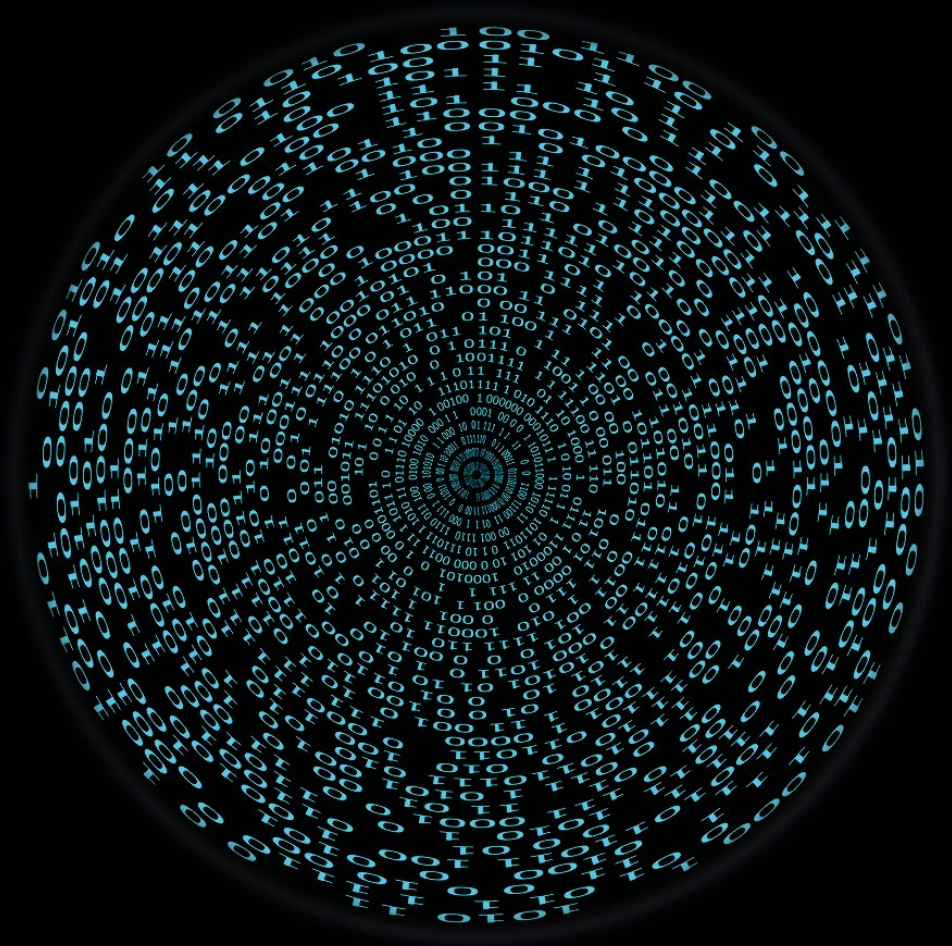
Deloitte.



Cyber risk and governance reporting in the UK: Improvement required!

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Foreword by William Touche

1. Do companies describe cyber risk clearly? The verdict: Improvement, but no cigar...

2. How do boards appear to be involved?

3. Are mitigating activities well explained?

4. How much are companies really saying about cyber security breaches?

5. Tech transformation is accelerating

Appendix 1: SEC proposal and FRC Lab recommendations

Appendix 2: Examples of cyber disclosures

In this survey we have looked at the most recent annual reports of the FTSE 100 which were published by 13 May 2022.

Foreword by William Touche

Technology has become pervasive in our lives, accelerated by the pandemic with the move to remote or hybrid working at many organisations. 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.

With board oversight of technological capability, opportunity and risk critical to company success, regulators are increasingly focused on how companies report cyber risk and breaches in security. The FRC's Financial Reporting Lab published its report Digital Security Risk Disclosure over the summer and earlier this year the US Securities and Exchange Commission (SEC) also published a proposal to improve disclosure in this area.

