Version 3

Digitalisation – software risk and resilience – a policy think piece

August 2022

This Policy Think Piece has been developed by a Working Group of the BCS (British Computer Society) ITLF (IT Leaders Forum). It has been written by the co-chairs based on input from working group members and other experts: see Section 5. Our purpose is 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.

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."

Contents

Executive Summary

This Policy Think Piece is the outcome of the first phase of work, by a Working Group of the IT Leaders Forum of the BCS, on software failure and lack of digital systems resilience. We have chosen to focus our analysis in Phase 1 on the effect on the UK economy and society but of course similar effects are seen in other countries and the provision of software is global.

Recent events – the pandemic, global supply chain disruption, extreme weather – have increased the awareness of the consequences of lack of resilience in our economy and society. Digital systems are increasingly a crucial part of the economy: but there is evidence that digital systems are increasingly liable to service breaches due to failures in software systems among other causes, and that these breaches are increasing in scale and duration (see section 2.4). The risks are similar to those from global warming or pandemics, in that major shocks are certain, but not their location or timing.

IT professionals and some others are aware of these risks, (see section 3.1) but risks from software failures have been "the elephant in the room". Wider awareness by senior professionals is needed before most organisations have adequate policies and processes to prevent software failures and are able to mitigate the consequences of these.

The purpose of this Policy Think Piece is to increase this awareness, and so our recommendations are for actions by professionals and their associations; including but not limited to IT professionals. The role of these recommendations is to suggest avenues for action to mitigate the failures and increase resilience, in the next phase of the work.

Recommendation 1: Software risk should be recognised as a threat alongside global warming, and pandemics.

> **Desired outcome: Plans nationally and in organisations to prevent software failures and to increase resilience after software failures.**

Underpinning this over-arching recommendation are three other recommendations which can support this outcome (section 4 for the detailed discussion):

Recommendation 2: Relevant education including causes of software failure and the resilience of digitalised systems.

> **Desired outcome: a broader and deeper understanding of causes and mitigation of software failure.**

Recommendation 3: Software risk visible across organisations in the UK.

> **Desired outcome: Integration of software risk into organisations' planning.**

Recommendation 4: Explore insurance initiatives focusing on both prudential and systemic software risk.

> **Desired outcome: UK insurers as leaders in the software risk, and consequential losses and damages, market.**

In the next phase of the project, from 2023, we aim to flesh out these recommendations, or updates based on consultation, and work with partners to implement them.

1. Introduction

In this Policy Think Piece we focus on collating data and creating awareness of the extent and economic and social cost of software risk.

1.1 Scope

This paper is the result of discussions with, and contributions from, the Working Group and external contributors. The Terms of Reference are in Appendix 4 and the members of the Working Group and external contributors are identified in section 5.

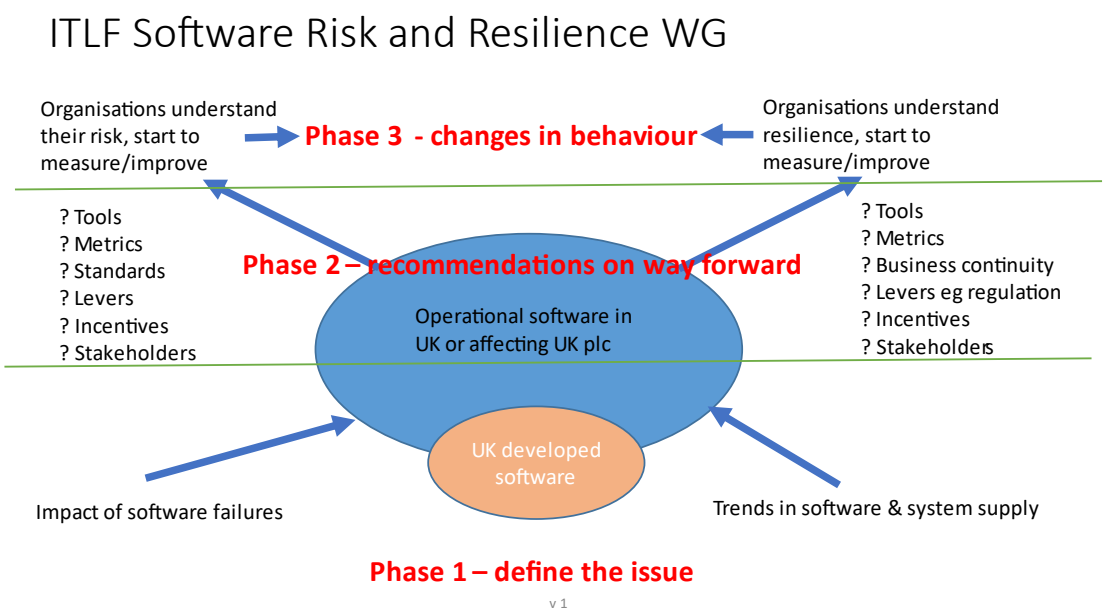


Figure "BCS Software Risk and Resilience WG Scope – Phase 1" illustrates the phases of the work as we see it. From bottom to top it represents the flow from Phase 1, in which we define the issue and make recommendations for Phase 2, to Phase 3 where changed approaches to software risk and resilience are observable.

The task in 2022 – Phase 1 - is to create a network of informed people who are aware of the economic consequences of software failures. Since digital systems are increasingly a crucial part of the economy, these people should be in a range of quality, audit, procurement, legal and financial roles.

In Phase 1 we have sought evidence for the effect of software failures on the UK economy. We have found that there is no source of UK-specific data on software failures and their cost to the economy. We have therefore made estimates based on data from several sources (see Section 2.5 and Appendix 3).

In Phase 1 we have also explored the trends to complexity and connectedness, with the provision of software as a service and the use of Open Source and Commercial Off the Shelf Software. As a result, it is clear that the central question for the UK is no longer "How can we improve software development standards?" This question continues to be important at a global level, but most organisations do not control the development of the software that runs their operations. Further, there is evidence that software errors are found in most software.

So the question for the UK economy and society becomes: "How can we help organisations to both reduce system failures arising from software errors, and also be more resilient in managing failures?"

In order to create a network of informed people, including professionals whose roles are not specifically "in IT", in Phase 1 we aim to connect with a range of professions and stakeholders: Risk Managers, Quality Managers, Procurement Managers, Internal Audit Managers, legal experts, as well as IT professionals working as CTOs, CISOs and CIOs.

As discussed in the Terms of Reference notes (in Appendix 4) we expect in Phase 2 to focus on Operators of Essential Services – covering Communications, Energy, Health, Transport and Water industry sectors. These sectors have a fragmented regulatory structure and an apparent lack of awareness of software risks (see section 4.4), and failures here have a wide effect on the economy and society.

This contrasts with Financial Services, where the regulators encompass digitalisation and there is visibility of software risk – as an example, the Financial Times Leader on 24th August is by-lined "the finance sector ought to strengthen its collective defences", referring to software failure.

Phase 2 should aim to develop a framework for tools and metrics to aid organisations. While some aspects of frameworks are generic, others will vary by sector, so that our focus on Operators of Essential Services will guide us on priorities. Phase 2 will also look for organisational levers for implementation, e.g.

- in organisations: Directors and NEDs;
- at UK level: Government and national bodies eg National Preparedness Commission[1], National Infrastructure Commission[2], DCMS[3] or other responsible Government Department;
- the insurance industry;
- major global players eg Google, Microsoft, SAP, AWS.

Finally, Phase 2 should define the metrics of success for Phase 3, as organisations become better prepared for avoiding, and reducing the consequences of, software risk.

Defining our scope within the potential IT issues

In the discussions leading to this Policy Think Piece we have chosen to focus on the specific issues surrounding the costs of failure of already installed and operational software.

So we exclude for instance, the costs of cancelled projects in estimating the financial effect of software failures.

We also wish to avoid duplicating other activities.

[1] https://nationalpreparednesscommission.uk/

[2] https://nic.org.uk/

[3] https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport

The obvious overlap is with work on responding to cyber-attacks. Software failures can of course be caused by cyber-attacks. Successful cyber-attacks often exploit known software vulnerabilities to cause system failure. However in this Think Piece we exclude consideration of direct risks from cyber-attacks or the approaches that might be taken to reduce these risks, except in so far as cyber-attacks are often based on exploitation of known vulnerabilities in the software supply chain (see section 2.2). There are specialist organisations offering advice on resilience to cyber-attack, and we do not need to duplicate this work[4].

The increasing scope of digitalisation extends the type of end user that operates or maintains software – many system failures are due to incorrect operation by untrained or naïve operators, as in the British Airways and Horizon cases in Appendix 2. While we know that an increased focus on usability during system design would reduce the number of failures, we have concluded that recommendations on design criteria are outside our scope.

We have not considered the risks which are specific to AI systems. AI systems are of course implemented in software and so are subject to the general risks that we describe: the implementation of AI software should be part of any discussion of software quality. However, AI systems are also subject to additional specific risks: these risks are widely discussed and covered in a recent BCS report[5] among many others.

As a final exclusion, there is alarm in some quarters at the weak rights of the purchaser in relation to software products and services, and to the services provided by digitalised systems, the "digital asymmetry." We do not feel able to provide any additional perspective or insight on this issue except in our short discussion of procurement (section 2.5).

1.2 Layout of this Policy Think Piece

We have divided our discussion into sections, aiming for a coherent narrative; we cross-refer to data in the Appendices for definitions, detail etc.

