Deloitte.



Cyber risk and governance reporting in the UK

The shift from resilience to readiness

Contents

Foreword 3

1. How do companies describe cyber risk? 5

2. How do boards report their involvement? 11

3. Are mitigating activities well explained? 14

4. Are cyber security breaches well-described? 17

5. Are companies discussing opportunities? 18

Appendix 1: Examples of cyber risk and governance disclosure 20

Appendix 2: Cyber security pledge and Cyber Governance Code of Practice 21

Contacts 23

The Deloitte Centre for Corporate Governance 24

For this survey, we have read the most recent annual reports of the FTSE 100 that were published by 15 August 2026. The results are described throughout as 2026 survey results. 2025 comparative results represent a similar survey of the full FTSE 100 conducted in 2025.

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 risk and governance disclosure

Appendix 2: Cyber security pledge and Cyber Governance Code of Practice

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.

2026 has been another year in which cyber resilience, along with geopolitics, has stayed at the top of the boardroom agenda. Building on the Cyber Governance Code of Practice published in April 2025, in March the government set out its Cyber Action Plan, followed in April by a voluntary Cyber Resilience Pledge, which asks signatories to make cyber a board responsibility, sign up to the National Cyber Security Centre's (NCSC) Early Warning service and require Cyber Essentials to be instituted across their supply chains. As this Pledge was published after most companies in our survey had already reported, we expect to see more disclosure referencing it in future years.

Artificial intelligence remains an area of focus. Companies are increasingly alert to the risk that AI makes attacks faster, more sophisticated and more relentless, even where the underlying techniques are not new. It is not the impact of the attack that is greater, rather it is the likelihood of an attack that increases. The message from our cyber specialists this year is that the fundamentals still matter most: organisations with strong cyber hygiene, patching and perimeter controls in place are best placed to withstand AI-enabled attacks. At the same time, boards and their advisers are at the start of the journey to explore how AI can be turned to their advantage both in defending organisations and in improving the efficiency of cyber security efforts.

Organisational resilience, and in particular the ability to recover quickly and effectively from an incident, has remained an area of close attention, brought into real focus by a number of high-profile attacks on UK businesses over the past year. Boards are increasingly asking management and cyber security leaders not only whether the organisation can prevent and respond to an attack, but whether they know the handover points between systems and even whether they have a workable "minimum viable company" design if the organisation needs to operate with minimal technology for an extended period.

This year has also seen the emergence of quantum computing as a boardroom topic. Around a fifth of the FTSE 100 referred to quantum computing in their annual reports, reflecting early recognition that it may in time undermine current encryption techniques, even as it also promises benefits for drug discovery, supply chain optimisation and other complex problems. While still an emerging rather than a mainstream disclosure topic, we expect quantum to feature more prominently in future surveys as organisations begin to plan for "quantum-safe" encryption.

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

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

- **Obsolete technology:** a marked increase in the number of companies citing obsolete technology as part of their cyber risk disclosure, often linked to the risk of failing to keep pace with new IT functionality and emerging technologies
- **Third-party and fourth-party risk:** a continued rise in the proportion of companies reporting on cyber risk arising from third parties, with a handful of companies also describing risk arising further down the supply chain ("fourth-party risk")
- **The rise of external assurance:** an increase in the number of companies citing external assurance, reviews and other outside support as part of their mitigation of cyber risk
- **Opportunities:** we noted an increase in the proportion of companies identifying opportunities from cyber and digital investment, largely linked to AI and focused around enhanced performance, efficiency and customer engagement.

In summary, our FTSE 100 annual report survey shows:

- almost all companies continue to include cyber and/or data security as a principal risk. The potential for value destruction from this type of risk is 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
- companies are describing increasingly specific risk factors associated with geopolitical threat, third and fourth parties, obsolete technology, AI and starting to mention quantum computing
- boards and board committees continue to discuss cyber and AI regularly, both at board level and in audit, risk, nomination and remuneration committees, with disclosures covering board education, skills, deep dives and challenge to management regarding the strength of controls.

We hope you find this survey useful. Do get in touch with your Deloitte partner, the cyber risk and crisis management specialists given 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
November 2026

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

1. How do companies describe cyber risk?

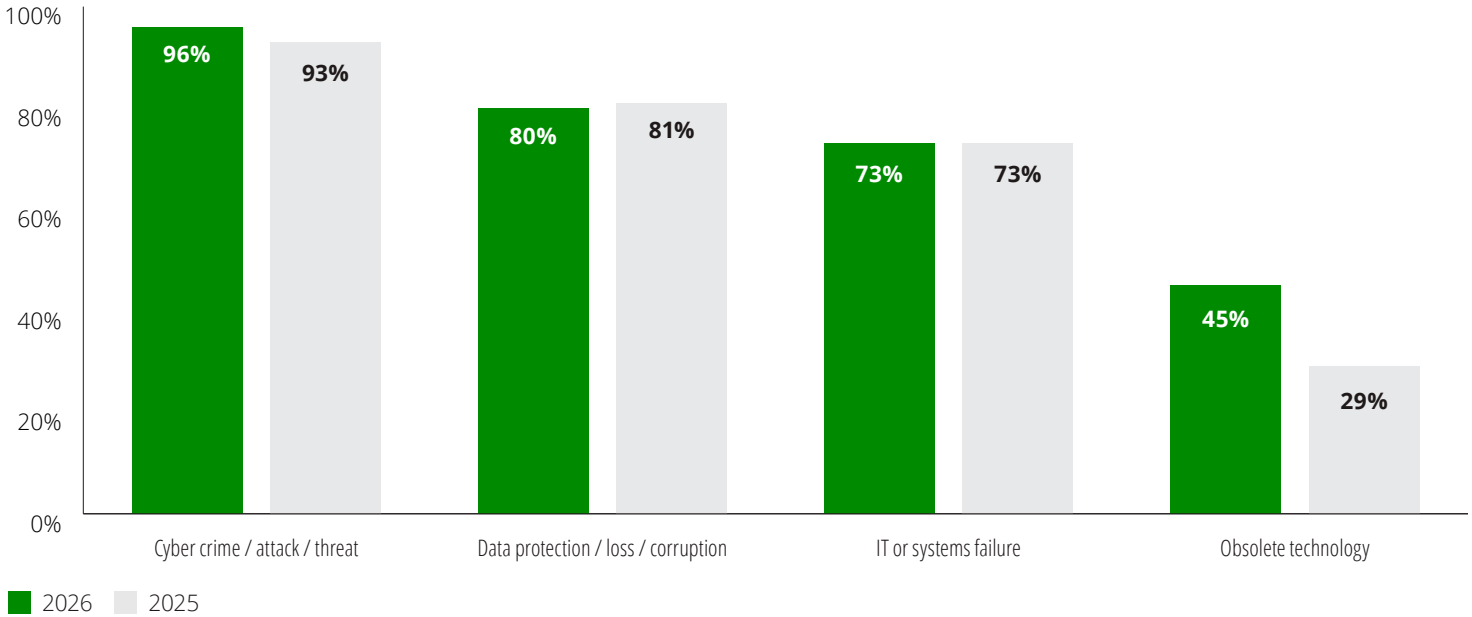
Cyber risk remains a key focus area for FTSE 100 companies and featured prominently in almost all annual reports we surveyed this year. Our 2026 survey indicates that 98 companies either included cyber risk as an independent principal risk or embedded it in another principal risk, in line with our 2025 report (2025: 99 companies).