In order to examine current reporting in the UK, we are pleased to present this survey of cyber opportunity, risk and governance reporting across the FTSE 100 which is 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. It is clear from our findings that the Lab's guidance will be useful to address the variability in current disclosure practice in the UK, given the importance of technology as a driver of both value and potential vulnerabilities (see Appendix 1).

We last examined FTSE 100 cyber risk and governance reporting in March 2018 and we are pleased to see progress in companies' disclosures. For example, 24% of companies now disclose a board member with cyber expertise compared to 8% previously. However, when compared to the SEC proposal on cyber reporting published in March 2022 and the FRC Lab's disclosure recommendations, more focus is needed to match the needs of investors as identified by these two market regulators.

In particular, a substantial majority of companies are still not reporting that they receive and deal with cyber attacks. Investors, regulators and the informed public are aware that companies will regularly be fending off cyber attacks of varying degrees of sophistication and success - and almost half of FTSE 100 companies report an increase in cyber attacks attributed to the pandemic, the move to remote/ hybrid working and geopolitical tensions. It is important to tell the full story. The SEC has also levied a substantial fine on a company which disclosed data theft as a risk but did not say that such theft had actually taken place.

In summary, our FTSE 100 annual report review shows:

- Companies in every sector, although not every company, identify cyber as a principal risk – so companies should think carefully if they do not
- The value destruction from cyber risk is very high and can include customer service issues, costly remediation, regulatory fines and longer-term reputational damage. Detailed disclosure is now being called for to highlight board oversight.
- 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.

- Generally, companies are doing a lot in this area and should take credit for what they are doing, including describing who has executive responsibility, how they report to the board, board level responsibilities, the policy framework, internal controls, internal and external assurance, and disaster recovery plans. It is the absence of regulatory guidance that has led to variability of disclosures.
- 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: disclosure can only report on what companies actually do.

Considering what companies are actually doing in practice, in Digital frontier: a technology deficit in the boardroom, the Deloitte Global Boardroom Program reports the findings of a survey covering more than 500 directors and C-suite executives and conversations with leaders, directors, and subject matter specialists to find out what's being done in boardrooms around the world when it comes to technology. The survey found that **fewer than half** of executives and board members surveyed believed their board is providing enough oversight of technology matters. Meanwhile, **44% of executives** said that their board directors lack the knowledge they need to provide effective stewardship over technology strategy.

This lack of experience could put investment at risk, and ultimately lead to a competitive disadvantage. Nearly half of respondents **(49%)** say their organisation isn't investing enough in technology to meet the key strategic objectives of outpacing the competition and addressing opportunities and risks.

The findings of the global survey offer some clear paths to future success. While the digitally connected world presents threats, it also presents opportunities - to improve engagement with customers and suppliers, implement technologies to improve sustainability, to increase efficiency and enhance decision making with richer data. Investment in technology can transform performance and our survey of FTSE 100 company reporting found that the better disclosures both explained these opportunities and explored the change in risk profile as a result. Good disclosure can help investors differentiate whether a company is doing enough to manage its risk and embrace opportunity.

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 are frequently on the agenda.

At a glance

- 97% of the FTSE 100 clearly pulled out one or more types of cyber risk as a principal risk in their disclosure.
- The most common potential impacts cited were disruption to operations 81%, reputational damage 76% and financial loss 69%.
- Under half (43 companies) acknowledged an increase in cyber attempts and sophistication since the pandemic and the shift to remote/ hybrid working environments.
- About one third of companies (32) acknowledged employee risk as part of cyber security and data loss.
- A quarter indicated that there is a board director with direct specialist expertise.
- 80% mentioned contingency plans, crisis management or disaster recovery plans as a mitigating action for cyber risk. However, under half of these said they completed testing on these plans in the reporting period.
- In an area requiring greater attention, only 12% actually acknowledged cyber security incidents in their organisation.
- 74% of the FTSE 100 disclosed digital strategy and 70% disclosed technology investments as an opportunity (with just over half mentioning both).

