Deloitte.

Cyber risk and governance reporting in the UK

Cyber resilience as a strategic imperative

MAKING AN IMPACT THAT MATTERS since 1845

Contents

For this survey, we have read the most recent annual reports of the FTSE 100 that were published by 15 August 2025. The results are described throughout as 2025 survey results. 2024 comparative results represent a similar survey of the full FTSE 100 conducted in 2024.

Foreword

How do companies describe cyber risk?

How do boards report their involvement?

Are mitigating activities well explained?

Are cyber security breaches well-described?

Are companies discussing opportunities?

Appendix 1:
Examples of cyber disclosures

Contacts

The Deloitte Centre for Corporate Governance

Foreword

We are pleased to present this survey of cyber risk and governance reporting across the FTSE 100, designed to help you identify examples of good practice and to offer insight about how to keep users of annual reports informed in this important area.

2025 has seen a number of high-profile and financially significant cyber attacks affecting UK businesses and commanding government attention. In October, the government wrote to the CEOs and Chairs of all FTSE 350 businesses along with a number of other leading firms, asking them to bring board-level scrutiny to cyber resilience.

Recognising that cyber security is already a critical priority for more than 90% of boards, the letter asked boards to ensure companies are taking advantage of a number of systems put in place by the government, including the early warning service run by the National Cyber Security Centre (NCSC) and the Cyber Essentials scheme for supply chains.

The primary ask however was to make cyber risk a Board-level priority. The government suggested using its new Cyber Governance Code of Practice, published in April following consultation during 2024. This Code is designed for organisations of all sizes and shows how to manage cyber risks effectively and reduce the likelihood and impact of cyber attacks. As it was finalised after many companies in our survey had already published their annual reports, there is likely to be more reporting on this Code in future years.

This year has also seen an assessment from the NCSC that AI will "almost certainly pose cyber resilience challenges to 2027 and beyond across critical systems and economy and society". This will be no surprise to the 49% of the FTSE 100 that identified an emerging risk relating to AI, in the main linked to cyber security. To read our further insights on FTSE 100 reporting on AI, we refer you to Deloitte's recently published Corporate Reporting Insights 2025 survey.

Some key areas that stood out to us this year in the annual reports of the FTSE 100:

- **The impact of geopolitics:** an increased number of companies reported on the impact of geopolitical and nation state threats on their cyber risk.
- **Third party risk:** a significant increase in the number of companies that reported on cyber risk arising from third party involvement – up to 66% from 42% in 2024 - with the nature of those disclosures becoming more informative and detailed. Mitigations disclosed for third party risk included early due diligence, contract reviews, external assurance or controls reports and detailed governance structures.
- **The governance of cyber risk:** in line with the focus on cyber risk raised in the government's letter, we saw an increased level of disclosure around the governance structures addressing cyber risk with companies going into more detail about the way boards are kept informed and the relationship between cyber risk and other risk management processes.

Changes in reporting requirements have been limited this year as companies with a dual listing with the US are already following the SEC's Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, which took effect in 2023 and has had a particular impact on the quality of disclosure around the governance of cyber risk.

In summary, our FTSE 100 annual report survey shows:

- almost all companies include cyber and / or data security as a principal risk. The potential for value destruction from this type of risk can be very high and includes customer service issues, costly remediation, regulatory fines and longer-term reputational damage
- the better disclosures are company specific, year specific and provide sufficient detail on actions and outcomes to give meaningful information to investors and other stakeholders
- increasingly, companies draw out specific and detailed risks associated with internal threat, geopolitical threat, third parties / suppliers and AI
- boards and board committees are discussing cyber and AI more regularly both at the board and in audit and risk committees. Disclosures cover board education, skills and performance reviews involving cyber and AI, deep dives into risk, and boards challenging management to implement stronger controls. Areas of focus have included technology capabilities and the risks associated with obsolescence, education of the workforce and engagement with suppliers.

Finally, if company disclosure does not look strong enough after taking credit for what the company is doing already, you should question whether enough is being done to manage the risks associated with IT, data and cyber security – which should be a strategic imperative for boards.

We hope you find this survey useful. Do get in touch with your Deloitte partner, the cyber risk and crisis management specialists whose names are in the contact list at the end of this survey or the Deloitte governance team if you would like to discuss any areas in more detail.