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.

This year we identified a notable increase in the proportion of FTSE 100 that reported obsolete technology as part of their cyber risk disclosure (2026: 45%; 2025: 29%). Around half of companies identifying this risk discussed the risk as relating to the failure to implement emerging technologies or stand up refreshed IT functionality. They identified that failure to adapt could adversely affect business growth, effective operations, the ability to enhance customer offerings and competitiveness.

A further quarter of companies that reported obsolete technology as a risk mentioned that the failure to adopt new

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



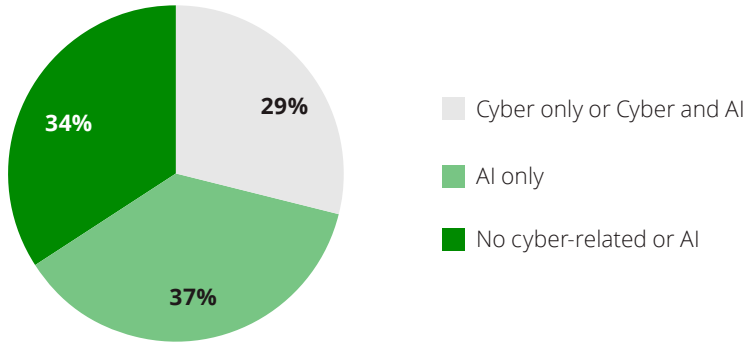
Foreword
How do companies describe cyber risk?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Examples of cyber risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

technologies could intensify the cyber threat environment and expose them to cyber security breaches. Some also mentioned the need to implement technological transformation safely and effectively to avoid disruption to systems, business activities, service delivery and cyber security.

The number of companies that attributed elements of their cyber-related risks to AI in the principal risks section of the annual report increased from 44 in 2025 to 65 this year. Companies expressed their concerns regarding the probability of increasingly sophisticated cyber criminals operating with the use of AI. Some indicated that it could be difficult to know which cyber crime techniques were used to manipulate systems until they were deployed against them or their third-party vendors. While AI was praised for its contribution to improving productivity and boosting efficiency, a few companies acknowledged that their application of AI in business operations could also result in increased risk of data security breaches, alongside ethical concerns, which could result in legal consequences such as fines.

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. We saw an increasing number of the FTSE 100 acknowledging the evolving landscape of cyber threat. This year, 29 companies included cyber and AI risks in their list of emerging risks (2025: 23 companies). 37 further companies identified separate AI-related emerging risks (2025: 11 companies).

Figure 2. Disclosure of cyber and AI as emerging risks



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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

Quantum computing

The constantly evolving cyber threat landscape, driven by emerging technologies, has challenged companies to enhance their existing IT systems and/or design new IT teams to support business growth, operational efficiency and cyber security. Over one fifth of the 45 companies citing obsolescent technology risk as part of cyber principal risks referenced above specifically mentioned quantum computing in the principal risk description as a disrupting technology that could increase cyber risks.

Excluding tangential references, quantum computing was mentioned by 15 companies in our sample. Roughly half of these disclosed it within their technology/cyber security principal risk, describing it as an advancing technology that could increase cyber security threats. The rest disclosed it within their emerging risks and threats descriptions, noting that while quantum technology opens up various business opportunities, it could threaten current encryption techniques, challenge existing services and introduce new competitors. One company suggested that addressing the implications of AI and emerging technologies such as quantum computing too early could result in sunk costs on initiatives that are either unnecessary or fail to integrate into daily operations.

A handful of the FTSE 100 had moved beyond simply flagging quantum computing as a risk to describing concrete mitigation steps, such as developing roadmaps to quantum-safe or post-quantum encryption, launching dedicated post-quantum cryptography programmes, and establishing monitoring processes involving proof-of-concepts, investment scanning and engagement with regulators. Regarding governance, one company shared the concern that quantum computing technology could advance faster than existing governance and control frameworks could adapt, while another addressed it at board committee level as a sector disruptor requiring ongoing readiness. This suggests differing maturity profiles in how companies are responding to quantum computing, ranging from those that have not yet put much thought to the topic and don't disclose at all, with some having completed initial risk identification through to the few that are evaluating active mitigation strategies and board-level oversight.

Types and impacts of cyber threats

The more specific the description of the nature of the cyber crime companies have experienced or believe they are exposed to, the more specific the description of their management or mitigation (see section 3).

Figure 3 presents the nature of cyber threats disclosed by the 98% of companies that reported at least one element of cyber security risk in the risk management section of their annual report. Around one third of the FTSE 100 cited ransomware (2026: 40%; 2025: 40%), unauthorised access (2026: 39%; 2025: 42%), phishing (2026: 38%; 2025: 37%) and geopolitical matters (2026: 33%; 2025: 35%) as the drivers of cyber threats facing their organisation, a similar level to last year. There was however a reduced number of companies mentioning the threat of malware/computer viruses as one of cyber threats faced (2026: 23 companies; 2025: 31 companies).

