was held at the BCS's London offices on 15th November. Twenty-six participants engaged in discussion on software risk and resilience, and how risk might be reduced, and resilience increased, for the benefit of the UK economy and society.

But which are the risks that are most important? With each business being different, there has been a historical lack of consensus about the risks faced and very little generalised guidance exists.

This report is intended to mark the beginning of the next phase of work to tackle this issue and provide a framework for action.

DIGITALISATION – SOFTWARE RISK AND RESILIENCE

Digital systems use physical infrastructure, algorithms, data and software. We know that physical networks underpinning the internet are vulnerable - the deliberate cutting of a single undersea cable could cripple the internet[4]. An analogy could be the blocking of the Suez Canal by a single container ship for several days[5]. We know that interconnected financial systems can crash the global economy through cumulative and catalytic processes – as in the 2008 financial crash caused by sub-prime mortgages[6]. We know that one of the side effects of social media has been to deepen divides[7] as we communicate with those 'like us'. We know that over half of all adults in the UK have no faith in the use of AI algorithms used to make decisions about them[8], and that many AI applications lock in ethnic or gender bias in recruitment[9]. Society has created algorithms for digital systems that in many cases prioritise wealth creation and productivity at the expense of other factors and which in many ways reflect our (pre-digital) behaviour and world views.

Estimating the costs to the UK economy of operational software failure is difficult. It is complicated by the lack of any systematic reporting of costs and the fact that very large numbers of software service users bear most of the costs. A recent BCS ITLF policy think piece attempts to gauge the scale of these costs.[10] The analysis there compares the UK with historical US experience, adjusting for relative size of the US and UK economies, adjusting for inflation and other assumptions. Employing these methods suggests that the costs may range between £8 and £14 billion, and the policy think piece suggests using £12 billion as an order of magnitude estimate.

This number lies between UK estimated costs of a 5-day outage of GNSS/GPS systems[11] on £5.2 billion and the £16.5 billion annual costs of road accidents estimated by the UK Department for Transport.[12] While there are ongoing exercises to reduce the number and cost of road accidents, there are no comparable national efforts to reduce the economic and social cost of software failures. This could be because the costs are widely dispersed across individuals and organisations, or simply that the extent of the cost is not well enough understood.

As financial services have been early and extensive adopters of software systems, they provide some of the case studies which illustrate the costs of failure. Consider for instance the failure of Bloomberg systems in 2015[13]. Bloomberg terminals crashed in an IT meltdown that forced the government to postpone a £3bn debt sale. The problems with the terminals emerged as the Asian markets closed and Europe's opened – at around 8.20am – and potentially affected more than 300,000 traders on financial markets. Another well-researched case study is of how an incomplete software upgrade left a trading company with $7 billion of unsaleable stocks in one hour – leading to its takeover by a rival a few months later[14]. Incidents like this have led to additional regulation of financial services, to protect the public.

Most organisations rely for their operation on software whose creation is outside their control, as for electricity or telecoms. Control is relinquished when software components are acquired – e.g., Commercial Off the Shelf Software (COTS), Open-Source software, or Software as a Service (SaaS). There is no widely used rating or quality assurance system for software so organisations are flying blind in terms of what they can expect with regard to the reliability and resilience of the digital systems that they buy and that they depend on.

Software is different from physical assets in that it can be reproduced at negligible cost and contains many 'moving parts' that are nonetheless intangible. It obeys rules that are new to us. For example, unlike mechanical or electrical systems, it does not degrade with use but fails abruptly without prior warning. Similarly, although preventative measures may be taken to reduce the risk of failure, these do not bear the same assurance of continued operation that preventative maintenance of other systems usually promise. Finally, software is often joined and recombined in tightly coupled networks. Their interdependence virtually assures that operational software failure at any of a myriad of points will propagate into a broader disruption, whose source may be time-consuming to identify and remedy. The language, terminology and processes for creating and maintaining software are evolving. Yet without fanfare, software is now everywhere. Services that were previously based on hardware - from automotive controls to telecoms networks - are now software- based. Local Councils deliver many services via software, as do doctors' surgeries. Software has become a utility but it is not managed or governed as such.