Claire Faulkner
Deloitte Academy Governance Chair
December 2025

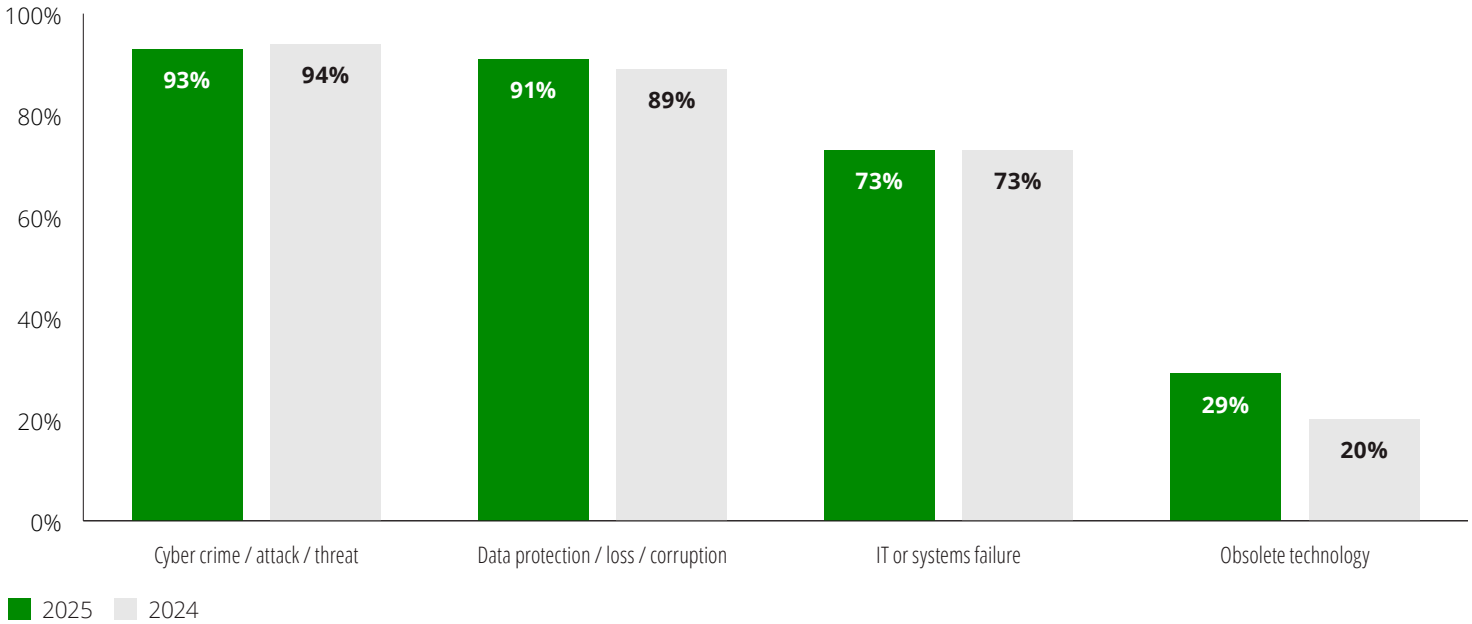
1. How do companies describe cyber risk?

Cyber risk remains a key focus area for FTSE 100 companies. Our 2025 survey identified that 99% of companies reported at least one element of cyber risk as a principal risk, in line with our 2024 report. All 100 companies included technology-related risk disclosures in their annual reports, highlighting the widespread recognition of this risk.

Companies continued to describe three main types of cyber risk as part of their principal risks: cyber crime, risks associated with data protection and IT or systems failure. The better disclosures reported on each of these types of cyber risk separately.

Beyond these types of cyber risks, the landscape of cyber threat is constantly evolving and is evidenced by the proportion of companies identifying specific aspects of their cyber risks as emerging risks, alongside those that have been identified as principal risks. 23 companies that reported cyber as a principal risk also identified elements of it as an emerging risk– up from 19 companies in 2024. In both years, 11 companies further attributed these cyber related emerging risks to the rapid advances in AI technology.

Figure 1. Types of cyber risk identified in FTSE 100 annual reports



49% of the FTSE 100 disclosed AI as part of their principal risk relating to cyber risk in their annual reports. The majority of these companies described how the use of AI contributed to increased cyber threats, including the potential exploitation of vulnerabilities within AI algorithms leading to data breaches, and the disruption caused by new AI technologies rendering existing systems obsolete and more susceptible to attacks. Other companies discussed leveraging AI as a mitigation tool against cyber threats, including through the use of AI-related standards and policies.

Our survey identified an increased proportion of companies (29%, up from 20% in 2024) reporting obsolete technology or a failure to implement transformation as a type of cyber risk they were exposed to. This was cited as a stand-alone principal risk by a handful of companies and as part of an existing cyber risk by others.

The risk associated with obsolete technology is expected to become more critical over the coming years with the emergence of quantum computing, which will in due course lead to the need for companies to update and redesign their IT security approach. One company mentioned systems obsolescence in the context of the advent of quantum computing1.