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

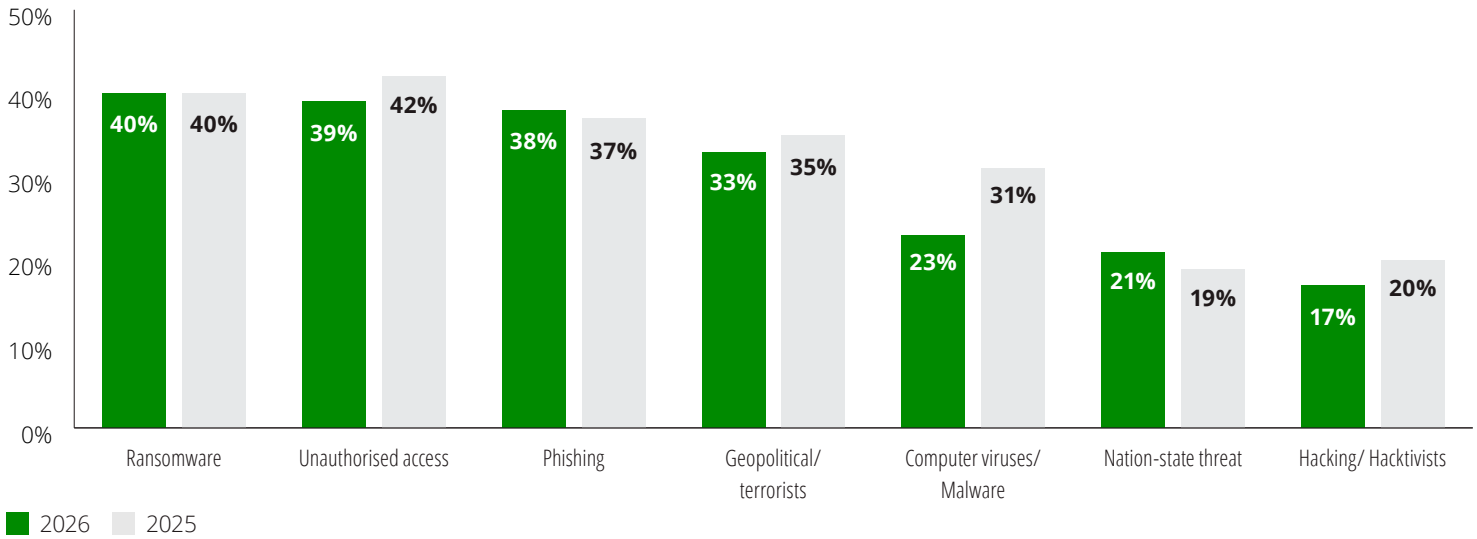
Diving into the impacts of cyber risk that companies are exposed to, our 2026 survey identified that business disruption (88%, slightly up from 86% in 2025) and reputational damage (85%, up from 78% in 2025) remained the top 2 impacts that are mentioned by most companies. Financial loss (76%, up from 60% in 2025) overtook legal implications (69%, up from 63% in 2025) to be in the third place of the most cited impact by FTSE 100 companies.

Disclosures on cyber, data security and AI in the annual report

We observed an increase in companies discussing cyber, data security or AI outside the risk management and principal risks section.

- **Section 172(1) statement** – 24 companies mentioned cyber, data or AI in the Section 172(1) statement, up from 19 in 2025. Most of these companies discussed it as a topic of engagement with stakeholders, for instance, customers, employees or government and regulators. Some disclosed their key decisions and activities related to cyber security, data protection and AI in detail including how those benefited business operations. For example, a financial services company presented a subsection of the s172(1) statement dedicated to cyber security, which clearly explained how the board oversaw three key technology matters, digital transformation, technology strategy and operational and cyber resilience and that continuous oversight of cyber security was critical to securing approval