Technological and societal trends are making the situation worse.

The main technological trend is growing complexity, arising from the increase in frequency and intensity of interactions between modules. According to Normal Accident Theory[15], accidents are inevitable in systems that have two characteristics – complexity as well as being tightly coupled. A further complexity is that the people using software-based systems have differing understanding of how software operates, what can go wrong and how to respond. So resilience includes more than system recovery, it needs to assess causes of failure. Finally, tight coupling means that components of a process are critically interdependent: they are linked with little room for error or time for recalibration or adjustment. It is clear then that these increasingly complex and tightly coupled systems need to be built to appropriate margins, even when they are not being used in 'safety critical' applications.

Meanwhile, the Internet of Things (IoT) is becoming the Internet of Everything (IoE) – further extending the ubiquity of software and the complexity of interactions and interdependencies. Smart Cities, for example, are highly interconnected[16]. This makes it difficult to model the cause and effect of software failures, or the social and economic impact due to them.

Software systems are often implemented on a standard blueprint[17]. Taking advantage of the low cost of software reproduction (or ability to share use) replicates and extends vulnerabilities.

Societal trends favour speed-to-market approaches[18] to writing software, which take precedence over considerations of risk and maintenance. The incentive to build resilience is offset by the commercial pressures to optimise profit and reduce cost. In so doing, costs of failure may be inappropriately transferred onto the users of software instead. In applications such as gaming, there are few societal or economic effects from system failures during early use (testing) by the user community. In other applications such as booking of medical appointments or traffic control, software failure can have life-threatening consequences.

Software is the elephant in the room.

ROUNDTABLE DISCUSSION – MAIN THEMES

1 | Software – what is it?

One barrier to the understanding of software is a lack of vocabulary or formal descriptions of what software is or does. It is largely conceptual and within the developer's control, unlike physical infrastructure or machines which have plans, drawings and specifications that can be shared, assured and tested. There is no widely used formal language for description of software, or the features of software interfaces which contribute to resilience – for instance, the ability to test or modify parts of a system.

There are ways to verify software and ensure iterative versions are backwardly compatible but investing in these requires a business mindset that accepts the cost as part of delivering shareholder value. Those organisations that foster a 'just in time' approach to delivery or a 'build it quickly, fix it when it breaks' approach to design, are likely to bypass planning and testing cycles.

2 | Software is now embedded in organisations

Digital systems have extended beyond conventional 'IT' used in in Financial Services and administration. In many cases, it is impossible to separate IT and its usage from the organisation itself. Increasingly, when we talk about IT, we mean software-enabled services and it is in these services that risk surfaces.

Service breaches are a key concept for tracking software failure and the effect on users of the service but provide only a partial view of the wider effects of software failure.

Software vulnerabilities apply to the goods and services produced by the automotive, healthcare, and wholesale and retail trade industries as well as public-facing services in government and charities. All of these have new types of users who are expected to deal with software systems without 'IT' support. The example (under Digital systems failure, below) of the productivity cost of working from home is a rare example of an attempt to capture the costs of software failure.

The next generation of networks will be based on 5G wireless standards which are implemented in software. Our phones have capabilities only dreamed of by previous generations. And AI is built into many decisions in public facing systems for travel, consumer purchases, investment decisions: if it gives the wrong advice or selection, it is not easy to challenge.

Examples of software include devices in homes that are doing things we don't realise – a Roundtable participant cited the recent case of an interactive doll that was also collecting data on its owner's behaviour – this illustrates how a user may focus on the desired utility without an understanding of what else might be happening as a by-product.

3 | Service breaches

How to communicate that the actual and potential impact of software failure is really serious, without panicking people?

A shift is needed in societal attitudes and awareness of the true nature and consequences of failures. When Primark's website crashed, their marketing team was quick to claim that this was a positive sign - because it meant that lots of people liked the new deal. Similarly, a politician proudly announced that the crash of a web site delivering time-critical services to the public was a good thing as it demonstrated a high demand for the services. The human cost of software failure is illustrated by the Red Cross example in the section below on Digital systems failure.