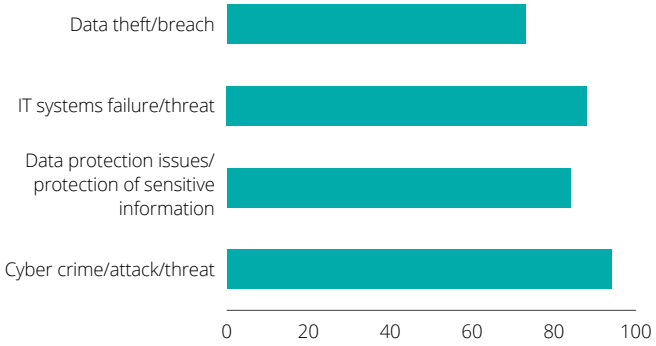
1. Do companies describe cyber risk clearly? The verdict: Improvement, but no cigar...

The good news is that now almost all (97%) of the FTSE 100 clearly show one or more elements of cyber risk as a principal risk, up from 89% in 2018, the last time we performed this analysis.

Companies described four types of cyber risk: cyber crime, IT systems failure (not necessarily related to cyber crime), data protection (the risk of data loss) and data theft or misappropriation. The better disclosures discussed all these.

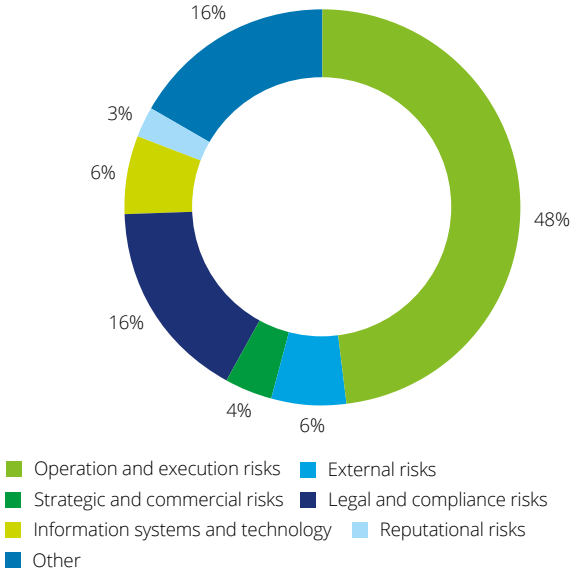
Nearly half (43%) of these companies described more frequent attacks following the shift to remote / hybrid working. Although it may seem contradictory, less than half (38%) identified an increase in risk compared to the previous year.

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.

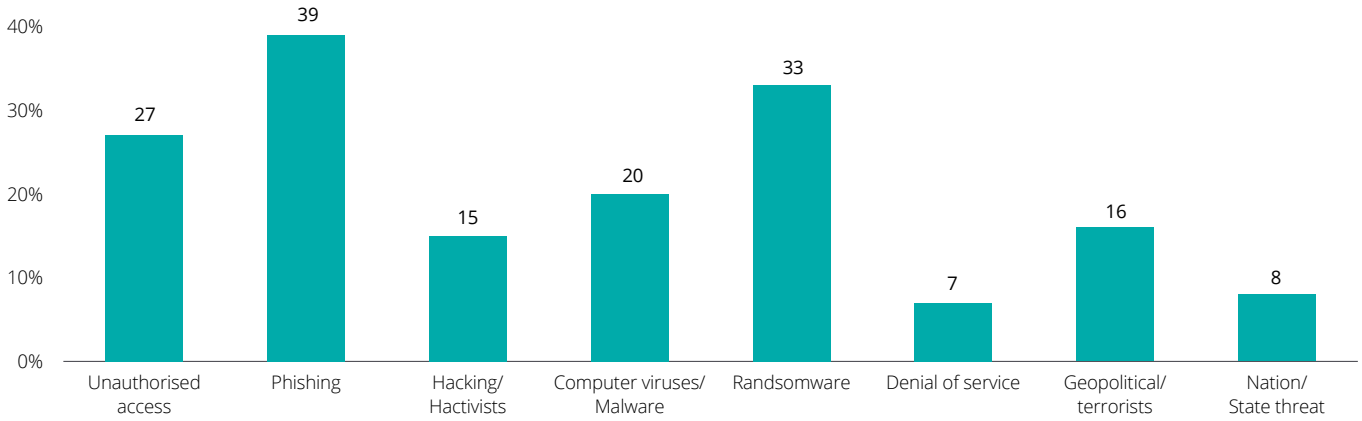
Figure 2. Cyber risks as categorised in FTSE 100 annual reports



