IT Leaders Forum

IT Failures in Nine Banks

Report from a RoundTable

Held at BCS London on 22nd April 2025

Contents

Report Authors: Gill Ringland, Ed Steinmueller

Table Facilitators: Mark Cook, Olu Odeniyi, Gill Ringland, Steve Sands, Ed Steinmueller.

Insights from Alan Farrell, Sarah Greasley, John Rattray.

May 2025

Summary and Recommendations

BBC's Today Programme on 6th March featured - "Nine major banks and building societies operating in the UK accumulated 803 hours of tech outages in the years 2023 and 2024"[1]. The item was based on data supplied by the banks to the UK Treasury Committee, covering over 150 outages.

The BCS IT Leaders Forum (ITLF) held a RoundTable on 22nd April at the BCS offices, on Lessons from IT failures at Nine Banks. The RoundTable discussed the data supplied by the Banks, and what could reduce the number and impact of IT failures on users, the economy and society. This report and recommendations are based on the discussions at that Round Table.

Key takeaways `

The data supplied by the banks has some clear features:

1. The headline was "accumulated tech outages of 803 hours". If the nine banks were running a single system and it was out for 803 hours over two years, that would be about 95.6% availability. However, there are a multiplicity of services across the nine banks, and if availability of each is averaged out, bank services have an average availability of over 99%.

   Commentary: We should not underestimate the potential impact of outages on customers' life and needs. For instance, outages in payments systems could disrupt house moves. And we should not underestimate the wide spread impact of some outages. which although only a few hours, caused mayhem across multiple industries and geographies.

2. Mobile, online and payments channels saw the most outages (70% in terms of volume and 80% of the hours of outage).

   Commentary: Outages in payments systems - an important business service - can have severe impacts on customers, businesses and banks, e.g. salary payments, house purchases, bill payments, regular payments and high value payments between businesses. Furthermore, Mobile and Online are the most popular way customers interact with their Banks and offer a level of user experience and convenience that when not available

[1] https://www.longfinance.net/news/pamphleteers/banking-system-failures/

aren't easily obtained from the remaining channels and generates negative sentiment about Banks.

3. Approximately half of the outages were due to attempted changes/updates to applications, the other half due to "events" in either applications or infrastructure.

   Commentary: The question was raised – what does good look like? The Round Table identified measures for better anticipation of problems to reduce impact on customers, using data on early warning signs through monitoring system performance. Methods for better management of problems included planned down time to incorporate new software and for testing of upgrades.

4. Fewer than 10 outages were described as possibly cyber related.

   Commentary: One of the three pillars of security is availability. Hence FS and CNI organisations that effectively apply established information and cyber security principles (e.g. secure by design, risk assessment processes, monitoring & observability) should see a reduction in other sources of outage.

5. 3rd party software/systems were the cause of 17% of the outages, mostly in applications and infrastructure.

   Commentary: However, the definition of 3rd party is unclear, and covers a wide variety of approaches. For instance, open-source components are integral to many inhouse applications.

   3rd party as "software (or IaaS or Paas)[2] as a Service is becoming recognised as a source of vulnerability. The period of reporting covers the Crowdstrike outage, which although only a few hours, caused mayhem across multiple industries and geographies. This suggests that sharing data on common software/systems and their vulnerabilities is a high priority; and that the number of people affected as well as outage time is an important metric.

[2] IaaS's host custom-built apps, as well as providing data storage. A PaaS is often built on top of an IaaS platform to reduce the need for system administration. SaaS offers ready-to-use, out-of-the-box solutions for a particular business need: most SaaS are built on IaaS or PaaS platforms.

The lessons could be applicable to other CNI sectors

6. Critical national infrastructure (CNI)[3] is made up of private firms. Other CNI sector firms, like FS firms, are expected to deliver a utility with high availability, and like FS they have a complex mix of software and systems delivering their services.

