Financial Reporting Council

FRC Lab Report:

Digital Security Risk Disclosure

August 2022

Contents

This report

This report has been prepared by the Financial Reporting Council Lab (the Lab).

Our report, and related example bank, highlights examples of current practice that were identified by the Lab team and investors. Not all of the examples are relevant for all companies, and all circumstances, but each provides an example of a company that demonstrates an approach to useful disclosures. Highlighting aspects of reporting by a particular company should not be considered an evaluation of that company's annual report as a whole. Investors have contributed to this project at a conceptual level. The examples used are selected to illustrate the principles that investors have highlighted and, in many cases, have been tested with investors.

If you have any feedback, or would like to get in touch with the Lab, please email us at: FRCLab@frc.org.uk.

Introduction and quick read

Digital and business resilience

Digital systems, processes and data and therefore digital security risk is fundamental to business continuity, resilience and value creation. Reporting on these areas should provide relevant information to investors and other stakeholders to assist them in assessing a company's ability to remain viable and resilient.

Digital security risk drivers

There are a number of factors driving a greater focus on digital security risk disclosures, including:

- recent high-profile cyber and data incidents that show the potential operational and financial impact on companies;
- government proposals to add digital security risk into companies' assessments and resilience disclosures;
- the accelerated pace of digital transformation and its impact on future business success and resilience;
- evolving stakeholder demands around digital and data security which make these relevant to the wider ESG debate; and
- intensified geopolitical tensions, which feed directly into digital risk and impact the digital supply chain.

The need for better disclosure

Our review of disclosures and discussions with investors identified that, whilst a significant proportion of FTSE 350 companies reported at least one digital-related principal risk (mainly cyber risk), the disclosures are not meeting investor needs, are often 'boilerplate' and overly static (see page 30 for participants and methodology).

Corporate reporting teams and audit committees that want to enhance disclosures and better meet the needs of investors might consider disclosures that:

- explain how digital security and strategy are important to the company's current and future business model, strategy and environment;
- detail the governance structures, culture and processes the company has in place to support digital security and strategy;
- identify digital security and strategy risks and opportunities the company is facing both now and in the future; and
- highlight the impact of internal and external events and the actions and activities that respond to these.

What is digital security risk?

For the purpose of this report we consider the following risks:

- Digital security risks - the operational, financial, reputational and stakeholder risks caused by cybersecurity threats, including the risk of major data breaches arising from internal lapses.
- Digital strategy risks - the operational, financial, reputational and stakeholder risks caused by moving to a digital business model (also referred to as digital transformation) and increased reliance on data.

Introduction and quick read

How to use this report

This report is designed to be of use to reporting teams and risk teams who are involved in reporting, and for audit committees who review the resultant disclosures.

It focuses on disclosure relating to digital security (and strategy) risk that can be optimised to provide users with useful information. It does not cover what controls a company should have or what general requirements around risk disclosure should be. However, it does refer to government guidance on actions that companies should take.

Each section of the report explores investor needs (being those investors we spoke to for the project) in more detail across strategy, governance, risk and events. The report is supported by a separate detailed example bank providing a number of practical examples to help companies improve their disclosures. It also provides potential questions for boards and audit committees to consider.

The following pages summarise these investor views, considerations for boards and audit committees, and disclosure recommendations. More detail regarding the difference between *Core* and *Advanced* disclosures is provided on page 10.

Appendix 1 and 2 provide links and details of key guidance in areas beyond the scope of this report. Specific guidance relating to best practice and incident reporting from the National Cyber Security Centre is provided on page 22.

Disclosure, materiality and the risk of 'over-disclosure'

As part of the project we engaged widely with various stakeholders. Participants noted that, on average, current disclosures are not sufficient to meet investor and other stakeholder needs. While there were concerns expressed from some that additional digital security-related disclosure in itself could create risks for companies, there was an equal number who highlighted the opposite, noting in their view, that a lack of disclosure or overly static 'boilerplate' disclosure was in itself a flag that a company was not sufficiently emphasising digital security.

When determining which disclosures to provide, consideration should be taken of materiality for the company, potential sensitivity of the information and whether they provide sufficient information to users.

Our discussions with participants identified information that could be of value to investors and other stakeholders. Based on these discussions, this report seeks to identify areas of disclosure that investors value, companies' internal discussion points and the types of disclosure that may reflect both.

While more and better-focused disclosure would enhance reporting, our recommendations are not meant to serve as a disclosure checklist – not all identified disclosures would be applicable to, or useful for, every company.

Strategy

Investors want (where relevant) disclosures that:	Audit committees should consider whether the disclosures:	Reporting and risk disclosure teams should consider: Core disclosures that:	Reporting and risk disclosure teams should consider: Enhanced disclosures that:
• provide the context for digital security and strategy and its importance to the company's broader strategy, business model and ability to generate value; • indicate how external trends associated with digital security and strategy are integrated into the company's approach; and • link digital security and strategy disclosure to the company's broader strategy.	• make sense in the context of the company's broader strategy; • clearly communicate the company's digital transformation and data strategy; and • explain how digital transformation and its related risks can advance or hinder the attainment of future strategic objectives.	• set out how the business model and strategy impact, and are impacted by, digital and data; • set out the company's (planned) approach to respond to internal and external digital factors; and • indicate how developed the company's data and digital transformation strategy is and whether there are any associated KPIs.	• set out how technology and digital support the future business model and the actions and investments the company has made; • provide specific details of digital transformation trends; and • provide a consistent narrative throughout the report (or are included in a report from the Chief Technology Officer (CTO)) with clear links to other strategic areas and related decisions.

