responsiv

IT Challenges and Priorities in UK Financial Services

PREPARED BY

Zoe Whyte

Introduction

This report presents some of the findings from research conducted and analysed by Responsiv.

The purpose of the research was to identify the challenges and priorities currently faced by Financial Services in the UK, exploring factors such as regulation, changes to technological innovation, and the increasing risks from cyber threats.

The survey interviewed 200 individuals working in Investment Banking, Retail Banking, Mutual Societies, and Insurance, in IT and C-Suite roles.

Reference to external reports including *IBM Cost of a Data Breach 2024*, *Flexera IT Priorities Report 2025*, and *Flexera State of Tech Spend 2023* provides further analysis of and context to the research responses.

The Audience

This section outlines the characteristics of research respondents, including the sector, people, and their strategic intentions.

200 individuals across the UK responded to the survey, having met the desired criteria.

This includes working in an IT or C-Suite role, being a sole or participant decision-maker, and working within Investment Banking, Retail Banking, Mutual Societies, or Insurance.

Company size and revenue is evenly spread to provide a representative sample.

The audience was screened based on their area of strategic influence.

For example, developing and updating software strategies, managing technology adoption across the organisation, managing workload migration to cloud, and maintaining software and middleware support contracts.

Whilst the overall sample size is 200, some graphs may represent more or less than this total due to multiple choice responses and questions targeting specific groups. Some graphs may also appear as over 100% due to combining group breakdowns.

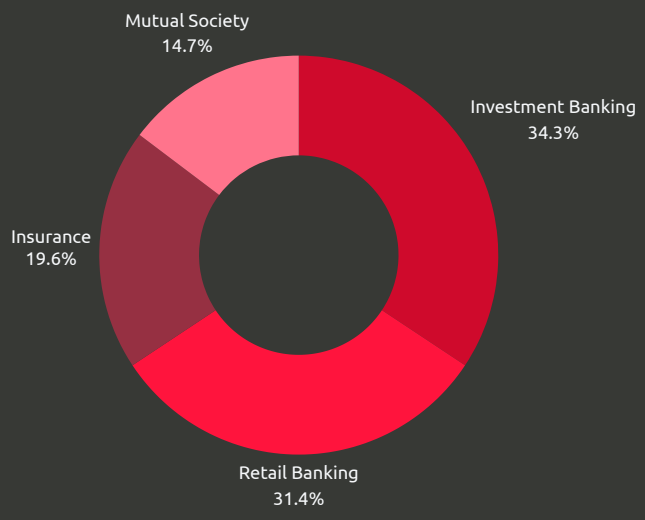


Figure 1: Respondent sectors within UK Financial Services

Audience

Company

Employees

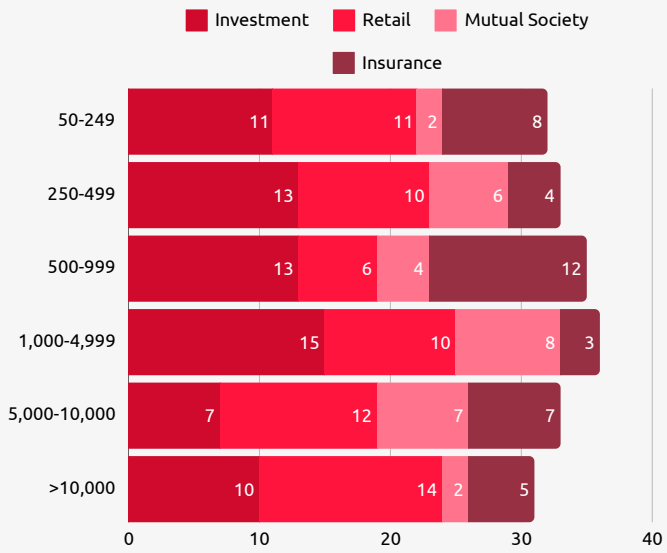


Figure 2: Sector breakdown: company size by employees (actual)

Figure 2 shows companies grouped by employee size. Each segment representing approximately 16% of the sample.

Flexera find that companies with 2,000-5,000 employees spend 12% of revenue on IT compared with 5,000-10,000 spending 13% and >10,000 spending 11%.

Revenue

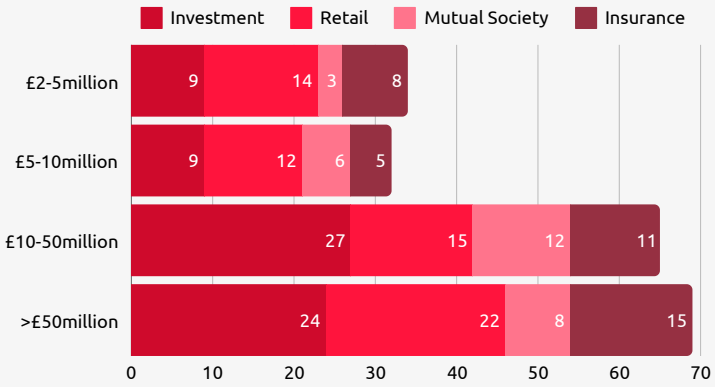


Figure 3: Sector breakdown: company size by annual revenue (actual)

European organisations spend 10% of annual revenue on IT.

