Deloitte.

Cyber risk and governance reporting in the UK: Renewed focus on the impacts of cyber risk

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Foreword by Claire Faulkner 3

1. Do companies describe cyber risk clearly? 5

2. How do boards report their involvement? 8

3. Are mitigating activities well explained? 10

4. Are cyber security breaches well-described? 12

5. Are companies discussing opportunities? 13

Appendix 1: Regulatory developments – new SEC Rule 14

Appendix 2: Examples of cyber disclosures 15

Contacts 16

The Deloitte Centre for Corporate Governance 17

Survey sample
In this survey we have looked at the most recent annual reports of the FTSE 100 which were published by 30 June 2024.

Foreword by Claire Faulkner

Do companies describe cyber risk clearly?

How do boards report their involvement?

Are mitigating activities well explained?

Are cyber security breaches well-described?

Are companies discussing opportunities?

Appendix 1:
Regulatory developments – new SEC Rule

Appendix 2:
Examples of cyber disclosures

Contacts

The Deloitte Centre for Corporate Governance

Foreword by Claire Faulkner

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 the users of annual reports informed in this important area.

The risks associated with technology have never been more at the forefront of boards' minds. In July, a software patch led to an estimated $5.4 billion cost to Fortune 500 entities alone,[1] with affected parties globally including banks, governments, airports and energy companies. Although the publicity made it seem otherwise, in fact it was a relatively low number of systems that were affected overall – however, some of these systems were embedded in important infrastructure.

This has led to a new appreciation by many companies of the vulnerabilities inherent in a global, connected environment with many potential "single points of failure" and of the benefits of robust stress testing and scenario planning. There is huge concentration in IT infrastructure – for example, three companies account for two-thirds of the cloud provider market.[2]

It is also a challenge for governments as technology and indeed cyber attacks do not respect physical borders, increasing the complexity of any regulatory action to minimise the risk of future global outages.

This complexity is underlined by a new white paper, Closing the cyber risk protection gap, published by two major insurers in September 2024 and calling for the public sector – i.e. governments – to address the insurance gap for catastrophic losses related to matters such as war and infrastructure failure.

Certain new regulations have nevertheless been passed in 2024: in August, the EU AI Act came into force, and in early September the US, EU and UK all signed the Council of Europe's convention on AI, with other countries to follow.

In 2023, the SEC finalised its Rule relating to cybersecurity risk management, strategy, governance, and incidents disclosures by its registrants. This took effect for US-registrant companies in our sample with a 15 December 2023 or subsequent year end and has had a particular impact on the quality of disclosure around the governance of cyber risk for those companies in our survey (see Appendix 1 for details of the Rule). This does not yet, however, appear to have had the effect of raising standards of disclosure on the governance of cyber risk across the FTSE 100 in general – change may well depend on how much investors value the new level of disclosure.

1. Cyber insurers are winners from the biggest ever IT outage', Financial Times, 13 August 2024.
2. Lessons from the global IT outage', Financial Times, 23 July 2024.

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

Foreword by Claire Faulkner

Boards have also started to include additional reporting on the opportunities and risks posed to their strategy and business models by generative artificial intelligence (AI) capability – AI that creates original content that would previously have taken human skill and expertise to create. Deloitte is conducting ongoing research in this area and some of these findings are shared in the course of this report.

Our survey included the annual reports of all FTSE 100 companies. In summary, we saw:

- 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 relating to the year, therefore providing meaningful information to investors and other stakeholders.
- Boards and board committees are increasingly educating themselves about the cyber threat and challenging management to implement stronger controls, focusing on technology capabilities, education of employees and engagement with suppliers, particularly cloud suppliers.
- Generally, companies are doing a lot in this area and should take credit for what they are doing. This year, we noted a significant increase in the number of companies reporting on their use of penetration testing as part of their arsenal of mitigating activities.
- Finally, if company disclosure does not look strong enough after reporting key risk management activities, boards should challenge whether enough is being done to manage cyber risk.