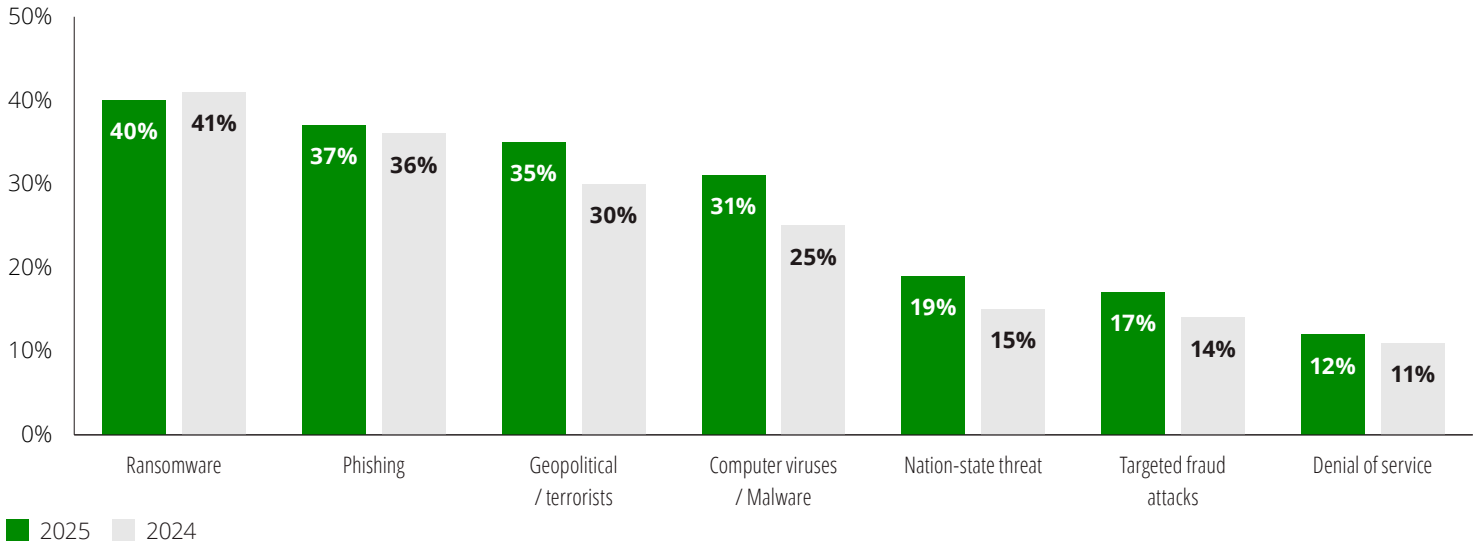
1. Quantum computing is a nascent computing technology that leverages quantum mechanics and in due course may render many current encryption methods obsolete, posing a significant challenge to existing IT security. McKinsey estimates that there will be 5,000 quantum computers by 2030.

44% of the FTSE 100 categorised the principal risks in their annual reports. 29 of these companies identified cyber risk as an operational risk. The others identified cyber risk in a variety of different categories, from legal or compliance risk for those that focused on the data protection elements, to categories specifically set up for IT-related risks.

As might be expected, the more specific the description of the nature of the cyber crime companies have experienced or are exposed to, the more specific the description of their management or mitigation (see Section 3). Figure 2 shows the nature of cyber threats disclosed by the 99% of companies that reported one or more elements of cyber risk in the risk management section of their annual report.

35% (2024: 30%) of companies cited geopolitical factors as a significant cyber security threat vector, reflecting a heightened awareness of the relationship between global instability and corporate cyber resilience. This growing concern stems from the recognition that geopolitical events can directly impact a company's cyber security posture, creating vulnerabilities that cyber criminals can exploit. For example, periods of conflict or instability can weaken a company's cyber resilience by limiting access to resources, making companies more susceptible to attack. Disruptions to supply chains, particularly when key suppliers operate in unstable regions, can force companies to prioritise operational continuity which may inadvertently increase their vulnerability to cyber threats.

