ITLF Availability/Service Resilience Paper 13

Availability: The impact of Third Party software and services on Resilience

Summary

The BCS ITLF Availability Working Group[1] is focussed on articulating methods for improving resilience within existing operational systems.

Relying on third party software and service providers has become essential in IT operations, so that the resilience of an organisation's services to users is now deeply intertwined with the resilience of the third parties in their supply chain.

This paper is focussed on the implications for operational resilience of third party software and services. These include open-source software, Commercial Off The Shelf Software (COTS), software (or IaaS or Paas) as a Service[2], and Cloud services. The proliferation of third party software and services gives extra impetus to the need for information sharing among user organisations[3].

The report to Parliament on IT failures at Nine Banks[4] showed 17% of incidents attributed to third party software and services[5]: it was not possible to determine whether third party software was also involved in other failures. Moreover, vulnerabilities and failures due to third party software and services can have a disproportional impact on the availability and resilience of systems[6] as their use by multiple banks or businesses within an industry can affect a very large numbers of users.

[1] In this text and others in the series of ITLF Availability Papers, "we" refers to the Availability/Service Resilience Working Group of the IT Leaders Forum of the BCS – the Chartered Institute for IT and co-opted colleagues who have provided additional insight.

[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.

[3] See for instance "Availability: Information Sharing in https://www.bcs.org/membership-and-registrations/member-communities/bcs-it-leaders-forum/papers/

[4] https://committees.parliament.uk/committee/158/treasury-committee/news/205611/more-than-one-months-worth-of-it-failures-at-major-banks-and-building-societies-in-the-last-two-years/

[5] https://www.bcs.org/media/rxdmjr5h/availability-6-report-nine-banks-data-roundtable-220425.pdf

[6] For instance, Crowdstrike: https://www.bbc.co.uk/news/articles/cr54m92ermgo

Implications of Third Party software and services for resilience

The implications on resilience of having third party services, products, software in your ecosystem can be categorised as follows:

- Increased Impact of Disruption spanning multiple organisations within an industry sector: The increased use of third party software and services failures means that operational incidents are likely to affect services from multiple organisations.

- Operational Resilience Dependency: The ability to recover from disruption is directly linked to the robustness of third-party systems and their own continuity planning. If a critical supplier lacks strong resilience measures, the risk of extended downtime increases.

- Supply Chain Complexity: the interconnectedness of supply chains means that a vulnerability or failure in one third party can cascade through the supply chain, potentially causing widespread disruption. This is especially relevant with complex software dependencies and cloud services.

- Challenges in Assurance and Oversight: gaining assurance about the resilience of large, critical third parties (such as cloud providers) is challenging, particularly for smaller firms trying to assess the practices of multinational vendors. Regulatory frameworks now require ongoing monitoring and due diligence, but implementation and enforcement are often limited.

- Regulatory and Compliance Pressures: regulations like the EU's Digital Operational Resilience Act (DORA[7]) and guidelines from financial authorities[8] require organizations to continuously monitor third-party risk and ensure suppliers meet resilience standards. Non-compliance can result in legal and reputational consequences.

[7] https://www.grantthornton.ie/insights/factsheets/digital-operational-resilience-act-dora-regulation-summary/

[8] https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-sop

- Need for Proactive Management: Organizations must assume that third-party outages will happen and plan accordingly. This includes mapping critical dependencies, developing Business Continuity and contingency plans, and regularly testing these plans.

- Continuous Monitoring and Automation: Whilst many software as a service providers will deliver this, there is still a requirement to ensure that the incident detection and management processes include the third party systems and service providers. Best practice is to use automated platforms for continuous assessment and monitoring of third-party resilience, including cyber, business, reputational, and financial risks. Manual processes are often too slow and complex for effective risk management: a promising area for AI based tools.

Specific implications of Open-Source Software for Resilience

Open-source software[9] (OSS) is foundational in today's operational systems, included in everything from infrastructure to consumer applications. It brings advantages such as transparency, flexibility and independence but brings challenges with respect to maintenance, longevity, resource constraints and integration into organisational processes. Its impact on resilience is very nuanced, offering unique strengths while introducing specific risks, in addition to those outlined above.

Strengths: How Open-Source Software Enhances Resilience

- Community-Driven Development: A diverse, global community can rapidly identify and fix bugs, respond to vulnerabilities, and continuously improve software. This distributed collaboration fosters adaptability and operational resilience, as projects are less dependent on any single entity or geography.

- Transparency and Verifiability: Open code allows anyone to inspect, audit, and improve security, making it easier to spot and remediate vulnerabilities. This transparency builds trust and can accelerate responses to incidents.

[9] https://opensource.com/resources/what-open-source

- Adaptability and Flexibility: Organizations can modify open source to suit their specific needs, supporting rapid adaptation to new threats or requirement. This flexibility is a key factor in long-term resilience.
- Independence and Sustainability: OSS reduces reliance on single vendors and proprietary lock-in, allowing organizations to maintain and evolve software even if the original maintainers depart or a company ceases operations.

Risks: Challenges to Resilience from Open-Source Software

- Maintenance and Resource Constraints: Many OSS projects rely on a small number of maintainers, making them vulnerable to burnout or loss of key contributors. If critical maintainers leave, it can trigger cascading failures across dependent systems[6].
- Supply Chain and Dependency Risks: Modern software often incorporates numerous open-source components. A vulnerability or disruption in a single widely used library can have far-reaching effects, and therefore the complexity and interconnectedness of open-source software dependencies amplify systemic risk.
- Variable Support and Longevity: Unlike commercial software, open-source projects may become unmaintained or "die quietly," leaving organizations exposed if they depend on outdated or unsupported code. This can become a significant issue if a security vulnerability is detected.
- Security and Social Engineering: publicly developed OSS can be targeted by social engineering or malicious contributions.
- Operational Resilience Challenges: OSS projects may lack formal processes for incident response, documentation, or handover, making them more susceptible to disruptions due to lack of contributor availability or changes in project leadership.

Recommendations for managing the implications on resilience of third party and/or open-source software

Risk, compliance and contractual checklist

- Identify and map critical third-party dependencies, using for instance a Software Bill of Materials (SBOM)[10].
- Establish clear Service Level Agreements (SLAs)[11] and disaster recovery plans with vendors.
- Continuously monitor third-party performance and risk profiles.
- Conduct regular security audits and resilience assessments of third parties.
- Benchmark vendors against industry standards and regulatory requirements.
- Collaborate with regulators, industry peers and user groups to share information[12] and address systemic risks.

BCS/ITLF should promote education and training around this checklist.

The organisational, process and management perspective

Providers of software products and services should make explicit their approach to problem management, service management[13] and collaboration on incident determination and resolution[14].

BCS/ ITLF should collaborate with CIO-Net on routes to developing education and training on the impact of third part supply on resilience of services to users.

[10] https://www.cisa.gov/sbom
[11] https://www.cio.com/article/274740/outsourcing-sla-definitions-and-solutions.html
[12] See Availability: Information Sharing in https://www.bcs.org/membership-and-registrations/member-communities/bcs-it-leaders-forum/papers/
[13] See Availability: ITIL vs ISO in https://www.bcs.org/membership-and-registrations/member-communities/bcs-it-leaders-forum/papers/
[14] As [9]