Governance

Investors want (where relevant) disclosures that:	Audit committees should consider whether the disclosures clearly communicate:	Reporting and risk disclosure teams should consider: Core disclosures that:	Reporting and risk disclosure teams should consider: Enhanced disclosures that:
• detail the governance structures, culture and processes the company has in place to support digital security and strategy; • link the governance of digital transformation and security risks to strategy and risk appetite; • show how the board, and its committees, have oversight of these risks. This may also include who within the company has ownership of specific risks, and the access they have to senior leaders; • explain what a company has done to foster a digital security (or cybersecurity) culture; and • outline the relevant skills of the board and any assurance obtained.	• who the risk owners or responsible officers are and how they contribute to 'senior-level' discussions; • what steps (including recruitment and training) are being taken to determine whether the appropriate skills exist within the board and company (and whether these steps are fit for purpose); and • what role internal audit and the audit committee play in relation to digital security and strategy risks.	• cross refer to strategic drivers or business model within the audit and risk committee section; • explain board and committee structure and the make-up of a digital committee if in place; and • reference surveys, cyber-related training and other activities conducted during the period.	• provide CTO (or equivalent) reports on opportunities and threats; • set out issues that the board and committees have considered, name owners of specific risks and detail how these tie to specific oversight committees and the role of the CTO (or equivalent); and • detail development of a cyber and digital culture within the organisation, including monitoring and targets.

Risks

Investors want (where relevant) disclosures that:	Audit committees should consider whether the disclosures clearly communicate:	Reporting and risk disclosure teams should consider: Core disclosures that:	Reporting and risk disclosure teams should consider: Enhanced disclosures that:
• link the digital security and strategy risks to strategic objectives and risk appetite; • consider the actions and activities taken to mitigate risk and how risks have evolved; • provide information about the risk and mitigations at the right level of granularity; and • connect digital security and strategy with disclosures on viability and resilience.	• whether a rigorous risk identification process has been undertaken; • what the company considers to be the optimal level of risk; • how the company's digital security strategy is communicated throughout the organisation and supply chain and how this is reviewed/monitored; • that the company/board understand the threat landscape, company vulnerabilities, risk appetite, mitigating actions and effectiveness; and • the extent to which there is reliance on third parties.	• cross refer to strategic objectives and risk appetite and indicate the owner of each risk; • provide detail of frameworks, mitigations and actions; • set out the elements that are reflective across the group or highlight specific areas of the business that are impacted; and • set out the impacts of digital transformation and data within the prospects assessment, assumptions and in the context of stress testing.	• provide more detail on the oversight process, identify associated opportunities and provide clear and specific links to viability and resilience scenarios; • provide risk actions and mitigations at a granular level relevant to the business (e.g. product, segment, operation or geography) or consider the wider value chain (customers, suppliers etc.); and • provide more detail of 'cyber scenarios' (e.g. length of disruption, cost, division, regulatory response) considered and/or of connected scenarios.

Events

Investors want (where relevant) disclosures that:	Audit committees should consider whether the disclosures clearly communicate:	Reporting and risk disclosure teams should consider: Core disclosures that:	Reporting and risk disclosure teams should consider: Enhanced disclosures that:
• highlight the impacts of events (internal and external) and the actions and activities that respond to these. Specifically where the company has been the subject of a cyber incident, provide information about: • the incident and its immediate impacts; • mitigating actions taken and their objective and effectiveness; • the work of the board to facilitate recovery from the incident; • the quantified financial impact of the incident; and • any improvements and amendments made, or to be made, in response to the incident.	• whether the incident response plans had functioned adequately; • whether incident escalation channels had been adequately established and functioned effectively to inform key decision makers about the incident in a timely manner; • whether the incident (or type of incident) had been anticipated in some form (or had the event not been foreseen at all); and • how accurately cyber-related risks had been considered in the company's various scenario analyses.	• provide information about the nature of the incident and its immediate impacts (subject to interaction with other reporting and regulatory requirements); and • explain the shorter term mitigations and actions taken to restore operations and reduce customer impacts.	• provide detail of response to the issue by internal audit, the board and its committees in understanding the issue, managing the incident, assessing the effectiveness of remediation work conducted and learning lessons for the future; • quantify the estimated financial impact (if material) of the incident and impacts on future capital expenditures; and • explain how learnings and changes have fed through to the net and gross risk and longer-term viability and resilience.

Regulatory context

Business continuity and resilience

For many companies digital security, and the management of related risks and opportunities, is key to their ability to continue to operate and generate value. As such it already features heavily in company reporting, especially around principal risk disclosures (Appendix 1 highlights the current regulatory reporting requirements around material items, risks and viability).

Recent developments

However, digital security is not just of relevance in the short and medium term. It is an increasingly fundamental aspect of a company's longer term resilience. The UK Government has therefore specifically identified digital security as a key business resilience issue to be addressed as part of forthcoming new reporting requirements. In the Government's Response to its White Paper on *Restoring trust in audit and corporate governance*, the government stated that it will be taking forward plans to require companies to produce a resilience statement. Companies within the scope of the legislation will be required to report on matters that they consider to pose a material challenge to their resilience over the short, medium and long term. Digital security risks must be explicitly considered as part of this process.

Amongst other considerations, companies will be required to have regard to:

- the company's operational and financial preparedness for a significant and prolonged disruption to its normal business trading;
- the company's ability to manage digital security risks, including cybersecurity threats and the risk of significant breaches of its data protection obligations; and
- any significant areas of business dependency with regard to the company's suppliers, customers, products, contracts, services or markets which may constitute a material risk.

Link to our findings

While these proposals are not yet final they are consistent with the findings of our outreach. For example, companies will be required to report for each identified short- to medium-term risk or resilience issue:

- the risk's likelihood and impact on the company's operations and financial health;
- the time period over which the risk is expected to remain, and potentially crystallise, if known;
- what mitigating action, if any, the company has put or plans to put in place to manage the risk; and
- any significant changes since the previous reporting period.

'Resilience is a business problem, not an IT problem. If people think otherwise, they have not understood what resilience is.' **Company**

Disclosure recommendations: Strategy

Companies utilise and leverage digital technology and data differently. To some, it is fundamental to the execution of their business model and strategy. To others, it is just one part of the resources necessary to enable their strategy. Providing clarity on its strategic relevance allows investors to judge and assess the appropriateness of the linked processes, procedures and structures.