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 3 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 risk(s).

The majority of companies did not call out the specific types of cyber threats faced. For instance, although unauthorised access is faced by all companies with digital assets, it was only mentioned by 27 companies. The most common threat mentioned was phishing (39 companies). Deloitte's 2022 On the board agenda explained that 65% of business leaders[1] identified ransomware as the single greatest threat to their organisation over the next 12 months; curiously, however, just 33 companies mentioned ransomware in their annual reports.

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

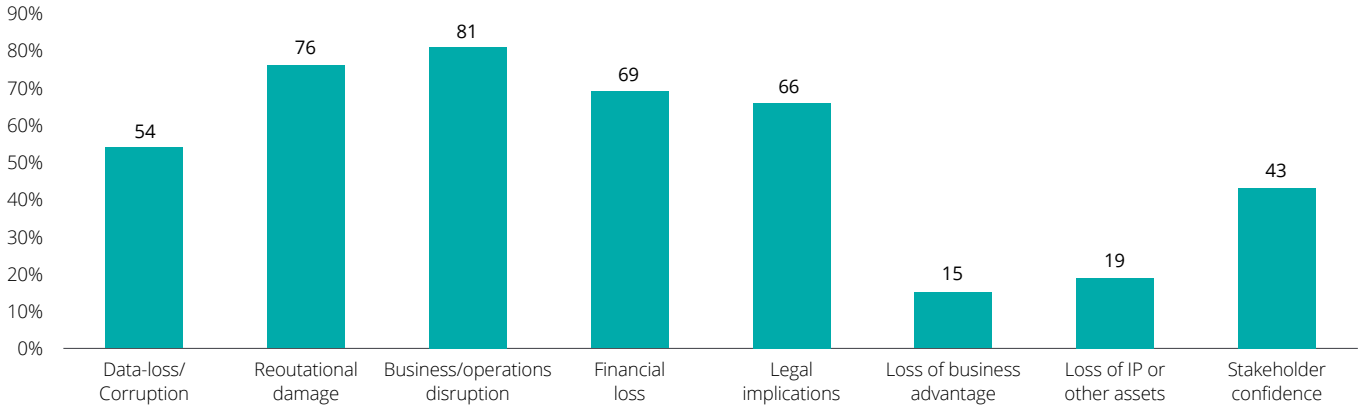


[1] Based on an online poll of more than 50 C-suite and other executives during a webcast held on June 24, 2021

How were impacts described? The most common cited were disruption to operations 81%, reputational damage 76% and financial loss 69%[2]. The majority also mentioned data loss and legal implications, including penalties arising from inability to meet contractual obligations or other regulatory non-compliances. (See Appendix 2, example 1.)

Just under half of companies described an impact on customers which could result in loss of customer and investor confidence or trust.

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



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

Some disclosures also considered the impact of cyber risk on the company's ongoing viability with inclusion of possible cyber security scenarios (see Appendix 2, example 3).