Figure 2. Types of cyber threats disclosed by the FTSE 100

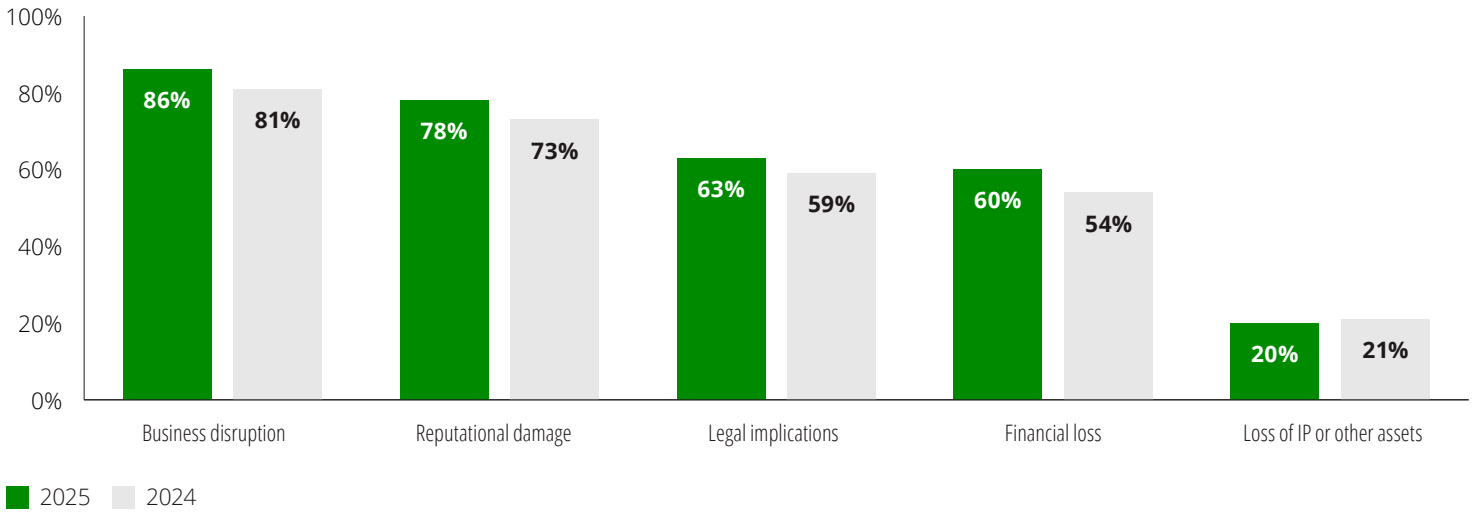


Our survey also identified that 19% (2024: 15%) of companies reported nation-state threat as an external factor affecting cyber risk. The superior resources and technological sophistication of nation-state actors pose a serious threat to corporate cyber security. It is also likely that once quantum computing is available, it will be nation states that are among the first with capability in this area.

In addition to the main risks and the attack vectors, most companies reported the potential impacts that cyber risks could have on their business. While business disruption (86%, up from 81% in 2024) and reputational damage (78%, up from 73% in 2024) remained the most frequently cited impacts of cyber risk, there was an increase in the number of companies reporting potential financial losses (60%, up from 54% in 2024). 63% of companies also reported potential legal implications which could include the risk of fines from regulatory non-compliance or the revocation of operating licences (2024: 59%).

Although most companies reported facing at least one specific type of cyber risk, it is important that boards continue to critically consider other types of cyber risks they could become exposed to in an ever-changing cyber threat landscape. It will remain critical for boards to consider if the organisation's current cyber threat monitoring and reporting practices will be able to keep pace with more advanced threats that may bypass existing detection methods.

Figure 3. Potential impact of cyber risk as described in FTSE 100 annual reports



We looked at where companies disclosed cyber risk or cyber security in the annual report and identified the following changes this year.

- An increased number of companies (19) specifically called out cyber in their **Section 172 (1) Statement** as a topic of engagement with one or more of their key stakeholders (2024: 11). The topic was mentioned in the context of customers, suppliers and regulators/ governments. Some of these companies included board decisions around cyber security as key decisions during the year.
- 36 companies also mentioned cyber as part of the **sustainability disclosures** in the strategic report (2024: 30).
- Similar to last year's survey, over half of companies identified the impact of cyber risk on the company's ongoing viability with **cyber security scenarios** being included in the viability statement. Some of these companies included **quantification** as part of the scenario, such as the anticipated financial impact on the business.

The vulnerability of third parties within a company's ecosystem continues to be a major cyber security concern for companies. Cybercriminals frequently exploit these relationships, including relationships with suppliers and customers, to gain unauthorised access to a company's system, a risk known as "fourth-party risk".

This year's survey identified 66 companies acknowledging third-party risk as a principal concern—a significant increase compared to 42 in 2024. Of these, 13 specifically highlighted cloud services as a key vulnerability (2024: 10), with the majority attributing this risk to cyberattacks targeting the security and resilience of their suppliers and other third-party providers.

Insider threat continues to represent a significant risk vector. Nearly a quarter of companies (24%, slightly up from 23% in 2024) explicitly identified this as a source of cyber vulnerabilities. These risks stem from both human error (e.g., phishing scams, weak passwords, mishandling sensitive data) and malicious intent (e.g., insider threats motivated by financial gain, revenge, or espionage). The multifaceted nature of internal threats suggests a need for board-level consideration of mitigation strategies beyond traditional employee training.