   Commentary: the regulatory and enforcement regimes vary across CNI sectors. The IT failures could be expected to have similar causes – and remedies – to those in the FS sector as typified by the Nine Banks. In the absence of a strong unified regulatory regime as for FS, there is an emerging "public good" case for developing mechanisms for sharing technical data on causes of IT failures within and across CNI sectors, and for publicising the user impact of outages in all CNI sectors

   At a breakfast discussion 'Preparing for a growing reliance on digital interdependencies' convened by the National Preparedness Commission and held at EY on 5th March[4], Lord Toby Harris posed the question, 'Should government consider creating a National Resilience Technology Authority (NRTA) similar to the NCSC (National Cyber Security Centre), which looks after cyber security?' As a first step such an Authority could serve as a clearinghouse for expertise and as a repository for data on availability and resilience issues: vulnerabilities, causes of outages, user impact.

   So, a possible framework for data sharing could be
   .

   - The NRTA to take on regulatory functions, initially for critical national infrastructure and later for a broader range of enterprises and organizations throughout the UK.
   - Data sharing – vulnerabilities, analysis of outages, user impact.
   - Operational Excellence Group - ways of improving resilience eg change management, large scale testing, predictive problem management, resilience by design, 3rd Party alignment, Important Business Services: sharing of expertise across sectors.
   - Industry Specific Focus – for FS, Payments, Mobile and Online outage reduction and resiliency improvements.

[3] In the UK there 13 Critical National Infrastructure Sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.

[4] https://nationalpreparednesscommission.uk/event-summary/preparing-for-a-growing-reliance-on-digital-interdependencies-event-summary/

Recommendations

BCS ITLF Availability Working Group will seek to establish, or promote any existing, education and training on:

Architecture, DevOps and resilience by design

The incorporation of resilience methodologies into Architecture, DevOps, and into the incorporation of these into operational systems.

Problem anticipation and Response

ITIL covers Problem and Incident Management. Training and education additionally on problem anticipation in these complex CNI systems, in order to inform preventive maintenance.

Testing in a 24/7 operation

Theory and practice for testing in a 7/24 operations environment where interdependencies of sub-systems, data flows and external events and upgrades will challenge operational systems.

BCS ITLF with support from RoundTable participants should explore how to increase sharing of data eg

3rd party supplier characteristics

Sharing information on 3rd parties is of increasing importance for resilience.

Industry codification

Avenues for piloting the use of the Common Vulnerability Scoring System for codifying technical threats, within FS and other CNI.

Metrics for user impact

Publicise information on the development and use of metrics for user impact.

FS sector

How best to add value to existing structures and networks eg the joint Bank of England/UK Finance's Cross Market Operational Resilience Group (CMORG).

Other CNI

How best to add value to existing structures and networks eg The National Cyber Security Centre.

Background

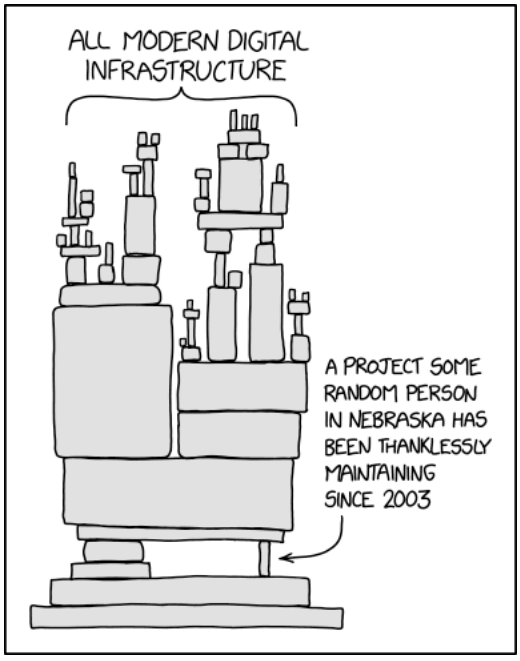
The BCS's IT Leaders Forum (ITLF) has over 4,000 members globally. It set up the Working Group on Service Resilience in 2022 with Terms of Reference: "*work with relevant bodies to provide a framework for action to reduce the impact of software failures on the UK economy*"[5].

