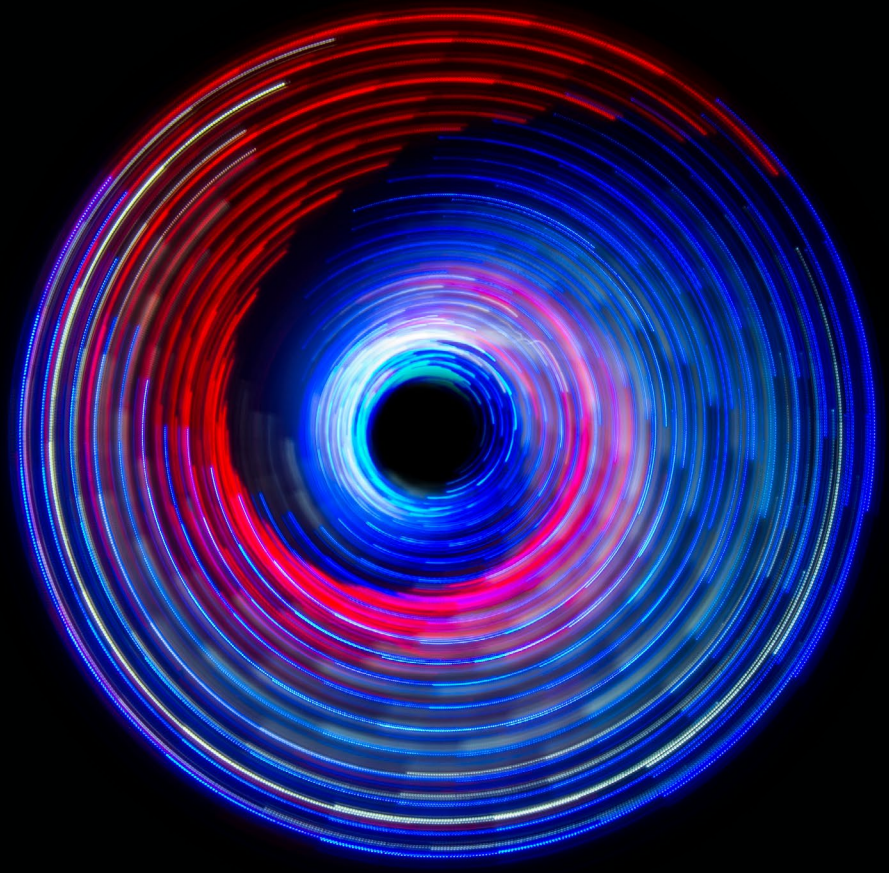
Deloitte.



Cyber risk and governance reporting in the UK: a changing landscape

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Foreword by Claire Faulkner

1.Do companies describe cyber risk clearly?

2.How do boards report their involvement?

3.Are mitigating activities well explained?

4.Are cyber security breaches well-described?

5.Are companies discussing opportunities?

Appendix 1: Regulatory developments – new SEC Rule

Appendix 2: Examples of cyber disclosures

Contacts

The Deloitte Centre for Corporate Governance

In this survey we have looked at the most recent annual reports of the FTSE 100 which were published by 30 June 2023.

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.

Technology is pervasive in our lives. We all depend on the privacy, integrity and accessibility of the data held within information systems. Its importance is reinforced by the size of regulatory fines able to be levied globally with regard to data breaches.

Since our last report, boards are grappling with a new challenge and opportunity posed to future business and risk models by generative artificial intelligence (AI) capability – AI that creates original content that would previously have taken human skill and expertise to create. As Generative AI became prevalent in public consciousness and media during 2023, information in the annual reports in our survey is naturally limited, however Deloitte has published some initial findings in a Corporate Reporting Insights survey and we anticipate there may be more widespread disclosures for 2023 year ends.

There have also been regulatory developments when it comes to disclosure. During July the US Securities and Exchange Commission (SEC) published its Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (the SEC Rule). This follows a rush of guidance in 2022 from the FRC's Financial Reporting Lab and has been published as work is ongoing from the EU and the UK Government regarding cyber and AI disclosure requirements.

Throughout this report we highlight some of the relevant SEC Rule requirements and how the FTSE 100 measure up based on existing reporting practices.