Finally, a small but growing number of companies (15%) included key risk indicators (KRIs) as part of their reporting of cyber risk (2024: 8%). Examples of KRIs included the number of material breaches, percentage of breaches involving personally identifiable information (PII), number of users affected, and time taken by the company to respond.

2. How do boards report their involvement?

Our survey found that 90% of boards (2024: 94%) reported on cyber risk. We looked at how companies described the board's ownership of cyber risk, with a particular focus on the board's expertise in guiding cyber risk assessments and mitigation strategies, as well as their oversight of management's actions in this area.

Our survey identified a positive trend in directors with expertise in digital and technology related matters: 70 companies reported such expertise, compared to 61 in 2024. It was encouraging to note an increase in directors with specialist expertise in cyber, with 36 boards reporting such specialisation (2024: 30), and 16 reporting AI expertise (2024: 12). These companies clearly described the directors' prior experience or certification level, allowing the reader to judge the depth of expertise on the board.

Cyber security is receiving significantly more attention at the board level. 75% of boards (2024: 59%) reported receiving dedicated cyber reports or presentations, including "deep dives". Executive responsibility for cyber most frequently resided with the Chief Financial Officer (CFO) and Chief Information Officer (CIO), although some companies assigned this to the Chief Information Security Officer (CISO). The CISO was not always part of the C-Suite in their own right, with several governance structures indicating that the CISO reported to the CIO or the Chief Technology Officer (CTO). 37% of companies disclosed that they have a CISO or similar as part of the executive team (2024: 42%). Better disclosures described the CISO's attendance at meetings and the process by which the board was informed about cyber risks and mitigations.

Very few companies indicated that any responsibility relating to cyber sat with a non-executive director, although many companies emphasised the role of non-executive directors with cyber expertise in the oversight process. Although board-level engagement with cyber security is growing, it continues to be critical for boards to consider where they may need to bring in expertise either from within the company or externally, particularly for specialist areas such as AI.

Cyber risk reporting to the audit committee increased compared to our 2024 survey. 76% of companies reported that management provided cyber risk reports to their audit or audit and risk committee (2024: 71%). However, only 13% of companies with a standalone risk committee received cyber security reports to that committee (2024: 16%).

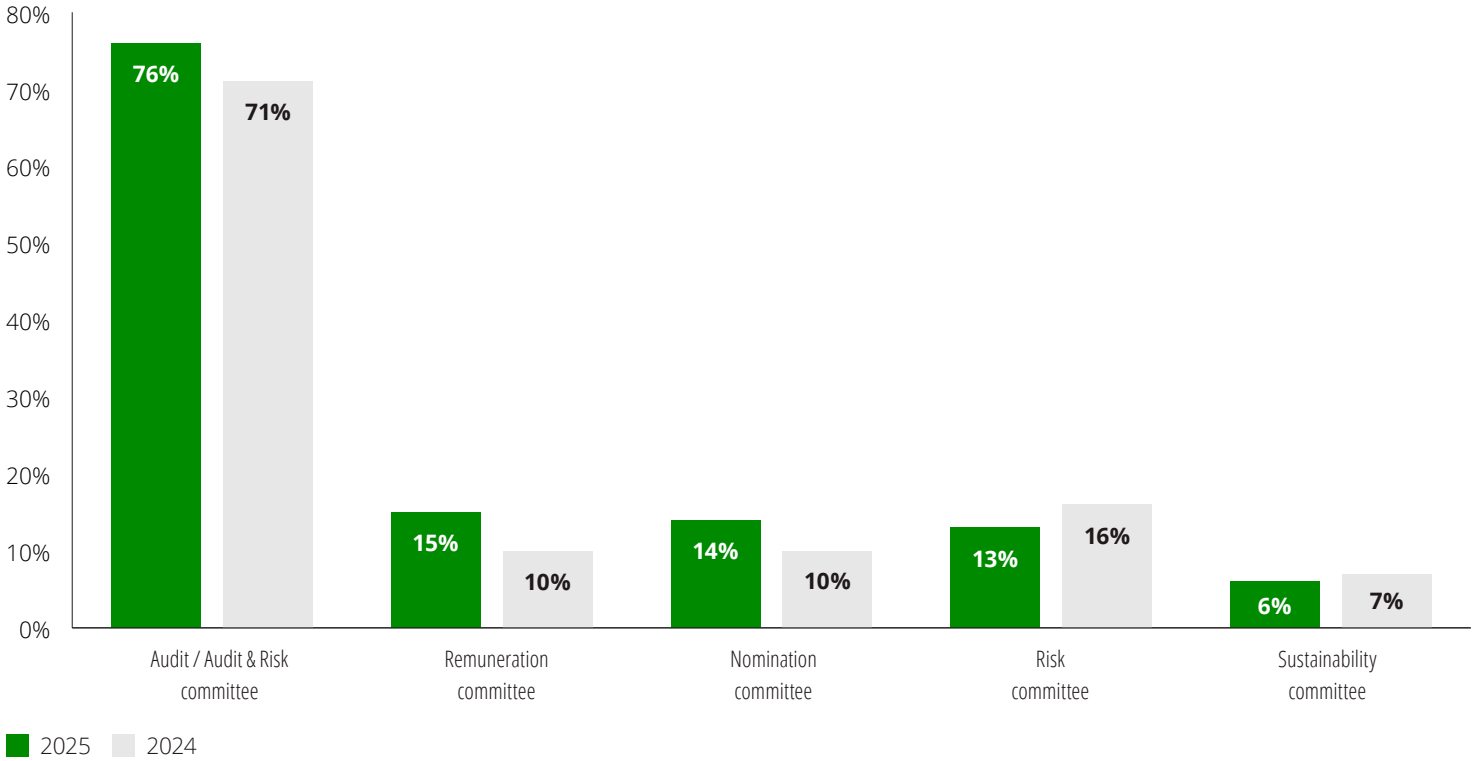
Disclosures in the nomination committee report (14%, 2024: 10%) mostly considered the depth of board expertise in this specialist topic, often within the context of board composition and succession planning for new non-executives.