Over 2022 to 2025 the Working Group has collaborated with organisations such as the National Preparedness Commission[6], Business Continuity Institute[7], Institute of Directors[8], Long Finance[9], to develop this framework[10], and published a book outlining the principles [11].

The landscape for delivery of digital (software) systems

Some aspects of the landscape within which customers rely on digital systems:

- IT is now a utility – users expect 7/24 availability
- Software is inherently fallible: it fails
- Software has a long life, and most new software is 3rd party
- IT failures have significant impacts on GDP and productivity



As many systems delivering services are complex and tightly coupled, new approaches to resilience are needed to "keep the lights on". Further, the increasing use of 3rd party software and services requires new skills to specify and manage supplier contracts.

[5] https://www.bcs.org/media/9679/itlf-software-risk-resilience.pdf
[6] https://nationalpreparednesscommission.uk/wp-content/uploads/2022/12/NPC_BCS_Software-Risk_-the-Elephant-in-the-Room_Dec-2022-Upload.pdf
[7] https://www.bcs.org/media/11134/itlf-service-resilience.pdf
[8] https://www.iod.com/resources/science-innovation-and-tech/board-directors-the-growing-risk-of-it-failures-and-how-to-be-accountable/
[9] https://www.longfinance.net/news/pamphleteers/banking-system-failures/
[10] https://www.bcs.org/media/3j1n1mhc/service-resilience-and-software-risk-2023.pdf
[11] https://londonpublishingpartnership.co.uk/books/resilience-of-services-reducing-the-impact-of-it-failures/

Approaches to reducing the impact of software failures on the UK economy

Earlier work informed the topics for discussion about the Nine Banks data, at the RoundTable.

Measurement and sharing of data on outages: codification

An existing framework for user impact is defined in NIS2[12], which measures availability in lost user hours.

The data reported to the Treasury Committee highlighted ambiguities in describing causes of outages.

Applying resilience by design to operational systems:

Ongoing maintenance of systems can introduce techniques such as compartmentalisation to limit the spread of outages, alternative processes to deliver user services (redundancy), or better recovery processes.

Problem management

Problem management– eg forensic incident and failure analysis after an outage – is often hindered by a "blame" culture. This can be reduced if effective problem anticipation systems are in place, eg the monitoring of system characteristics for early warnings.

Introducing changes - testing

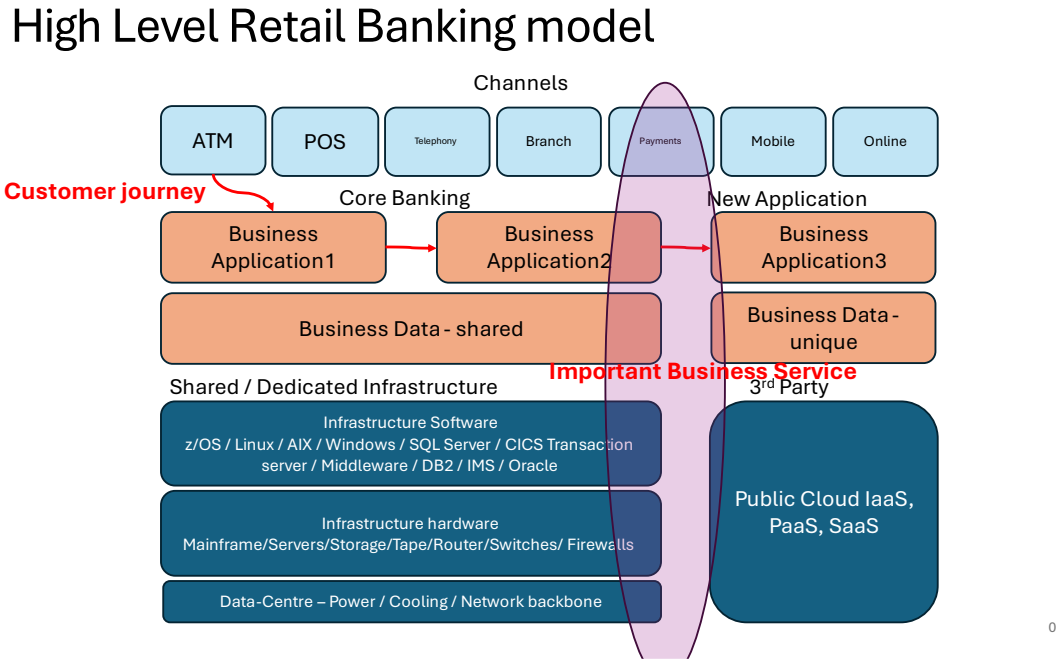
Many systems operate 24/7. But changes introduced into live systems are a well-known source of outages. Testing potential changes can for instance use "canary" systems, where failures are less important to the organisation.