There are sectoral differences in attitude to service breaches. While disaster recovery is widely accepted, many organisations have an aversion to audits of potential risks. Banks will routinely carry out checks on software when an error is discovered, but others tend to blame the users. In the Post Office's Horizon system, this led to accusations of fraud without further corroboration seemingly required. Lack of disclosure of outages could be driven by commercial considerations, for instance the damage to reputation if the contractor's software errors became public knowledge.

It is reported that 95% of software outages are caused by the introduction of changes through incorporating new software modules.

4 | Software may give faulty answers

The current legal presumption in the UK is that the computer is correct. This was one of the hurdles faced by sub-postmasters in the Post Office Horizon system rollout. There were many instances where the answer – such as the amount of money that the system thought had been deposited – was inaccurate. (The Horizon system was often being used by people unfamiliar with the new system and with little training or back-up such as helplines. This is the case for many other systems in use today. 'Wrong' answers are less likely to be detected in these circumstances).

Health services have started to use AI for a number of applications, such as clinical interpretation of medical scans – formerly the responsibility of expert practitioners. This is raising the question of how to equip the workforce to question the reliability of AI-derived results and to know when to intervene to overturn decisions. This means that organisations need to have trust in staff in order to accept their decisions.

5 | Digital systems failure - a cost to economy and society

The examples below provide illustrations in terms of the costs in lost productivity, in withdrawal of services, and in improper allegations of fraud.

- **Service breaches** - A recent survey of 1,006 people has led to estimates that working from home has cost the UK economy £60 billion per year, with more than a quarter describing technical difficulties occurring 'very' or 'fairly' often. Data transmission delays led to 'chaos' for City traders and caused pricing errors in fast moving transactions[20].
- **Catastrophic breakdown** - ICRC (Red Cross) had to shut down the computer systems running its Restoring Family Links programme when hackers gained access to data about 515,000 extremely vulnerable people. The programme seeks to reunite family members separated by conflict, disaster or migration[21]. While in this instance, the breach was through a hacking attack, users can often cause similar effects innocently trying to get answers from a computer system.
- **Wrong answers/decisions** – the Post Office's Horizon project is an example of tragic consequences to individuals resulting from unquestioning faith in 'the system'. This excerpt from High Court Trial Day 8[22] illustrates helplessness on the part of the sub-postmasters to argue their innocence in the face of jail sentences. "On the 1st of March at the close of business we found that on node 5 [each Horizon terminal within a branch is known as a node] the cash was short of £1,000. All of the figures for that day match the figures presented at the time of each transaction. An Instant Saver withdrawal of £1,000 was transacted that day, but I was unable to find this transaction using the online report facility. I feel very anxious as I believe a system error has occurred at the time of this transaction."

6 | Levers to tackle service breaches and faulty answers

Two statutory levers to tackle service failures that could be employed are regulation (to reduce the likelihood of such failure) or accountability (remediation or compensation of incurred losses).

The role of regulation is to insert the public interest into the private choices of firms. Good regulation can therefore create powerful incentives to invest in resilience, which otherwise might not make the 'business case'. The UK's recent Operational Resilience Regulations[23] for the finance sector have had a profound impact on the way that UK and indeed global financial services is now thinking about non-financial risk. But the same approach may not be effective in other sectors where regulation is not so strong or the focus of regulation different (e.g., competition-based, rather than harm-based regulation). Software risk audits will require new skills in many organisations. And introducing new forms of audit can be seen as an unnecessary overhead cost if an organisation has not had to bear the costs of operational software failure.

A focus on accountability deals with the consequences of failure. As pursuing remedies through the courts can be very costly, prevention may be more cost effective.

Industries differ as to the value they place on minimising software risk. Safety-critical systems such as air traffic control are more likely to be optimised for resilience and rigorously tested than those with purely financial risk considerations. Incentives need to align with sector or business values. Misaligned incentives may indicate a market failure that will not self-correct without a regulatory or legal intervention. In sectors where life-safety issues arise from failure, incentives generally exist to drive corrections. In sectors where only a focus on near term financial incentives exists, then it is possible for compromises on risk and resilience to be made in order to drive profit and pass costs of failure onto the consumer – largely without due consideration to the impacts which are passed on. Near term performance may prevail over long term stability.