Some companies (15%; 2024: 10%) mentioned cyber in the remuneration committee report in relation to executive director targets such as delivering on cyber security programmes. This increase reflects the growing recognition of cyber risk as a significant business risk impacting key financial and non-financial metrics.

6% of companies included cyber risk reporting within their sustainability committee reports. (2024: 7%). These disclosures focused on risks related to privacy and personal data, particularly those arising from cyber attacks, AI deployment and data breaches. The reports also highlighted the potential impacts from such incidents and the strategies in place to mitigate these risks, including through the adoption of company-wide AI standards.

Overall, the quality of disclosure on cyber risk within committee reports remains highly variable with many audit and/or risk committee reports providing cursory mention of cyber security within broader risk management and internal control discussions.

Figure 4. Cyber mentions in committee reports



3. Are mitigating activities well explained?

All companies are expected by investors and other stakeholders to have internal controls and IT policies in place to manage IT security issues.

Consistent with last year's survey, we found that not all companies explained their processes clearly in respect of cyber and data security.

- Only 55% of companies clearly described a governance process in relation to cyber risk (2024: 54%).
- 80% of companies described having internal policies in relation to cyber / data security within their risk mitigations – up from 75% in 2024.
- 92% of companies mentioned internal controls in place as a mitigating factor in relation to cyber risk (2024: 71%) and 30% of companies also disclosed improvements in these internal controls during the year (2024 : 34%).

There continues to be a lot of activity to upgrade cyber security defences, and 33% of companies mentioned an external framework for their cyber security, such as ISO 27001, the UK Cyber Essentials programme or the NIST Cyber Security Framework (2024: 30%).

Only one company cited the UK's Cyber Governance Code of Practice, a UK government framework that was introduced in April 2025 to guide boards in governing cyber risks. This is not surprising given the majority of annual reports included in our survey were published prior to April.

Training of the workforce continues to be an area of focus:

- 70% of FTSE 100 companies mentioned delivering staff training on cyber or data risk during the year (2024: 76%). 27% of companies also mentioned staff training on AI during the year[2].
- 22% of companies specifically mentioned cyber or data risk training delivered to the board during the year (2024: 30%).

Some companies reported that the board had been trained in different topics but did not specifically mention cyber, data risk or AI. Other companies mentioned delivering training in cyber to the board or the workforce but did not specify whether this was during the year.

44% of the FTSE 100 cited penetration testing as a mitigating factor and many of these companies also mentioned vulnerability testing (either internal or external) as a mitigation against cyber attack. There was an increase this year in companies that reported engaging in "red team" exercises – a type of scenario planning derived from wargaming – as a proactive management practice, with some of these exercises involving the board and/or executive team.

2. This question is new in 2025 and as such no comparatives are provided.

26% (2024: 29%) of companies mentioned external assurance, including audits of new security systems and 30% (2024: 29%) cited external assistance on cyber matters, such as a report on the maturity of the cyber security control framework in identifying, assessing and managing material cyber risks. 51% of companies reported mitigation of third-party risks including third-party due-diligence, vendor on-boarding security assessments and reviewing third-party control reports (2024: 47%).

73% of companies cited contingency plans, crisis management or disaster recovery plans as a mitigation for cyber risk (2024: 60%). 24% of these companies also mentioned testing their plans during the year (2024: 25%) and 11% of companies further discussed board and executive level involvement in assessing these plans (2024: 8%).