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. And don't forget you can join us at the Deloitte Academy where cyber and tech trends, including deep-dives on Generative AI, are frequently on the agenda.

Claire Faulkner
Deloitte Academy Governance Chair
December 2024

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

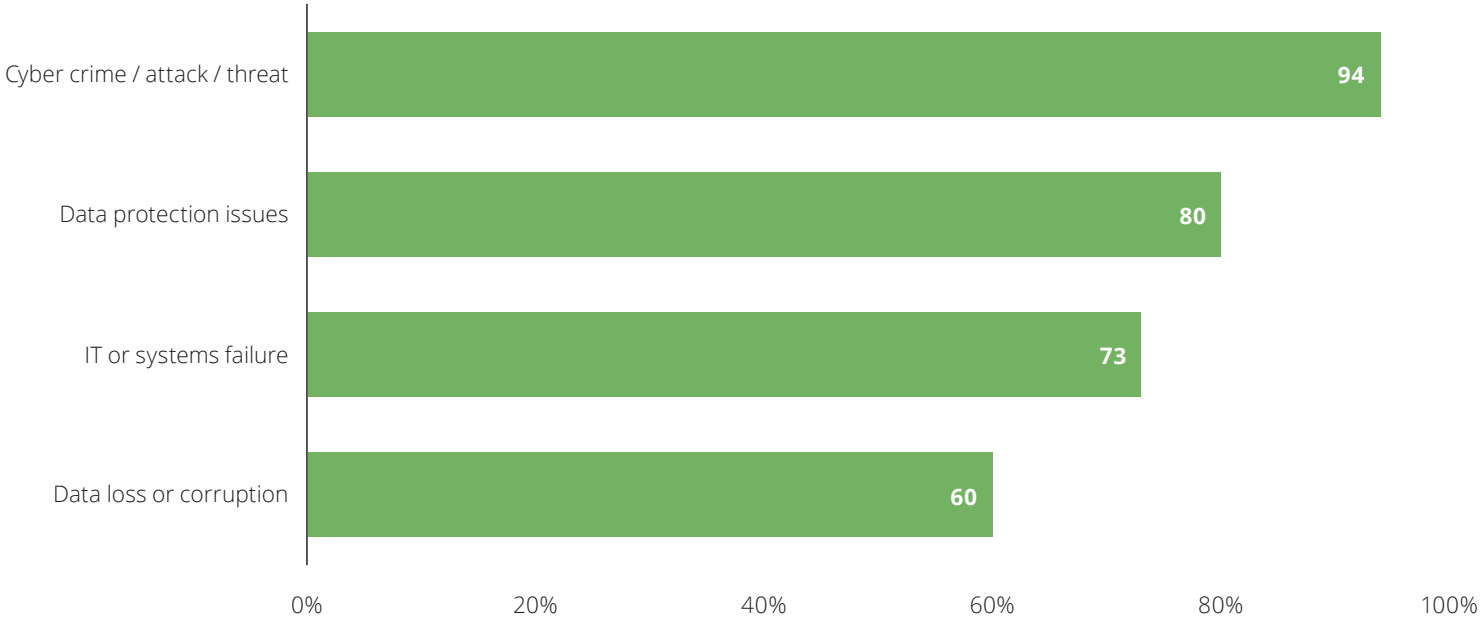
1. Do companies describe cyber risk clearly?

The focus on cyber risk has continued with 99% of companies reporting one or more elements of cyber risk as a principal risk (2023: 97%). 19 companies also disclosed elements of cyber risk, data privacy or technology disruption as an emerging risk and 39 companies identified AI as an emerging risk to their business.

Companies described four main types of cyber risk as part of their principal risks: cyber crime, data protection (the risk of theft or misappropriation), IT or systems failure and data loss or corruption. The better disclosures discussed all of these. 24% of companies also cited AI as part of cyber risk.