Other levers include the availability and cost of insurance, standards bodies and government procurement. However the theme throughout is of the need for organisations to have increased awareness of the actual and potential impact of software failures. Here the roles of business schools and business networks are important.

7 | Organisations and software failure

CEOs and board members of organisations have responsibility for the services delivered by the organisation, but many boards lack confidence to understand threats to their services. They are often sensitive to GDPR and reputational risks, and increasingly to cyber threats. To tackle cyber threats, the US Securities and Exchange Commission proposed amendments to its rules to enhance and standardise disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. The proposed amendments would require, amongst other things, the board of directors' oversight of cyber security risk, and management's role and expertise in assessing and managing cyber security risk and implementing cyber security policies and procedures. The proposal further would require annual reporting or certain proxy disclosures about the board of directors' cyber security expertise, if any.

Many large organisations now have insurance against cyber attacks. Extending insurance to cover business discontinuity due to software failure might provoke beneficial changes, particularly if insurance providers require organisations to undertake better due diligence of the software they are using.

IT system risk responsibility is often passed to a single person on the board for governance – the CTO/CIO is expected to know it all. This is not sufficient – every member of the board needs to be able to understand warning signals from IT function. An analogy with the role of the CFO is helpful – they lead the financial governance, but all board members are expected to have a working knowledge of what's involved. In the case of IT, the board needs to recognise there could be unknown unknowns[24] and so endorse 'what if?' planning for catastrophic failure.

Organisations come in different sizes, and this will influence who has software awareness of software risk. SMEs are more likely to buy Software as a Service, or customised dashboard interfaces to complex datasets, or off-the-shelf 'black box' solutions. They may think that their risk exposure is covered by Service Level Agreements (SLAs) with their suppliers. Their processes are more likely to be driven by the system design than vice versa. Software and/or IT (many won't understand the difference) is seen as an enabler or a way of cutting costs and the inherent risks may not be appreciated, let alone actively managed.

Federated organisations such as local government networks are an interesting testbed for risk prevention and resilience strategies. The differences in software configuration and use across each affiliated organisation could contribute to collective resilience. For this to happen, experiences must be collected, shared and analysed. Conversely, the drive for efficiency or effectiveness through functions such as shared data, or single sign-on, could introduce common risk across organisations and enlarge the scale of risk. Users rarely have the skillset to understand the risks and/or do anything about them and smaller organisations may well not have IT support.

Larger organisations have an opportunity to establish what is being managed by mapping software to business outcomes, and mapping failures to likely consequences. This mapping needs to result in tools and measures that allow Boards to understand what they have and importantly, what they can do without in a crisis. How can organisations get to this position with regard to the role of IT and software in a business? It could be useful to map technology reliance onto core business processes as a first step to understanding risk and agreeing tolerance for failure. But this needs to be on a selective and most critical/ prioritised basis, otherwise the task simply becomes business process mapping.

8 | The first need is to raise awareness

The methods of raising awareness are different for the three actors on the supply chain – software suppliers, purchasers (organisations) and end users, in which we include the public good.

Software suppliers

Software suppliers are sensitive to purchasers, also to policy makers, regulators, and to standards bodies. We discuss below how purchasers (organisations) could become more aware. Policy makers and some regulators are now directly engaged with issues of service continuity and reliability, e.g., finance[25] and its supply chains and in health[26]. Regulators of operators of essential services in particular could consider applying FCA definitions of 'operational resilience' to energy, transport, health, water, and digital infrastructure. Standards bodies – such as the EU and ISO – who are addressing cyber security and AI could extend to their considerations to also cover underlying software. Cyber-attack is one source of software failure, though similar effects can and are caused by users who do not intend to be malign. AI can give wrong answers for causes embedded in the AI algorithms or because of defects in the software: most discussion of AI focuses on the selection of algorithms or data for machine learning. Defects in the software need to also be considered.