The focus on organisations with annual revenue over £10million provides insight into organisations with an IT budget over £1million.

Audience

Who

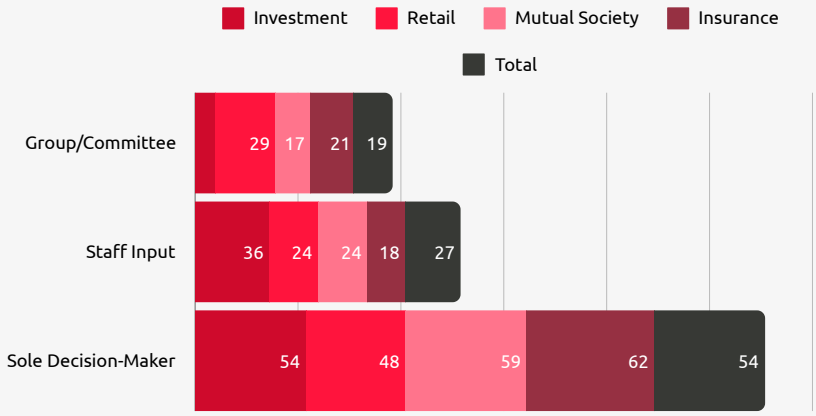


Figure 4: Sector breakdown: decision-making function within IT strategy development (%)

Sole decision-makers make up **54%** of the sample

These individuals have direct knowledge of the challenges their organisation is seeking to address with IT strategy and procurement; they will also understand their budget alignment.

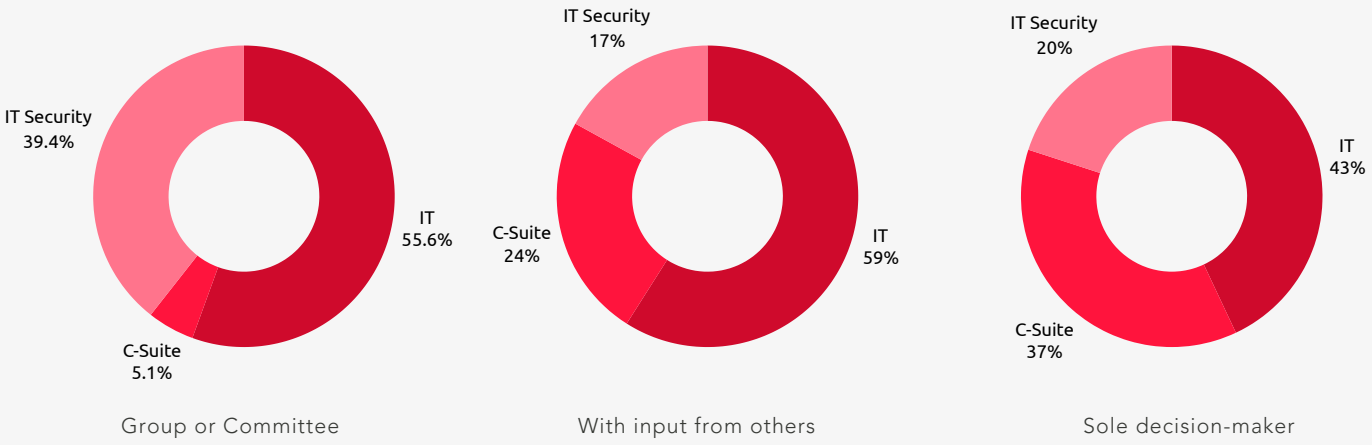


Figure 5: Decision-making breakdown by job function

Audience

What

Figure 6: Decision-making responsibility and decision-maker role/power (multiple choice) (%)

This research surveyed decision-makers responsible for IT strategy and implementation. Figure 6 shows categories for which respondents are responsible.

Over 50% of those surveyed have some form of input into developing IT strategy, but also cross into selecting technologies and managing adoption and projects.

Sole decision-makers have a larger spread of responsibility than those who form part of a group/committee, or make decisions with input from others.

In all responsibility areas, the percentage of sole decision-makers is larger than group members and those who make decisions with other input, suggesting they have a wider influence on IT decisions.

The Results

This section outlines results of the research, exploring different vectors for interpretation.

The results of this survey are broken into key findings and explored across the different vectors of interpretation based on the sample characteristics.

Key Findings

The key findings include:

- Increasing risk of cyber threats is the most significant change facing the UK Financial industry
- Data protection and GDPR is still the greatest burden for organisations subjected to regulation
- Concentrated third-party risk is a concern across sectors

This section incorporates external research reports to provide in-depth analysis and context to the findings.

These reports are:

- *IBM Cost of a Data Breach 2024*
- *Flexera State of Tech Spend 2024*
- *Flexera 2025 IT Priorities Report*

Results are presented as a percentage unless stated otherwise, indicated by *(actual)* in the figure note.

Due to the use of percentages to represent the result data, it is important to note that not all responses are from the full sample (200). The percentage shows the proportion of each respondent group selecting specific responses.

Key Findings

These are the three key findings that will be explored in more detail below.