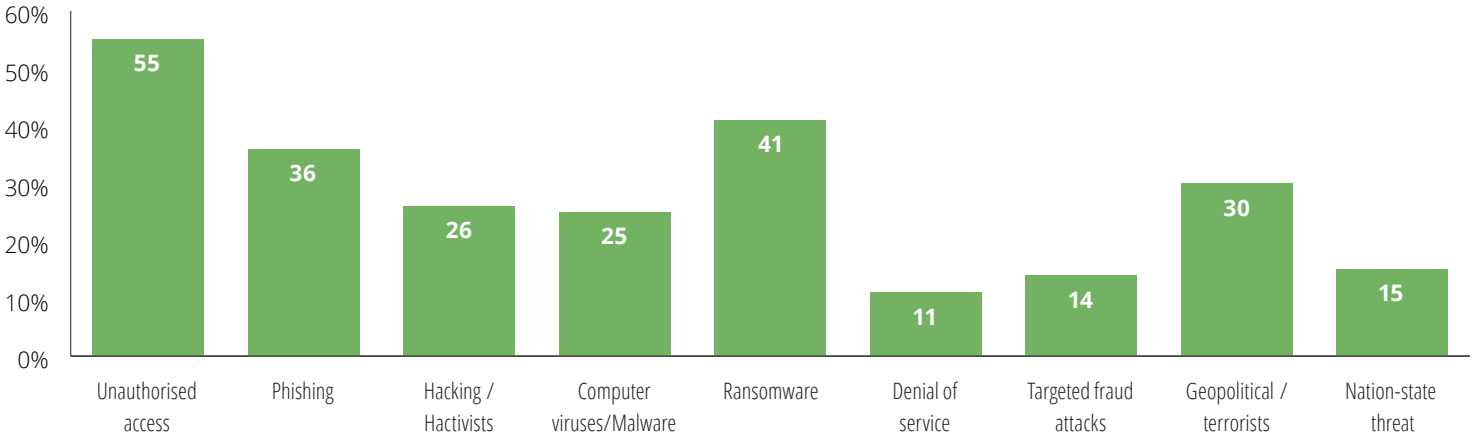
31% of companies identified an increase in risk related to cyber and IT. Whereas last year the main rationale for increased risk was associated with global instability, this year we noted a trend for companies to cite the risk of cyber attacks increasing due to the use of AI.

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



Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

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



61% of companies grouped principal risks into categories in their annual reports. Cyber risk was generally shown as an operating risk (38 companies). Companies which recognised cyber risk and data risk separately generally showed cyber as an operating risk and data as a legal or compliance risk.

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 2 shows the nature of cyber threat referenced by the 99 companies that identified one or more elements of cyber risk as an aspect of their principal or emerging risk(s).

This year, almost every company identified at least one specific type of cyber threat they faced.