What factors reduce software risk and increase the digital resilience of new software? If industry were to move towards self-regulation or standards, whose role is it? Perhaps the DRCF[27] (Digital Regulation Cooperation Forum) could be expanded and formalised. The challenge is that software is general purpose, so industry specific regulation in the form understood by industries like aerospace or construction is unlikely to be sufficient.

The quality of software design is invisible to an untrained eye and nature of delivered software is that it is often 'closed' to examination (absence of source code). However, there could be standards and assurance kitemarks for functions like design process or testing protocols. Assuring deployment of a software component would involve specifying boundaries of what it can and can't do, perhaps with usage guidelines. A potential model for this is the use of Building Information Management (BIM) in construction[28].

Purchasers (organisations)

Board members need to be as aware of IT risks as financial or legal risks – to understand the language of service breaches and misinformation, and the productivity impacts. Business schools and adult learning courses could provide enough education on IT to raise the collective competence of existing and future board members.

Greater attention to the significance of business continuity and the analysis of organisational vulnerability is a useful starting point as it directs attention to the dependence of an organisation on specific systems. By following the trail from potential consequences to vulnerability and finally to underlying sources of breakdown it is possible to prioritise preventative measures. The same process can indicate more immediate measures to improve resilience such as assuring effective recovery from breakdown.

Nonetheless, purchasers (organisations) often find that they have difficulty in assessing software or understanding their existing software. Organisation leaders' fears and concerns are rarely expressed in software terms, so a common language or translation mechanism is needed, to expose the software risks in their IT systems. The language of 'operational resilience' may be useful here.

As noted earlier, insurance against cyber related damage is increasingly commonplace – could this be extended to cover other sources of software failure. One effect could be to incentivise measures designed to avoid failures, although there is also a danger that an indemnity approach could lead to complacency.

IT and risk professionals could establish early warning systems for software failures – service breaches and misfunctioning - for use by boards; and add software risk to business continuity processes. Collaboratively they could explore tools and methods for anticipating risks, monitoring and enhancing software systems.

Users and public good

Government has a role in creating common knowledge of software risk, for instance through visibility in the National Risk Register.

Business schools and providers of education to middle managers could start building skills in the next generation of C-Suite officers.

Business confederations could provide workshops and mentoring on the impact of software failure and its reduction. This could be useful especially for SMEs. Other business networks mentioned as possible influencers included B Corp[29], a network of companies verified by B Lab to meet high standards of social and environmental performance, transparency, and accountability.

How can communication and learning from software failures across organisations be facilitated? Managers are likely to express fears without direct mention of software or even systems, using instead the language of service availability and business continuity. Another very real hurdle to sharing information about software failures is the conflict between corporate confidentiality and common good.

CONCLUSIONS OF THE ROUNDTABLE

The first need is to raise awareness.

Different actors influence end users, purchasers (organisations) and software suppliers and there are business and policy options for creating or improving the performance of intermediaries.

Recommendations

As a first step, IT leaders in organisations should establish dialogue with managers responsible for service delivery to understand the organisation's exposure to software failure.

Professional and consumer associations and business networks could determine how best to address the lack of skills and awareness in end users.

Business schools could determine how best to address the lack of skills and awareness in managers and Board members.

The inclusion in government procurement standards of a requirement for organisational resilience commitments would have the effect of raising awareness in software suppliers of their vulnerabilities, and hence encourage remediation in pursuit of competitive advantage.

Policy makers could determine how to increase the visibility of software risk and potential impact of failures.

Software is different

It has unpredictable qualities, and it is now a utility but not treated as such by policy makers, governments or end users.

Recommendations

IT professionals should establish dialogue with policy makers and standards bodies to explore the implications of the fact that software is different.

Standards bodies could determine if it is desirable to extend current work on AI standards and on cyber standards to include the underlying software.

Software failures will be an increasing cost to economy and society.

The dependence of our economy and society on digitalisation has been gradually increasing. This dependence has not been accompanied by an understanding of the associated risks.

Recommendations

IT professionals should create a set of guidelines for organisations to improve the resilience of their digital systems.

Insurers could determine whether it is desirable to develop insurance products for organisations against software failure perhaps as indemnity for business continuity risks. Experience with expanding the scope of insurance coverage is that it provides incentives for gathering better and more complete data on the sources of risk.