Section 2 shows that software errors will persist in digitalised systems: that the costs to the UK economy are already high and will increase. We summarise the reasons for our anticipation of existential risk from software failures.

Section 3 on "What can be done?" identifies that organisations can protect themselves and reduce the consequences of software failure and discusses existential threats outside their control.

Section 4 is our recommendations: most IT professionals are aware of software risk but need to engage with others to reduce operational risk from software failures and improve system resilience. The recommendations suggest avenues for this cooperation.

Section 5 is Acknowledgements: the Working Group has had wide and deep support from IT Professionals and others with an informed view of digitalisation.

In early days of the Working Group we found that some terms were being used with different meanings by contributors, so we have included a Glossary as Appendix 1.

---

[4] https://www.gov.uk/government/news/new-laws-proposed-to-strengthen-the-uks-resilience-from-cyber-attack

[5] https://www.bcs.org/media/9378/ai-briefing.pdf

Appendix 2 contains some cases of software failure affecting the UK which are in the public domain.

Appendix 3 details the workings behind our estimates of the cost of software failures to the economy.

Appendix 4 contains the Working Group's Terms of Reference.

Appendix 5 is an excerpt from the UK government's web site[6] on the role of regulators for Network and Information Systems.

[6] https://ico.org.uk/for-organisations/the-guide-to-nis/key-concepts-and-definitions/

1 Digital systems risk – historically and in the future

Software errors will persist in digitalised systems: the costs to the UK economy are already high and will increase.

2.1 Software failures

Software fails because code has errors or is not set up to handle the data supplied. Software failures may not be evident to users (as in the Post Office Horizon case, see Appendix 2).

Code errors are referred to as defects. They do not necessarily produce failures but instead represent a vulnerability or weakness of the software to failure should particular conditions occur ranging from unexpected inputs to atypical combinations of instructions. Defects may not cause a failure until many years after the system goes live, see the NATS example in Appendix 2. A 2019 study of defects found that, after completion of testing, software typically continued to have 25 defects per 1,000 lines of code[7]. This error rate has not significantly changed over the last 20 years[8].

There are two main approaches to reducing the number of errors in code – formal methods and testing. The Working Group has assumed that neither approach will deliver "zero defect" software in the short to medium term, and that there is therefore a need to mitigate the consequences of software failures.

There may be useful lessons to be learnt from the fact that a typical car now contains more than 100 million lines of code, implying that there could be 2,500,000 errors per car. But most cars work OK most of the time. And when they do not it is common to assign blame to user error[9]. It may also be the case that a very small proportion of the code in a car is used to control moving parts.

In Appendix 1 we illustrate the differences between defects and failures.

2.2 Software failures – empirical data

The CAST Crash 2020 report[10] gives insight into sources of failure, based on 2,505 applications consisting of 1.549 BLOC (billions of lines of code), distributed across 533 organizations and 26 countries. The sample covered a range of implementation methods and sizes of system: neither methods nor size were correlated with quality as measured by number of failures.

The report finds that Telecom, Software vendors, and IT consulting had the highest densities of critical Robustness, Security, and Changeability weaknesses. Most industries showed wide variability in critical weaknesses and numerous extreme outlier scores, suggesting there are factors that have greater impact on software quality than the industry segment in which the application was developed or operates.

---

[7] Philosophy & Technology (2019) 32:363–378 https://doi.org/10.1007/s13347-019-00342-1: Understanding Error Rates in Software Engineering: Conceptual, Empirical, and Experimental Approaches, Jack K. Horner & John Symons

[8] https://www.academia.edu/30961190/Should_We_Trust_Computers

[9] https://abcnews.go.com/Blotter/toyota-pay-12b-hiding-deadly-unintended-acceleration/story?id=22972214

[10] https://content.castsoftware.com/crash-report_cast-research-on-application-software-health

It also finds that many failures were caused by the organisation not implementing fixes supplied for known vulnerabilities in software supplied by third parties, whether Open Source or Commercial Off the Shelf Software, and the report also finds that this share is increasing. The practical problems of implementing fixes are illustrated in Appendix 2 – O2's 4G network. It is not reasonable to expect TfL as a customer of the O2 network to be aware of the ongoing state of Ericsson's software certificates – but it is TfL users that are inconvenienced.

Purchasers of Commercial Off the Shelf Software may assume that this is secure. However, security is not proven and the software may never be patched or updated. An example is a software package to create automation control systems which are programmed via the IEC61131 standards language[11]. This was already embedded within 261 different manufacturers products when it was revealed to have vulnerabilities in 2012[12]. Unfortunately, the latest version of the same software has been found to have similar or worse issues, including being able to execute arbitrary uploaded code - which makes it open to hackers[13].

2.3 Costs of software failures

Software failures constitute risks to those who use and rely upon software.

In Appendix 3 we discuss the practical and conceptual problems in capturing data on the costs of software failures. Software failures will cause suppliers to bear the cost of fixing the causes, and they may suffer reputational risk. But the immediate cost or risk of software failure is felt by the individual or organisation using it. The cost may be spread across many users, which makes measuring it more difficult[14].

Data specific to the UK

In the UK, there does not appear to be an archive of major software failures and/or their cost to the economy. Nonetheless, anecdotes such as those about TSB's problems in transferring from a legacy system[15], BA's cancelled flights[16] due to inability to recover from software failures, and the Post Office's Horizon[17] system are in the public domain and indicate the potential severity of consequences stemming from software failure. Appendix 2 includes some case studies describing some consequences of software failure. And a bird's eye view of healthcare is a useful perspective on the cost of software failures to one of the essential services.

---

[11] https://control.com/technical-articles/an-overview-of-iec-61131-3-Industrial-Automation-Systems/

[12] https://arstechnica.com/information-technology/2012/10/backdoor-in-computer-controls-opens-critical-infrastructure-to-hackers/

[13] https://thehackernews.com/2022/06/critical-security-flaws-identified-in.html + https://thehackernews.com/2021/06/10-critical-flaws-found-in-codesys.html

[14] https://www.longfinance.net/news/pamphleteers/digitalisation-risk-and-resilience/

[15] TSB IT meltdown cost bank £330m and 80,000 customers | The Independent | The Independent

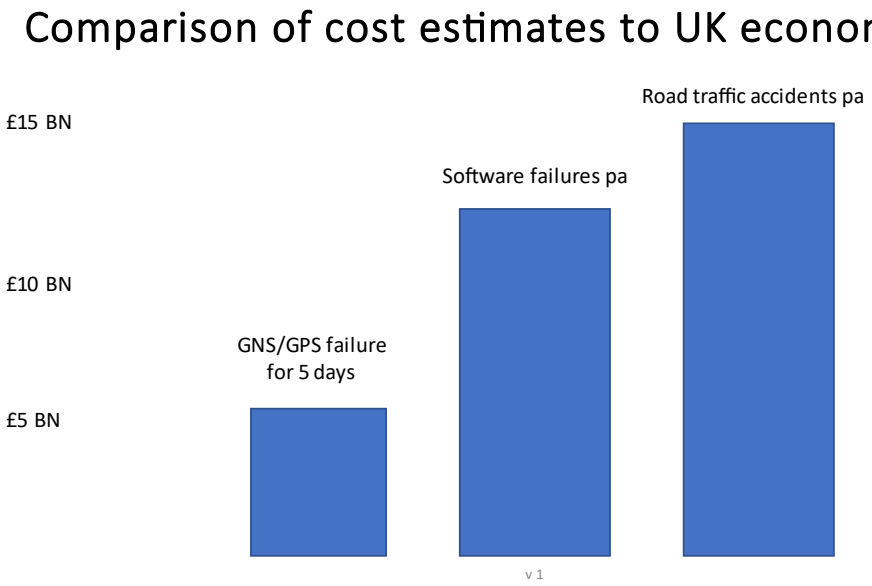
[16] BA IT systems failure results in cancelled flights and delays at London airports (computerweekly.com)

[17] Horizon inquiry questioning raises hopes of fair compensation for victims so far left out (computerweekly.com)

Appendix 3 fleshes out and critiques some sources of the data for estimates of costs of software failures to the UK economy, the estimating methods, and the implications. It suggests that £12 billion pa is a conservative estimate of the costs of software failure to the UK economy. This is compared with estimates from London Economics of the cost of the UK economy should GNSS/GPS be out of action for 5 days – this is £5.2 billion[18].

For further comparison, the Department for Transport reported that road accidents cost the national economy almost £15 billion in 2013, a figure that includes vehicle and property damage, police costs and insurance costs[19]. Prevention costs are estimated at £16.5 billion[20].

Figure "Comparison of cost estimates to the UK economy" illustrates the relative size of these costs.



2.4 Future trends increasing the risk from software failures.

Increase in volume of software

"First, there's more bad software out there—a lot more." Susie Wee, vice president at Cisco, said in May 2017 that there were more than 111 billion lines of new software code being produced each year. We estimate that this could mean 2.5 billion new software defects.

---

[18] 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

[19] https://www.fonsecalaw.co.uk/blog/patricks-blog/2014/10/22/the-cost-of-road-traffic-accidents-in-the-uk#:~:text=The%20cost%20of%20road%20traffic%20accidents%20in%20the,and%20property%20damage%2C%20police%20costs%20and%20insurance%20costs.