[12] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Why the Nine Banks data is important

FS organisations in the UK are intensive users of digital systems and the nine banks reporting data all provide services through a complex collection of systems. Some are 50 years old; others are recently bought in from 3rd parties. The sector is stringently regulated and known for best practice.

This installed base is likely to be similar to other suppliers of Critical National Infrastructure (CNI) and so lessons learnt from analysis of the Nine Banks data may be useful in CNI sectors.



The analysis of the data looked at

- Which channels had most outages?
- Which type of software was involved[13]?
- What was the role of 3rd Party software/systems?
- What was the availability – where are potential areas of improvement?

[13] IaaS hosts custom-built apps, as well as providing a general data center for data storage. PaaS is most often built on top of an IaaS platform. SaaS offers ready-to-use, out-of-the-box solutions that meet a particular business need (such as a website or email).

Analysis of the data, and what can be done?

Which channels had most outages?

Mobile, online and payments channels saw the most outages (70% in terms of number and 80% of the hours of outage).

Commentary: Outages in payments systems - an important business service, can have severe impacts on customers, businesses and banks, e.g. salary payments, house purchases, bill payments, regular payments and high value payments between businesses. Furthermore, Mobile and Online are the most popular way customers interact with their Banks. These channels offer a level of user experience and convenience that aren't easily obtained from the remaining channels if they are down. Outages generate negative public sentiment about Banks.

What can be done?

- Organisations should focus on Important Business Services eg Payments, as having greatest customer impact. Some of the mechanisms for underpinning the resilience of service delivery are described in Resilience of Services[14] and were discussed in the RoundTable as described in the next section.
- Organisations are not required by the regulator to specify their Important Business Services, which introduce hurdles into sharing of data on common causes of outages across organisations.
- For channels such as mobile or online, customers – government, business or private customers – who require "100%" availability need to make arrangements for routes to service delivery without common software/systems. The difficulty of achieving this is highlighted by the widespread impact of 3rd part software as in the Crowdstrike outage[15].

[14] https://londonpublishingpartnership.co.uk/books/resilience-of-services-reducing-the-impact-of-it-failures/

[15] https://www.bbc.co.uk/news/articles/cr54m92ermgo

Which type of software was involved, what were the causes?

Approximately half of the outages were due to attempted changes/updates to applications, the other half due to "events" in applications or infrastructure.

Commentary: Approximately 50% of the outage impacts were driven by change activity as a root cause driver, with the remainder due to an 'event' impacting the application or infrastructure environments.

What can be done?

The question was raised – what does good look like? The focus was improving the service perceived by customers. The disruption of outages due to changes could be reduced through planned "maintenance" outages. The disruption of "events" could be reduced through better anticipation and preventive maintenance to avoid problems.