IT and risk professionals in organisations could determine if cooperation across organisational reporting boundaries on software risk is desirable and feasible.

Organisations could consider whether the process behind the FCA's 'operational resilience' is a useful model.

ACKNOWLEDGEMENTS

The authors are grateful to Lord Toby Harris and Katie Barnes of the National Preparedness Commission for their support and input, and to Toby for chairing the discussion sessions during the Roundtable.

The authors, and Toby and Katie, were joined by David Miller, Chair of the BCS's ITLF, and Patricia Lustig, Board Member, Association of Professional Futurists, to facilitate the discussion.

The participants were:

Adam Leon Smith, Chair, Software Testing Group, BCS

Alexander Woods, Policy Manager, Chartered Quality Institute

Azalea Raad, Senior Lecturer, Imperial College

Bill Mitchell, Policy Director, BCS

Billy McNeil, Director, IT and Operations, BCS

Colin Butcher, Member, Software Risk and Resilience Working Group, ITLF, BCS

David Miller, Chair, IT Leaders' Forum, BCS

Ed Steinmueller, Professor, Sussex University

Gill Ringland, Co-chair, Software Risk and Resilience Working Group, ITLF, BCS

Jenny McEneaney, Senior Improvement Policy Adviser - Cyber, Digital and Technology,
Local Government Association

John Cully, Policy Officer, RAEng

Jon Hall, Professor, Open University

Karen Salt, Deputy Director, UKRI

Katie Barnes, Executive Director, National Preparedness Commission

Katie Owen, Improvement Policy Adviser - Cyber, Digital and Technology,
Local Government Association

Matthew Killick, UK Director – Crisis Response & Community Resilience, British Red Cross

Mike Turner, Head of Profession, Chartered Quality Institute

Neil Chue Hong, Professor, Edinburgh Parallel Computing Centre

Patricia Lustig, Board Member, Association of Professional Futurists

Paul Marshall, Barrister, Cornerstone Barristers

Paul Williams, Managing Director, Phoenix Resilience UK

Stephen Castell, Member, Software Risk and Resilience Working Group, ITLF, BCS

Stephen Groves, Director, EPRR, NHS England

Terry Downing, Head of Operational Resilience, Mastercard

Toby (Lord) Harris, Chair, National Preparedness Commission

Tom Venning, Principal Consultant, Peru Consulting

In addition, a number of colleagues who were unable to take part on the day have contributed to this report: Thank you!

The BCS provided the meeting facilities at their office at 25 Copthall Street in central London, with lunch, plus tea and coffee on tap. We are grateful to the team there who made everything work.

AUTHORS

Gill Ringland's books on Scenario Planning and strategy are used at Business Schools including Harvard. Her most recent book, the 9th, with Patricia Lustig, is New Shoots – people making fresh choices in a changing world.

Gill's early career included the Universities of Bristol (B. Sc.), Edinburgh, Newcastle (M.Sc.), California at Berkeley, and Oxford. She did pioneering work in IT on systems and data architecture, at CAP, Inmos and Modcomp. She has been active in seven start-ups and built a £3bn new business at computer firm ICL. She was CEO, Director and a Fellow of SAMI Consulting (Strategy with a view of the future) from 2002 to 2017, with clients in the public, private and NGO sector from Mexico to Malaysia. From September 2017 to February 2021 she was a Director of Ethical Reading. She is now a trustee of u3a in Newbury.

She is a Fellow of the BCS (previously known as the British Computer Society), an Emeritus Fellow of SAMI and ICL (now Fujitsu), and a Fellow of the World Academy of Art & Science. She is a graduate of Stanford University's Senior Executive Program, and a Liveryman of the City of London. She has been co-opted for various UK Government and EC advisory roles.

She writes often for Long Finance Pamphleteers and writing Global Risks – Is Software The Vlieg In De Soep*? with Patricia Lustig prompted her to think about software again. She is co-chair of the BCS's IT Leaders Forum's Software Risk and Resilience Working Group, which has developed the work on which this Roundtable was based.