51%

of respondents consider the increasing risk of cyber threats to be the most significant change facing the UK Financial industry over the next 2-3 years.

48%

of respondents consider data protection (GDPR) to be the greatest burden to their organisation.

30%

of respondents are concerned about the increased risk of the concentrated third-party model associated with using critical vendors such as Microsoft, AWS, and IBM.

Key Finding 1

The increased risk of cyber threats is the most significant change facing the UK Financial industry over the next two to three years

51% of respondents consider the increasing risk of cyber threats to be the most significant change facing the Financial industry. This view is held by both IT and C-Suite functions, who both have cyber threats as their most frequently selected challenge.

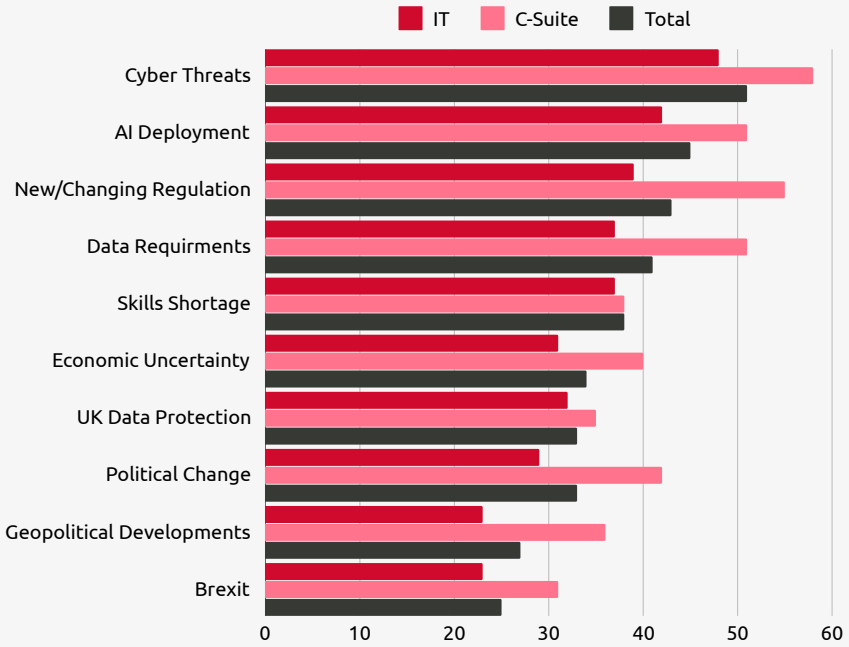
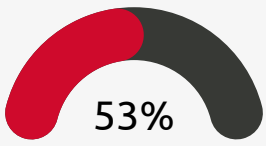
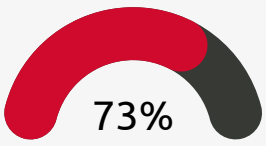


Figure 7: Most significant changes facing UK Financial industry over the next 2-3 years by job function (%)

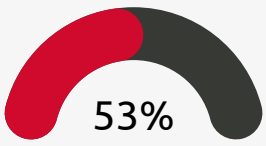
This is supported by responses about meeting IT challenges and use of external IT services, which both claim cybersecurity and cyber defence as the top priority.



Using external cyber security services



Agree their budget is aligned to cyber defence



See cyber defence as an organisational priority

Figure 8: Views on cyber defence: use of external services, budget alignment, and organisational priorities (%)

Key Finding 2

Data protection (GDPR) is the largest burden facing their institution in terms of compliance, including the invested time, costs, and reporting

48% of respondents consider data protection to be the greatest regulatory burden.

This burden is shared across the surveyed sectors, job role, and decision-making responsibility.

GDPR applies to organisations across industries operating in the EU. Non-compliance risks reputation and business damage as well as personal and organisational fines of up to €20million or 4% annual revenue respectively.