Outages due to attempted changes:

- Training and education are needed on theory and practice for testing in a 7/24 operations environment where interdependencies of sub-systems, data flows and external events and upgrades will challenge operational systems.
- Batching upgrades and planning outages for testing and installing new software and systems could improve customer perception through increased predictability.
- New technology such as AI and 'Digital Twins' be investigated to overcome the conditions of testing at scale and volume. However, AI adds an additional layer of complexity, with additional threat (in terms of complexity) as well as opportunity (eg process knowledge for rarely used recovery processes)
- The RoundTable saw the need to learn and share best practice around Change, especially when Banks utilise heterogeneous systems at scale for their customer channels.

Outages due to "events":

- Training and education are needed on theory and practice of "problem anticipation", covering greater use of data around observability and predictability across these complex systems.
- The RoundTable swathe need to insert Problem Anticipation into the ITIL Framework which covers Problem Management (analysis after the event) and Incident Management (recovery processes).

What was the role of 3rd Party software/systems?

3rd party software/systems were the cause of 17% of the outages, mostly in applications and infrastructure.

Commentary: The definition of 3rd party is unclear, and covers a wide variety of approaches. For instance, open-source components are integral to many inhouse applications. 3rd party as "software (or IaaS or Paas) as a Service is becoming recognised as a source of vulnerability (see below). However, the report period included the infamous Crowdstrike outage, which Microsoft estimated directly affected approximately 8.5 million Windows devices[16] and disrupted organisations from airlines to hospitals. 3rd party software/systems are emerging as sources of failure across apparently diverse systems.

What can be done?

The European Central Bank provides an annual outsourcing analysis[17] which shows increasing dependence on 3rd Party suppliers for critical services in European Banks.

An open letter to third-party suppliers from Patrick Opet, Chief Information Security Officer of JP Morgan reads in part[18]:
"The modern 'software as a service' (SaaS) delivery model is quietly enabling cyber attackers and – as its adoption grows – is creating a substantial vulnerability that is weakening the global economic system.

- Software providers must prioritize security over rushing features.
- Comprehensive security should be built in or enabled by default.
- We must modernize security architecture to optimize SaaS integration and minimize risk.
- Security practitioners must work collaboratively to prevent the abuse of interconnected systems.
- There is a growing risk in our software supply chain and we need your action."

Data sharing on common causes of failures within the FS/CNI ecosystems would help to focus on the challenges and the opportunities of 3rd party software.

[16] https://www.bbc.co.uk/news/articles/cr54m92ermgo
[17] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.outsourcing_horizontal_analysis_202502~c54626829c.en.pdf
[18] https://www.jpmorgan.com/technology/technology-blog/open-letter-to-our-suppliers

What was the availability – where were potential areas of improvement for FS?

Commentary: The headline was "accumulated tech outages of 803 hours". If the nine banks were running a single system and it was out for 803 hours over two years, that would be about 95.6% availability. However, there are a multiplicity of services across the nine banks, and if availability of each is averaged out, bank services have an average availability of over 99%.

It was also noticeable that fewer than 10 outages were described as possibly cyber related, each with short outage durations.

What can be done?

Given the high % availability already achieved, improvements might not appear significant in % terms, even if they improve customer satisfaction. So, it was suggested that potential areas of improvement included:

- Focus on Important Business Services eg Payments, as having greatest customer impact.
- Outages due to introduction of change, eg software upgrades, new applications: batching upgrades and planning outages for test and installing new software and systems could improve customer perception.
- Ongoing attention to preventive maintenance of operational systems, understanding their complexity: use of AI for data analysis and early warnings.
- Training and education on "Design for Resilience" and use of those approaches in both the DevOps environment and in manging change and fixes in the operational environment after events. The approaches include compartmentalisation to localise the impact of failures, enhanced validation of data at application interfaces, definition and testing of recovery points.

Implications for other CNI sectors

CNI sectors have a multiplicity of regulatory regimes. The RoundTable asked if the analysis of the data from the Nine Banks could be useful to firms and public sector organisations in other CNI sectors, and how this might be introduced into their agenda. Cyber incidents across the total critical national infrastructure are reported to a central body. Could this be applied to outages due to digital failures more widely?