In summary, our FTSE 100 annual report review shows:

- The vast majority of 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.
- 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 have been pleased to see an increase in companies reporting that work has been done on cyber security policies and controls.
- Finally, if company disclosure does not look strong enough after taking credit for what the company is doing already, it is worth enquiring if enough is being done to manage cyber risk.

We hope you find this review useful. Do get in touch with your Deloitte partner, the cyber risk and crisis management specialists whose names are in the contact list 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 a regular deep-dive on Generative AI, are frequently on the agenda.

Claire Faulkner
Deloitte Academy Governance Chair November 2023

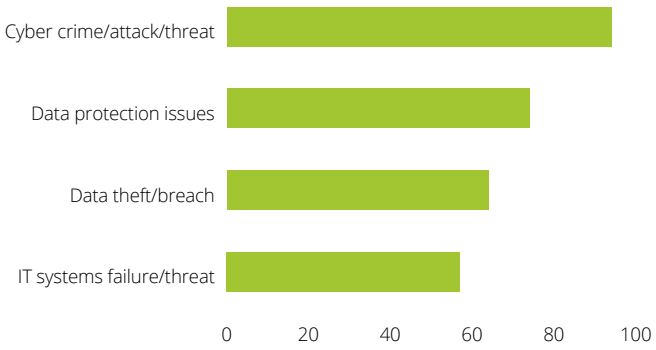
1. Do companies describe cyber risk clearly?

Despite changes to the constituents of the index, the focus on cyber risk has continued with 97% of companies reporting one or more elements of cyber risk as a principal risk, the same proportion as last year. Some of these companies also disclosed elements of cyber risk as an emerging risk.

Companies described four main types of cyber risk: cyber crime, data protection (the risk of data loss), data theft or misappropriation and IT or systems failure. The better disclosures discussed all of these. 11% of companies also cited AI as part of cyber risk.

41% of companies identified an increase in risk around cyber and IT.

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



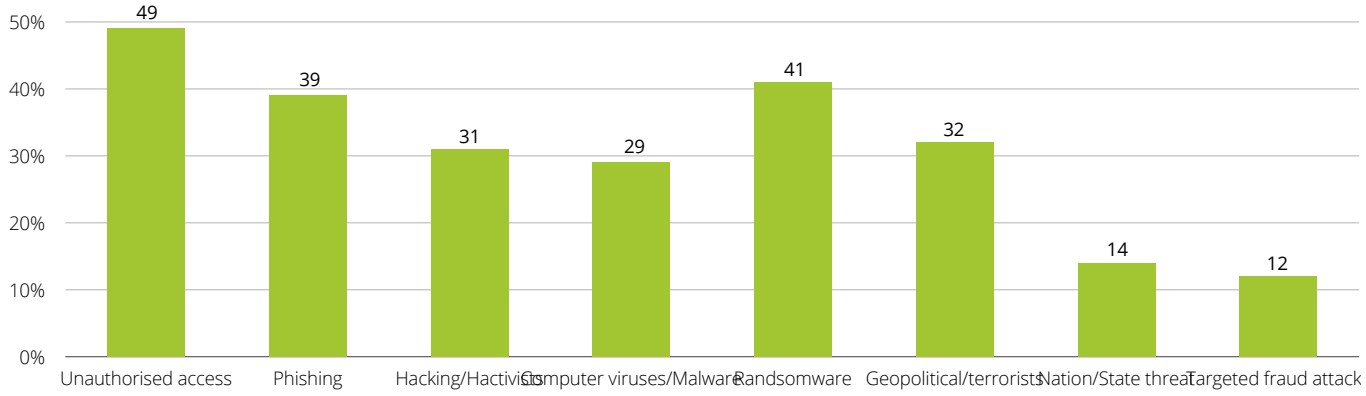
Some companies recognised cyber risk and data risk separately, with cyber generally shown as an operating risk and data as a legal or compliance risk.

71% of companies categorised risks in their annual reports. Cyber risk was generally shown as an operating risk (40 companies) or a reputational risk (8 companies).

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 the management or mitigation they apply (see section 3), conveying focus and confidence. Figure 2 explains the nature of cyber crime mentioned by the 97 companies that identified one or more element of cyber risk as an aspect of their principal or emerging risk(s).

We noted a step-change this year in that more than half of companies now called out the specific types of cyber crime they faced. Particularly notable increases were seen in the discussion of the risks of unauthorised access (up from 29 to 49), ransomware (up from 33 to 41), and geopolitical or terrorist threats (doubled from 16 to 32).

