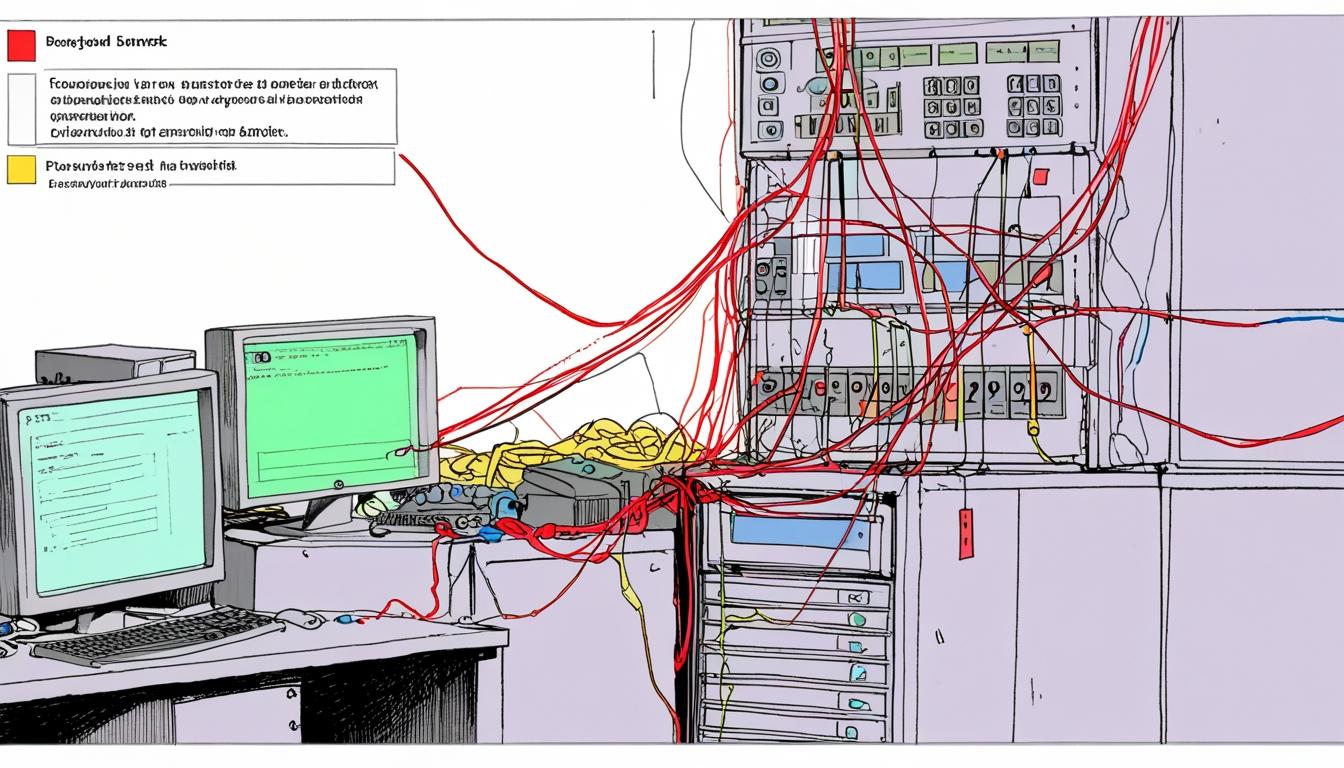
# Barclays and UK banks face rising costs and risks from legacy IT failures amid digital transition



Earlier this year, Barclays faced significant operational issues as a result of a three-day outage caused by a mainframe failure, leaving millions of customers in the UK unable to access basic banking services. This incident not only compromised the bank’s reputation but also resulted in a potential compensation bill estimated at £7.5 million. Such events have raised concerns, as similar incidents in the financial services sector appear to be increasingly prevalent.

Despite substantial investments in advanced security technologies and efforts to assure customers and regulators of their resilience, banks remain susceptible to various disruptions. A significant factor contributing to this vulnerability is the complexity of their software ecosystems and the complicated supply chains that support them. Data from the House of Commons Treasury Select Committee indicates that Barclays experienced 33 system failures between January 2023 and February 2025, while HSBC and Santander reported 32 outages in the same timeframe.

Moreover, the banking sector is not only grappling with system outages; operational errors have also surfaced. For instance, a notable case involved Citigroup mistakenly crediting a client’s account with $81 trillion due to a data entry error in a backup system designed with a complicated user interface, when the intended transfer amount was only $280.

"These applications run on highly distributed cloud infrastructures, draw data from multiple stores, and rely on the support of a variety of third-party vendors," explained Alois Reitbauer, Chief Technology Strategist at Dynatrace, highlighting the intricate environments banks operate in. He added that even minor miscalculations in this complex framework can cause widespread service disruptions.