Only 18 companies disclosed having cyber insurance in place as a mitigating factor (2024: 18). This suggests that boards may be prioritising proactive cyber risk measures (prevention) over reactive measures. It is also possible that companies perceive the cost of insurance to outweigh its benefits, given that cyber insurance premiums can be substantial, particularly for large companies with complex IT infrastructure and data holdings.

4. Are cyber security breaches well-described?

Cyber threats represent a pervasive and significant risk across all sectors.

Some cyber attacks are repelled or result in limited business disruption or limited compromise of customer data. However, in other cases, cyber attacks can have wide reaching impact, including public awareness, financial and other consequences, as demonstrated by recent instances across the UK retail, healthcare and transportation industries.

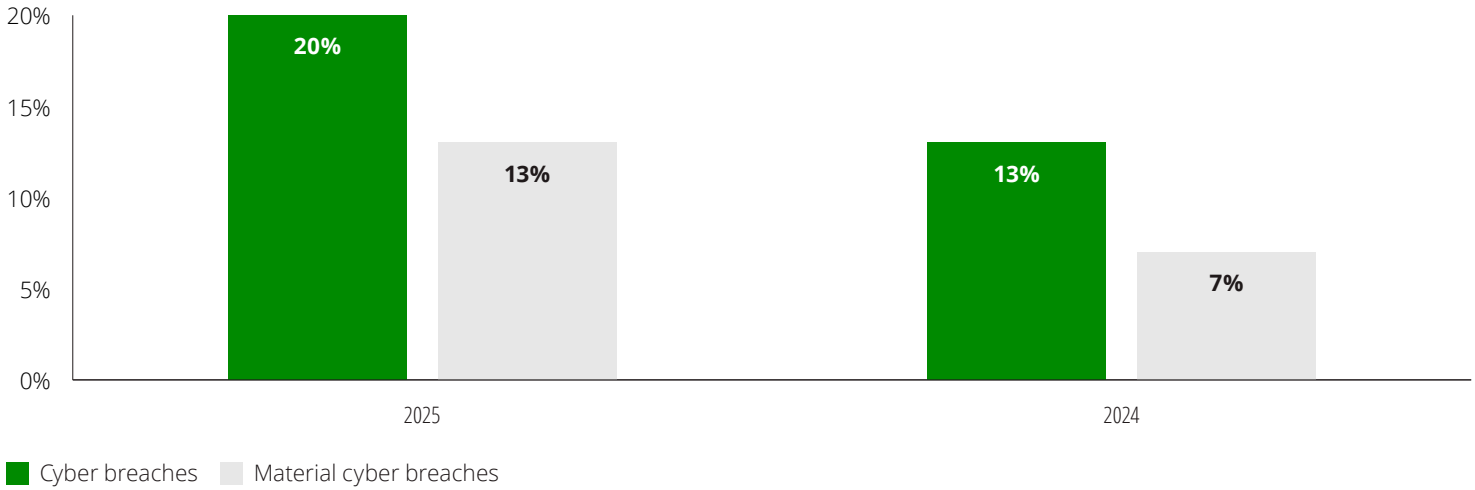
Although many of the FTSE 100 mentioned an increase in the prevalence of cyber crime, only 20% reported that they had experienced cyber security breaches (2024: 13%). 13 of these companies indicated whether the breach was material or not (2024: 7 companies).

No company reported **material** cyber security breaches during the year (2024: 1 company).

However, two companies disclosed material cyber security breaches post year end – in one case an unauthorised access to systems and in the other a ransomware attack. Both companies disclosed these breaches in the financial statements under post balance sheet events, with an estimation of the financial impact.

The increase in companies that reported experiencing cyber security breaches and stated that they were not material was primarily among companies with a US listing.

Figure 5. Cyber breaches reported in annual reports



One company cited reputational damage because of cyber breaches (2024: 2 companies). 2 companies disclosed engagement with external cyber security professionals (2024: 1 company), 1 company mentioned how the breach was remediated (2024: 4 companies) and 1 company reported that the remediation process was ongoing (2024: none). The variation year on year is affected by the small sample size.

A significant proportion of companies did not disclose any information on breaches in their annual reports. This could result in users of annual reports underestimating the true presence of cyber risks faced by an entity .

The most informative disclosures acknowledged the reality of frequent cyber incidents and provided some detail about how these were managed as a set of incidents. Where there was an incident that was either public or material in nature, better disclosures provided clear detail about how the board considered these and the response or remediation implemented by management.

Companies sometimes raise questions about whether disclosure of breaches or weaknesses in cyber security expose their organisation to hackers. In our view, the level of detail provided will never be so extensive as to constitute a risk.