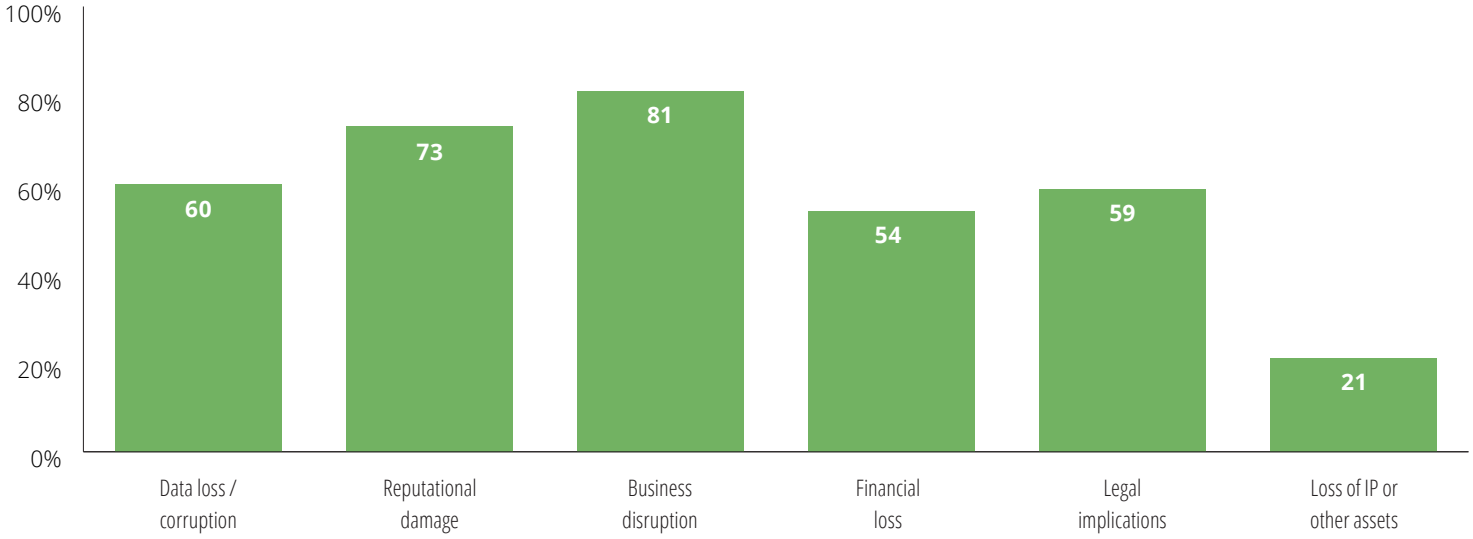
"The more specific the description of the nature of the cyber crime companies have experienced or believe they are exposed to, the more specific the description of their management or mitigation."

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

This year, companies provided more detail regarding the potential impacts these risks could have on their business. The most common impacts disclosed remained the same, although business disruption at 81% (2023: 74%) had overtaken reputational damage at 73% (2023: 76%).

Compared to last year, a similar number of companies reported the impacts of data loss or corruption (60%) and potential legal implications (59%) which include the risk of penalties arising from the inability to meet contractual obligations or other regulatory non-compliances. The number of companies mentioning the impact of financial loss had fallen noticeably this year at 54% (2023: 64%).[3]

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



3. Financial loss has been classified as distinct from theft or fraud leading to funds being misappropriated.

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

We looked at where companies disclosed cyber risk or cyber security in the annual report and identified the following key movements in the year:

- 11 companies had specifically called out cyber in their **Section 172(1) statement** as a topic of engagement with one or more of their key stakeholders – 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.
- 30 companies also mentioned cyber as part of the **sustainability disclosures** in the strategic report.
- Over half of companies this year identified the impact of cyber risk on the company's ongoing viability with **cyber security scenarios** being included in the viability statement – a significant increase compared to previous years. A handful of these included **quantification** as part of the scenario, such as the time period required for remediation or the anticipated financial impact on the business.

There continues to be recognition of the threat from the wider ecosystem that companies operate in: cyber criminals can use third parties to gain unauthorised access where a supplier or customer interacts with a company's system – sometimes known as "fourth party risk". This area is also covered by the new SEC Rule, which requires disclosure of the processes for identifying, assessing and managing material risks, including third party threats (see Appendix 1 for details). 42 companies disclosed third party risk as an aspect of their principal risk(s) this year. Ten of these companies cited cloud as a particular area of focus.

There was a fall this year in the number of companies explicitly drawing out the risk from company employees, at 23% (2023: 32%).

A handful of companies continued to include key risk indicators (performance measures to monitor risk) in their cyber principal risk(s). Examples included the number of phishing incidents and targets for patching IT breaches.