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



On the other hand, companies were more reticent this year in describing impacts. Those most commonly mentioned remained the same, although reputational damage at 76% had overtaken disruption to operations (74%) and financial loss (64%)[1] compared to last year. The majority also mentioned data loss or corruption and legal implications, including penalties arising from the inability to meet contractual obligations or other regulatory non-compliances.

Just over half of companies that mentioned reputational damage also described an impact on customers which could result in loss of customer and investor confidence or trust.

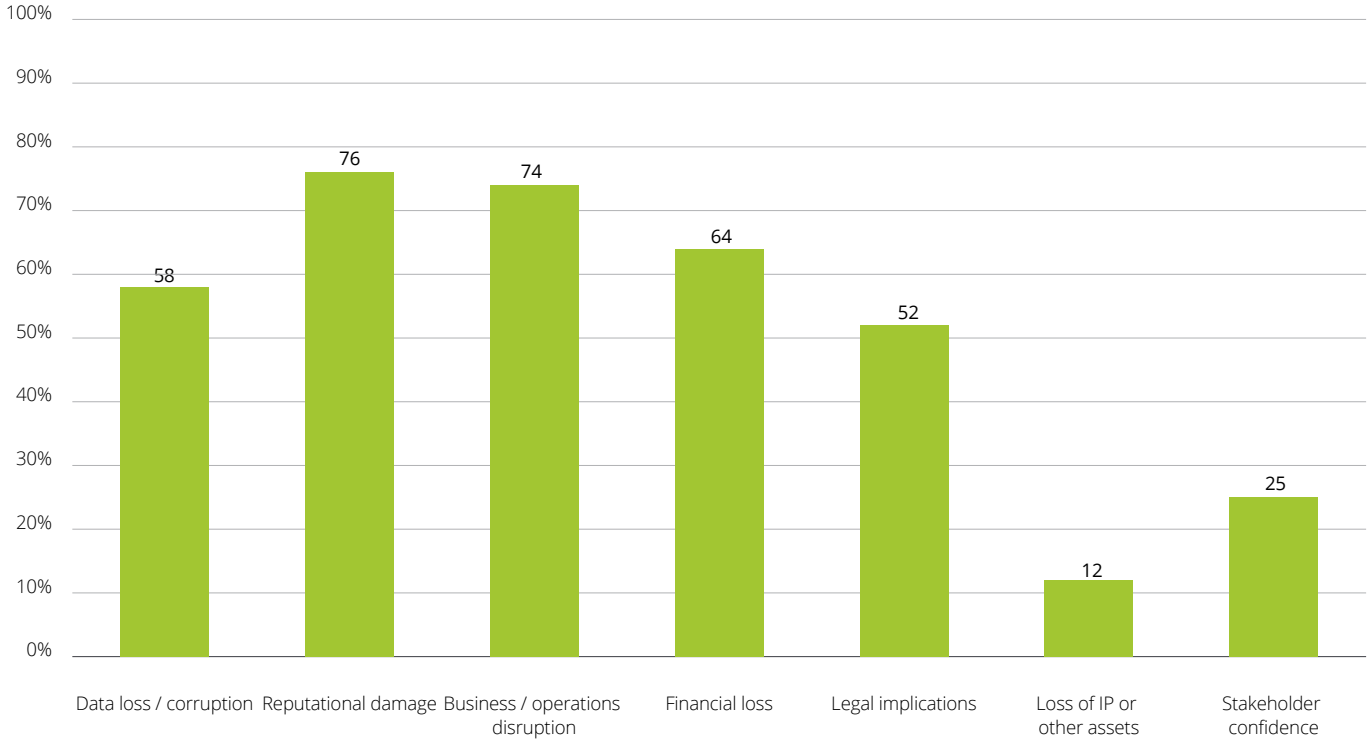
Some disclosures also considered the impact of cyber risk on the company's ongoing viability with inclusion of possible cyber security scenarios in the viability statement. One company had prepared a disclosure it described as a resilience statement and specifically evaluated the impact of cyber risk over the medium term.

There is increasing recognition of the threat from the ecosystem 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. Just under half (49%) of companies disclosed third party risk as an aspect of their principal risk(s) – slightly higher than last year.

Technology transition is also a risk: 37% of companies highlighted the risk of not keeping up with technology changes or failure to successfully implement new technologies. This year, 25% made the link between technology transformation and cyber risks – up from 17% last year.