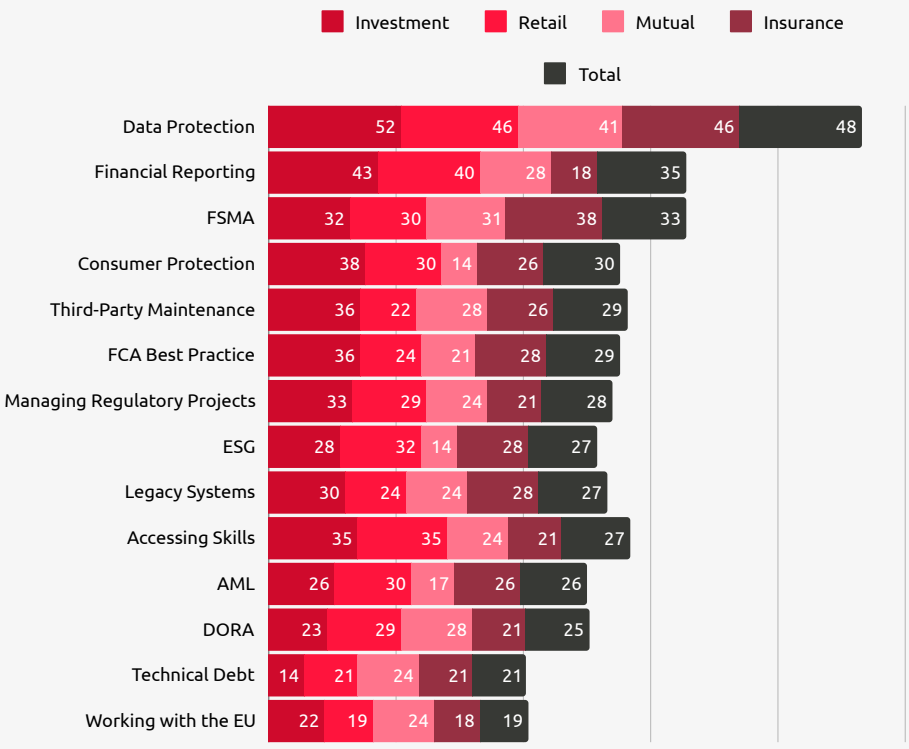


Figure 9: Compliance burdens (multiple choice) (%)

Data Security Challenges

This section analyses the state of data and cyber security as an industry priority focus (key findings 1 and 2).

Research from *IBM Cost of a Data Breach 2024* is used for insight into costs, attack frequencies, and threats. The IBM results does not distinguish between country and industry, causing statistics to represent the worldwide and cross-industry sample.

The cost of a data breach is determined by factors, including technologies and skills, business disruptions, time to identify and contain, attack vector, and more.

$4.53m

The UK ranked 7th for the average cost of a data breach, compared with the USA ($9.36m), Middle East ($8.75m), Italy ($4.73m), Canada ($4.66m), and more.*

$6.08m

Financial organisations ranked second for the average cost of a data breach, compared with industries including Healthcare ($9.77m), Industrial ($5.56m), and Technology ($5.45m).*

258 days

The mean time to identify and contain a data breach reduced by 19 days, from 277 days (2023) to 258 days (2024).*

**IBM Cost of a Data Breach*

Regulatory Burden

Responsiv found that 48% of respondents consider data protection and GDPR to be the largest regulatory/compliance burden to their organisation.

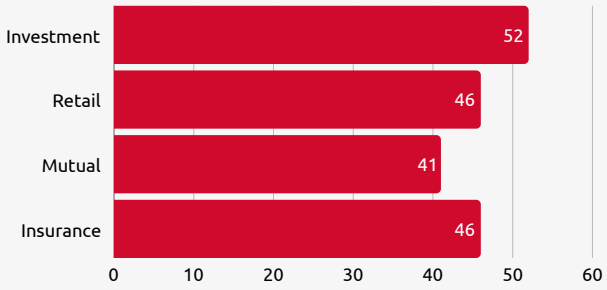


Figure 10: Data protection as the biggest burden by sector (%) (Responsiv)

Each respective decision-making role sees data protection and GDPR as the greatest regulatory burden compared to other options (multiple choice).

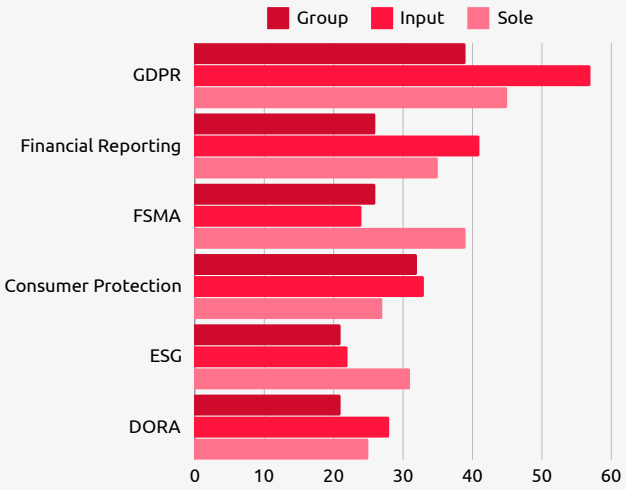


Figure 11: Greatest regulatory burdens by decision-making/strategy responsibility (%) (Responsiv)

As part of this burden, IBM found that over half (55%) of their sampled organisations reported their data breach within 72-hours, while 34% took over 72-hours, and 11% were not required to report.

This is 72-hours after the breach *identification*, which means the report is ~194 days after the initial breach.

The ability to report on a data breach or cyber attack requires data and oversight. Many organisations do not have the tools, teams, or ability to audit their data environments and privileged user access to provide detailed reports about breach activity.

IBM also found a 22.7% increase in organisations paying over $50,000 and 19.5% increase in those over $100,000 in regulatory fines.

With new regulations such as DORA, this regulatory reporting burden (in relation to data and ICT related incidents) is likely to increase further.

Attack Vectors

Privileged users were used as access points for the two most costly breach attack vectors: stolen/compromised credentials (16%) and phishing (15%).

The four most costly attack vectors were also traced back to privileged access, utilising compromised business emails ($4.88m) and malicious insiders ($4.99m) as well as stolen/compromised credentials ($4.81m) and phishing ($4.88m).

Utilising the trust of a privileged user to access data and systems makes identifying a breach more of a challenge due to the lack of 'abnormal' access.