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

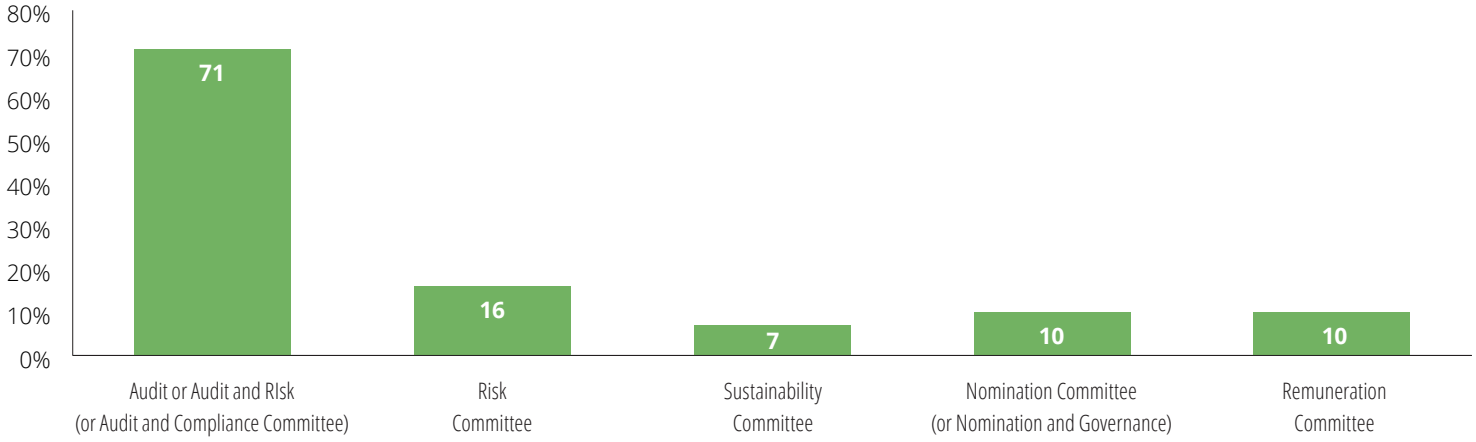
2. How do boards report their involvement?

We looked at how companies described the board's ownership of cyber risk. This year, 94% of companies mentioned cyber risk in their corporate governance disclosures (up from 87% last year). We focused on whether these companies indicated that the board had the expertise to guide the business through appropriate cyber risk assessments and mitigations, as well as how the board provided oversight of management.

Just over half of boards (61) reported having a director with experience in digital matters. Specialist expertise in cyber[4] was reported by 30 FTSE 100 boards and 12 disclosed a director's specialist expertise or experience in AI. Many companies clearly described the director's prior experience or certification level, allowing the reader to judge the depth of expertise on the board.

In describing their oversight, fewer boards this year reported that they or a committee had received either a report or presentation on cyber in the year, including 'deep dives' – 59% compared to 79% in 2023. Around one in five companies described where executive responsibility for cyber sits at C-suite level – most often with the CFO, CIO or CISO. One company this year attributed responsibility for cyber to a non-executive director, although several made a point of emphasising the role of their non-executive directors with cyber expertise in the oversight process.

Figure 4. Cyber mentions in committee reports



4. We have included references to cyber, information technology and information security for this assessment, including where the expertise isn't mentioned in the board member's CV but is mentioned within the nomination committee report.

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

The role of the board and management in overseeing and implementing cybersecurity governance is a disclosure required by the new SEC Rule (see Appendix 1 for details) so it is encouraging to see so many boards providing some detail on the ways they have maintained oversight during the year.

Most boards covered the topic at the audit committee or the risk committee – although there was a noticeable fall in the number of audit committees disclosing that they focused on cyber this year. Disclosures identified in the nomination committee report mostly considered the depth of board expertise in this specialist topic, often in the context of board composition and succession planning for new non-executives. We noted a small increase in the number of companies mentioning cyber in the remuneration committee report, with these mentions relating to executive director targets such as delivering on cyber security programmes.

Overall, the level of disclosure on cyber risk remains highly variable with many audit or risk committee reports simply listing cyber security in a collection of topics considered as part of risk management and internal control.