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

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



Compared to technology transition, fewer companies mentioned the risk from company employees, which remained the same as the previous year at 32%.

Metrics continue to be in short supply, although the move towards disclosure in line with the TCFD recommendations and adoption of SASB sustainability metrics has led to a notable increase in disclosure of metrics or targets, although from a very low base. This year, 21 companies mentioned a cyber-related key performance indicator (KPI), metric or target, up from only five companies last year. The most common metric was number of cyber attacks or breaches, with other examples including the number of digital visits or technology uptime availability (proportion of time technology platforms were available to customers).

13 companies included key risk indicators (performance measures to monitor risk) in their cyber principal risk(s) – compared to 3 last year. Examples included the number of phishing incidents and targets for patching IT breaches.

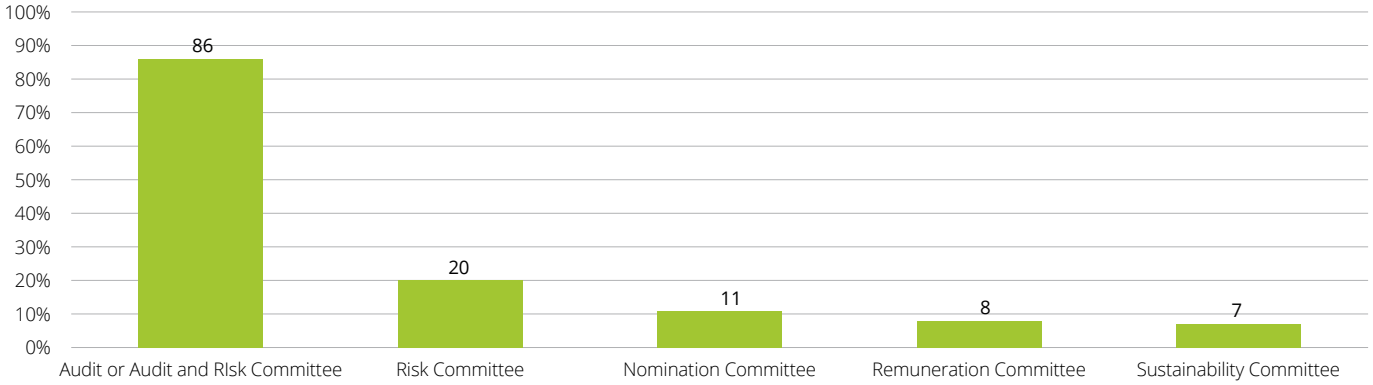
2. How do boards report their involvement?

We looked at how companies described the board's ownership of cyber risk. We focused on whether the 87% of companies that mentioned cyber risk in the corporate governance disclosures suggested the board had the expertise to guide the business through appropriate cyber risk assessments and mitigations, as well as how the board provides oversight of management.

Just over half of boards (52%) reported having a director with experience in digital matters. Specialist expertise in cyber[2] was reported by one in four (24%) FTSE 100 boards and 6% disclosed a director's specialist expertise in AI. 42% of 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, 79% of boards reported that they or a committee had received either a report or presentation on cyber in the year, including 'deep dives' – a notable increase from 61% last year. Around one in ten companies also described where executive responsibility for cyber sits at board level – most often with the CFO. Notably, two companies also attributed responsibility for cyber to a non-executive director. The role of the board and management in overseeing and implementing cybersecurity governance is a requirement of the SEC Rule so it is encouraging to see so many boards disclosing how they have maintained oversight during the year.

Figure 4. Cyber mentions in committee reports



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

Most boards covered the topic at the audit committee or the risk committee. Disclosures identified in the nomination committee mostly considered the depth of board expertise in this specialist topic, often in the context of seeking new non-executives.

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 describing who takes responsibility for cyber risk, with well over half attributing responsibility to an individual or team below board level.

Although only 30% of companies disclosed having a CISO or similar security role as part of the executive team, this is likely to understate the number of companies that include an information security role in their structure. Last year for instance, around half of companies mentioned a CISO and it seems more likely that they have not been mentioned in this year's annual report than that the need for the role has declined suddenly. The 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.

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 these clearly:

- 84% described having internal policies in relation to cyber/data security within their risk mitigations, with 34% of all companies mentioning improvements in these policies during the year.
- 79% mentioned internal controls in place as a mitigating factor in relation to cyber risk, and the majority of these disclosed improvements in these internal controls during the year. Clearly there is a lot of activity to upgrade defences.