5. Are companies discussing opportunities?

76% of FTSE 100 companies described opportunities relating to cyber or digital investment in addition to highlighting risks, down from 88% in the 2024 survey.

The opportunities described by companies tended to be industry specific. For example, some companies in the healthcare industry reported that digital and technology investment will improve the identification process for potential new drugs while others reported that it will help them understand underlying conditions, helping new medicines to be approved and marketed more quickly.

Some companies in the consumer sector reported that investing in digital tools will improve the ease of e-commerce and the effectiveness of marketing spend. Similarly, some companies in the technology industry largely reported investing in new technologies such as AI to take advantage of cloud-based capabilities and storage opportunities. Companies in the financial services sector also reported digitising processes to improve how employees work and interact with customers.

The industry specific nature of opportunities highlights the importance for boards to consider tailored strategies and proactive monitoring of the evolving landscape rather than a one-size fits all approach, and measurable outcomes of investments in digital and technological tools.

The general theme of opportunities disclosed by companies included:

- improved performance (44%, 2024: 49%) - for example using enhanced systems that produce goods and provide services in a timely fashion and with potentially less use of resources
- improved engagement with customers (44%, 2024: 61%) - for example through enhanced online platforms that target a specific audience and automated systems that provide customers with faster service delivery
- sustainability improvements (14%, 2024: 38%) – in particular, the investment in new sustainable technologies, such as lower emissions technology, digital control of operations to target efficiency gains and data-driven sourcing decisions. This has fallen substantially over the past year. It is not clear from disclosures whether this is due to the implementation of these new technologies and therefore it now being an achievement rather than an opportunity, or due to reduced ambition for this type of opportunity
- increased efficiency (53%, 2024: 54%) - for example replacing manual and time-consuming processes with automated processes.

Other benefits cited by more than one in ten companies were competitive advantage, value accretion and better information exchange.

Appendix 1: Examples of cyber risk and governance disclosures

Within this appendix we have provided links to some examples of cyber risk and governance disclosure from our survey of FTSE 100 annual reports.

Company	Example disclosure	Page and link
Fresnillo plc	Detailed reporting on cyber security in the principal risk section including a clearly written description, factors contributing to the risk, controls, mitigating actions and outlook, link to strategy, risk appetite, risk owner, risk oversight and risk rating (relative position).	p126 Annual report
HSBC Holdings plc	Additional detailed reporting on data privacy and cyber security outside of the principal risk section.	p83-84 Annual report
Auto Trader Group plc	Quantified scenario of a ransomware attack in viability statement.	p60 Annual report
Coca-Cola Europacific Partners plc	Detailed description of a governance structure/process for cyber risk.	p77 Annual report
Rightmove plc	Detailed description of cyber security simulation at the board level and a disaster recovery/business continuity plan.	p67 and p91 Annual report
Land Securities Group PLC	Key Risk Indicators/Key Performance Indicators for cyber risk included in annual report.	p44 Annual report
Smith & Nephew plc	Board decisions around cyber security included in s172 statement.	p117 Annual report
Vodafone Group Plc	Detailed reporting on significant financial reporting judgements and actions taken as well as risk deep-dive reviews section in audit committee report.	p87 Annual report

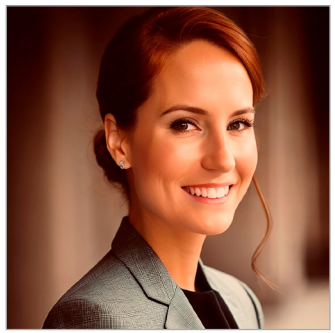
Contacts

Cyber risk

Peter Gooch
Tel:+44 (0) 20 7303 0972
Email: pgooch@deloitte.co.uk

Kristian Park
Tel:+44 (0) 20 7303 4110
Email: krpark@deloitte.co.uk

Technology and digital risk



Charlotte Gribben
Tel +44 (0)77 3621 2539
Email: cgribben@deloitte.co.uk

The Deloitte Centre for Corporate Governance

If you would like to contact us please email corporategovernance@deloitte.co.uk or use the details provided below:

Claire Faulkner
Tel: +44 (0) 20 7007 0116
Mob: +44 (0) 7876 478924
Email: cfaulkner@deloitte.co.uk

Tracy Gordon
Tel: +44 (0) 20 7007 3812
Mob: +44 (0) 7930 364431
Email: trgordon@deloitte.co.uk

Corinne Sheriff
Tel: +44 (0) 20 7007 8368
Mob: +44 (0) 7824 609772
Email: csheriff@deloitte.co.uk

Deloitte.

Designed by CoRe Creative Services. RITM2331363