[20] https://www.statista.com/statistics/322862/average-cost-of-road-accidents-and-casualties-in-great-britain-uk/

Impact/risk from defects

Three trends magnify the effect of software defects:

- **Digitalisation**: a far greater slice of business operations is integrated and controlled by software, thus rapidly spreading the effects of any malfunction. The Internet of Things (IoT) is becoming the Internet of Everything (IoE). And when "everything is a computer," software is in everything.
- **Systems of Systems**: Complexity arises from the frequency and intensity of interaction. Software from multiple sources is increasingly connected and the number and nature of such connections makes it difficult to model all potential consequences, so the systems become increasingly likely to fail when faced with unforeseen events.
- **Increased Competition**: increased demand for online working in both the consumer and business-to-business sectors has prioritized the speed-to-business approaches such as DevOps over consideration of operational risk and corrective maintenance costs.

Effect of openness to [cyber]attack

A report by the Consortium for Information and Software Quality[21] points out: It's not just that fixing poor-quality software is expensive. It also makes online systems, networks, and products easier to attack, which is another colossal expense. And the so-called "attack surface" is expanding rapidly, because of the evolution of technology. The report refers to a report from consultancy Synopsis which identifies actions which could reduce vulnerability to attack[22].

Software failure from cyber-attack is in many ways similar to climate related system failures. The digitalisation "climate" contains clouds of malware that will attack any system that happens to be exposed and vulnerable. Many cyber-attacks are not targeted but result from a failure to apply patches for known bugs or to close unneeded services and internet ports. The NHS Wannacry[23] failures and the widespread NotPetya[24] failures are examples of the huge costs resulting from untargeted infections.

2.5 The position in the UK

The operational software relied on by most organisations is outside their control. Therefore, while we believe that UK based research on software is an important area where the UK contributes to the world stage, we conclude that this is not likely to alter the current status of the operational software environment in the UK in the short to medium term.

The purpose of this Policy Think Piece is to engage a wider set of contributors to a discussion of how and where to start to tackle the economic and social risks to the UK economy. Two potential contributors are data centres, and procurement.

---

[21] https://www.it-cisq.org/the-cost-of-poor-software-quality-in-the-us-a-2020-report.htm

[22] Software Security Assessment Report | BSIMM

[23] https://www.computerweekly.com/news/252434444/NHS-WannaCry-review-highlights-need-for-accountability-and-skills

[24] https://www.computerweekly.com/news/450429175/NotPetya-tops-list-of-worst-ransomware-attacks

Data Centres

A recent article by the UK and Ireland Channel Director of Schneider Electric[25] summarised the increasing dependence of organisations on their digitalised infrastructure: "---- many customers are concerned about the resiliency of their infrastructure and the impact of failures on their customer base. Recent research from the Uptime Institute[26] notes that despite improving technology and better management processes, outages remain a major concern, with both the impact and cost of downtime increasing. Power remains the leading cause of outages: however, software and IT configuration and network issues are gaining ground as common causes of major IT service outages"[27].

Procurement

As organisations buy in software and services, procurement functions face challenges[28]. The valuation of intangibles like software or cloud services can be difficult, and another complexity is the duration for which the software will be in place – typically ten years – increasing long term "digital entanglement." Further, the shift towards the decentralisation of purchasing authority can lead to using the Silicon Valley mantra: 'move fast and break things' in domains where the risks to the organisation of "break things" is significant.

2.6 Summarising

- IT professionals are aware that digitalisation is an increasing part of the economy and society.
- Digitalisation is built on, among other components, software which has defects which can cause failures of the system and hence a breach in service.
- These failures cause considerable costs to the economy.
- The amount of software in use is increasing – causing billions of extra defects each year.
- The interconnectedness and complexity of systems is likely to cause unexpected modes of failure.

[25] Emerging digital service models: Addressing the need to prevent downtime (computerweekly.com)

[26] https://uptimeinstitute.com/2021-data-center-industry-survey-results

[27] The current (at time of writing) DCMS consultation focuses on factors affecting the resilience of data centres, recognising their importance to the digitalisation of the UK. Professor Steinmueller has submitted a response to the consultation, on the importance of software.

[28] https://www.youtube.com/watch?v=TxnaRJ-8X2k

3. What can be done?

Organisations can protect themselves and reduce the consequences of software failure but there are also existential threats outside their control.

3.1 How can organisations protect themselves against software failure?

The CRASH report (see Section 2) identified as good practice:

"1. Benchmarking should be conducted within technology and type of application to get accurate insight into comparable performance. Results from benchmarking purely against industry segment can be misleading because of effects by other factors with greater influence that may vary across organizations.

2. Greater attention must be given to secure coding practices as many applications had densities of critical Security weaknesses that were unacceptably high. Security scores displayed wider variation than those of any other Health Factor.

3. Analyze source code on a regular basis prior to release to detect violations of quality rules that put operations or costs at risk. System-level violations are the most critical since they cost far more to fix and may take several release cycles to fully eliminate.

4. Treat structural quality improvement as an iterative process pursued over numerous releases to achieve the optimal quality thresholds.

While adopting these evidence-based recommendations cannot guarantee high structural quality, they have been shown empirically to be associated with lower risk applications."

These good practice guidelines can be supported by checklists such as CISQ's on architectural features underpinning resilience[29] and by recent standards work. For instance, the recently published ISO standard (5055) measures the internal structure of a software product on four business-critical factors: Security, Reliability, Performance Efficiency, and Maintainability. These are the factors that determine how trustworthy, dependable, and resilient a software system will be[30]. Tools implementing an evaluation aligned to this standard can provide part of a wider toolkit.

3.2 WEF – four principles[31] for building resilience to digital risk

The discussion below closely follows the World Economic Forum's list.

There are at least four straightforward principles to thinking about how to identify, mitigate and build resilience to digital risks.

The first is to approach digital risk as an enterprise-wide issue and not just an IT issue. Digital risk is a combination of people, processes and technologies[32]. Determining what matters and what doesn't, starts with a risk assessment to help identify the most valued assets, where

[29] How Do You Measure Software Resilience? (it-cisq.org)

[30] Publicly Available Standards (iso.org)

[31] Converting digital risk into opportunity in the COVID-19 era | World Economic Forum (weforum.org)

[32] BCS reviewers have pointed out that in today's world, supply chains and partners are critical sources of digital risk.

they're located, how they are protected and who has access. It means deciding who is in charge, and delegating authority and accountability as appropriate.

A second principle requires assessing and understanding the legal applications of digital risk. The regulatory environment for new technologies is fluid and fast changing. It is shaped by politics from the international to the local levels. Concerns with foreign interference or privacy and loss of personal data are real and consequential; corporations can be fined and executives can be jailed.

The third principle is to ensure that company leadership is on top of the emerging risks and in constant contact with management. Executives must be able to answer the following questions: How secure are we and how do we know? What's the value at risk? What are the geopolitical and geo-digital threats to the company? What are the gaps, what do we need to know next? A constant dialogue with experts within the company and outside – keeping a pulse on global trends – is more essential than ever.

A fourth principle involves setting up a clear playbook to appraise and respond to digital risk. Approaches will vary and evolve, but all companies need to start by measuring the value at risk. This means assessing digital exposure as it relates to impacts on earnings, the amount of time required to fix attacks, the capital and operational costs required, the loss of revenue, and the potential for fines. Firms should also create a risk register – integrate digital threats into the business risk model – to easily communicate threats to corporate leadership. Risk management standards are key, as is applying them so they provide the right metrics to drive decision-making.

These four principles from WEF can provide a context for more detailed Disaster Recovery Planning and Business Continuity Planning[33] which reduce the consequences of operational software failure.

3.3 Consequences of operational software failure

The consequences of operational software failure range from small inconveniencies to life changing catastrophe:

- Interruptions that cause minutes of disruption such as those that require restarting a programme with few or no effects on data integrity, but inconvenience to the end user;
- System interruptions that halt operations for hours and that involve significant repair and restoration costs, with financial and reputational costs to the organisation and financial costs to the end user;
- System collapse that requires substantial rebuilding of data or other system elements or that create substantial harm in other systems (such as power outages on an electrical grid).

In all three cases, the consequences are borne by organisations and individuals in the public and private sector, who are dependent on the software or service, rather than the software supplier.

[33] https://www.disasterrecoveryplantemplate.org/difference-between-drp-and-bcp/

Clearly the first approach to reduce the effect is for organisations to act as sketched above to keep their systems well maintained and processes widely understood.

However the move towards buying in software and software as a service means that breaks in service may be outside the control of the organisation supplying the service to their customers. As an example, when O2's mobile network went down due to an expired certificate installed on their systems, the TfL information display boards and the Shropshire Council car park machines failed (Appendix 2: Some software failure examples).

Further, end users are increasingly faced by systems which combine IT with multiple networks, warehouse robotics or medical equipment. Here, software failures can affect health and safety as well as creating operational costs. And attempts to gain redress – as in the Horizon Project (see Appendix 2) – are subject to the legal 'presumption of the reliability of computer evidence'[34].

End users do not have a track record of successfully claiming after they have suffered a breach in an IT based service they have paid for. Ofcom[35] has defined a set of payments due if broadband or landline services are unavailable for more than 2 days: these payments are aligned to the rental costs of the line rather than the loss of amenity to the user. And the Ombudsman web site states[36] "If you have issues with intermittent faults or loss of service issues with your communications provider, we can help you. Unfortunately, these kinds of problems aren't uncommon. We deal with a high volume of complaints every year." Meanwhile, the recommendation that the internet be declared a utility has not passed into law, so users' rights to internet service are limited to their service contracts with internet service providers.