What about the weak link – the risk from company employees? As companies become more reliant on technology and remote and hybrid working there is an increased risk to cyber security from employee action or inaction - only 32% of companies recognised this, but this was up from 23% in our 2018 survey.

There is increasing recognition of the threat from the ecosystem: 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". Just under half (47%) of companies disclosed third party risk as an aspect of their principal risk(s).

Technology transition is also a risk: 41% of companies highlighted the risk of not keeping up with technology changes or failure to successfully implement new technologies, but only 17% made the link between technology transformation and cyber risks.

Metrics are in short supply: Just five companies mentioned a cyber-related key performance indicator (KPI), for example the number of digital visits or technology uptime availability (proportion of time technology platforms were available to customers). However, all of these disclosures were brief and most omitted a clear definition, quantification, and target for the KPI.

In addition, three companies included key risk indicators (performance measures to monitor risk) in their cyber principal risk(s). Examples included the number of serious IT incidents and time taken to respond. (See Appendix 2, examples 2 and 5.)

2. How do boards appear to be involved?

We looked at how companies described how their boards take ownership of cyber risk. We focused on whether the board appeared to have sufficient expertise and experience disclosed to guide the business through appropriate cyber risk assessments and mitigations, as well as how the board provided oversight of management.

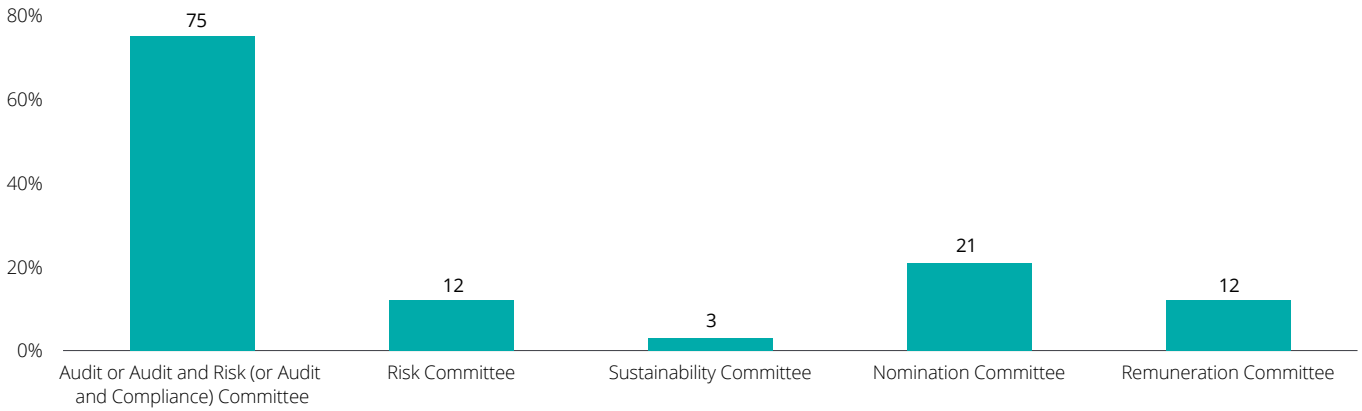
One in four (24%) FTSE 100 boards appeared to have a director with direct specialist expertise in cyber[3], up from 8% in 2018, whereas three in four boards (74%) claimed to have a digital specialist. Where there was a cyber specialist all disclosures included some description of the board member's prior experience.

In describing their oversight, while 61% of boards reported they had received either a report or presentation on cyber in the year, including 'deep dives', only one in four boards (23%) disclosed this as a regular agenda item.

The best cyber improvement programmes included a description of the board's role throughout, how they are kept informed on progress, whether external experts have been engaged and a description of the programme leader.

Nearly all boards (95%) of boards mentioned cyber security in their corporate governance statement, most frequently as a matter covered by the audit committee or the risk committee. Disclosures identified in the nomination committee mostly considered the board expertise in this specialist topic, perhaps in seeking new recruits.