As financial institutions push to modernise their operations—shifting to cloud platforms and adopting emerging technologies like artificial intelligence (AI) and quantum computing—they often encounter what is termed “technical debt.” This refers to the escalating costs associated with maintaining and building upon outdated code, which has been identified as a core contributor to lapses in service quality. Justin Kuruvilla, Chief Cyber Security Strategist at Risk Ledger, noted that recent errors at Barclays and Citigroup are likely linked to legacy IT systems developed during earlier, less advanced development cycles.

Alicja Cade, Director of the Office of the Chief Information Security Officer for Google Cloud, echoed this sentiment, pointing out the operational fragility stemming from legacy technologies and obsolete processes. She remarked that insufficient testing in new contexts can exacerbate these risks.

A survey conducted by 10x Banking in 2024 of 200 IT decision-makers revealed that 53% of respondents identified data silos and production bottlenecks as significant hurdles to scaling legacy systems. Furthermore, addressing technical debt not only promises to improve the security of IT systems but is also essential for countering increasing cyber threats from both state-sponsored actors and criminal enterprises.

However, upgrading systems and conducting comprehensive testing presents challenges for banks, as such changes can be disruptive and costly. The growing demand for modern user experiences in financial services—where consumers expect convenience comparable to that of platforms like Instagram or PayPal—places additional pressure on banks to rapidly scale their application development and IT operations.

Joshua McKenty, Chief Executive and Co-founder of Polyguard, highlighted the challenges banks face in balancing innovation with security, noting the expectation for “new features, faster, and for everyone” amidst increasingly intricate financial operations.

In response, banks are increasingly outsourcing their IT functions to cloud service providers. Advocates of this approach argue that it can enhance security through automated updates and real-time global monitoring. Nevertheless, sceptics warn that this strategy centralises data, potentially heightening exposure to risks.

Jayant Dave, Chief Information Security Officer for Check Point Software Technologies in Asia Pacific and Japan, noted that the complexities of hybrid architectures comprising various systems and platforms create additional layers of risk. Julien Richard, Vice-President of Information Security at Lastwall, stressed the importance of effective processes for managing third-party vendors to mitigate these risks continuously.

In light of the increasing operational risks, experts emphasise the necessity of maintaining strong security measures. John Shier, Field Chief Information Security Officer at Sophos, advocated for better controls to prevent both malicious acts and inadvertent errors, suggesting that overlapping protective measures could mitigate the impact of potential failures.

With the advent of AI, some experts propose leveraging automation to enhance the modernisation of technology stacks and workflows, thereby minimising the potential for human error. Reitbauer recommended that banks transition from reactive to proactive strategies, employing AI to predict and prevent IT incidents.

However, the rapid integration of AI into critical banking operations introduces new challenges and vulnerabilities, as pointed out by Cade. Financial services, being attractive targets for cyber attackers, must navigate the risks associated with poorly secured AI applications.

Lastly, as discussions surrounding heightened deregulation gain momentum, experts suggest that financial institutions should reflect on the instabilities witnessed in the less regulated cryptocurrency sector. Richard encapsulated the prevailing sentiment by stating that reinforcing fundamental security principles—comprising robust policies, clear processes, and informed personnel—is crucial for minimising risk in these evolving landscapes.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.ft.com/content/52cfc63b-2d14-48b7-b5a9-42879c74cd4b> - This article reports on Barclays' three-day IT outage in January 2025, which affected millions of UK customers and led to compensation payouts of up to £7.5 million.
2. <https://www.ft.com/content/86d7b252-be88-4ddc-a803-f9a94995e158> - This piece details Citigroup's $81 trillion transaction error, highlighting operational issues within the bank's systems.
3. <https://www.ft.com/content/c148d46f-8c6f-487e-b8d7-8e7b9eddc324> - This article discusses the increasing vulnerability of banks to service disruptions due to complex, legacy technology systems, citing Barclays' recent outage as an example.
4. <https://www.theguardian.com/business/2025/feb/28/citigroup-credited-client-account-with-81tn-before-error-spotted> - This report covers Citigroup's $81 trillion crediting error, emphasizing the operational challenges faced by the bank.
5. <https://www.the-independent.com/business/barclays-app-website-customers-outages-compensation-b2709965.html> - This article provides details on Barclays' IT outage, including the compensation plans and the impact on customers.
6. <https://www.fintechfutures.com/2025/03/barclays-set-to-pay-out-millions-in-customer-compensation-after-it-outage/> - This piece discusses Barclays' compensation plans following a significant IT outage, highlighting the bank's response to the incident.
7. <https://www.ft.com/content/c148d46f-8c6f-487e-b8d7-8e7b9eddc324> - Please view link - unable to able to access data