Having the skills and capability to identify and shut down abnormal access from privileged users is important in mitigating breach risks originating from these sources. It isn't about zero-trust, it is about understanding the risk profiles of the vector.

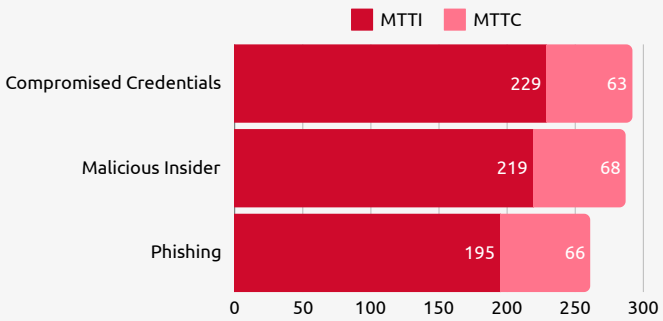


Figure 12: MTTI and MTTC based on attack vector (days) (IBM)

The mean time to identify (MTTI) and mean time to contain (MTTC) breaches originating from these attack vectors take upwards of 261 days, contributing to the high costs.

The difficulty to identify a breach, seen by the high MTTI, may be attributed to the privileged user trust and lack of independent oversight and tooling to effectively monitor and shut down breaches.

**Data from IBM Cost of a Data Breach*

Breach Identification

IBM highlights the three main ways a data breach is identified; by the attacker, by a benign third-party, or by an organisation's internal teams and tools.

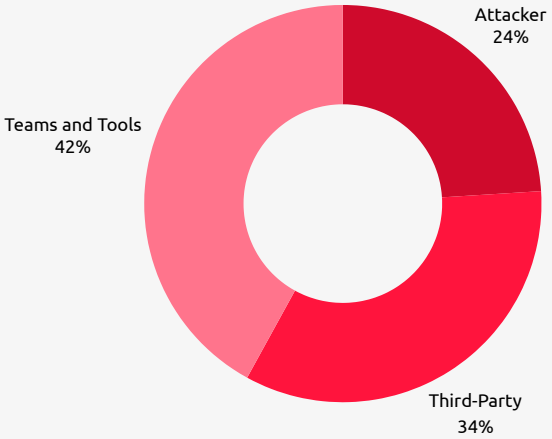


Figure 13: Method of identification frequency (IBM)

The frequency of breach identification by an organisation's own teams and tools (42%) has increased from 2023, where only one-third of breaches were identified internally.

Responsiv found that 51% of respondents fear increasing cyber threats and 53% are looking to prioritise cyber security and cyber defence to meet current and future demands. With these attitudes, internal identification is likely to become more frequent over the next 2-3 years.

The method of breach identification significantly impacts the total cost of a data breach.

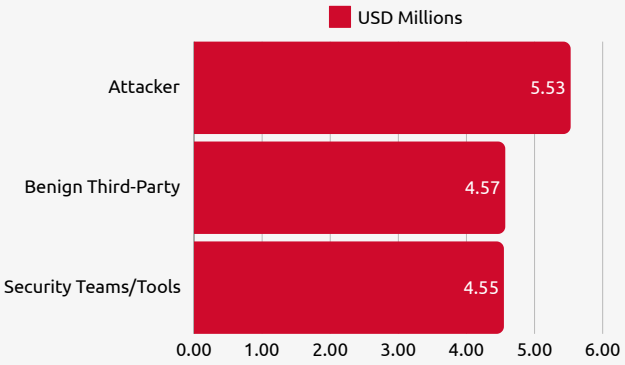


Figure 14: Cost of a data breach by method of identification (IBM)

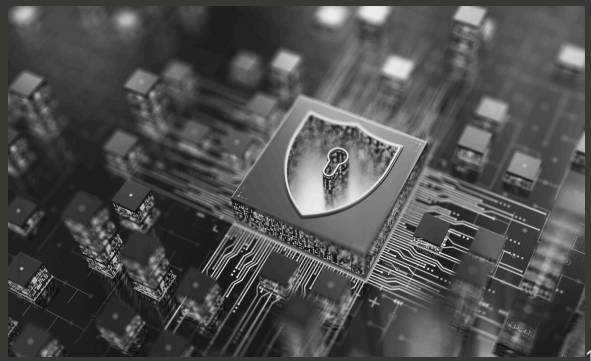
Investing in data protection and cyber defence tools/skills means organisations can save an average of $1million per breach.

Removing the complexity of these security systems can save ~$256,529.

Read more about the Total Economic Impact of IBM Guardium to find out how much organisations can save with data protection technology.

More Resources

- 2024 Cybersecurity Trends
- Ensuring Trustworthy Data Access
- International Bank Maintains Secure and Compliant Databases



Skills Shortage

Responsiv found the scarcity of qualified IT staff to be a significant challenge facing UK Financial organisations over the next 2-3 years, with 48% of Retail Bank respondents selecting this as their top challenge.