ICO as the regulator of Registered Data Service Providers fines companies for data breaches but does not appear to have implemented regulatory activity for service breaches[37].

The fall-back for "who to bear the cost" would seem to be insurance. Many organisations now have insurance against the damage caused by a cyber-attack, i.e. an external attack: though increasingly this may only be provided subject to passing an audit of the organisation's systems by the insurer. Should organisations be able to insure against software failures, now that IT is as central to organisations as electricity?

It may be that organisations will need to continue to bear the costs of the first two types of operational failure, but that failures of the third type could be covered by a third party insurance scheme on the lines of "cyber-catastrophe" insurance – software and hurricane risk being treated similarly.

---

[34] https://www.computerweekly.com/opinion/A-trial-relying-on-computer-evidence-should-start-with-a-trial-of-the-computer-evidence

[35] Automatic compensation for broadband and landline users - Ofcom

[36] https://www.ombudsman-services.org/problems/loss-of-service

[37] https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/nis-regulations/

4. Recommendations

While many IT professionals are aware of software risk, they need to engage with other professionals to reduce the risks from software failure and improve the resilience of the UK economy and society.

4.1 The role and style of our recommendations

We propose that Phase 2 of the Working Group, from 2023, be targeted at progressing the recommendations below, or updated versions after consultation, in conjunction with partners.

Factors which have guided the directions of our recommendations are:

- The dominance of companies owned from outside the UK in the supply of Essential Services, and a range of other (government, business to business, financial and consumer) services in the UK;
- The dominance of software owned, managed and /or implemented outside the UK in the operation of many Operators of Essential Services and a range of other (government, business to business, financial and consumer) organisations;
- The policy direction of travel of the UK government which implies a reduction in the extent of regulation;
- The framework proposed by the Information Commissioner's Office for capturing the impact of service breaches by Registered Data Service Providers (see Appendix 5).

The Working Group discussed the lack of UK-based data on software failures and costs. It is not clear that gathering and publicising data on the effect of software failures is the role of government. There is no analogy with the role of eg the Department of Transport which collates the cost of road accidents. This is because software is embedded in the operation of most organisations to an increasing extent: so no government department has oversight across the necessary range. In gathering anecdotal data, we have found Computer Weekly to be a useful resource. It has published information about a number service breaches in the UK, as some of the case studies in Appendix 2 indicate[38].

We considered recommending the establishment of a knowledge hub for sharing case studies of software failure and their costs, perhaps as part of a research centre. We decided that the demand for a hub might emerge from the implementation of our other recommendations, but that the hurdles to success of a hub are such that it should not be recommended as a standalone initiative. First steps could be capturing how other industries – eg chemicals, aerospace – share accident reports and disaster information, and how these processes could be applied to software.

4.2 Recognition of the existential threat from software failure

Recent events – the pandemic, global disruption, extreme weather – have increased the awareness of the consequences of lack of resilience in our economy and society. Digital systems are increasingly a crucial part of the economy: but there is evidence that digital

[38] BCS reviewers have suggested additional sources: https://londonwebstandards.org/about/ ; https://owasp.org/ ; https://technation.io/

systems are increasingly liable to service breaches due to software failures, and that these breaches are increasing in scale and duration (see section 2). The risks are similar to those from global warming or pandemics, in that major shocks are certain, but not their location or timing.

IT professionals and some others are aware of these risks, (see section 3) but they have been "the elephant in the room". More widespread awareness is needed before most organisations have adequate policies and processes to prevent software failures and are able to mitigate the consequences of these. The purpose of this Policy Think Piece is to increase this awareness, and so our recommendations are for professionals and their associations; including but not limited to IT professionals.

Recommendation 1: Software risk should be recognised as a threat alongside global warming, or pandemics.

Desired outcome: Plans nationally and in organisations to prevent software failures and to increase resilience after software failures.

4.3 Skills to support a digital strategy

The UK government's Digital Strategy[39] is a "vision for harnessing digital transformation and building a more inclusive, competitive and innovative digital economy." It implicitly assumes that the enabling conditions such as resilient systems are in place. As the discussion above showed, this is a brave assumption. It is clear from comparisons with other developed countries that software failures are a large cost the economy. It is also clear that this is likely to increase for well-understood reasons (see 2.4).

Skills in the IT profession

In order to deliver the digital strategy, digitalisation needs to work robustly and reliably. Many IT Leaders assess that the necessary technical skills to deliver this are lacking, particularly at senior levels. The exponentially expanding complexity of systems provides the triggers for huge failures through multiple cross-system interactions. While triage of IT assets in order to focus on maintenance of software for delivery of critical services is always prudent, software failures can also arise because of vulnerabilities in peripheral systems. Increased awareness of the importance of segmentation – establishing interfaces between systems – is needed.

For instance, the US government issued an executive order requiring those companies selling to the federal government to take precautionary measures to identify and remediate vulnerabilities in software and to provide agency customers with a software bill of materials[40] (SBOM) enumerating the various software components, including open-source components, contained in their products[41].

And new approaches and tools to testing and recovery/resilience are emerging. In section 3 we mentioned tools based on the recently published ISO standard (5055): and the use of AI

[39] UK's Digital Strategy - GOV.UK (www.gov.uk)

[40] https://mybcs.bcs.org/knowledge-and-resources/thought-leadership-and-insight/what-is-a-software-bill-of-materials-and-will-it-improve-security/

[41] https://www.lawfareblog.com/open-source-security-how-digital-infrastructure-built-house-cards

in software testing can support more tests in a shorter timeframe than could be accomplished with people.

Software is anomalous among engineering professions in that, in the UK and elsewhere, software engineers do not have to be licenced. We do not know if the licencing of software engineers by Canadian provinces[42] has led to fewer software failures in Canadian software systems or has had any other effects: the BCS might wish to explore this. Similarly, the crucial role of software in delivering services in the UK economy suggests that the profession might review the scope and nature of approaches to cost and safety/impact of breaches, learning from other engineering disciplines.

In addition to the technical skills to deliver the complex systems of digitalisation, IT management and its corporate governance should become much more focused on service and business outcomes[43].

Skills in the audit and legal professions and among senior managers

Similarly, in the audit professions – quality, risk, health and safety, and finance – auditors need education and training to recognise and enforce robust and reliable digitalised systems. The Y2K crash that never happened [44] was, it is thought, at least partly because auditors were reluctant to sign off the "going concern" statement unless the organisation was able to identify their Y2K plan.

Also, the legal profession has few members comfortable with digitalisation. This is relevant to purchasing decisions – see section 2.5. Developments such as the protocol for objective determination as to whether a code error, or other systems fault, is a software material defect[45] can provide the framework for legal and procurement professionals. This approach focuses on the financial consequences of the defect.

Understanding the nature of failures of digitalised systems needs to be part of skills development for technology, finance, legal and audit staff. While this could be the immediate focus, we are also conscious of the thinking that "The current roles and responsibilities of the CTO will become essential skills for every future CEO[46]."

Professional associations have an important role in working with private and public sector organisations including universities. They should encourage relevant skills education including causes of software failure and resilience of digitalised systems.

Recommendation 2: Relevant education including causes of software failure and the resilience of digitalised systems.

---

[42] https://www.jobbank.gc.ca/marketreport/requirements/5485/ca

[43] "Managing Agile Business Technology", David Miller, Springer, 2022, ISBN 978-3-030-90597-2. https://link.springer.com/book/10.1007/978-3-030-90598-9

[44] https://www.britannica.com/technology/Y2K-bug

[45] https://www.cutter.com/article/forensic-systems-analysis-methodology-assessment-and-avoidance-it-disasters-and-disputes

[46] https://www.information-age.com/cto-role-evolve-ceo-role-123481596/

Desired outcome: a broader and deeper understanding of causes and mitigation of software failure.

4.4 Increasing awareness of risk from digitalisation

As we noted above, many industries are now dependent on digitalised systems.

Financial services were early adopters of digitalisation, and regulators have been concerned with software risk for several years. For instance, the Financial Conduct Authority states[47]: "We've introduced new rules and guidance to strengthen operational resilience. We'll assess the impact of this by testing firms' operational resilience, business continuity and incident response plans, cyber security and third-party management. We will look at how resilient firms are to disruptions as well as the severity and scale of actual disruptions. We will also assess the resilience of third parties that provide critical services to the financial sector. We are focusing our efforts on those firms who can't meet our new standards on the impact of disruptions."

Registered Data Service Providers are regulated by the Information Commissioner's Office in the Department of Culture, Media and Sport in accordance with the framework in Appendix 5. There does not appear to be any published data on service breaches.

The regulatory regime for Operators of Essential Services is fragmented, and the National Infrastructure Commission 2nd Baseline Plan does not mention software risk. Ofcom's recent consultation[48] addresses failure rates for telecoms networks: the Code of Practice is remarkably detailed and shows how the government can regulate the engineering of systems that contain software.

Meanwhile, the evidence is that digitalised systems are becoming more subject to failure, and that these outages – service breaches - last longer and affect more end users[49]. We also noted (see 2.2) that a significant and increasing proportion of software failures are due to known vulnerabilities for which the fix has not been installed in the organisation's system. Software risk should be routinely included in existing mechanisms such as KPIs and Risk Registers. A Software Bill of Materials can start to assess the extent of this risk[50].