Figure 3. Types of cyber threats disclosed by FTSE 100 companies

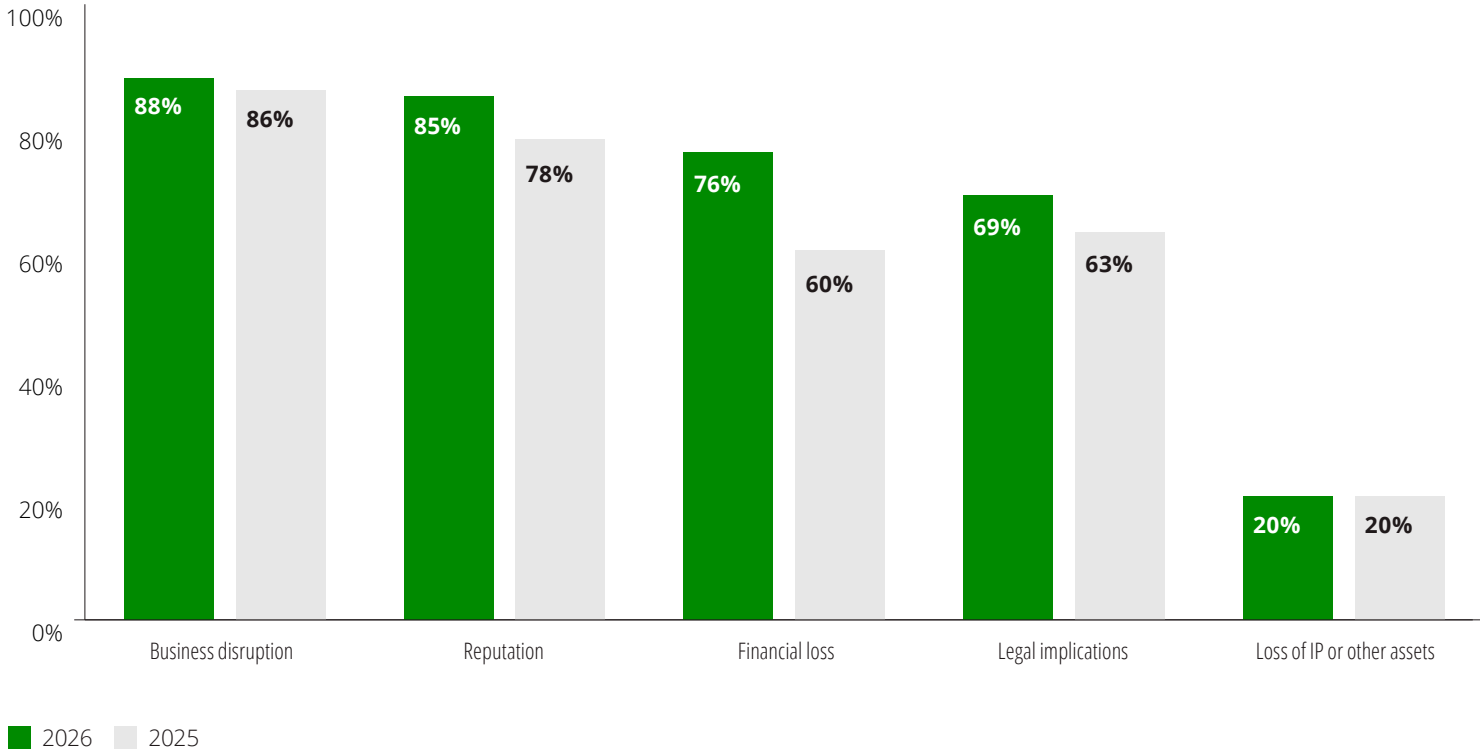


Foreword
How do companies describe cyber risk?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Examples of cyber risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

from the UK regulator of the group's Operational Resilience Self-Assessment (ORSA). A handful of companies also disclosed in the s172(1) statement how they had engaged and communicated with various stakeholders following a cyber incident experience in the year.

- **Sustainability-related statement** – 50 companies (2025: 36 companies) discussed cyber, data or AI in this statement. Around two-thirds of these mentioned the cyber and data security risks facing the entity or the need to handle stakeholder data carefully and how they managed cyber security and data holdings. Around one in four disclosed these topics as part of their policy, due diligence and training disclosures.

Figure 4. Potential impact of cyber risk as described in FTSE 100 annual reports



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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

- **Viability statement** – 55 companies (2025: 47) mentioned cyber, data or AI in their longer term viability statement. They are mentioned either in the context of risks facing the entities, or in evaluating a scenario of a cyber incident to assess the impacts on the business, or as part of their stress testing.

Third-party threats

72% of companies this year recognised the increasing risk of cyber threats arising from third parties, up from 66% in our previous survey. Similar to last year, 13 companies specifically identified cloud-based risks as part of their third-party cyber risk exposure. Companies acknowledged that their reliance on third-party systems exposes them to cyber risks arising from external vendors' system failures and infrastructure vulnerabilities, creating additional challenges for data management and cyber defence. These risks can also lead to operational disruption, data loss, and financial and regulatory consequences.

A few companies disclosed cyber incidents involving both third- and fourth-party suppliers during the year. While third-party risk refers to threats arising from vendors that contract directly with a company, fourth-party risk extends to the subcontractors, suppliers and partners on which those third parties themselves depend. One company reported cyber incidents resulting from attacks on third-party service providers, which affected both business operations and customers. Another reported an incident involving a fourth-party provider used by one of its outsourcing partners, which also caused disruption to the business. These incidents reinforce the need for companies to establish and strengthen controls over how they deal with external parties and to maintain robust oversight of their wider supply chains. Overall, 53% of FTSE 100 companies disclosed mitigation measures relating to third-party cyber risk (2025: 51%), including pre-engagement assessments, ongoing monitoring, enhanced due diligence, contractual cyber security requirements, and reviews of suppliers' cyber security reports.

We also noted an example of a company that experienced a breach during the year and reported support for its third-party suppliers. It introduced a supplier financing scheme, providing upfront cash payments to suppliers during the recovery period. These measures helped the company's business return to normal operations more quickly when operations fully restarted. This example highlights the importance of incorporating into business continuity planning not only preventative measures to address cyber threats across the value chain, but also effective recovery strategies to enable businesses to respond to, and recover from, cyber incidents efficiently.

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

2. How do boards report their involvement?

Our survey found that 94% of boards reported on cyber risk, slightly up from 90% in the previous year. We focused on how the FTSE 100 entities described their board's ownership of cyber risk, in many cases covering their expertise in guiding cyber security risk assessments and mitigation strategies as well as their oversight of management's activities.

We found that there are a growing number of boards disclosing directors with knowledge around digital and technology related matters. 79 companies reported such skills, compared to 70 companies in 2025. Around a third of boards (34%) further disclosed that they had directors on the board with specific skillsets and / or experience in cyber, data or AI related matters. These 34 companies clearly described the directors' prior experience or certification level, allowing the reader to judge the depth of expertise on the board.

Cyber security continues to be a key focus area at the board level. The UK Government sent a ministerial letter on cyber security in October 2025 to all UK FTSE 350 companies; this was mentioned explicitly by two companies. One of these disclosed that the Government wrote a letter to major UK businesses regarding 'making cyber security a board responsibility' and mentioned how they focused on strengthening its cyber and control environment. The other described receiving a letter from the UK Government outlining the Cyber Governance Code of Practice and the board's request to include this in the agenda for discussion twice per year.

Similar to last year, 73% of FTSE 100 governance disclosures (2025: 73%) reported the board or a committee receiving dedicated cyber reports or presentations, including 'deep dives'. Cyber governance is described variously as being led by an IT related department or executive from a specific group formed to govern cyber, such as a Cyber Security Steering Committee and in some cases, by a specific cyber security office. 34 companies in our survey reported that they have a CISO or similar in the executive team in charge of cyber security (2025: 37). In general, consistent with our 2025 survey, companies did not reference allocating responsibility regarding cyber security to a non-executive director, even though many mentioned their oversight roles.