Only 16% of companies 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.

Training of employees continues to be an area of focus:

- 79% of FTSE 100 companies mentioned delivering staff training on cyber or data risk during the year (down from 85%).
- Only one in four companies (24%) mentioned cyber or data risk training delivered to the board (down from 30%).

25% of FTSE 100 companies mentioned some form of vulnerability testing, 35% mentioned penetration testing and 22% mentioned other cyber risk testing performed during the year. The best disclosures described an iterative process to identifying risks, implementing mitigations and detecting flaws.

This is also a requirement of the new SEC Rule, which requires detail of the processes for identifying, assessing, and managing material risks, including assurance obtained.

There was a noticeable fall in the number of companies that mentioned contingency plans, crisis management or disaster recovery plans as a mitigation for cyber risk, down to 58% from 80% in the previous year. Over half of the companies that disclosed these plans also mentioned testing the plans during the year and six companies further discussed board involvement in assessing these plans. We expect that some companies did not take credit for having suitable plans in place or for their regular testing.

Only 14 companies disclosed having cyber insurance in place – this is perhaps unsurprising given recent media discussion of the limitations of such policies.

4. Are cyber security breaches well-described?

Almost all companies will be experiencing regular cyber attacks of some form. Fortunately, many are repelled and not all those that get in result in sufficiently significant issues that they become public knowledge, even if they are reported to the Information Commissioner.

Most companies mentioned an increase in cyber crime in their industry, however substantially fewer (17 - up from 12 in our 2022 survey) cited cyber security breaches in their organisation. Only eight companies indicated whether the breach was material and five explained a resultant change to policies and procedures.

The better disclosures explained the reputational damage as a result of the breach (one company), the legal implications (three companies) and business disruption suffered (two companies). Two companies mentioned data protection breaches following a cyber attack.

5. Are companies discussing opportunities?

90% of FTSE 100 companies described opportunities relating to digital or cyber.

Strategy examples given included moving to cloud-based platforms and big data. Examples of short-to medium-term investment included introduction of new AI platforms and products, and new or improved ERP systems.

Some areas companies cited frequently as opportunities related to digital development included:

- Enhancing or improving performance (49%) – for example, using technology to respond more quickly or accurately to customer queries.
- Sustainability improvements (64%) – 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.
- Improved engagement with customers (63%) – for example, to target particular audiences or increase effectiveness of engagement with consumers (plus measuring the engagement).

Other benefits cited by more than one in ten companies included improved engagement with suppliers, improved digital or cyber security and competitive advantage.

Appendix 1: Regulatory developments – new SEC Rule

In our 2022 publication "Cyber risk and governance reporting in the UK: Improvement required" we explored the SEC's proposed rule relating to cybersecurity risk management, strategy, governance, and incidents disclosures by its registrants.

In summary, registrants will be 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 will need to disclose 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.

Effective Date:

The final rule will become effective 30 days after it has been published in the Federal Register, for years ending on or after 15 December 2023, subject to some transitional provisions.

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	p276-8 Annual report
Bunzl plc	Clear mapping of cyber security procedures; Q&A with CISO; description of breaches and materiality	p124-5 Annual report
Experian plc	Prioritisation of cyber security measures and the extent of mitigations in place. Disclosure on the fairness, transparency and inclusion principles in their data framework. Cyber-related sustainability SASB metrics.	p45-9; p65 Annual report
Flutter plc	Description of board involvement including Governance in action section	p152 Annual report
Auto Trader	Disclosure of the board succession plan and future composition of the board, with focus on introducing more cyber and digital expertise.	p68-9 Annual report
WPP plc	Data ethics, privacy and security disclosures with a focus on the opportunities of artificial intelligence.	P64 Annual report

Contacts

Cyber risk

If you would like to contact a specialist in cyber risk regarding any matters in this report, please use the details provided below:

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

Cyber risk: industry leads

Corporate

Susan Sharawi
Tel: +44 (0) 20 7303 7383
Email: ssharawi@deloitte.co.uk

Financial services

Andrew Johnson
Tel: +44 (0) 20 7303 7329
Email: andrewjohnson@deloitte.co.uk

Government and public services

Ed Burton
Tel: +44 (0) 20 7303 8906
Email: eburton@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. RITM1599896