Financial Reporting Council

FRC Lab Report:

Digital Security Risk Disclosure

Summary of findings

August 2022

Summary of findings

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 discussion 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.

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.

Summary of findings

The full 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. 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. It also provides potential questions for boards and audit committees to consider.

The full report is supported by a separate detailed example bank providing a number of practical examples of current better practice to help companies improve their disclosures.

The following pages summarise these investor views, considerations for boards and audit committees, and disclosure recommendations.

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

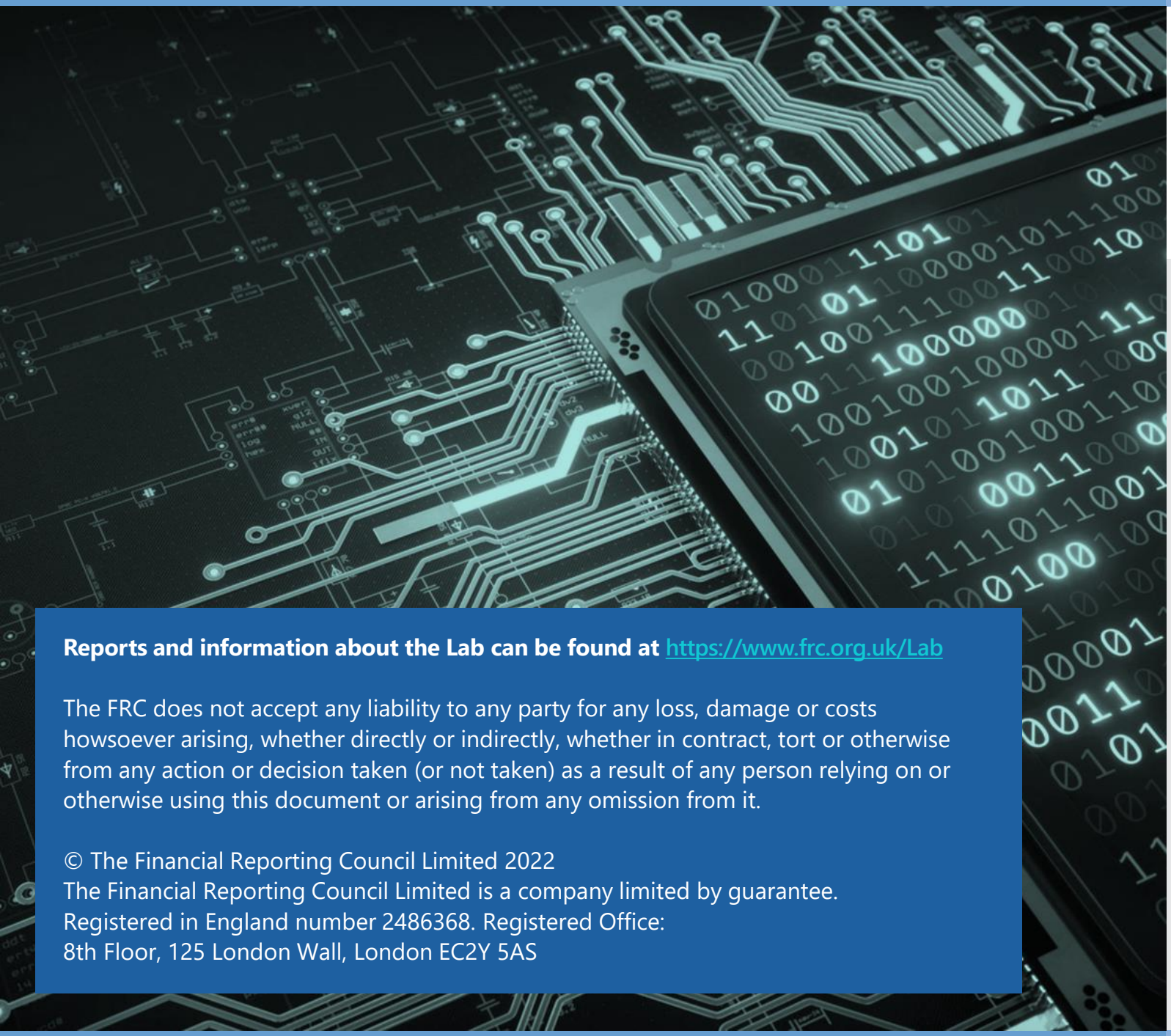
Investors want (where relevant) disclosures that:	Audit committees should consider whether the disclosures clearly communicate:	Reporting and risk disclosure teams should consider: Core disclosures that:	Reporting and risk disclosure teams should consider: Enhanced disclosures that:
• detail the governance 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. • explain how learnings and changes have fed through to the net and gross risk and longer-term viability and resilience.



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.