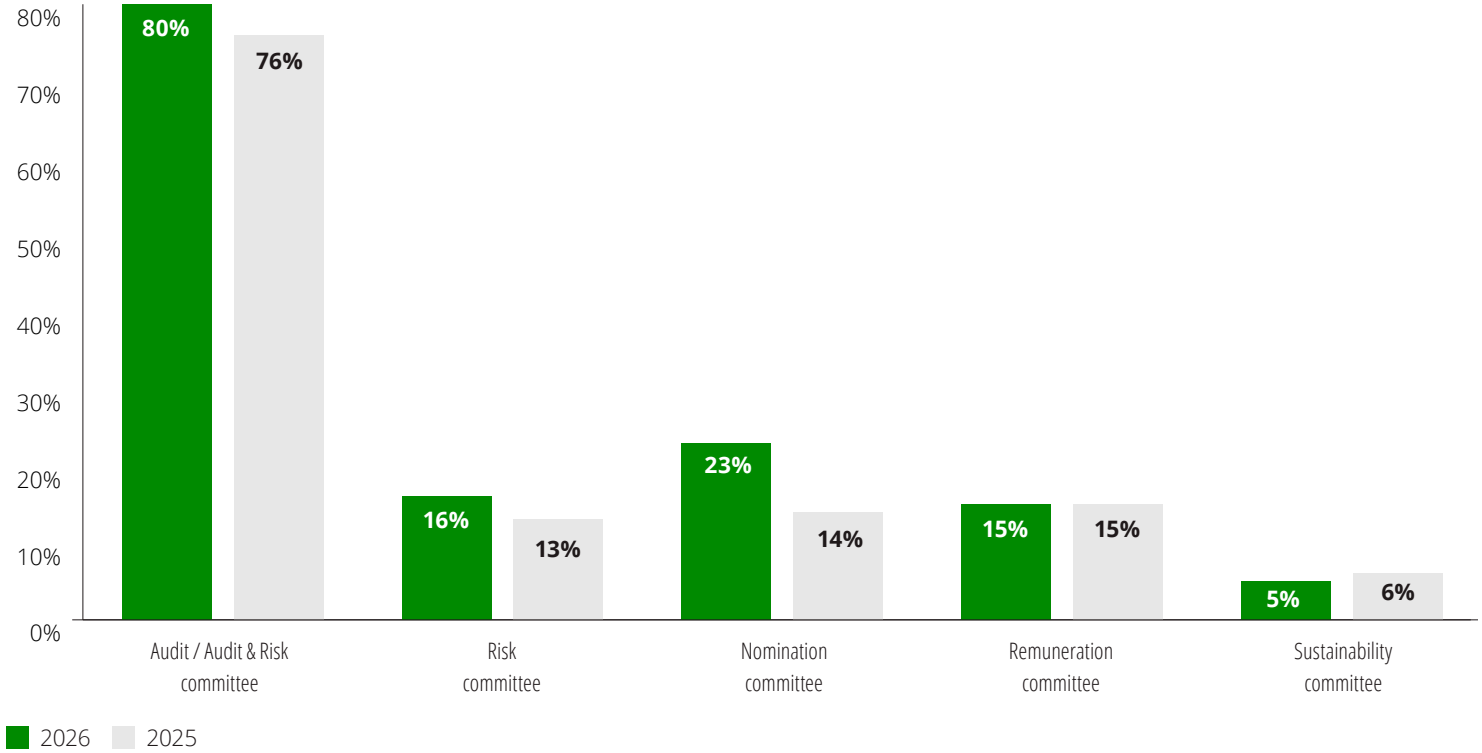
Fourteen FTSE 100 governance reports disclosed that boards had involved cyber or digital experts in their meetings or held strategic sessions with experts to discuss or advise on their cyber security strategies and management approaches (up from 11 in 2025). Half of these fourteen companies also reported having board members with expertise in these areas that are therefore able to provide quality inputs into the discussion of cyber governance strategies; the others added the expertise via the use of expert input. An increasing number of boards can demonstrate that they are engaging with specialised expertise, whether on the board or as an invitee with the right skillset, in order to upgrade their defences in a constantly evolving cyber threat landscape.

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

We identified an increase in the number of audit committee reports or audit and risk committee reports discussing cyber risk (2026: 80%; 2025: 76%). 16% of FTSE 100 companies reported that stand-alone risk committees received cyber security reports, up from 13% in 2025.

In general, we noted that committees disclosed cyber-related matters at different levels of depth, likely demonstrating a significant variation in the attention paid to these matters. For instance, audit and / or risk committee reports varied between brief acknowledgement of cyber risks as part of wider risk management and internal control discussions and detailed disclosures regarding management approaches towards cyber security, incorporating the improvements made during the year and plans for the coming year.

Figure 5. Cyber mentioned in committee reports



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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

Some of this related to the upcoming implementation of Provision 29 of the UK Corporate Governance Code, which was cited by 29% of the FTSE 100 when mentioning cyber-related matters, generally in the audit committee reports or audit and risk committee reports. Provision 29 will require companies that follow the UK Corporate Governance Code to make a declaration regarding the effectiveness of material controls for periods commencing on or after 1 January 2026. Some interesting disclosures in this area included one company with a dedicated section to describe their Provision 29 activities, which included the establishment of an Internal Controls Steering Committee, with frequent meetings and attendance from Group Risk, Finance, Sustainability Finance, Internal Audit, Legal and IT. Another company described deep dives on cyber, technology, data governance and AI that were undertaken during the year and linked to Provision 29 preparation.

More companies this year disclosed cyber security in the nomination and governance committee reports (23%, up from 14% in 2025). Some disclosed cyber and data security as a training and development topic; while some included it in the disclosure of the board members' skills and experience. A few mentioned it as part of the performance review process.

15% of companies discussed cyber in the remuneration committee report in respect of remuneration objectives, achievements by board members, and the companies' focus on cyber security, in line with prior year (15%). 5% of companies mentioned cyber security in their sustainability committee report (2025: 6%).

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 risk and governance disclosure

Appendix 2: Cyber security pledge and Cyber Governance Code of Practice

Contacts

The Deloitte Centre for Corporate Governance

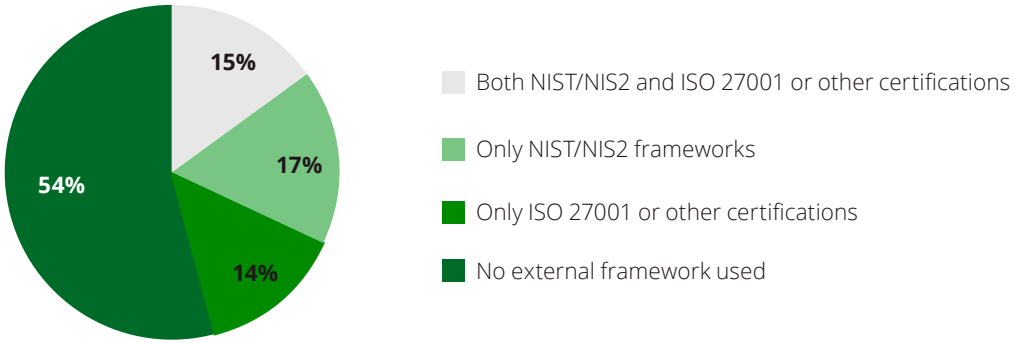
3. Are mitigating activities well explained?