Figure 5. Cyber mentions in committee reports



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

At least one in ten companies (12%) included cyber considerations in the remuneration report, usually as part of a director's personal objectives, with the best explaining the objective that was set and the progress the director made during the year.

However, overall the level of disclosure on cyber risk was highly variable with many audit or risk committee reports simply citing cyber security in a list of topics considered as part of internal control. Many did not enhance by one jot an investor's understanding of the board's interest in, and ownership of, the area.

Just under half (48%) disclosed that they have a Chief Information Security Officer (CISO), or similar position, as part of the executive team. However, only 12% commented on the CISO's role and reporting lines. 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.

The SEC's recent cyber reporting proposal contemplates disclosure of the company's cyber risk assessment programme and inclusion of a description. Currently, less than one in five companies (only 17%) describe a formal cyber risk assessment within their annual report. (See Appendix 2, example 6).

3. Are mitigating activities well explained?

Companies can demonstrate to investors that addressing cyber risk is a priority by showing they have thought about where responsibility lies at executive level, the reporting lines to the CEO and the board and the board oversight structures in place.

However, just one third (33%) clearly identified in their annual report a person or team with responsibility for cyber security and only six companies reported that this was a board member.

One company mentioned that an external cyber expert – neither a director nor an employee – attended a number of board and committee meetings in the year, ensuring that the board has access to expertise without adding a "specialist" director.

All companies are expected by their investors and other stakeholders to have internal controls and IT policies in place to manage IT security issues. But we found that not all companies mentioned these:

- 81% described having internal policies in relation to cyber/data security within their risk mitigations, with 10% of all companies mentioning improvements in these policies during the year.
- 90% mentioned internal controls in place as a mitigating factor in relation to cyber risk, and 23% disclosed improvements in these internal controls during the year.

A low four in ten (42%) of companies discuss 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.

If employees are the soft entry point, 85% of FTSE 100 companies mentioned delivering staff training on cyber or data risk during the year, substantially higher than the 30% of companies that mentioned cyber or data training delivered to the board!

Investment in training was accompanied by testing: Four in ten (39%) mentioned some form of vulnerability testing, penetration testing or other cyber risk testing performed during the year. The best disclosures described an iterative process to identifying risks, implementing mitigations and detecting flaws (see Appendix 2, example 7).

But, while four in five companies (80%) mentioned contingency plans, crisis management or disaster recovery plans as a mitigation for cyber risk, under half mentioned testing these plans in the year. More common was disclosure of periodic testing with no information on frequency. We expect that companies did not take credit for having suitable plans in place and regular testing.

Surprisingly, we did not find evidence of board involvement in assessing disaster recovery, crisis management or contingency plans in the annual reports. Perhaps a topic for companies to consider?

Investment in cloud solutions is growing fast and 21 companies mentioned cloud solutions as a mitigation of cyber risk, and of these about half (12) also discussed third party due diligence or monitoring of compliance with internal controls and policies. Governance of third parties is a growing area of focus.

4. How much are companies really saying about cyber breaches?

Almost all companies will be experiencing regular cyber attacks. 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 (12%) cited cyber security breaches in their organisation. Only seven companies indicated whether the breach was material.

The best disclosures explained the reputational damage as a result of the breach (one company), the legal implications (three companies) and any resultant changes to cyber security policies/ procedures (four companies).

One company disclosed a fine from the SEC following an insufficient prior period disclosure of a data breach, clearly showing the SEC stance that generic descriptions without detail of the incident is not providing sufficient information to investors.

Only one company included clear disclosure of how the breach was remediated, an area included within the SEC's recent proposal.

Although not in the FTSE 100 and therefore not within our survey population, The Weir Group PLC provided detailed disclosure in their audit committee report of a cyber incident they experienced during 2021 (Appendix 2, example 8). This disclosure includes a description of the attack, materiality level, steps taken in the days following the attack to remediate, how the board was kept informed, and how policies and procedures have been updated to help prevent a repeat.