While all industry sectors and government are exposed to risk of failure of digitalised systems, the leverage effect of failures in infrastructure services mean that these can have a major effect on the economy of the UK. We therefore propose that professional associations should undertake research, publications and engagements that makes software risk visible across organisations in the UK, with priority given to Operators of Essential Services, learning from the experience of regulation in financial services. The type of framework proposed by the ICO (see Appendix 5), which highlights outcomes of failures, is another way of communicating the impact of software failures as well as other reasons for lack of service.

---

[47] https://www.fca.org.uk/publication/corporate/our-strategy-2022-25.pdf

48 https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice

49 https://uptimeinstitute.com/resources/research-and-reports

[50] https://www.cisa.gov/sbom

Recommendation 3: Software risk visible across organisations in the UK, with priority given to Operators of Essential Services.

Desired outcome: Integration of software risk into organisations' planning.

4.5 Who pays for software failures?

Who is accountable for software failures and who should bear the associated costs?

Protection for organisations or end users against software failure is rarely found through suing the supplier: "digital asymmetry"[51] leads to many software contracts being written to protect the supplier in case of failure. Software liability insurance, which is taken out by suppliers, IT consultants and experts, may cover the costs to the user organisation if lack of suitable professional skill, care and diligence, of the supplier is proven or admitted to be the cause of the failure. It is clear that software failures can cause prudential risk .

Many organisations have cyber liability insurance, which may extend to business interruption[52] costs. Data loss after a cyber-attack has been accepted as a cause of business interruption, and the costs covered by insurance. Cyber insurance is often subject to audit by the insurers of the organisation's cyber defences.

As the discussion earlier suggested, the scope and duration of software failures is increasing. As the probability increases of systemic failure[53] due to software, an approach which was first suggested by Michael Mainelli[54] is to transfer some catastrophe risk on to the financial markets. "Linking together machines around the world might have made the world a smaller place, but it has also made it more susceptible to the possible effects of a single disastrous event. For that reason, it is imperative that the insurance industry adapts the ways it manages catastrophe risk. Software risk could be transferred to the capital markets in ways similar to, say, hurricane risk. With the help of Smart Ledgers, insurers and reinsurers can be certain that their clients are covered for anything."

Recommendation 4: Explore insurance initiatives focusing on both prudential and systemic software risk.

Desired outcome: UK insurers as leaders in the software risk, and consequential losses and damages, market.

---

[51] https://www.youtube.com/watch?v=TxnaRJ-8X2k

[52] https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/business-interruption-insurance/

[53] Systemic risk can be defined as the risk associated with the collapse or failure of a company, industry, financial institution or an entire economy.

[54] https://www.longfinance.net/publications/long-finance-reports/cyber-catastrophe-insurance-linked-securities-smart-ledgers/

5. Acknowledgements, contributors and Achievements

The Working Group has had wide and deep support from IT Professionals and others with a view of digitalisation.

5.1 BCS-wide Support

The Working Group has been supported throughout by Bill Mitchell, BCS Director of Policy, and James Woodward, BCS Head of Policy and Public Relations. The BCS IT Leaders Forum which commissioned the Working Group has provided encouragement and a framework throughout, through Chair David Miller and Executive Committee sponsor Jon Hall: the Executive Committee Members are David Miller, Norman King, Paul Chung, Matthew Taylor, Jon Hall, Jacqui Hogan, Jonathan Leeson, Philip Crewe, Shakeeb Niazi, Algirdas Pakštas, Haiyan Wu, Adrian Steel, Christos Stavroulakis, Ian Golding.

The BCS Information Security Specialist Group, the Quality Special Interest Group and Information Risk Management and Assurance Group have provided critiques and helped us to define the problem; and comments through the BCS Community Portal have given extra insights.

The Working Group members have provided freely of their time and expertise. We (co-chairs Gill Ringland and Ed Steinmueller) thank them for their individual contributions as well as stimulating discussions during and between Working Group meetings. They are Colin Butcher, Stephen Castell, Neville De Mendonca, Andy Ellis, Ian Fish, Tom Gilb, William Hooper, Lucy Hunt, Adeel Javaid, Adam Leon Smith, David Miller, Jeff Parker, Yus Woozer. In particular, Stephen Castell has been influential in engaging with his wide network to extend the scope of inputs to the Working Group and in providing generous access to his experience. Tom Gilb has made his analytic tools and glossary available (the glossary is the basis for Appendix 1).

5.2 Other contributors have included

We have been greatly encouraged by support from many experts and policy influencers and thank them for their thinking and stimulus: William Adams, Paul Bailey, Simon Buckland, Estelle Clark, Vince Desmond, Phil Johnson, Sophie Isaacson, Patricia Lustig, Michael Mainelli, Stephen Mason, Natasha McCarthy, John McDermid, Chris Skinner, Tom Sykes, Philip Virgo, Alexander Wood, Chris Yapp.

Martyn Thomas has been extremely generous with his time and with his expertise which he has gained on many assignments relating to software capability, for the UK government and more widely. Among many sources of data he has pointed us to is the London Economics study of costs to the UK economy should the GNSS/GPS system be down for 5 days.

We especially thank Chelsea Frischknecht, a former marketing professional with Tricentis who generously provided her analysis of worldwide costs of software failures for 2017. This analysis, though informal, is perhaps the best estimate of total costs of software failure available at present.

5.3 Achievements to date

The purpose of Phase 1 of the Working Group's activities was stated in the Terms of Reference as to raise awareness of the extent of software failure and its effect on the UK economy.

Prior to the publication of this Policy Think Piece, achievements towards this have included:

- A submission by Gill Ringland to the National Infrastructure Commission 2nd Baseline Plan on 25th February.

- Creation of an active Working Group with 17 members who have contributed to the discussions and with input from their expertise and publications (see 5.1).
- Establishment of links with other BCS groups: the Information Security Specialist Group, the Quality Special Interest Group, Enterprise Architecture Special Interest Group, Information Risk Management and Assurance Specialist Group, Software Practice Advancement Group.
- Advice has been taken from external experts and those with influence in public life, (see 5.2) who have helped steer these recommendations.
- A Long Finance Pamphleteer "Digitalisation – risk and resilience"[55] (authors Jon Hall, Patricia Lustig, Gill Ringland) has had 635 downloads at time of writing.
- The Engineering Council and National Engineering Policy Council are supporting the project with advice and expertise on resilience.
- The Chartered Quality Institute is planning to extend their guidance on processes to cover software risk.
- A submission by Ed Steinmueller to the DCMS consultation on Data storage and processing infrastructure security and resilience - call for views - GOV.UK (www.gov.uk)
- Plans for a conference at BCS London Centre for IT and related professionals, on November 15th.
- Plans for a Long Finance webinar for finance and insurance experts, on November 23rd.
- Plans for a consultation virtual webinar across BCS Groups etc, to brainstorm next actions for Phase 2, on December 6th.

[55] https://www.longfinance.net/news/pamphleteers/digitalisation-risk-and-resilience/

6. Appendix 1: Glossary

This glossary is based on Tom Gilb's Planguage glossary. The complete glossary can be found at

Tom Gilb & Kai Gilb - Helping you deliver Value to your Stakeholders | ConceptGlossary

Agile

A method of software development stressing incremental development in collaboration with end users and favouring individual programmer initiative in responding to an evolving understanding of requirements and constraints.

Cloud

The application of Internet capacity to flexibly allocate storage, processing memory and processing power to execute applications and to retain data with reliable backup provisions. Cloud applications often involve significant machine to machine interactions in addition to user-machine interactions. Cloud based services allow the configuration of virtual machines to accomplish computational tasks.

Complex

A complex system is composed of more than one elementary and/or complex component.

Data centre

A large group of networked computers typically used by organizations for the remote storage, processing, or distribution of large amounts of data.

Digitalisation

Digitalisation is the process of using digital technology – such as computers and the internet – which restructures many domains of social life around digital communication and media infrastructures[56]. Gartner's glossary emphasises the view from business, "Digitalisation is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities. It is the process of moving to a digital business."