This year, we found a significant increase in companies that disclosed having a CISO or similar security role as part of the executive team – up to 42% from 30%. This increase appears largely to have been driven by the SEC Rule changes. Better disclosures described the CISO's attendance at board or committee meetings and the process by which the board is informed about cyber risk and mitigations. However, not all FTSE 100 companies that include an information security role in their senior executive structure disclose this in their annual reports.

"Better disclosures described the CISO's attendance at board or committee meetings and the process by which the board is informed about cyber risk and mitigations."

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
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.

We found that not all companies explained their processes clearly in respect of cyber and data security:

- only 54% of companies clearly described a governance process in relation to cyber risk;
- 75% described having internal policies in relation to cyber/data security within their risk mitigations – down from 84% in 2023;
- 34% mentioned improvements in internal policies in relation to cyber/data security during the year (2023: 34%); and
- 71% mentioned internal controls in place as a mitigating factor in relation to cyber risk, and just under half of these disclosed improvements in these internal controls during the year. There continues to be a lot of activity to upgrade defences.

30% of companies also mentioned an external framework for their cyber security, such as ISO 27001, the UK Cyber Essentials programme or the NIST Cyber Security Framework.

We saw an increase in the number of companies that discussed how they ensure and monitor adherence to group policies and controls by their commercial partners, suppliers and contractors, and/or what measures they have in place to protect their data and information technologies where third parties are involved – up to 28% from 16% in 2023.

Training of employees continues to be an area of focus:

- 76% of FTSE 100 companies mentioned delivering staff training on cyber or data risk during the year (down from 79% in 2023). A quarter of companies also mentioned staff training on AI during the year; and
- 30% of companies mentioned cyber or data risk training delivered to the board (up from 24% in 2023).

> "30% of companies mentioned cyber or data risk training delivered to the board."

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

There was a step-change this year in the number of companies disclosing that penetration testing was part of their arsenal of mitigating activities, at 59% (up from 35% in 2023). In addition, 32% of FTSE 100 companies mentioned some form of vulnerability testing (either internal or external) and 24% mentioned other forms of external assurance, including audits of new security systems. 29% identified another form of 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. The best disclosures described an iterative process to identifying risks, implementing mitigations and detecting and remediating flaws in controls or infrastructure.

"The best disclosures described an iterative process to identifying risks, implementing mitigations and detecting and remediating flaws in controls or infrastructure."

The number of companies that mentioned contingency plans, crisis management or disaster recovery plans as a mitigation for cyber risk remained at a similar level at 60% (compared to 58% in the previous year). 25 of the 60 companies that disclosed these plans also mentioned testing the plans during the year and eight companies further discussed board involvement in assessing these plans.

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

4. Are cyber security breaches well-described?

Only 18 companies disclosed having cyber insurance in place – this is perhaps unsurprising given continuing media discussion of the limitations of such policies and the recent white paper from major insurers calling for public sector involvement.

Almost all companies will be experiencing regular cyber attacks of some form. Fortunately, many are repelled and even where a company's defences are penetrated, these often do not result in sufficiently significant issues for them to become public knowledge, even if they are reported to the Information Commissioner.[5] Public reporting may change in time following the requirements of the recent SEC Rule (see Appendix 1).

"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."

Although many companies mentioned an increase in cyber crime in their industry, substantially fewer (13 - down from 17 in our 2023 survey) cited cyber security breaches in their organisation. Only seven companies indicated whether the breach was material and four provided some detail on how the breach had been remediated. 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.

The better disclosures explained the reputational damage as a result of the breach (two companies), the legal implications (three companies) and engagement with external cyber security professionals (one company). Two companies out of the three that referred to legal implications also mentioned data protection breaches following the cyber attack. Examples of disclosures are included in Appendix 2.

5. A personal data breach must be reported to the ICO within 72 hours if the associated accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data is likely to pose a risk to people's rights and freedoms.

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

5. Are companies discussing opportunities?

88% of FTSE 100 companies described opportunities relating to digital or cyber in addition to highlighting risks.