Professor Ed Steinmueller has been Professorial Fellow at SPRU since 1997.

He began his studies in the areas of computer science, mathematics, economics, and Chinese language and history at the University of Oregon and Stanford University. He has a BA, University of Oregon, PhD Stanford University (economics). At Stanford (1974-1994), he was engaged in teaching, research, consulting while being a Deputy Director of what is now the Stanford Institute for Economic Policy Research. He was appointed professor at MERIT at the University of Maastricht, The Netherlands where he developed a Doctoral training school.

He has published widely in the field of the industrial economics of information and communication technology industries including integrated circuits, computers, telecommunications, software and the economic, social and policy issues of the Information Society. He has also contributed to research in science policy and the economics of basic research. He has been an advisor to several Directorates at the European Commission, the National Academies of Science and Engineering (US), and the Department of Trade and Industry and Office of Telecommunications (UK). His current research is aimed at systemic change for environmental sustainability and social justice.

He is co-chair of the BCS's IT Leaders Forum's Software Risk and Resilience Working Group, which has developed the work on which this Roundtable was based.

REFERENCES

1. The BCS is the UK's professional body for computing. It is governed by Royal Charter to advance education and practice in computing and information technology for the benefit of the public, implementing "Making IT good for society."
2. itlf-software-risk-resilience.pdf (bcs.org)
3. https://nationalpreparednesscommission.uk
4. https://www.wired.co.uk/article/submarine-internet-cables-egypt
5. https://www.bbc.co.uk/news/business-56559073
6. https://blogs.lse.ac.uk/politicsandpolicy/systemic-risk-was-the-real-culprit-in-the-2008-financial-crisis-and-with-banks-continuing-to-borrow-huge-amounts-the-dangers-are-still-there/
7. https://www.aspeninstitute.org/blog-posts/social-media-divides-us/
8. https://www.bcs.org/articles-opinion-and-research/open-letter-to-the-new-prime-minister-rishi-sunak-from-rashik-parmer-bcs-ceo/
9. https://www.euronews.com/next/2022/03/08/gender-bias-in-recruitment-how-ai-hiring-tools-are-hindering-women-s-careers
10. See Appendix 3 of https://www.bcs.org/media/9679/itlf-software-risk-resilience.pdf
11. https://webarchive.nationalarchives.gov.uk/ukgwa/20170630014518/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf
12. https://www.fonsecalaw.co.uk/blog/patricks-blog/2014/10/22/the-cost-of-road-traffic-accidents-in-the-uk
13. https://www.theguardian.com/business/2015/apr/17/uk-halts-bond-sale-bloomberg-terminals-crash-worldwide
14. https://www.henricodolfing.com/2019/06/project-failure-case-study-knight-capital.html
15. https://www.theifod.com/the-normal-accident-theory/
16. https://www.idb.org/what-are-the-cybersecurity-risks-for-smart-cities/
17. https://www.theiotintegrator.com/smart-city/a-blueprint-for-smart-communities-understanding-the-municipal-iot
18. Agile definition in https://www.bcs.org/media/9679/itlf-software-risk-resilience.pdf
19. https://www.imperial.ac.uk/business-school/news/all-models-are-wrong-some-are-useful/
20. Sunday Telegraph, 13/11/2022
21. Hacking attack on Red Cross exposes data of 515,000 vulnerable people | International Committee of the Red Cross (ICRC)
22. https://www.bcs.org/media/9679/itlf-software-risk-resilience.pdf
23. https://nationalpreparednesscommission.uk/2021/09/operational-resilience-in-financial-services/
24. Rumsfeld's Knowns and Unknowns: The Intellectual History of a Quip - The Atlantic
25. Operational Resilience | FCA
26. WHO's 7 policy recommendations on building resilient health systems
27. DRCF: Terms of reference - GOV.UK (www.gov.uk)
28. https://www.citb.co.uk/about-citb/partnerships-and-initiatives/building-information-management-bim-for-site-workers/what-is-bim/
29. The UK B Corporation Movement

NATIONAL
PREPAREDNESS
COMMISSION

www.nationalpreparednesscommission.uk