Investors seek strategy disclosures that:

- provide the context for digital security and strategy and its importance to a company's broader strategy and business model and ability to generate value;
- indicate how external trends associated with digital security and strategy are integrated into the company's approach; and
- link digital security and strategy disclosure to the company's broader strategy (and risk appetite – see the Governance section).

Provides the context

Investors value a company's views on the macroeconomic and geopolitical landscape in which it operates, with enhanced detail relating directly to any specific digital or data transformation. Company reporting that clearly demonstrates the importance to the company of digital transformation, how it is considered as part of strategy and how it impacts its business model is most useful to users. Furthermore, consistent messaging throughout the annual report is important to users i.e. if digital transformation is fundamental to a company, a user would expect this to be reflected within the principal risk and mitigation reporting.

Core and Enhanced disclosure and proportionality

As a result of our discussions with investors and companies, some disclosures were identified that are almost always relevant to the topic (which we define as *Core*) and certain disclosures (subject to broader materiality, security and sensitivity considerations) which are most relevant to those companies and situations where digital security is fundamental to the organisation (which we define as *Enhanced*). Both *Core* and *Enhanced* disclosures can provide useful information to investors, but companies should consider which disclosures are most relevant to them and their audience.

- **Core disclosure -** sets out how the current business model and strategy impact, and are impacted by, digital and data assets (e.g. a customer lists) and risks and whether a company has a formal data strategy (including information relating to key strategic assets and relationships).
- **Enhanced disclosure** - sets out how technology and 'digital' support the future business model, and the actions and investments the company has made within the period in relation to its strategic objectives.

Incorporate trends

Investors want disclosure that explains how digital and data trends (for example, digitisation of the workforce, hybrid working and new technologies) are monitored and how that informs the risks and opportunities, strategy and business model of the company.

Information on proactive actions, is also useful. This could include reporting actions taken or to be taken to enhance how technology and data are leveraged or utilised more effectively or efficiently or how potential regulatory change is being monitored and considered for changes to internal processes and, therefore external reporting.

- **Core disclosure** - sets out how the company intends to respond, or has responded to, internal and external factors.
- **Enhanced disclosure** - provides specific details of trends, how they might impact the business and the size and nature of the opportunity, the impact of the relevant internal and external factors on the company and detailed response plans or anticipated changes to business model or strategy.

Linking digital security and strategy

Investors want digital security and strategy to be communicated as part of an integrated story which connects back to the rationale of the company's overall strategy and be consistent with the related board discussions.

- **Core disclosure** - provides an indication of how developed the company's data and digital strategy is and whether there are any associated KPIs.
- **Enhanced disclosure** - provides a consistent narrative throughout the report or are included in a report from the CTO (or equivalent) with clear links to other strategic areas and stakeholder-related decisions and how these aspects link to management performance objectives.

Developing topic: Digitisation of the workforce

The pandemic accelerated the trend towards omni-working; having employees working at home, in the office and a hybrid of both. In fact, a recent CIPD survey showed that two-thirds (63%) of employers surveyed report that they plan to introduce or expand the use of hybrid working. This digitisation of the workforce creates both risks and opportunities for companies and shows how cyber and digital risk might interact, overlap and increase other risks within an organisation. Disclosures on digital working are of interest to investors, as well as current and future employees.

Actions and examples

On page 26 we highlight, as actions, considerations for boards and audit committees to assist them to decide whether disclosures meet investor needs.

We have identified examples from current practice that illustrate a specific aspect of disclosure or a number of aspects in an integrated fashion. Some extracts have been included directly in the report, but more detail, and further examples, have been included via a table in each section and in a separate example bank.

Examples of practice

IAG
Annual Report 2021

What is useful?
IAG has included a report from the Chief Information Officer which clearly explains the current and future digital and technology-based strategy in the context of the company's markets and stakeholders.

Reporting 'directly from the CIO' further illustrates the company's commitment to technology and digitisation in achieving its strategic objectives.


Strategic Report

Driving towards technology excellence

IAGTech

"In 2021, we completed the work on our new IT/ Digital operating model and are focused on driving continuous improvements to our ways of working, including creating an environment where our technology professionals can thrive."

Overview

Our people

Our customers

Our planet

Looking forward

Experian
Annual Report 2021

What is useful?
Experian details how data, digital and cyber trends are developing and feeding directly into the strategy, risks and opportunities for the business over the short, medium and long term.

This disclosure sets the tone for the rest of the report. The company then includes detailed disclosure on the processes, approaches and actions it is taking in these areas.

Other useful examples

Helping investors understand	Extract
The context for digital security and strategy and its importance to the company's broader strategy	IAG, Experian
How external trends are integrated into the company's approach	IAG, Experian
How digital security and strategy risk disclosures link to the company's broader strategy	BAE Systems

Disclosure recommendations: Governance

Understanding risk is partly about understanding how the external environment impacts an organisation and partly about how the organisation manages and mitigates those risks. Business actions start with, and are driven by, the board, but what triggers their considerations and actions? Our discussions with companies identified a number of drivers for board discussions, including regulatory interest, strategic opportunities, employees, suppliers and wider considerations related to the S172 statement and ESG agenda. Whilst company disclosures on governance often cover the 'What', they neglect the 'Why' and 'How'. The opportunity for improving company disclosure is therefore focused on a more integrated approach to digital security and strategy governance which provides a clear connection to the wider internal and external stakeholder context.

Investors seek governance disclosures that:

- link the governance of digital transformation and security risks to strategy and risk appetite;
- show how the board and its committees have oversight of these risks. This may also include who within the company has ownership of specific risks, and the access they have to senior leaders;
- explain what a company has done to foster a digital security (or cybersecurity) culture; and
- outline the relevant skills of the board and assurance obtained.

Developing topic: Cyber, data, stakeholders, and society

The development of safe and secure digital services that protect the data rights of individuals has become critical as companies transition into the provision of 'digital business models'. Similarly, a drive by organisations to a wider company purpose introduces considerations around digital ethics, inclusion and accessibility.