Strategy examples given included moving to cloud-based platforms and big data, alongside more generic references to "investment in innovation". Examples of short- to medium-term investment included introduction of new AI platforms and products to decarbonise vehicles or improve supply chain operations, resource efficiency, and new or improved ERP systems. Opportunities tended to be industry-specific, such as advances in drug discovery or the move to biologics.

> "Opportunities tended to be industry-specific, such as advances in drug discovery or the move to biologics."

Opportunities from digital development cited frequently by companies included:

- Performance enhancement (49%) – for example, using technology to respond more quickly or accurately to customer queries.
- Sustainability improvements (37%) – 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 from 64% in 2023 – it is not clear whether this is due to the implementation of these new technologies or reduced ambition for this type of improvement.
- Customer engagement improvements (61%) – for example, to target particular audiences or increase effectiveness of engagement with consumers (plus measuring the engagement).

Other benefits cited by more than 10% of companies included improved engagement with suppliers, improved business efficiency and competitive advantage.

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

Appendix 1: Regulatory developments – new SEC Rule

In 2023, the SEC finalised its Rule relating to cybersecurity risk management, strategy, governance, and incidents disclosures by its registrants. This took effect for US-registrant companies in our sample with a 15 December 2023 or subsequent year end.

In summary, registrants are now required to disclose the following information relating to risk management, strategy, and governance of cybersecurity threats in their annual reports:

Risk Management and Strategy	The processes for identifying, assessing, and managing material risks relating to cybersecurity threats. This disclosure should include, but is not limited to: • whether (and how) the registrant's cybersecurity processes have been integrated into the overall risk management framework • whether (and how) any assurance has been provided, or third parties have been engaged as part of this process • whether the registrant has processes in place to oversee and identify cybersecurity threats from third-party providers.
Governance	The role of the board and management in overseeing and implementing cybersecurity governance as follows: **Board's disclosure:** • how the board oversees the risks arising from cyber threats and if applicable, the delegated committee responsible for overseeing these risks • how the board and/or its delegated committee are informed about cyber-related risks. **Management's disclosure:** • whether management or delegated committees are responsible for assessing and monitoring cyber risks, including their relevant expertise and the processes followed • whether and how management reports cybersecurity matters to the board or delegated committees of the board.

In addition, registrants are required to submit a disclosure regarding the nature, scope, timing and impact of material cybersecurity incidents on a separate SEC form within four business days from when the event has been determined to be material.

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

Appendix 2: Examples of cyber risk and governance disclosure

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

Company	Illustrative example	Page and link
Barclays Plc	Detailed and clearly written description of cyber risk – note that data risk and mitigations are described separately	p266-7 Annual report
Haleon plc	Clear summary in one place of risk, governance and mitigation activity, including experience of key staff	p21 Annual report
Pearson plc	Disclosure of board skills matrix, separated into core capabilities and supplemental capabilities	p90 Annual report
Prudential plc	Clear disclosure regarding tailored mitigating actions on ransomware; governance over technology development and associated risk; description of breach and impact; metrics on cyber security incidents	p67-68; p116 Annual report
RS Group	Managing risks in action section on cyber risk	p33 Annual report
Spirax Group	Quantified scenario of a cyber attack in viability statement; description of cyber-related executive director targets	p42; p165 Annual report

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

Contacts

Cyber risk

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

Mark Ward
Tel:+44 (0) 20 7007 0670
Email: mdward@deloitte.co.uk

Technology and digital risk

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

Foreword by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
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 by Claire Faulkner
Do companies describe cyber risk clearly?
How do boards report their involvement?
Are mitigating activities well explained?
Are cyber security breaches well-described?
Are companies discussing opportunities?
Appendix 1: Regulatory developments – new SEC Rule
Appendix 2: Examples of cyber disclosures
Contacts
The Deloitte Centre for Corporate Governance

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

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 is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please click here to learn more about our global network of member firms.

© 2024 Deloitte LLP. All rights reserved.

Designed by CoRe Creative Services. RITM1884337