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

Similar to the finding in prior year, it is noted that the cyber governance process was not well described by all companies.

- 52% of companies clearly explained a governance process regarding cyber and data security (2025: 55%). Some presented in detail their various layers of governance, including having a dedicated function with cyber and digital experts to monitor the matter on a daily basis, and how each level managed the cyber risk and collaborated with each other to ensure robust governance.
- 82% of companies described having internal policies with regards to cyber and data security as part of their risk mitigations (2025: 80%).
- 94% of companies mentioned internal controls in place as a mitigating factor in relation to cyber risk (2025: 92%) and 46% of companies also disclosed improvements in these internal controls during the year (2025: 30%) – this may be linked in some cases to the work being performed in preparation for Provision 29 of the UK Corporate Governance Code (see section 2).

Figure 6. External frameworks used by FTSE 100



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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

A majority of the FTSE 100 are continuing to improve their cyber security and data protection programmes. 46% of companies mentioned applying an external framework for their cyber security (2025: 33%). 15% of companies stated that their information security policies and compliance are in line with both NIST/NIS2 frameworks and ISO 27001 or other certifications. 17% reported only that cyber and IT policies are in compliance with NIST or NIS2 frameworks, or that they assessed and benchmarked their management against those. 14% mentioned only that their cyber security governance is aligned with ISO 27001 or other certifications.

8 companies mentioned 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, which is an increase compared to only 1 company that cited it last year. One company mentioned that upon receiving the letter from the Government outlining the Cyber Governance Code of Practice and its recommendations, the board got updates on the how the company aligned with the code. The board asked for the inclusion of this topic in the agenda every half year. Another company's board reviewed how the company followed the principles of the Cyber Governance Code of Practice and signed up to the National Cyber Security Centre's Early Warning service. The board also ensured the company required their vendors to comply with cyber security standards, in this case Cyber Essentials.

The number of companies providing training sessions/assessments, including deep-dive sessions, to their employees and the boards is also increasing. 81% of companies mentioned delivering staff training on cyber or data risk during the year, up from 70% in 2025. Our 2026 survey found that this year only 14 companies expressed their concerns regarding cyber risk arising from their employees (2025: 24 companies). However, offsetting this, more companies emphasised the importance of raising employees' awareness of cyber threats, especially phishing, and the ways to protect themselves from those. As part of the training exercises, several of the FTSE 100 described the delivery of cyber security awareness training or programmes during the year to promote a strong security culture across the company. Some companies also delivered specific AI training to their employees in various topics such as prompt engineering and ethical or responsible AI use, including practical applications, for example, utilising AI in financial reporting and AI-driven solutions in business operations. The forms of training described varied between companies but often included email phishing training activities, crisis simulation exercises and awareness tests.

29% of the FTSE 100 specifically mentioned cyber or data risk training delivered to the board during the year, up from 22% in 2025. Boards updated their cyber knowledge about external trends, regulatory developments, practical cyber risk governance, and AI via specific sessions with external experts, or with the companies' Chief Information Security Officer (CISO) and other internal professionals.

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

40% of the FTSE 100 cited penetration testing as a mitigating factor (2025: 44%) and 29% of companies mentioned vulnerability testing (either internal or external) as a mitigation against cyber attacks (2025: 41%). 13% of companies 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.

Our survey observed a significant increase in the number of companies citing external assurance/reviews and other external supports as part of their mitigation strategies (2026: 60; 2025: 26). 32 companies mentioned having external parties reviewing or evaluating the quality of their cyber security risk management (2025: 30). Companies engaged external expertise in a variety of areas, such as identification of cyber threats, system testing, business continuity testing and management, assessment of the effectiveness of their cyber security defences and external benchmarking exercises.

We identified an increase in the number of the FTSE 100 disclosing contingency plans, crisis management or disaster recovery plans as a mitigation for cyber risk (2026: 85; 2025: 73). Consistent with last year's survey, 22 companies mentioned testing their plans during the year (2025: 24) and 9 companies further cited board involvement in evaluating these business continuity plans (2025: 11).

Only 17 companies cited having cyber insurance in place as part of their mitigations, in line with last year's finding of 18 companies. Around 20% expressed that their insurance did not cover all potential loss scenarios. A similar proportion stated that they have appropriate insurance coverage. Most did not clearly state the level of their insurance and the items covered by such insurance. Only one company said their cyber insurance included financial protection, with expanded coverage.

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

4. Are cyber security breaches well-described?

Cyber threats represent a pervasive and significant risk across all sectors. While some attacks are contained, leading to minimal operational disruption or compromise of data, other attacks may have profound repercussions, extending to financial damage, public attention and other adverse effects.

Even though 38% of the FTSE 100 identified an increase in cyber-related risk in their business environment and 96% identified cyber crime as a principal risk they were exposed to, only 11 companies disclosed that they had experienced a cyber security breach (2025: 20 companies). Only 7 out of these companies indicated whether the breach was material: two companies reported the costs resulting from the breach and we noted that those were material compared with the audit materiality (2025: none), while 5 stated that they did not experience any material security incidents.

We noted that four companies disclosed the effects of the breaches they suffered this year (2025: 3 companies). Four companies mentioned broader business disruption and one company reported disruption to manufacturing due to the incidents they experienced.

This year, three companies mentioned how they had approached remediating the breach (2025: 1 company), for example, by taking their systems offline to contain and eliminate the issue, promptly notifying impacted employees and applicable data protection authorities and engaging cyber security experts.

The majority of companies did not disclose if they had experienced any security breaches or near misses during the year. There is a possibility that the genuine extent of an entity's exposure to cyber risks may be underestimated by users of annual reports. Improved disclosures relating to material or already public incidents can enhance investor confidence by offering clear insights into the board's ownership and the remedial actions taken by management.