The themes of safety and inclusion are also moving up the agenda of investors and other stakeholders as a key part of a wider ESG focus. Examples include:

- a coalition of 25 investors in the UK have created the Cybersecurity Coalition which is engaging with companies on cyber risk issues;
- the Digital Rights initiative has created a scorecard of company policies and processes around digital rights. A number of UK investors are using the index to score their portfolios on this issue;
- the World Benchmarking Alliance has created a digital inclusion index that ranks 150 companies on their support for digital inclusion; and
- the PRI and their investor signatories continue to engage on cyber related topics.

Linking governance, strategy and risk

Investors want to understand the context of digital security and strategy for the organisation. This helps them judge how important these areas are to the company and its business model and allows them to consider the appropriateness of the governance around these topics.

- **Core disclosure** - provides cross references to strategic drivers or business model resources within the audit and risk committee section.
- **Enhanced disclosure** - includes messages 'directly from' the CTO (or equivalent) within their annual reports to explicitly explain what has been done in response to the opportunities and threats posed to the business over the period and in the future.

Showing the governance structure

Investors want to understand the relevant governance structures related to these risks. This allows them to assess if the structure meets best practice, balances the risks and opportunities and provides sufficient visibility for the issues.

- **Core disclosure** - includes a narrative or illustrative disclosure of board and committee structure, details of scope and make-up of digital and security specific committees.
- **Enhanced disclosure** - sets out, potentially through the use of case studies, issues that the board and committees have considered, names owners for specific risks (and how these tie to specific oversight committees) and provides narrative on the relationship and reporting by the CTO (or equivalent) to the committees.

Thinking about culture

Whilst process, procedures and controls are important to managing risk, developing a strong corporate culture related to cyber is also important. As evidenced in the report Creating Positive Culture, corporate culture is inextricably linked to performance and achievement of objectives.

This is no different when considering the opportunities and threats associated with digital security and strategy.

Boards and management play a critical role in setting the organisation's culture. Transparent communication between all components of a company is necessary to facilitate the cultivation or continued growth of a positive company culture in this respect. A positive culture enables policies to be converted into organisational awareness and actions.

Several participants indicated that culture can itself be an effective risk mitigation tool. Fostering a culture that values 'security' makes all parties understand the related contributions. They can then assist management and the board to mitigate risk. It can also give boards and stakeholders more confidence in the functioning of the existing governance structures.

Investors (and employees) want to understand what steps companies have taken to foster their 'cyber culture' and how the board has engaged in the topic.

- **Core disclosure** - references surveys, training and other activities that been conducted during the period that emphasise the importance of a 'cyber-aware' culture.
- **Enhanced disclosure** - provides further insight into the findings of the surveys, future plans relating to training, how cyber (and security in general) is considered in company policies and codes of conduct. The format of reporting itself communicates this commitment from senior leadership. Discussion about progress towards digital, data and cyber-related objectives, for example, can be directly presented in reports from the CTO (or equivalent) within their annual reports.

Skills and assurance

Investors, regulators and others want to understand the relevant governance structures related to these risks and how they have been developed to address the specific challenges associated with digital security and strategy. This allows them to assess if a structure meets best practice, balances the risks and opportunities and provides sufficient visibility for the issues.

Investors can obtain comfort over the processes adopted by a company to understand and manage risks. These fall broadly into three categories: the frameworks adopted and complied with by the company (including Cyber Essentials and Cyber Essentials Plus and ISO27001), the skill-set of the board and any training activities conducted with the board and whether any internal or external assurance has been obtained over aspects of the risk management framework (for example, who compiled the company's disaster recovery plan, whether this been externally reviewed and whether this review is a one-off or if it is conducted on a regular basis).

- **Core disclosure** - indicates which frameworks, if any, have been adopted, relevant experience of board members, specific training provided to the board and whether any assurance (internal or external) has been obtained over risk-related processes and structures.
- **Enhanced disclosure** - provides greater detail regarding the specific frameworks adopted, training provided to the board and the frequency and outcomes thereof, the scope of the assurance work conducted, the frequency thereof and whether, and how, any findings have been incorporated in the year or are planned to be in the future.

Developing topic: Board skills and training

A Cyber Security Longitudinal Survey published by the Department for Digital, Culture, Media and Sport (DCMS) highlighted this limitation. The survey found that companies **"are relatively unlikely to report that their board members have received any cybersecurity training"**. It also noted that the level of training for the board tends to lag that of general staff.

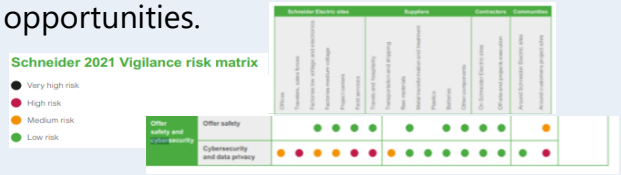
The National Cyber Security Centre (NCSC) has made available a Board Toolkit of resources designed to encourage essential cybersecurity discussions between the board and their technical experts.

Examples of practice

Schneider Electric
Universal Registration Document 2021

What is useful?
The company further builds on the cyber culture disclosure and demonstrates through its disclosure that it considers cybersecurity risk beyond the company boundary, i.e. suppliers, contractors and communities.

These risk considerations then connect with the company's detailed exploration of risks, mitigations and opportunities.



Other useful examples

Helping investors understand	Extract
The links between the governance of digital transformation and security risks to strategy and risk appetite	Schneider Electric; Landsec; UBS
How the board and its committees have oversight of these risks	Flutter; Reach; LSE Group; RELX; Admiral; NatWest; Ocado
What the company has done to foster a digital security (or cybersecurity) culture	Schneider Electric; Admiral
The relevant skills of the board and assurance obtained	Flutter; RELX; Admiral; NatWest

Company insight: Schneider Electric SE
During a discussion with Schneider Electric to understand more about their approach to 'cybersecurity disclosure' they identified some key considerations:

1. The more disclosure, the better – rather than focus on just what is required, report the maximum allowable by the company's policies
2. Be proactive, not reactive – integrate cyber, digital and data risks into the broader enterprise risk management framework and try to anticipate regulations before they are implemented – this allows systems, processes and reporting to be ahead of the game
3. Own the narrative – this can only be achieved if you report and make information visible to your community. If not reported directly by the company, information may be obtained through other channels, potentially resulting in an alternative narrative being presented to the market and other stakeholders
4. Consider the company's importance and role in the value chain especially for critical infrastructure – report information that allows others to fully understand the company and its cybersecurity posture

Disclosure recommendations: Risk

Digital security and strategy risks are cross-cutting risks. IT departments can, to an extent, mitigate many related risks. However, risk management is ultimately owned by senior management and the board to ensure that it is considered consistently and in the context of strategy. All stakeholders (including employees and third-party service providers) play a vital role in mitigation of risk.