5. Tech transformation is accelerating

Three in four companies (74%) described their digital strategy (long-term strategy) and 70% described their technology investment plans (short-medium term strategy) as opportunities (with just over half mentioning both).

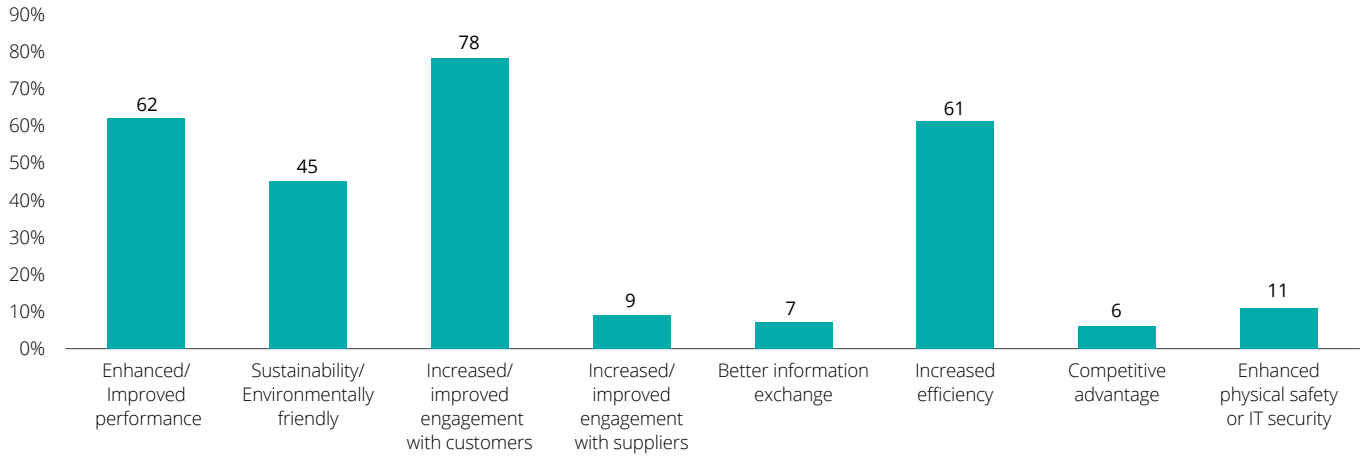
Strategy examples given included moving to cloud-based platforms and big data. Examples of short-medium term investment included new ERP systems and hiring the scarce talent with technology expertise.

The best disclosures showed a link between the opportunities and the principal risk(s) identified. For example, Barclays PLC described some of the opportunities of technology advancements but also explained that introducing new technologies can increase inherent cyber risk.

Companies identified significant benefits from their investments, with the most common being increased or improved engagement with customers, followed by Increased efficiencies and enhanced performance.

Just under half of companies recognised a link between technology / digital opportunities and sustainability. This was predominantly in the investment in new sustainable technologies and was primarily discussed within the companies' TCFD disclosures.

Figure 6. Benefits identified by the FTSE 100



Appendix 1: SEC proposal and FRC Lab recommendations

Currently there is no specific cyber disclosure requirement in the UK or the EU, however, in March 2022 the U.S. Securities and Exchange Commission (SEC) published a proposal to mandate cybersecurity disclosures by U.S. public companies. The UK has followed suit, with the FRC's Financial Reporting Lab publishing the results of its own research and advising on better disclosure on 3 August.