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

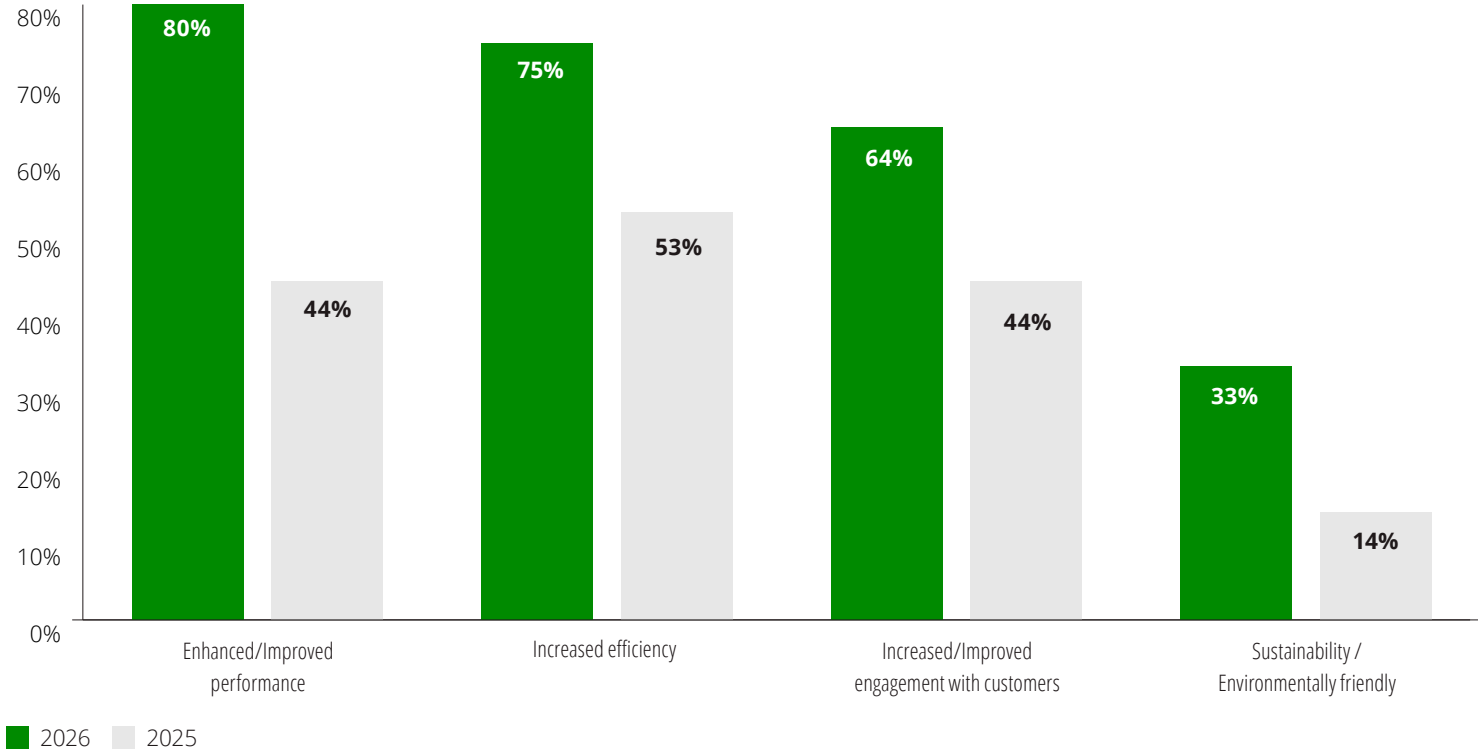
5. Are companies discussing opportunities?

We identified a significant increase in the proportion of FTSE 100 companies identifying opportunities thanks to cyber or digital investments, from 76% in 2025 to 92% this year.

Enhanced performance (80%, up from 44% in 2025) and **increased efficiency** (75%, up from 53% in 2025) were the most frequently cited opportunities, often linked to the implementation of AI tools and platforms. Several healthcare companies highlighted the benefits of AI in accelerating innovation and improving outcomes. One company recognised that advanced technologies, including AI, had improved the precision, speed and success rates of delivering medicines and vaccines to patients.

Companies in the IT services and telecommunications sectors highlighted AI's potential to demonstrate practical

Figure 7. Top opportunities identified by FTSE 100 companies



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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

use cases, helping to establish credibility with customers. Others noted that generative AI solutions can leverage multiple fine-tuned large language models using high-quality, trusted content, extensive datasets, deep customer understanding and industry expertise to improve response quality and deliver more personalised insights. This, in turn, can help customers make critical decisions with greater confidence. Banking and financial services companies also highlighted AI's ability to improve employee productivity and enhance the customer experience, for example by reducing the average time taken to resolve customer queries.

Improving customer engagement was identified as an opportunity by 64% of companies, up from 44% in 2025. Companies in the consumer sector highlighted AI's ability to use data-driven insights to develop customer-centric tools and solutions, offer more tailored products and services, and help frontline staff respond to customer queries more accurately and efficiently. One energy company expanded its fleet services by providing a comprehensive suite of fuel, energy, payment and digital solutions. This enabled the company to leverage its data, network reach and strategic partnerships to meet evolving fleet requirements and deliver greater convenience for customers.

A total of 33% of FTSE 100 companies identified sustainability-related opportunities through the use of innovative technologies and solutions, a significant increase from 14% in 2025. One pharmaceutical and biotechnology company implemented new automation and robotics technologies to increase production efficiency and reduce material waste. Another company specialising in safety equipment developed a laser-induced breakdown spectroscopy system that improves the filtering and recycling of aluminium scrap, helping to reduce energy consumption and carbon emissions. A medical equipment and services company enhanced its digital product sustainability database with improved carbon-intensity data and analytics, enabling more accurate emissions profiling and helping to reduce the environmental impact of its products.

Other opportunities identified by more than 10 companies related to improvements for competitive advantage (2026: 27 companies; 2025: 19), value creation (2026: 25; 2025: 18), improved information exchange (2026: 14; 2025: 11), and enhanced physical safety or IT security (2026: 13; 2025: 5).