In many areas of risk reporting the messages we have heard mirror those in our 2021 report on risk. In addition to previous findings, investors seek risk disclosures that:

- link the digital security and strategy risks to strategic objectives and risk appetite;
- consider the actions and activities taken to mitigate risk and how risks have evolved;
- provide information about the risk and mitigations at the right level of granularity; and
- connect digital security and strategy with disclosures on viability and resilience.

Linking to strategic objectives and risk appetite

Investors want a clear understanding of the link between strategic objectives and key risk indicators. Furthermore, an explanation of how risk appetite relates to a company's business model aids contextualisation of risk management and mitigation activities and ties into strategy and business model. A balanced narrative highlights both the opportunities and threats associated with the company's data and digital strategies and long-term viability.

Reporting risk owners demonstrates accountability and link to strategic decision-making. It also provides a clear indication of the level at which decision-makers sit within the company and their connection to the board.

In times of uncertainty, investors want to understand how quickly a company can take action to respond to external and internal factors. It is useful to users for a company to communicate the actions taken, or planned to be taken, in response to these factors.

- **Core disclosure** - provides cross references to strategic objectives and risk appetite and indicates the owner of each risk (or principal risk).
- **Enhanced disclosure** - provides more detail regarding the oversight process associated with the risk, identifies potential associated opportunities and provides clear and specific links to viability and resilience scenarios.

Actions, activities and risk evolution

Investors want to understand the actions and activities that link to the risk and the evolution in the risk and how this ties to business continuity.

- **Actions and activities** - investors are not expecting cyber risk to be reduced to zero, but they do want to understand how a company plans to mitigate and manage the issue. In the disclosures we reviewed, company mitigating activities are often a list of options, incident response plans or IT policies in place rather than concrete actions. Better disclosure provides specific actions undertaken in the period to enhance security, actions planned in the year ahead that will further improve response to risk and facts and circumstances that mitigate or reduce risk when a cyber event crystallises (e.g. cyber insurance, or a cyber resilience plan).
- **Risk evolutions** - investors want to understand companies' assessments of how risks are expected to move. Simply stating that a 'risk has increased/decreased /remained the same' in isolation is not useful – investors want to understand the significance of the change (if any), what led to that assessment, whether further changes are expected, and what actions the assessment led to. When explaining the driver of the change, detailing whether this was an internal or external factor, provides further insight into how effectively management and the board reacted to and managed the situation. For cyber-related risk this might include details of an evolving cyber threat (e.g., a specific malware, or increase in cyber attacks) and offset by changes in the business, systems and tools employed by the company.

Provide information at the right level of granularity

Investors want disclosure that assists them to determine whether the company has clear oversight over its critical assets, data and critical third-party relationships (including supply chain). Obtaining full understanding and oversight over the risks posed by multiple third-party relationships and complex supply chains is an ever-increasing challenge.

Investors are not the only party interested in this type of disclosure. Information needs to be shared with other companies within networks (the company, other members of its group and its supply chain) to remain as secure as possible. Further to this 'internal information share', external disclosures are most useful when they are provided at the appropriate level (i.e. per product, operating unit or region). This allows users to understand the mitigating activities and their effectiveness – providing these at a group or global level may not be sufficient.

'It's about having a connected organisation that talks with each other rather than people at local level thinking that they have that authority. It's about the board saying how we make decisions on deals. The first step is to have that discussion on cyber strategy, which is not a simple thing to put down.' **Company**

Cyber (and therefore, operational) resilience is highly dependent on the risk mitigation activities and underlying processes relating to these areas.

- **Core disclosure** - sets out the elements that are applicable across the group and its supply chain. This includes disclosure of insurance arrangements (or whether the company is self-insured) associated with critical assets, data safeguarding and back-up plans. It is also helpful to set out the existence and testing of critical incident response plans and processes including whether third-party testing and assurance took place. Where relevant, reporting whether any recognised credentials have been obtained (e.g. Cyber Essentials Plus) or frameworks have been incorporated in infrastructure design (e.g. ISO27001) provides insight to users.
- **Enhanced disclosure** - provides risk actions and mitigations at a relevant level of detail for the business. This may be at a product level (versus the impact on the company's central operation), country level, subsidiary or segment level or it may consider the wider value chain (customers, suppliers etc.). Specifically for supply chains, enhanced disclosure provides more detail regarding the procurement process when contracting with critical third-parties (and cyber-related contractual terms and covenants) and how performance relating to such contracts is measured and monitored. Enhanced useful information includes how cyber is considered and incorporated into acquisitions and project implementations and whether any third-party assurance has been obtained over any aspects of the network.

Connecting with viability and resilience

For many companies, the possible disruption and impact on operations, customers and suppliers or the financial penalties from a data breach might be so significant that it warrants consideration within the company's assessment of longer-term viability and resilience. Investors consider the potential impact of such events on the companies they invest in and want to see this also included in management's own consideration and scenarios.

- **Core disclosure** - sets out the impacts of digital and data within the prospects assessment, assumptions and in the context of stress testing.
- **Enhanced disclosure** - provides more detail of the 'cyber scenarios' (e.g. length of disruption, cost, division, regulatory response) considered or of multiple overlapping and connected scenarios.