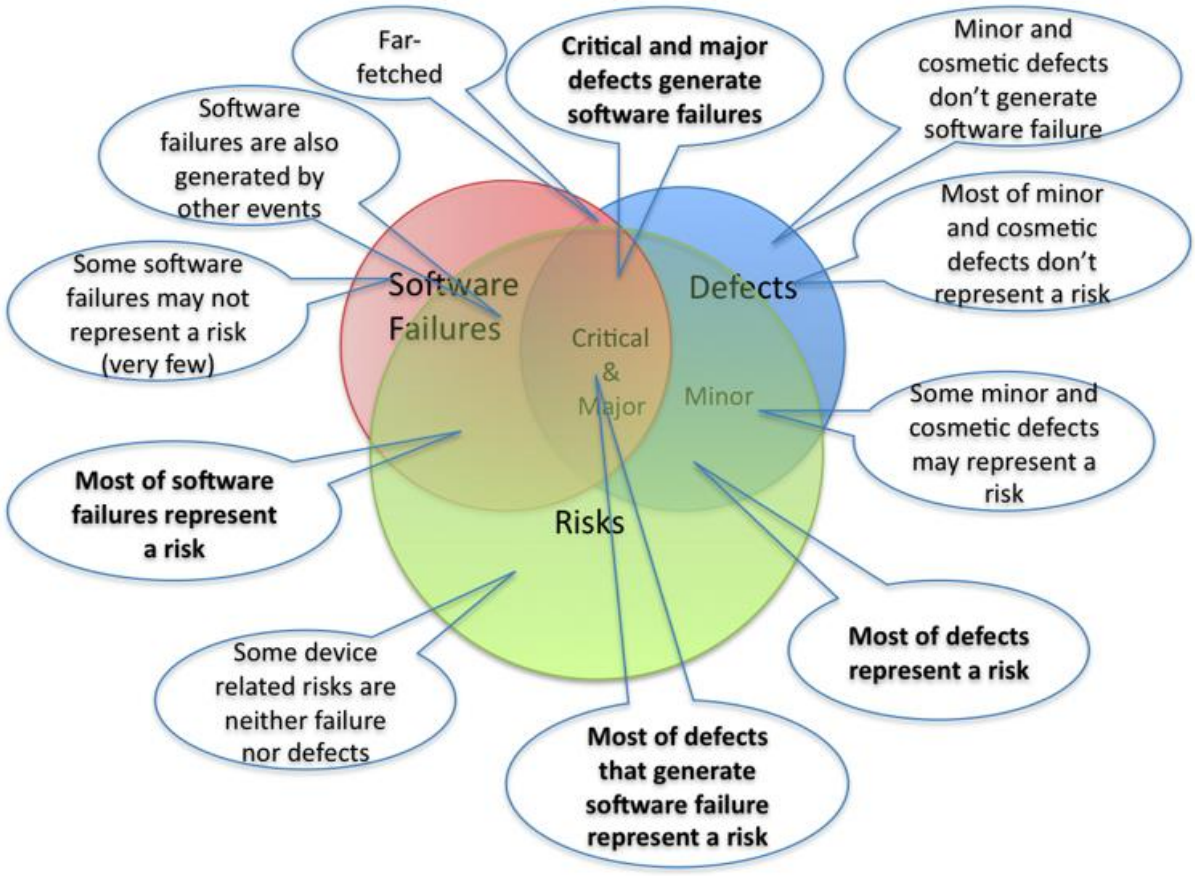
Digitalised systems have four main components – hardware which is visible, software which is an intangible, data, and networks (telecoms, internet) which are constructed of a mixture of hardware and software. Data is increasingly seen as a source of strategic advantage. Hardware failures are decreasing in importance whereas software failures are increasing in importance.

Defect

A shortcoming, imperfection or lack. The Figure shows the relationship between Defect, risk and failure.

[56] Digitization, Digitalization, And Digital Transformation: Confuse Them at Your Peril (forbes.com)

Source: https://blog.cm-dm.com/post/2012/09/14/How-to-differenciate-Bugs%2C-Software-Risks-and-Software-Failures-Part-2



DevOps

An approach to system development that emphasizes shortening the time between committing to a system change and its implementation while ensuring high quality. Complementary to agile programming, it also includes rapid feedback and simplification. DevOps is of particular importance in situations requiring the sustained operation and regular upgrading/revision of a system of critical operational importance.

EDGE

Edge computing is an architecture in which data is processed at the periphery of the network, as close to the originating source as possible.

Fail

'Failure' signals an undesirable and unacceptable system state. For example, a state of failure can result from issues such as safety problems, operator discomfort, customer discomfort, but not all are critical to a system's continued survival. Total failure is defined by catastrophe levels.

Fog

Fog computing is the computing, storage, and communication architecture that employs EDGE devices to perform a significant portion of computation, storage, and communication locally before routing it over the Internet backbone. Fog computing is a type of distributed computing that connects a cloud to "peripheral" devices.

Formal methods

The use of mathematically precise notations to specify and to reason about systems. The use of tools based on formal methods is increasing but are challenged by the relentless growth of new areas of computing such cloud based computing, the Internet of Things (IoT), and robotics.

Hardware

Computer hardware is the name for the physical components that a digital system requires to function.

Impact

An 'impact' is the estimated or actual numeric effect of an event, in our case a failure.

Internet

The computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Metric

A metric is any kind of numerically expressed system attribute. A metric is defined in terms of a specified scale of measure, and usually one or more numeric points on that scale.

Open Source

This is generally used to refer to a business model in which source code is made available under a license that permits organisations or individuals to use, modify, share, and improve the software, but limits the ability to incorporate the code in proprietary products whose source code is not publicly available. The means for organising collective activities to write and modify such code are continuously evolving from their voluntaristic origins.

Claimed advantages of open source software stem from the proposition that large numbers of skilled individuals may be more effective in discovering errors and that the negotiation over software features is more inclusive than proprietary products. Claimed disadvantages of open source software include the frequent absence of technical support, particularly for end users, and the potential for organisers to lose interest in maintaining and upgrading the software over time.

Platform

A general term for a web site designed to be accessible to large numbers of users. Sites designed for online sales may serve as platforms when they support multiple sellers.

Requirements

Requirements, or in the case of an Agile project, user stories, document the capabilities you want in a planned system. This typically covers:

- External interfaces (product inputs and tasks)
- Features (to process inputs and tasks)
- Usability requirements
- Performance requirements
- How information should be stored and accessed
- Design limitations

Risk

A risk is any factor that could result in a future negative consequence. Risks are quantifiable when they are known and their probability of occurrence can be assessed. (See Uncertainty)

Resilience

In general usage, the ability of a system to operate with some degree of effectiveness despite unanticipated or unusual events that challenge the systems performance or viability. In the context of information technology, the ability of a system to deal with operational software or hardware failure in ways that do not destroy or corrupt data and, ideally, the preserve some degree of functionality and operational service.

For example, an interactive system may shunt users to a 'waiting room' if allowing them to access the system would create system failure or severely degraded performance.

Software

The traditional meaning of software was a set of instructions that were or could be translated into the code needed to operate a stored program computer. More recent usage tends to use software as a term for the non-hardware components of a computer system with an additional adjective such as 'operating system' or 'application' used to distinguish the software's function in the system. Software is copyright by default (see open source).

Software failure

A software failure occurs when a software system no longer complies with the specifications that were initially defined for it, which means that it does behave as expected.

Software resilience is the capability of a software system to recover from a software failure.

Specification

A 'specification' communicates one or more system ideas and/or descriptions to an intended audience. A specification is usually a formal, written means for communicating information.

Stakeholder

A stakeholder is any person, group or object, which has some direct or indirect interest in a system.

System

A system is any useful subset of the universe that we choose to specify. It can be conceptual or real. A system can be described fundamentally by a set of attributes. The attributes are of the following types:

- function: 'what' the system does
- performance: 'how good' (quality, resource saving, workload capacity)

- resource: ‘at what cost’ (resource expenditure)
- design: ‘by what means.’
- requirements
- dependencies
- risks
- priorities.

Test

To test is to plan and execute an analytical process on any system, product or process, to understand if the system performs as expected, or not, that is to determine if the requirements are met.

The existence of reliable procedures for testing systems is a "solved" problem. However, the coverage and efficacy of testing is dependent upon the available budget, the risk appetite of the organisation, and the availability of skilled personnel. Hence solved in principle does not mean solved in practice because outside of safety-critical sectors (software-as-a-medical-device, automotive, etc) there is no regulation on levels of testing, and full implementation of testing procedures is costly and time consuming.

Uncertainty

Uncertainty is an expression of doubt about how an impact estimate, or measurement, of an attribute reflects reality. We are ‘uncertain’ as to whether the current or future reality is better or worse with respect to an observed or estimated value of an attribute, and by how much it differs.

Vulnerability

In cybersecurity, a vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. We use the term more widely, to include known weaknesses in operational software.

xG (1G, ---- 5G)

The succession of technical standards defining mobile communication. G stands for Generation. Mobile communication standards began with a predominant focus on voice telephony and each succeeding generation has expanded data communication capability. All of the generations are based upon cellular networks in which handsets or devices communicate using radiofrequency signalling with a ‘base station.’ The ‘base station,’ in turn, is connected to the telephone network and the Internet.

Y2K

Y2K was commonly used to refer to a widespread computer programming shortcut that was expected to cause extensive havoc as the year changed from 1999 to 2000.

7. Appendix 2: Some software failure examples

British Airways

On August 7, 2019, over one hundred British Airways flights were cancelled and near to three hundred flights delayed. During the busiest month for air travel, their computer system went down completely. Thousands of passengers had to stay behind and wait long hours in packed airports. The check-in procedures had to be switched to manual which made the queues start to resemble Dante's "Inferno." This was not the first time the system screwed up. The pattern of software failures over the last couple of years suggests poor computer management and calls for concern. Investors are worked up because the financial risk with such issues is high.

Source: CISQ 2020 Report.

The Post Office Horizon Project – High Court Trial Day 8

"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 transactions. 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."

and

"On the 2nd of March, a transaction for a cash withdrawal was completed where the system commanded a member of staff to issue the money to the customer on screen but the receipt printed for that transaction printed out a decline slip. The customer was honest enough to bring back the decline receipt a day later with the money."

Source: Post Office Trial: The Smoking Gun: or "Whither Gareth?" March 2019

"Between 2000 and 2014, the Post Office prosecuted 736 sub-postmasters and sub-postmistresses - an average of one a week - based on information from the computer system called Horizon.

Some went to prison following convictions for false accounting and theft, many were financially ruined and have described being shunned by their communities. Some have since committed suicide or died."

Source: https://www.bbc.co.uk/news/business-56718036

Useful account: 'The Post Office Horizon Scandal a brief chronology', Digital Evidence and Electronic Signature Law Review, Volume 18, 2021, https://journals.sas.ac.uk/deeslr/article/view/5390

Microsoft Cloud

Microsoft has identified a recent change to an authentication system as a possible cause of an outage that blighted users of its cloud-based portfolio of productivity and back-office apps across the world. User reports of technical difficulties with the software giant's Microsoft 365 online productivity suite first started emerging around 7pm on Monday 15 March 2021.