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

Appendix 1: Examples of cyber risk and governance disclosure

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
BT Group plc	Examples of quantum technologies that operators and industry leaders are exploring. Discussion of effect of quantum computing on current encryption methods.	Page 17 and page 60 Annual report
Barclays PLC	Detailed reporting on the governance of data privacy, data security and operational resilience. Detailed description of the drivers of cyber threats, the risks from new and emergent technology, and the risk related to data management, information protection and AI. Discussion of cyber security in a separate sub-section in Section 172(1) Statement.	Page 219 Page 236 Page 42 Annual report
International Consolidated Airlines Group S.A.	Disclosure regarding cyber breaches experienced by third parties and the impact on the group.	Page 78 Annual report (IAG Annual report and Accounts 2025)
St. James's Place plc	Disclosure of a cyber incident at a fourth party used by one of the company's key sourcing partners.	Page 83 Annual report
Haleon plc	Disclosure highlighting the roll-out of the security culture programme, including a group-wide awareness campaign and enhanced security training.	Page 73 Annual report
Persimmon Plc	Disclosure within Section 172(1) Statement that the Government wrote a letter to all major UK companies in 2025 regarding 'making cyber security a board responsibility'.	Page 57 Annual report
GSK plc	Disclosure of opportunities to enhance performance with AI. Disclosure of sustainability opportunities using new automation and robotics.	Page 9 Page 46 Annual report

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

Appendix 2:
Cyber security pledge and Cyber Governance Code of Practice

Cyber security pledge

The UK has been experiencing an increase in hostile cyber activity, which is becoming more intense, frequent and sophisticated. This inflicts considerable financial and societal harm upon UK enterprises and citizens. The UK government sent a ministerial letter on cyber security to all FTSE 100 and FTSE 250 and a number of leading UK companies in October 2025, outlining a commitment to enhance cyber resilience in the UK.

The government has advanced its cyber security approach by setting out the Government Cyber Action Plan in March 2026 and then a voluntary Cyber Resilience Pledge in July 2026.

The voluntary Cyber Resilience Pledge serves to counter the increasing cyber threats faced by businesses. This initiative builds on previous recommendations and requires signatory organisations to undertake three core actions:

- Make cyber a board responsibility: Boards must implement the Cyber Governance Code of Practice and ensure all members complete annual NCSC Cyber Governance Training within three months and then on an annual basis.
- Sign up to Early Warning: Companies are to register for the Early Warning service within one month of signing the pledge.
- Require Cyber Essentials across supply chains: Organisations must register for the Cyber Essentials Supplier Check Tool within two months of signing the pledge, conduct a thorough audit of Cyber Essentials coverage across their supply chain, which is presented and discussed by the board, and adopt a risk-based approach to its implementation, with board oversight.
- Further details on the Cyber Resilience Pledge can be found **here**.

Cyber Governance Code of Practice

In April 2025, the Government published the Cyber Governance Code of Practice to assist boards with their governance of cyber security risks. The Cyber Governance Code of Practice is specifically developed for the boards and directors of both public and private organisations. Its purpose is to provide practical guidance to the boards and directors with regard to the cyber risk governance on high-level oversight and accountability. There are five key areas as follows.

- **Risk management** – Critical technology processes, information and services are identified, prioritised and agreed. Cyber security risks are integrated into the enterprise risk management and internal controls, while senior ownership of cyber security risks are agreed. Cyber security risk appetite is defined and clearly communicated. There is an action plan to meet the risk expectations. Regular, proportional risk assessments of suppliers are performed and the entity is resilient to the cyber risk arising from its supply chain. Cyber risks are regularly assessed and mitigating actions consider changes in the organisation, technology, regulations or wider threat landscape.

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

Appendix 2:
Cyber security pledge and Cyber Governance Code of Practice

- **Strategy** –The organisation develops a cybersecurity strategy aligned with and embedded within the wider organisational strategy. The strategy is in line with the defined risk appetite of the organisation, meets regulatory requirements, and accounts for changes. Resources are allocated effectively to manage the agreed cyber security risks. Cyber strategy is delivered effectively and achieves its intended outcomes.
- **People** – The organisation promotes a cyber security culture that encourages responsible behaviours and accountability at all levels and is aligned with the organisation's strategy. Clear policies are designed to support such culture. Board members and directors undertake training to ensure their own cyber literacy and take responsibility for the security of the data and digital assets used by the organisation. The organisation has effective cyber security training, education and awareness programs and could use appropriate metrics to assess that.
- **Incident planning, response and recovery** – A comprehensive incident response and recovery plan for cyber incidents impacting business critical technology processes, information and services is developed, maintained, and regularly tested (at least annually), with the involvement of relevant internal and external stakeholders. Responsibilities for individual regulatory obligations and communication during incidents are clearly defined. A structured post-incident review mechanism is in place to extract valuable insights, which are subsequently leveraged to refine and enhance future strategies and recovery plans.
- **Assurance and oversight** – A cyber governance framework is implemented and fully integrated into the organisation's overarching governance structure. This framework clearly defines roles and responsibilities, including explicit ownership of cybersecurity at both executive and non-executive director levels. Formal reporting is delivered regularly (at least quarterly), with suitable metrics to track and agree tolerances. Regular two-way dialogue with relevant senior executives, including the Chief Information Security Officer or equivalent, is established. Cyber security considerations are integrated and aligned with existing internal and external audit and assurance mechanisms. Senior executives are aware of relevant regulations, and of the best practice contained in the other Cyber Security Codes of Practice.

Further details can be found at Strengthening cyber resilience: the UK's Cyber Governance Code of Practice.

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

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

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

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

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 risk and governance disclosure
Appendix 2: Cyber security pledge and Cyber Governance Code of Practice
Contacts
The Deloitte Centre for Corporate Governance

Deloitte.

This document is confidential and it is not to be copied or made available to any other party. Deloitte LLP does not accept any liability for use of or reliance on the contents of this document by any person save by the intended recipient(s) to the extent agreed in a Deloitte LLP engagement contract.

If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities).

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP's affiliate (Deloitte Management Services Limited) is a shareholder in Deloitte EMEA BV (Deloitte EMEA). Deloitte EMEA is a member firm of Deloitte Touche Tohmatsu Limited (DTTL). DTTL and Deloitte EMEA do not provide services to clients. Services may be provided by other Deloitte entities within the global network of member firms, each of which are separate and independent legal entities. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2026 Deloitte LLP. All rights reserved.

Designed by CoRe Creative Services. RITM257446