Developing topic: Company and customer tolerance

The FCA and Bank of England recently highlighted the need for financial service companies to focus more fully on the risks caused by outsourcing and the cloud. They require companies to consider and map key service providers. They will also consider obtaining information directly from key cloud providers. They ask companies to also think about disruption and service interruption not just in terms of the company's own tolerance for risk but also from a customer perspective. A focus on stakeholder tolerance demonstrates the importance of digital security and availability to customers and those within the supply chain. Therefore, disclosure around these topics can be helpful across user groups.

Examples of practice

Derwent
Annual Report 2021

What is useful?

Derwent provides context of how cyber risk connects to its operations and business model. The company considers the changing environment and describes the key aspects of its approach.

The relevance to the company's business model is also clear in the detailed risk section. This is achieved through splitting the risks between internal operational risk and customer/product risk, providing a direct link to strategic objectives, business model and KPIs and detailing the mitigations for each risk. The company also provides details of executive responsibility and where internal audit review of the cyber issue was obtained.

Other useful examples

Helping investors understand	Extract
The links between the digital security and strategy risks, strategic objectives and risk appetite	Derwent; Pennon Group; Legal & General Group
The actions and activities taken to mitigate risk and how risks have evolved	Chesnara; Next; Ocado Group
The risk and mitigations at the right level of granularity	Convatec Group

Disclosure recommendations: Events

Companies face many internal and external digital security events that will impact their strategy, risk management and governance structures and processes. In addition to information about the actions taken and events themselves, investors want to understand the effectiveness of a company's response and how lessons learned from the event will be, or have been, incorporated into changes to relevant structures and processes.

The dominant theme in our discussions with participants indicated that it is important to set out the actions taken or to be taken should a company (or a key supplier or third-party service provider) experience a cybersecurity event particularly during periods of heightened political risk.

Responding to cyber incidents

No company is immune to cyber risks; attacks can and do happen. It is clear that such incidents are disruptive regardless of the level of the company's preparation and planning. The number of attacks is increasing and is likely to increase further as a company's digital transformation continues. In the unfortunate event that a company (or a member of its supply chain) is subject to a cyber attack, reporting provides a vital vehicle for a company to explain the nature of the event, actions taken and to be taken and immediate and anticipated impact of the event. Proactive actions will enable the company to control the narrative and provide accurate information directly to stakeholders.

- **Core disclosure** - provides information about the nature of the incident (or 'near miss') and its immediate impacts (including whether any personal data has been exfiltrated) and explains what mitigations were taken, their objectives and effectiveness.
- **Enhanced disclosure** - provides greater detail of the work conducted by the board to facilitate the recovery from the incident and by internal audit, the board and its committees in assessing the effectiveness of remediation work conducted. Quantification of the estimated financial impact of the incident (including future capital expenditures) provides greater insight to investors. Explanations of any planned amendments or improvements to systems, processes or response plans allow users to assess the company's future resilience to similar attacks.

Where to go for more: Reporting a cyber incident

- The FCA issued Good cyber security – the foundations in 2017. This provides guidance on how regulated companies should respond to a cyber incident and how to report a cyber incident.
- The Information Commissioner's Office provided detailed guidance relating to personal data breaches.
- The NCSC has made available advice on dealing with cyber incidents and how the NCSC can assist any company experiencing one.

National Cyber Security Centre guidance: best practice and incident reporting

The National Cyber Security Centre's (NCSC) aim is to make the UK the safest place to live and work online. As the UK's technical authority, the NCSC has created resources to make information and practical guidance available to all. When cyber security incidents occur, the NCSC provides effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

The NCSC has a number of resources available to assist organisations as they consider cybersecurity:

Cyber Security Board Toolkit - Resources designed to encourage essential cyber security discussions between the Board and their technical experts.

Cyber Essentials and **Cyber Essentials Readiness Tool** - Cyber Essentials is a government backed certification scheme that helps companies to guard against the most common cyber threats and demonstrate their commitment to cyber security.

Cyber Aware - Cyber Aware is the government's advice on how to stay secure online.

Ten Steps to Cyber Security - Breaks down the task of defending networks into ten essential components.

Supply Chain Security - The guidance will provide organisations with an improved awareness of supply chain security.

Early Warning - Helps organisations investigate cyber attacks on their networks by notifying them of any malicious activity that has been detected in information feeds.

Exercise in a Box - A free online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment.

GDPR security outcomes - Guidance describing technical security outcomes considered to represent appropriate measures for GDPR.

Cyber incidents

If an organisation has experienced a severe cyber incident, which poses a risk to the ongoing operation or to its customers or supply chain, the NCSC encourages the company to report this to the NCSC.

Further, the Response & Recovery Guide provides guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident. The guide also includes information on how and when to report cyber incidents to NCSC.

Geopolitical issues and impacts on digital security

Companies have always been subject to risk from geopolitical activities and tensions. Investors are experienced in factoring these risks into their investment decisions. However, since the Russian invasion of Ukraine the risk to a company's digital supply chain and the risk of cyber incidents have been brought to the fore. Unlike traditional geopolitical risks, cyber risks are not attached to specific locations and therefore it can be more difficult for investors to assess.

'Since Russia's invasion of Ukraine, many companies have experienced heightened cybersecurity risks, increased or ongoing supply chain challenges, and volatility related to the trading prices of commodities regardless of whether they have operations in Russia, Belarus, or Ukraine that warrant disclosure." **SEC**

'You should consider your ability, and that of your third-party providers, to withstand a cyber attack. You should take all appropriate steps to shore up your controls' **FCA**

Given the continuation of the conflict investors would value reporting on the impact on companies. The impact of the conflict on cybersecurity risk includes both the increase in risk of cyber attacks but also the effects on the wider digital supply chain. The FRC Lab recently released an insight into supply chain issues.

Company insight: Weir plc

Weir PLC was subject to a cybersecurity incident in September 2021. During our discussion, we asked about the experience and the resultant approach taken to the reporting thereof:

The cyber incident was complex, touching various aspects of our business and numerous stakeholders in different ways. Our aim was to reflect that through our Annual Report disclosures. We formed a small team of people from the relevant functional areas – audit, risk, cybersecurity, finance, governance, communications etc. to discuss and agree our approach and to ensure consistency. Our response was also influenced by those specific areas of interest identified by certain stakeholders post incident.