Microsoft confirmed that users could not access the company's key online collaboration, communication and productivity tools; and that any service that relies on its cloud-based identity and access management service Azure Active Directory (AAD) could be affected. These include Outlook, Word, Excel and PowerPoint, and access to the firm's wider

portfolio of cloud services was also affected by the issues such as the business intelligence software Dynamics 365, and the Microsoft Managed Desktop service.
The company confirmed around 9.17pm that it was rolling out a "mitigation worldwide" to address the issue, with a full "remediation" expected within 60 minutes of its deployment. "Service health has improved across multiple Microsoft 365 services," said a post on the Microsoft 365 Twitter account at 11.19pm. "However, we are taking steps to resolve some isolated residual impact for services that are still experiencing impact."
Source: Microsoft cloud users hit by global outage linked to Azure Active Directory issue (computerweekly.com)

NHSmail Accenture
The NHS email system crashed in December 2018, locking staff out of their accounts as NHS Digital and its supplier, Accenture, scrambled to fix the issue. It suffered a national outage, which meant most staff were unable to access their email accounts across all platforms. NHS Digital said the crash was "caused by a software issue in the supplier's internal infrastructure."
The outage began in the morning and by 5pm, access had been restored for some users. NHS Digital said Accenture had run an "automatic fix," and by 10.30pm, "all users", including those that had been locked out "as a result of multiple login attempts", had seen their access restored.
Source: https://www.computerweekly.com/news/252453812/NHS-email-outage-caused-by-internal-software-issues

O2's 4G network outage
Mobile network operator O2 has blamed a problem with a third-party software installation for a nationwide network outage that has left 32 million subscribers unable to access 4G data services on their smartphones. The problem – which began at around 4.45am on 6 December 2018 – affected operators in a number of other countries besides the UK. The Japan Times has reported that services on the SoftBank network are also down in parts of Japan, with the outage beginning at 1.39pm local time, the same time as O2's.
The issue also hit a number of other organisations that rely on O2's network, including Transport for London (TfL), which reported that its bus information display boards had stopped working at approximately 5am. Similarly, Shropshire Council has reported the same problem with its car park payment machines, which also rely on O2 data connections.
As of 4.00pm on Thursday 6 December, almost 12 hours since the outage began, the third party software issue had been identified as originating at Ericsson. It identified issues in certain nodes on the core network, which led to outages for customers using two specific versions of the Serving GPRS Support Node - Mobility Management Entity (SGSN-MME). The supplier's analysis indicates that the specific problem was an expired certificate in the software installed with customers such as O2 and SoftBank.
Source: Software failure paralyses O2's 4G network (computerweekly.com)

Oxford City Council

A botched platform security system upgrade at one of its data centres led to technical difficulties affecting Oxford City Council's IT and email systems over the weekend of 11/12 December 2021. The local authority was unable to process transactions through the council website because of an infrastructure fault affecting the data centre of its IT services partner, SCC. The council had no access to its IT systems and email platforms.

Just before 9am on Monday 13 December, the council confirmed that normal service had resumed. "Whilst we experienced some issues over the weekend, these have now been fully resolved," a council spokesperson told Computer Weekly.

Source: Oxford City Council services back online after weekend outage at SCC datacentre (computerweekly.com)

Zoom Hacking a mac

Video conferencing software Zoom recently announced a patch for a vulnerability found in versions 5.7.3 to 5.11.3 on Zoom for macOS. The flaw would give hackers the ability to use the Zoom package installer to take over a Mac-based computer.

While the Zoom client usually has well-defined permissions when it comes to accessing vital system files, the auto-update function that runs in the background has far more widespread system privileges. A security tool that checks Zoom update files are legitimate does so by verifying a cryptographic signature from the company.

But Patrick Wardle, founder of macOS security tools creator Objective-See, found that any file that was renamed with the Zoom cryptographic signature would be seen as legitimate by the system. A fault like this allows rogue actors to maliciously use the Zoom system to run files that can cause damage. Wardle spoke about this issue recently at the DEF CON Conference, and in a security bulletin, Zoom said: "The Zoom Client for Meetings for macOS (Standard and for IT Admin) contains a vulnerability in the auto-update process. A local low-privileged user could exploit this vulnerability to escalate their privileges to root."

The first patch Zoom released to address this issue was, according to Wardle, not enough to remove the flaw, with a second fix after the DEF CON Conference fully fixing the problem.

https://www.techerati.com/news-hub/zoom-releases-patch-for-mac-root-access-flaw/

8. Appendix 3: Methodologies for Estimating the Costs of Operational Software Failure

We have not found a peer reviewed academic study that estimates the costs of operational software failure in any area of the world. In the last 20 years there have been several attempts to estimate these costs or a collection of costs that represent a share of these costs. Below we discuss why data on costs is difficult to capture, before briefly describing the basis of three estimates and the resulting estimated costs in £ or $.

Capturing data on costs of operational software failure

While the definition of operational software failure is straightforward as illustrated in the main text, the cost of these failures is conceptually more complex. This is because of the variety of failure types and the different parties that can be affected by these failures.

Regulators have treated failures that lead to unavailability of service differently from those that lead to the loss or corruption of data, see Appendix 5.

We are primarily concerned here with service loss, in which those affected are those that are relying on the service, the users. These users may be internal or external to the organisation making the software available. Putting values on service losses is difficult because in most cases the user bears the cost without a recourse. As noted in the main text, the asymmetry in contracting for software generally absolves the software provider from liability and this lack of financial responsibility is usually extended to the provision of software-based services.

The cost to users, internal or external is, however, only the beginning. The defects responsible for the failure need to be corrected to restore a system's function and to assure that the failure will not recur. The cost of correction can manifest in different ways. It may be that the company providing the software service can task its own employees to finding and fixing the defects responsible for the failure. When a company is using software obtained from another party, that party may or may not be willing to expend the efforts and costs necessary to fix the problem, either urgently or "in the next release." In some cases like open source software which is no longer supported by an active community, it may be difficult and expensive to get the defects fixed: and it is not unusual even for commercial software that the original software producer is no longer taking responsibility for 'legacy' software products. In this case, the costs of failure will entail the procurement of alternative software, its testing and installation, and integration of the new software with other software systems, a task that is becoming more complex as the complexity of enterprise software infrastructures grows.

In short, there are many sources of added cost, both to the company providing software based services and to that company's customers. Few of these costs will appear directly in the ledgers of either supplier or user.

In addition, there are additional more intangible costs of company reputation and customer base that can occur as the result of operational software failure.

In many cases, organisations do not wish to share information on failures of their IT systems. In consumer sectors, some failures are visible through information sharing on social media, whereas in business applications there is often no perceived advantage to either party in making the failure or ensuing costs visible.

RTI/NIST study

The most systematic and directly related effort appears to be one conducted under the direction of Gregory Tassey for the US National Institute of Standards and Technology (NIST) in 2002 by RTI (Research Triangle Institute), an independent consulting company.[57] The study, hereafter called the RTI/NIST study, was based upon a questionnaire survey of firms in the US transport equipment and financial services industries. The aim of the study was to estimate the savings available by making feasible improvements in the software testing infrastructure. To derive this estimate, survey respondents were asked about the incidence and repair costs of 'bugs' (the 2002 term for software faults) as well as the potential cost savings by making feasible improvements in the testing infrastructure.

The conceptual framework of the RTI/NIST study was an attempt to construct a series of counter-factual scenarios in which there were fewer software faults. It was recognised that a fault-free scenario was infeasible. Respondents were queried as to cost reductions possible by less faulty software in the following categories: major failure costs, minor failure costs, purchase decision costs, installation costs, maintenance costs and redundant system costs. While our concern is primarily with the first of these, each cost category is affected by operational software failure. In both sectors, 60% of respondents indicated that they had experienced major failures.

The RTI/NIST study can be interpreted as measuring the costs of software errors with a total estimate of US$59 billion in 2002 (or, adjusting for inflation, $97 billion in 2022). This total is for the entire US economy (excluding the public sector) based upon taking the two sectors as representative of the others and scaling up by number of employees. The RTI/NIST study recognises several limitations. Three are of particular note:

- "Quantifying the impact of inadequate testing on mission critical software was beyond the scope of this report. Mission critical software refers to software where there is extremely high cost to failure, such as loss of life. Including software failures associated with airbags or antilock brakes would increase the national impact estimates."
- "…the costs of software errors and bugs to residential households is not included in the national cost estimates. As the use of computers in residential households to facilitate transactions and provide services and entertainment increases, software bugs and errors will increasingly affect household production and leisure. Whereas these software problems do not directly affect economic metrics such as GDP, they do affect social welfare and continue to limit the adoption of new computer applications."
- In addition, the scaling up process is done based upon calculating the cost consequences per employee of the software 'bugs' in the surveyed firms and then using these costs per employee figures to scale to other service and manufacturing

[57] RTI/NIST, The Economic Impacts of Inadequate Infrastructure for Software Testing, Final Report May 2002 (Prepared for Gregory Tassey by RTI Health, Social, and Economics Research, at Research Triangle Park, NC 27709. Available at

https://lara.epfl.ch/w/_media/misc/rti02economicimpactsinadequateinfrastructuresoftwaretesting.pdf

sectors of the US economy. As the authors of the report note, this involves an important assumption about constancy of costs across sectors.