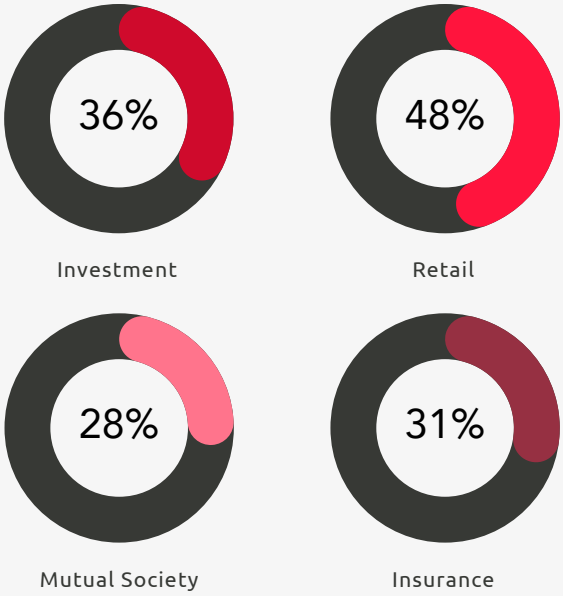


Figure 15: Scarcity of qualified/tech staff as a significant challenge by sector (Responsiv)

People in the role of attacker or defender contribute most to the total cost of a data breach.

IBM find that 53% of organisations face a lack of security skills in 2024 (compared with 42% in 2023). This scarcity of skills correlates strongly with the rising cost of data breach.

This shortage of security skills directly contributes to increasing the average cost of a data breach (+$251,940); most likely due to the lack of ability to identify and contain the breach, elongating the exposure, reputation damage, and need for external support.

IBM also found that Employee Training was the top contributor to reducing the cost of a data breach (-$258,629). This is likely due to the increased awareness of phishing (the second most frequent and costly attack vector) and other suspicious activity.

Key Finding 3

Increased risk of a concentrated third-party model associated with using critical vendors such as Microsoft, AWS, and IBM is a concern for decision-makers

30% of respondents see the dependence on key vendors (Microsoft, AWS, IBM) as a concern due to the increased risk of a concentrated third-party vendor model... Followed closely by **27%** of respondents being concerned about distributed third-party risk.

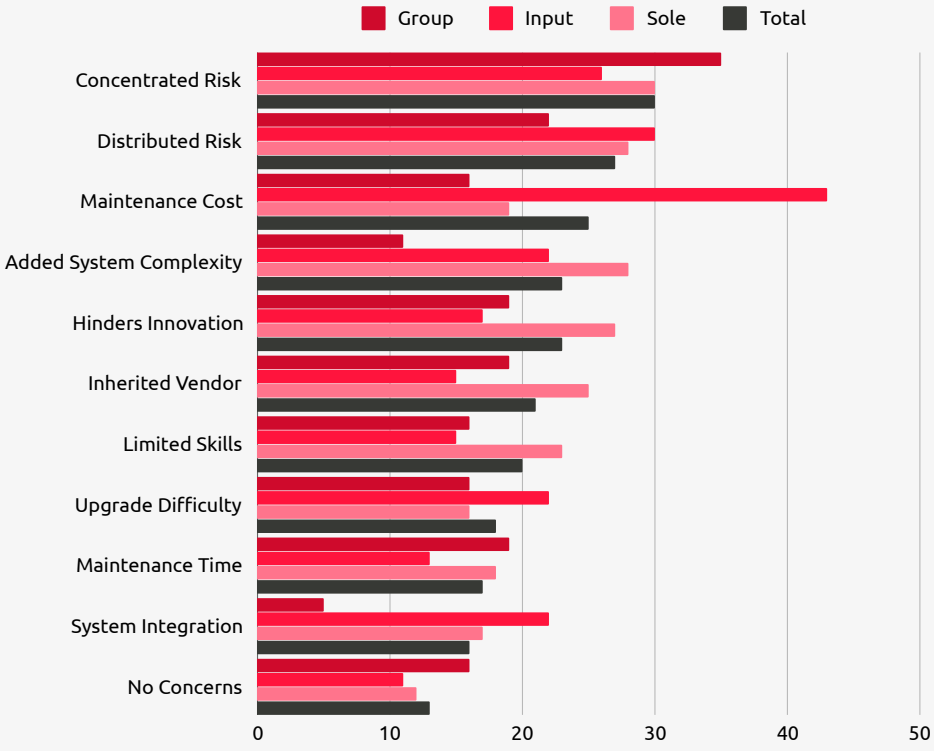


Figure 16: What concerns you about having a strategic vendor such as Microsoft, AWS, IBM? (multiple choice) (%) (Responsiv)

Group and sole decision-makers are most concerned with the increased concentrated third-party risk, with 35% and 30% of each respondent demographic selecting this option respectively.

43% of those who make decisions with input from others are concerned with the maintenance costs associated with their vendor strategy.

As this was a multiple choice question, it is not to say that the response with the largest selection is a respondent's highest concern, rather that more people share the same concern.

IT Procurement

This section analyses the tech spending prioritisation and vendor consumption attitudes using Responsiv findings and Flexera *State of Tech Spend 2023* and *2025 IT Priorities* reports.

It will look at the top technology vendors across Europe, IT budgets and decision-makers, and spend priorities.