We wanted to provide enough detail to assist all parties in their understanding of the incident, its impact and our risk response, but without being repetitive. As such, we presented specific aspects in the most relevant section. For example, the Chairman's statement included the view from and action by the Board, while the CEO Report discussed the operational aspects. Similarly, we covered impact on our employees in the People section, while financial aspects were disclosed in the CFO review… and so on. In doing so, we aimed to give our audience a clear and balanced understanding of what happened and ultimately how we managed it.

Examples of practice

Weir
Weir Q3 Trading update

What is useful?
Weir was subject to a cybersecurity incident in September 2021. The company included initial information in its Q3 update to the market. This was supplemented at year end with more detail in the year end results presentation. The timeline and key outcomes provide users with a quick understanding of the event and its impacts.

Other useful examples

Helping investors understand	Extract
The impact of events and incidents	Weir
The company's response to a cyber incident or data security issue	Weir
The impact of geopolitical issues on digital security	Chesnara

Conclusion and what's next

Our review of digital security risk reporting identified that there is a need for more useful disclosures around:

Strategy - Establish how important digital security and strategy are to the company's current and future business model, strategy and environment.

Governance - Detail the governance structures, culture and processes the company has in place to support digital security and strategy.

Risk - Indicate the risks and opportunities connected to digital security and strategy that the company is facing both now and in the future.

Events - Highlight the impacts of events (internal and external) and the actions and activities which respond to these.

Given the importance of these issues to investors, regulators and others (and their importance and contribution to building business resilience) we consider that this is an area that corporate reporting teams, risk teams and audit committees should consider. The disclosure-related actions that can be taken by audit committees have been summarised on the following page.

While we hope this report and its related example bank provide some useful guidance, we expect that market disclosures will evolve as investor expectations and reporting requirements increase, in particular, in relation to:

- Resilience, viability and business continuity
- ESG aspects of digital security
- Horizon scanning and longer-term impacts on strategy

Actions

Digital security risk is growing in relevance to businesses and investors. Current disclosures are not sufficient. Reporting teams, risk teams and audit committees should pay increasing attention to this topic.

Disclosure actions

In order to be meet stakeholder information needs, audit committees should consider if the company's disclosure clearly communicates:

Strategy

- whether the information reported externally relating to digital security and strategy makes sense in the context of the company's broader strategy.
- the company's digital transformation and data strategy.
- how digital transformation and its related risks can advance or hinder the attainment of future strategic objectives.

Governance

- who the risk owners or responsible officers are and how they contribute to 'senior-level' discussions.
- what steps (including recruitment and training) are being taken to determine whether the appropriate skills exist within the board and company (and whether these steps are fit for purpose).
- what role internal audit and the audit committee play in relation to digital security and strategy risks.

Risk

- whether a rigorous risk identification process has been undertaken, and if digital security and data risks are material.
- what the company considers to be the optimal level of risk and risk appetite.
- how the company's digital security strategy is communicated throughout the organisation and supply chain and how this is reviewed/monitored.
- that the company and board understand the full threat landscape, company vulnerabilities, mitigating actions and their effectiveness.
- the level of reliance on third parties and resultant risks.

Events

- where applicable, whether the incident response plans had functioned adequately.
- whether incident escalation channels had been adequately established and functioned effectively to inform key decision makers about the attack in a timely manner.
- whether disclosure adequately balances transparency with security.
- whether the incident (or type of incident) had been anticipated in some form (or if the event had not been foreseen).
- how accurately cyber-related risks had been considered in the company's various scenario analyses.

Appendices

Appendix 1: Useful resources – Corporate reporting

The following regulations and guidance provide valuable corporate reporting context for this report.

- **The Companies Act 2006 (Companies Act)**
  - Section 414C(2)(b) requires that the Strategic Report contains a description of the principal risks and uncertainties facing the company. This requirement applies to a wide range of companies, including UK AIM and many private companies. It sits alongside the requirement for a balanced and comprehensive analysis of the development, performance and position of the company in Section 414C(3).
  - The requirement to disclose a non-financial information statement was introduced as part of the changes presented by The Companies (Miscellaneous Reporting) Regulations 2018 and subsection 414CB(2) includes a requirement for a description of principal risks and, where relevant and proportionate, relationships that are likely to have an adverse effect on these risks and how the risks are being managed.
- **Guidance on the Strategic Report 2018 (the Guidance)**
  - The Guidance supports and expands on ways to approach the legislative requirements within the Strategic Report section of the Companies Act.
  - Paragraph 7A.28 of the Guidance explains that the risks and uncertainties included in the Strategic Report should be those considered by the entity's management to be material to the development, performance, position or future prospects of the entity. They will generally be matters that the board regularly monitors and discusses because of their likelihood, the magnitude of their potential effect on the entity, or a combination of the two.
- **The UK Corporate Governance Code 2018 (the Code)**
  - The Code was updated in 2018 and applies to accounting periods beginning on or after 1 January 2019. There are a number of relevant Code principles and provisions related to risk and a company's prospects. For example, the Code reinforces the need for risk considerations to sit within the wider context of the company's business model and long-term success.
- **FRC Guidance on Risk Management, Internal Control and Related Financial and Business Reporting (2014)**
  - The FRC also issued Guidance on Risk Management, Internal Control and Related Financial and Business Reporting in 2014. This provides further guidance on risk and viability reporting, including a section on the 'Long Term Viability Statement'.

Appendix 2: Useful resources – Cyber risk

The following table provides valuable cyber and digital security risk material that was considered during this report. This is not intended to be an exhaustive list.