Much has changed over the past 20 years. The failure of household based software systems now has an effect on GDP. In 2002, the distribution of software-based systems was much more uneven with the finance, insurance and real estate sectors having a much more dominant share of IT systems and investments than other sectors. The method of using total employees for the scaling up is therefore more likely to be appropriate today than it was then.

In summary, a 2002 estimate of US$59 billion (or $97 billion adjusting for inflation to 2022) appears to be a sound estimate for the US economy.

More recent estimates have been made by business consultancy organisations for inclusion in white paper-type reports.

Tricentis and CISQ estimates

One estimate comes from Tricentis, an Austin, Texas based company that provides software testing solutions.[58] As a part of their effort to raise awareness of software quality issues they performed systematic review of English language press accounts of operational software failure (as well as other types of failure) recording a mix of actual losses, repair costs and the size of affected assets to financial costs and aggregating these to make a global estimate.

Tricentis' 2018 report was based upon 606 reported failures affecting 314 companies in 2017 although only 80 of these had an estimate of loss or assets affected.[59] The report estimates that, for 2017, the total global loss and assets affected in the English language press amounted to US$1.72 trillion.[60] This total reflects reporting from the English language press and reveals a limitation of the earlier RTI/NIST report. A few incidents resulted in hundreds of millions of actual losses – these 'outliers' do contribute to real world totals but are likely to be missed by the survey method employed in the RTI/NIST study. The major shortcoming to the Tricentis study is that a preponderant share of the total comes from the 'assets affected' category as these are not properly losses. For example, the software problems with the F-35 fighter jet program are reported to have added $1.7 billion to the cost of the $400 billion programme. The number recorded as part of the above total is $400 billion not $1.8 billion. For this reason, the Tricentis estimate appears to be a substantial over-estimate of directly incurred costs of operational software failure.

[58] The developer of the Tricentis study and author of the software failure reports for 2017 and 2018 Chelsea Frischknecht generously provided the underlying dataset which reveals ambiguities in how costs were measured primarily because of the 'assets affected' category which dominated the reported total.

[59] https://www.tricentis.com/blog/how-to-avoid-the-tricentis-software-fail-watch/

[60] Tricentis, Software Fail Watch 5th Edition, https://www.scribd.com/document/427481278/Software-Fails-Watch. This link is to an online archive Scribd as the Tricentis site no longer carries the report. The link may be a summary of the original report but definitively states the US$1.72 trillion (actually US$1,715,430,778,504) as the loss from software failures.

Despite its informal methodology, the Tricentis report from 2018 has become a basis for a further report from CISQ.[61] At p.12 of CISQ, The Cost of Poor Quality Software in the US: A 2018 Report, the US$1.7 trillion (taken to be a global sum of actual losses) is translated into a US loss of $1.275 trillion on the somewhat dubious basis that 75% of the world's English speakers are Americans.[62] A 2020 CISQ report raises the estimate to $1.56 trillion based on the assumption that the growth has been 22% over the two years (the rate is not further substantiated).

Returning to the Tricentis study, it appears that actual costs might be more in the range of $20 billion for the eighty companies reporting. Taking the average of these losses and attributing the same average for the other 234 companies would suggest a loss of $51 billion.

Using the RTI/NIST inflation adjusted estimate of $97 billion an upper bound and the very approximate $51 billion derived from the Tricentis study as a range we now attempt to translate this into the UK both in size and currency.

Scaling for the UK economy

The US labour force was about 148 million in 2020 while in the same year UK was thirty-three million. So UK employment is 23% of the US. Employing this share to attribute costs of US failure ($51-97 billion in 2020) yields an estimated range of UK costs of US$12-22 billion or £10-18 billion.

In terms of GDP, the 2020 UK was $2.7 trillion or 12.9% of the US GDP in that year of $20.94 trillion. This provides another, lower, estimate of the range of costs of operational software failure as $6.6-12.5 billion or £5.4-10.2 billion.

Estimates of costs of GNSS/GPS failure

A further means to gauge whether these ranges are appropriate is to compare with the estimate of a prolonged GNSS/GPS outage in the UK.

A study of this eventuality was conducted by London Economics for Innovate UK, the UK Space Agency and Royal Institute of Navigation[63]. This study estimates that the related costs of a 5-day disruption would be £5.2 billion. This total is comprised of £1.7 billion in lost GVA (Gross Value Added), which is the principal component of GDP; and £3.5 billion in lost utility benefits (including damages). GNSS/GPS systems use substantial amounts of software and are thus subject to operational software failure. Their services are broadly distributed but by no means universal (88% of the effect occurs in road, emergency and justice services and maritime sectors of the economy). The parts of the economy that are at risk from operational software failure include these sectors, but also finance, insurance, real estate, wholesale and retail

[61] https://www.it-cisq.org/the-cost-of-poor-quality-software-in-the-us-a-2018-report/The-Cost-of-Poor-Quality-Software-in-the-US-2018-Report.pdf

[62] For example, there are 125 million English speakers in India. There are 67 million people in the UK and over 30 million people in Australia and New Zealand (the vast majority of whom are English speakers). The 2021 US population is 331 million.

[63] 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

trade, and the public sector (e.g. DWP (Department of Work and Pensions)) as well as manufacturing and infrastructure (e.g. gas, water, electricity). Hence the range of losses noted above are reasonable extensions of the estimate provided for a 5-day GNSS/GPS outage.

Summary

In summary, as noted throughout, the methods available for estimating the costs of operational software failure are varied. They all indicate a very substantial cost for the US and there is every reason to believe that the costs for the UK are similar.

In this Appendix we have critically considered these estimates and conclude that the current (2022) costs for the UK are likely to be in the range of £8-14 billion pa. **For purposes of discussion, we suggest using £12 billion pa as the estimate.**

This is a conservative estimate, as it largely neglects the opportunity costs imposed on users. it is dominated by the costs incurred directly by the organisations providing software services in their remediation of operational software failure.

9. Appendix 4: Terms of Reference

The Terms of Reference of the Working Group were:

"Preamble to the Terms of Reference

There is clear if anecdotal evidence that our economy is increasingly dependent on software and that software failures are occurring in operational systems, leading to loss of service with a range of consequences from inconvenience to major financial loss. We have not found any systematic effort in the UK to collect case studies of failures leading to economic impact and/or their cost to the economy and/or trends which may increase or decrease frequency or impact.

Purpose

The BCS IT Leaders Forum has set up a Working Group (WG) to:

- In the short term, create a network of people and organisations with an understanding of software risks and their potential impact. It will focus initially on the six infrastructure sectors (energy, transport, water and wastewater (drainage and sewerage), waste, flood risk management and digital communications).
- In the longer term the aim is to work with relevant bodies to provide a framework for action to reduce the impact of software failures on the UK economy.

Responsibilities

To create a network and gather data to provide in 2022

- an event for BCS IT Leaders and outsiders, and think-pieces for relevant channels
- a BCS/ITLF White Paper to communicate about software risks to those without an IT background."

Notes to the Terms of Reference – August 2022

1. This Policy Think Piece is the "BCS/ITLF White Paper" identified above.
2. The ToR suggested a focus on infrastructure because of the effect on a wide part of the economy and society should their services fail. The list of infrastructure sectors is taken from a definition in the National Infrastructure 2nd Baseline Plan[64]. A wider definitions of Infrastructure[65] is provided by the Centre for the Protection of National Infrastructure: the list is Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Operators of Essential Services[66] are subject to the NIS (Network and Information Systems) Regulations 2018: the list is Communications, Energy, Health, Transport and Water. We have refined our scope for Phase 2 to Operators of Essential Services.

[64] https://nic.org.uk/studies-reports/national-infrastructure-assessment/baseline-report/

[65] https://www.cpni.gov.uk/critical-national-infrastructure-0

[66] https://www.itgovernance.co.uk/nis-regulations-oes-operators-essential-services

10. Appendix 5: UK regulatory regime.

The NIS Regulations are the 'Network and Information Systems Regulations 2018' which came into force on 10 May 2018.

'Network and information systems' are any systems that process 'digital data' for operation, use, protection and maintenance purposes. Network and information systems play a vital role in the economy and wider society, and NIS aims to address the threats posed to them from a range of areas, most notably cyber-attacks. NIS requires these systems to have sufficient security to prevent any action that compromises either the data they store, or any related services they provide. Although NIS primarily concerns cybersecurity, it also covers physical and environmental factors.

NIS is regulated by sector-specific 'competent authorities. NIS applies to two groups of organisations: 'operators of essential services' (OES) and 'relevant digital service providers' (RDSPs).

The Information Commissioners Office (ICO) is the 'competent authority' for RDSPs, with a range of powers to enforce NIS, including issuing fines of up to £17 million in the most serious cases.

RDSPs are organisations that provide specific types of digital services: online search engines, online marketplaces and cloud computing services. To be an RDSP, you must provide one or more of these services, have your head office in the UK (or have nominated a UK representative) and be a medium-sized enterprise.

The framework and thresholds for capturing information on service breaches is:

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.

OES are organisations that operate services deemed critical to the economy and wider society. They include Communications, Energy, Health, Transport and Water. NIS is regulated by sector-specific 'competent authorities' for Operators of Essential Services.

The National Cyber Security Centre (NCSC) also has two functions: it is the UK's 'single point of contact' (SPOC), as well as the 'computer security incident response team' (CSIRT).