Data sharing – the issues and proposals

This important topic underlies many of the discussions and so the rationale and hurdles are collected here.

Sharing data on causes of service failure relating to digital systems

Rationale

Many organisations face similar challenges in delivering services based on digital systems. By pooling data, they can improve overall system reliability. Collecting and analysing data on causes of system outages can significantly enhance the ability to foresee and mitigate potential issues. This proactive approach allows for timely interventions, reducing the risk of outages.

Hurdles

In the past, it has been considered that competition and confidentiality concerns will preclude sharing of causes of outages between private firms. It is believed that this applies for instance to the visibility of the definition of Important Business Services within the UK regulatory regime. As the economy becomes even more dependent on CNI, the public good concern is becoming stronger[19].

The discussion in the RoundTable explored the reasons that the ITIL processes for Problem management were underused compared with those for Incident Management. A significant reason identified was that “problems” were those failures not caused by external forces such as cyber-attacks, and so those responsible for software or systems commonly tried to avoid blame.

Ongoing monitoring of system performance indicators to anticipate problems requires focussed attention – and budget- and may be difficult to get up, running and effectively used.

The analysis of the data from the Nine Banks has underscored the need for a framework and common terminology for describing parts of complex systems as a root cause of a system failure. However, the brownfield nature of the banks application ecosystems means that many of the challenges we have today stem from layers of change on older less well-architected systems, unique to each major bank.

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

What frameworks are available?

It was proposed that CVSS (Common Vulnerability Scoring System)[20] scores could be a starting point for codifying (and reporting) information about technical issues. This framework and its scoring system was developed for cyber defence purposes.

It can identify resilience vulnerabilities more widely, since higher level scores are likely to reflect 'common elements' shared across applications, systems, and organisations. While applications are likely to differ significantly between organisations, so reducing the value of attempting to identify common elements, this is not the case for system architectures where common elements are often linked to root causes and affect more than one organisation. And it was observed that shared 3rd party suppliers were a likely origin for 'common elements.'

What can be done?

Outages are increasingly visible due to services like 'Down Detector'[21] so it becomes less easy for organisations to keep information about them private. This could encourage sharing of information about the root causes as this may prove of some benefit to them if others also share information.

The RoundTable proposed that we liaise with the CMORG[22] (Cross Market Operational Resilience Group, a joint initiative of the Bank of England and UK Finance) to discuss next steps on data sharing by the BCS ITLF in relation to Financial Services.

There are multiple regulators covering CNI sectors. Some issues are likely to cross over or fall between regulatory remits. This may point to the need for a common agency concerned with resilience as a UK PLC issue much as we have a cyber defence coordinator in the NCSC (National Cyber Security Centre). CISP[23] is a platform for cyber security professionals in the UK to collaborate on cyber threat information in a secure and confidential environment. It is managed by the NCSC and membership is free.

The RoundTable proposed that we liaise with the NCSC[24] to discuss next steps by the BCS ITLF on data sharing across CNI sectors.

---

[20] https://nvd.nist.gov/vuln-metrics/cvss
[21] https://downdetector.co.uk/
[22] https://www.cmorg.org.uk/
[23] https://www.ncsc.gov.uk/cisp/home
[24] https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/resilience/engaging-and-supporting-sectors

Sharing data on user impacts of failure

Rationale

Outages are increasingly visible due to services like 'Down Detector'[25]. As the economic and societal effect of IT outages increases, they become of interest to Policy Makers.

Hurdles

Taking a customer perspective on the impact of outages will require developing new ways to codify them, that distinguish between inconvenience and harm/loss. For instance, in a time critical application the impact of a lost user hour could run to £millions, whereas if an ecommerce application is down for an hour, many potential customers can log in later.

What frameworks are available?