Organisation	Resource
National Cyber Security Centre	• Board Toolkit • Supplier assurance questions • Cyber Aware
Information Commissioner's Office	• Responding to a cybersecurity incident • Guide to Data Protection
Financial Conduct Authority	• Cyber security - industry insights • Cyber and Technology Resilience • Good cyber security – the foundations
Centre for the Protection of National Infrastructure	• Cyber Assurance of Physical Security Systems
UN Principles for Responsible Investment	• Stepping up governance on cyber security: What is corporate disclosure telling investors? • Engaging on cyber security: Results of the PRI collaborative engagement
Securities and Exchange Commission	• Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
Department for Digital, Culture, Media and Sport	• Collection: Cyber resilience
Department for Business, Energy and Industrial Strategy	• Government's Response to its White Paper on *Restoring trust in audit and corporate governance*

Appendix 3: Methodology and Participants

Participants join projects by responding to a public call or being approached by the Lab. An iterative approach is taken, with additional participants sought during the project, though it is not intended that the participants represent a statistical sample. References made to views of 'companies' and 'investors' refer to the individuals from companies and investment organisations that participated in this project. Views do not necessarily represent those of the participants' companies or organisations.

Views were received from a range of UK and international institutional investors, analysts and retail investors through a series of in-depth interviews. We also heard from a range of companies through one-to-one interviews or roundtables.

Thank you to all of the participants for contributing their time to this project. Some participants have consented to be named.

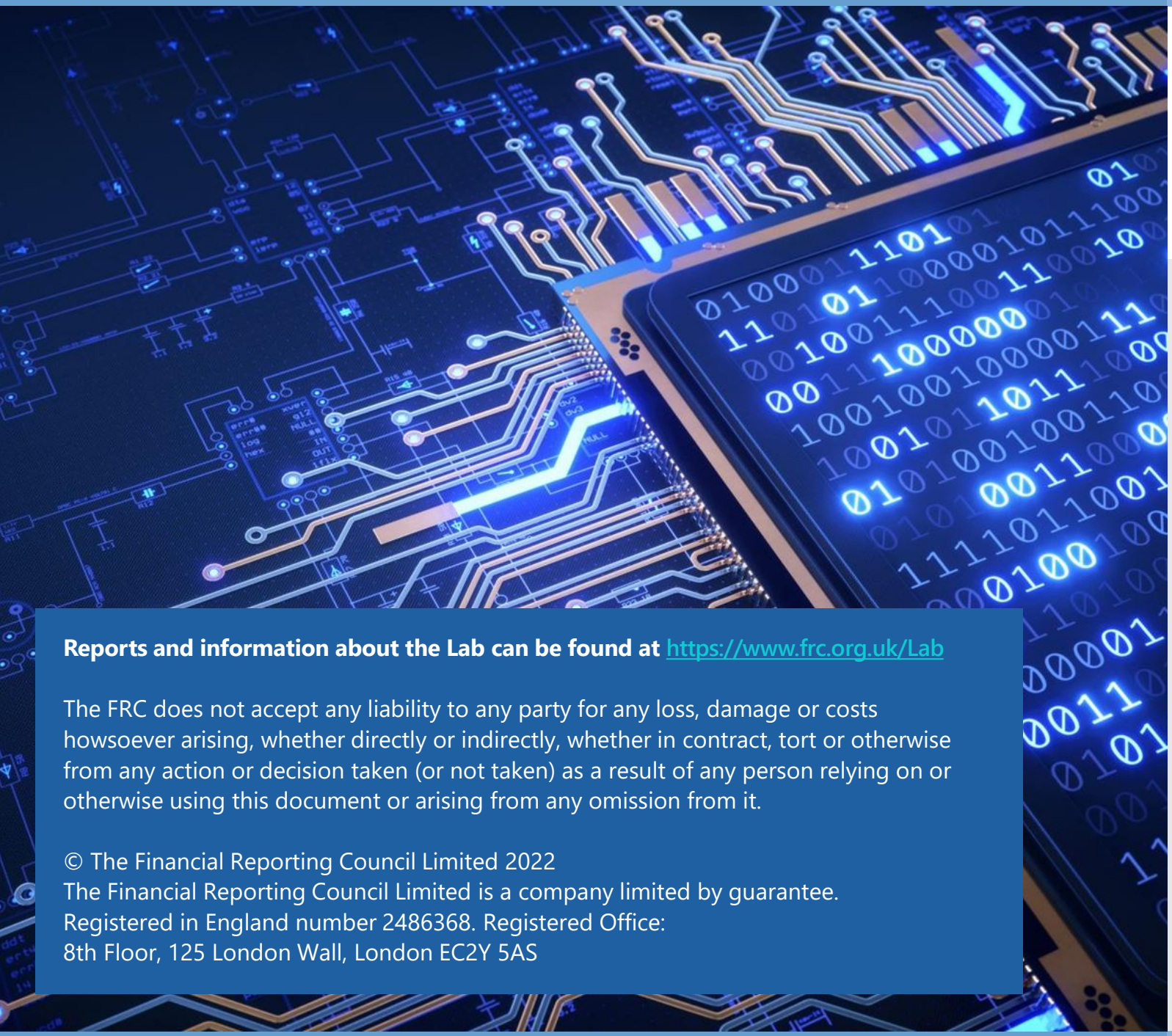
The Lab also received a great deal of support from a wide range of organisations, advisors and others throughout this project, particularly those organisations that have been working in this area for a number of years. This assistance has been invaluable, and we thank these organisations for giving so generously of their time.

Companies:

- BT Group plc
- Coca-Cola Europacific Partners plc
- Experian plc
- International Consolidated Airlines Group S.A.
- InterContinental Hotels Group plc
- Lloyds Bank plc
- Santander UK plc
- Schneider Electric SE
- Smith & Nephew plc
- Weir plc

Investors and other users:

- BAE Systems Pension Funds Investment Management Ltd
- Castlefield Investment Partners LLP
- Evenlode Investment Management Ltd
- Representatives of the UK Shareholders' Association
- Schroders plc
- Principles for Responsible Investment



Reports and information about the Lab can be found at https://www.frc.org.uk/Lab

FRC
Financial Reporting Council

Financial Reporting Council
8th Floor
125 London Wall
London EC2Y 5AS
+44 (0)20 7492 230

www.frc.org.uk

Follow us on
Twitter@FRCnews
or LinkedIn.