It is important to note that Flexera samples include industries outside of Financial Services.

61%

Microsoft is the largest vendor in 61% of European respondent organisations. This likely includes the Office 365 suite (Outlook, Word, PowerPoint).*

80%

Of European respondents see **cybersecurity** as their top technology initiative followed by cloud/cloud migration (77%), digital transformation (72%), cost saving/optimisation (58%), and modernise/reduce technical debt (52%).*

10%

Of annual revenue (average) is spent on IT in Europe, compared with 13% in the USA, and 12% globally.*

**Flexera State of Tech Spend 2023*

Vendor Strategy

Responsiv found that sole decision-makers (29%) prefer a single supplier across all areas of IT, group decision-makers (32%) prefer a main supplier with additional specialists, and those who make decisions with input from others (35%) prefer a very small number of suppliers.

These preferences are despite the concern of increased concentrated third-party risk.

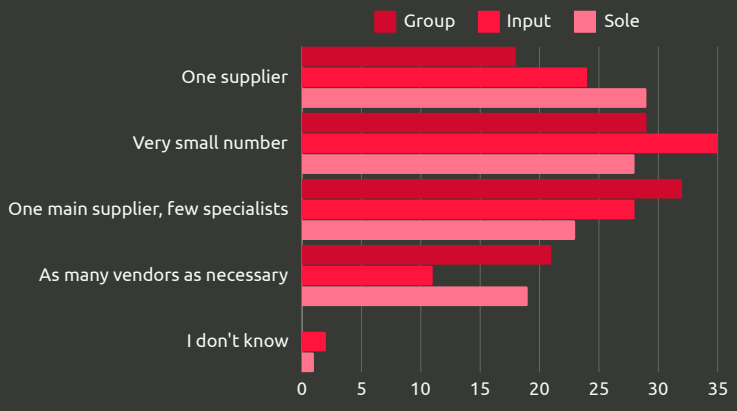


Figure 17: My ideal scenario for external IT vendors is...(%) (Responsiv)

Flexera found that Microsoft dominated Europe as the largest IT vendor (61%), followed by SAP (23%), AWS (24%), Oracle (10%), and IBM (8%).

What isn't indicated in Flexera's data is if Microsoft includes or excludes the Office 365 suite. Flexera's data is also an amalgamation of industries, so does not represent the Financial Services.

IBM was ranked much higher by Responsiv respondents, with 54% selecting them as a strategic IT vendor. This may be due to the Financial Services focus, knowing that IBM technology is heavily embedded in the industry.

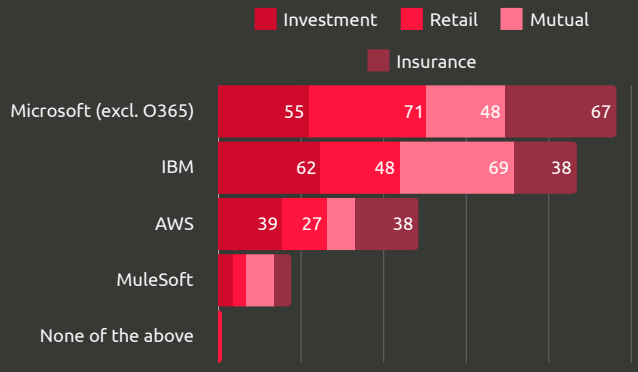


Figure 18: Vendors playing a strategic role as part of your IT infrastructure by sector (%) (Responsiv)

For Investment Banks and Mutual Societies, IBM was the most selected strategic vendor; whereas Retail Banks and Insurance respondents both selected Microsoft most frequently.

Decision-Maker Concerns

68% of Responsiv respondents believe that the CIO/Director of IT hold the budget and make the final financial decision about IT procurement and spending.

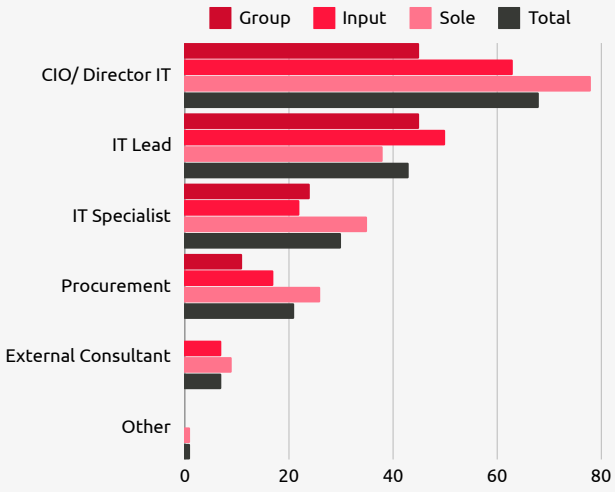


Figure 19: Who holds the IT budget and gets final financial decision? From decision-maker perspectives (multiple choice) (%) (Responsiv)

Flexera's *2025 IT Priorities Report* found that IT overspending was a constant concern for IT decision-makers. Only 15% of respondents thought their spending was 'fine.' This will highly impact the way they make decisions about spending and procurement.