The NIS2 guidelines[26] include a definition of Availability in terms of "lost user hours". However, the economic and societal cost of a lost user hour can vary by orders of magnitude, as above. This could be handled through coding on a scale – eg 1 to 10 – with annual reporting and sharing of high score items required by the regulator.

A useful step in FS could be characterising different customer groups – e.g. CHAPS[27] (a high-value sterling payment system) customers are affected differently than BACS[28] (Bankers' Automated Clearing System) customers; and customers attempting to use POS (Point of Sale) payment are affected by outages differently than those making online payments.

What can be done?

DORA pillar 5[29] seeks to raise operational resilience awareness and increase the sharing of practices/lessons learned throughout the FS sector. Organisations must share information securely to increase collaboration and resiliency among financial institutions. The approach for Cyber is for one body reporting centrally for incidents across the total critical national infrastructure. Could this be applied to outages due to digital failures more widely?

[25] https://downdetector.co.uk/
[26] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[27] https://www.bankofengland.co.uk/payment-and-settlement/chaps
[28] https://www.bacs.co.uk/
[29] https://www.grantthornton.ie/insights/factsheets/digital-operational-resilience-act-dora-regulation-summary/

Conclusions

- The publication of the Nine Banks data represents an invaluable opportunity to learn lessons on the behaviour of complex well managed IT systems and the effect of outages on customers. It has highlighted the benefits of data sharing to improve the availability of CNI systems and the need for technical education and training in new skills to manage this environment.
- BCS is the Institute of IT professionals, and we bring our IT expertise to play across all sectors.
- Lack of visibility of the definition of Important Business Services in FS firms limits the ability to anticipate vulnerabilities caused by common use of 3rd party software/systems.
- 3rd party software and systems were seen as an increasing potential cause of failures across the whole FS infrastructure.
- Education and training in three areas were highlighted, but it was noted that delivery channels for such was not clear. The areas were
    a. Architecture and DevOps – adding resilience features
    b. Problem anticipation – an addition to the ITIL framework
    c. Testing in a 24/7 operation
- Sharing of data and expertise/best practice in introducing change – beyond the ITIL definitions – would improve availability.
- Sharing of thinking and investigation around Problem Anticipation – greater use of data around observability and predictability, and the use of new technology such as AI and 'Digital Twins' should be investigated to overcome the conditions of testing at scale and volume.
- Sharing of data requires a common set of terms: we identified
    a. CVSS (Common Vulnerability Scoring System)[30]
    b. NIS2 (focused on the cyber security of networked and information systems) [31]
- In FS in the UK there are existing structures for sharing of data on outages (eg CMORG[32]): we should explore how best to provide added value.
- In CNI in the UK there is a central body for reporting and sharing data on cyber incidents[33] (NCSC): we should explore how reporting of other types of IT failure and outage could be added to this structure.

[30] https://nvd.nist.gov/vuln-metrics/cvss
[31] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[32] https://www.cmorg.org.uk/
[33] https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/resilience/engaging-and-supporting-sectors

Appendix 1: Participants

Ali	Shehzad
Amafonye	Richard
Brooks	Dave
Brown	Jeremy
Bryans	Toby
Carter	Eric
Cavanagh	Paul
Chakraborty	Seb
Chowdhury	Arif
Cook	Mark
Crooymans	Michael
Downing	Terry
Excell	Paul
Farrell	Alan
Ford	Adrian
Francis	Gary
Graham	Andy
Greasley	Sarah
Hitch	Esther
King	Vince
Lowrie	Heather
McElwaine-Johnn	Peter
McNeil	Billy
Merrett	Jon
Moattari	Andy
Odeniyi	Olu
Okanlawon	Gabriel
Panchanathan	Vidya S.
Parmar	Rashik
Perriam	Susan
Rattray	John
Rehal	Daljit
Ringland	Gill
Sands	Steve
Scott	Wayne
Steinmueller	Ed
Shkurti	Ardita
Tear	Fred
Wolton	Edward