Despite the earlier indication that cybersecurity/defence was a key priority for Financial Services respondents (Responsiv, Flexera, and IBM reports), Flexera find that 31% of IT decision-makers feel they are overspending on security tools.

Whilst this may seem in contradiction, there are various factors to consider; security may still be a priority, but the tools are viewed as complex and costly. The cross-industry sample also conflates the results; priorities and concerns will differ across industries.

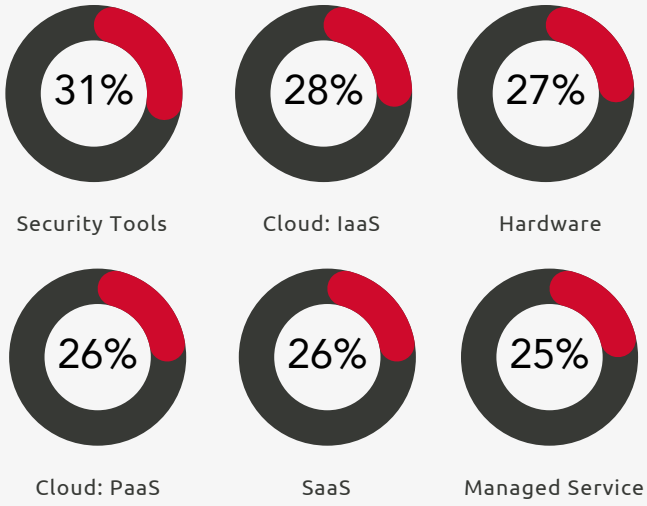


Figure 20: Overspending on technology - security vs. next 5 technologies (Flexera)

Whilst security and regulatory compliance is recognised as important and given the required budgets, they are a distraction from the primary activities of the organisation.

Budgets

Responsiv found that respondents consider their budgets to be fully aligned to IT priorities.

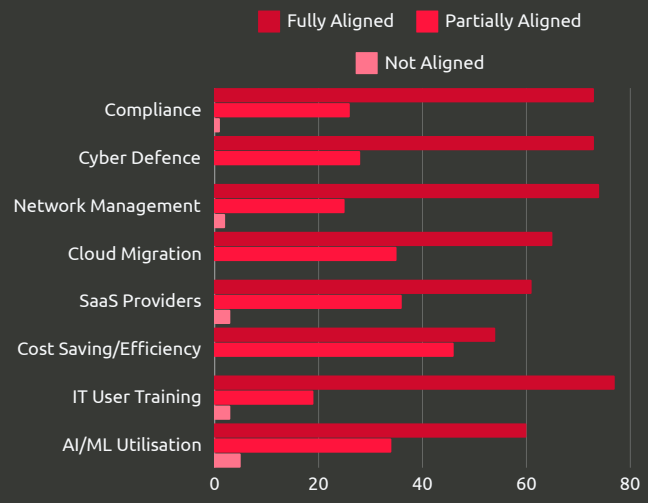


Figure 21: Technology initiative and budget alignment (% breakdown of each response (<200)) (Responsiv)

Alignment indicates that budget is authorised for a specific purpose; organisations are willing to invest where their decision-makers dictate as priority.

According to Flexera's *Tech Spend Report*, most European organisations expect their IT investments to stay the same or slightly increase.

The main technologies expected to decrease in investment are 'traditional' and on-premises, such as servers, data centres, and traditional software.

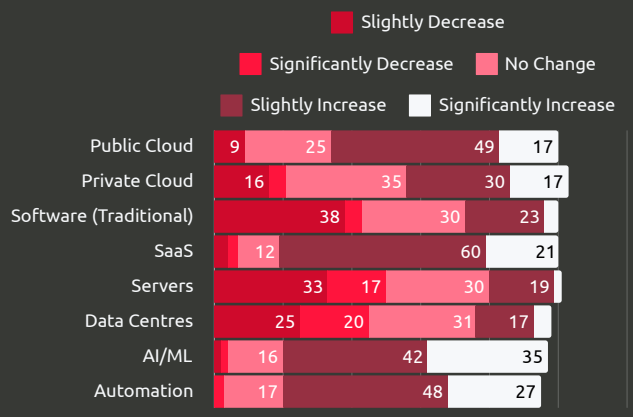


Figure 22: Expected change in IT investments over 12 months (Flexera, 2023) (%)

responsiv

Responsiv deliver technical expertise and solutions to UK Financial Services.

Data compliance made simple.

Managed services for data compliance designed to remove the strain from internal IT and compliance teams.

Utilise best practice policies for GDPR and SOX so you can plug-in and comply with ease. Automated reporting reduces the time spent collating and formatting data for the regulator.

Monitor privileged users and shut down suspicious activity within your data environments before they have the chance to become malicious.

Deliver on time and to budget.

Responsiv deliver projects on time and to budget. Compliance project deadlines? Hit them with Responsiv.

Read More

Read more from this research series, below:

- IT Hypotheses in UK Financial Services
- IT Procurement in UK Financial Services

Optimise data compliance - contact Responsiv, today!

sales@responsiv.co.uk

01344 266 980

UK Finance 2024 Associate Member

IBM Gold Partner