Key features of the SEC proposal include:

Cyber incident reporting (8-K) to be filed within four business days of the point that the incident was deemed material (rather than the date the incident occurred/was discovered) along with proposed annual report disclosures to include:

Cyber incident reporting	• Any material impact of the incident on the registrant's operations and financial condition • Any potential material future impacts on the registrant's operations and financial condition • Whether the registrant has remediated or is currently remediating the incident • Any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes
Disclosure of governance regarding cybersecurity risks	• Whether responsibility for oversight sits with the board, specific board members or a committee • How the board is informed about cybersecurity risks, and how frequently this is discussed • Whether and how risks are considered as part of the board's business strategy, risk management, and financial oversight • Management's role assessing and managing risks and implementing policies procedures, strategies • Whether there is a CISO or equivalent, their role and reporting structure • Any director with cybersecurity expertise and their prior work experience and certification or degree
Disclosure of risk management and strategy regarding cybersecurity risks	• Description of risk assessment program • Policies and procedures for third party providers • Activities to prevent, detect and minimise effects of cybersecurity incidents • Business continuity, contingency and recovery plans in the event of a cybersecurity incident • Whether incidents have led to changes in governance, policy, procedures, technology • Whether and how risks and incidents have or are reasonably likely to affect results • Whether and how risks are considered as part of strategy, financial planning and capital allocation

Appendix 1: SEC proposal and FRC Lab recommendations

Key recommendations from the FRC Lab report include:

Based on discussions with investors and stakeholders, the FRC Lab encourages companies to avoid "boilerplate" or overly static disclosure and draws out how more, relevant, better-focused disclosure can enhance reporting and will be considered valuable by investors.

Strategy	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.
Governance	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.
Risks	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.
Events	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.

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.

Example 1 – Fresnillo plc	Detailed risk description regarding the nature of cyber crime the company faces	Annual report Page 137
Example 2 – Taylor Wimpey plc	Provides examples of 'key risk indicators' to describe how they are monitoring the risk level	Annual report Page 65
Example 3 – Spirax-Sarco Engineering plc	Includes cyber risk in its viability statement, with a description of the expected impact of a cyber attack	Annual report Page 44
Example 4 – RELX PLC	Describes the impact that extreme weather events caused by climate change could have on information security systems	Annual report Page 68
Example 5 – Flutter Entertainment plc	Includes a tech-related key non-financial indicator	Annual report Page 30
Example 6 – Standard Chartered	See example disclosure below	Annual report Page 272
Example 7 – Intertek Group plc	Explains their iterative risk-based framework backed up with a clear diagram	Annual report Page 169
Example 8 – The Weir Group PLC	See example disclosure below	Annual report Page 113
Example 9 – Barclays PLC	Describes the opportunities of new technology and links this to the cyber security risk	Annual report Page 212

Example 6

Standard Chartered PLC describes the relevant cyber security roles and responsibilities, as well as the Risk Committee oversight. This example includes mention of a risk assessment and stress testing which further strengthens investors' understanding of the company's cybersecurity practices.

Information and Cyber Security (ICS) Risk

The Group defines Information and Cyber Security Risk as the risk to the Group's assets, operations and individuals due to the potential for unauthorised access, use, disclosure, disruption, modification, or destruction of information assets and/or information systems.

Risk Appetite Statement
The Group seeks to minimise ICS risk from threats to the Group's most critical information assets and systems, and has a low appetite for material incidents affecting these or the wider operations and reputation of the Group.

Roles and responsibilities
The Group's Information and Cyber Security Risk Type Framework (ICS RTF) defines the roles and responsibilities of the first and second lines of defence in managing and governing ICS Risk respectively across the Group with emphasis on business ownership and individual accountability.

The Group Chief Operating Officer has overall first line of defence responsibility for ICS Risk and holds accountability for the Group's ICS strategy. The Group Chief Information Security Officer (CISO) leads the development and execution of the ICS strategy.

The Group Chief Information Security Risk Officer (CISRO) function within Group Risk, led by the Group CISRO, operates as the second line of defence and sets the strategy and methodology for assessing, scoring and prioritising ICS risks across the Group. This function has overall responsibility for governance, oversight and independent challenge of ICS Risk.

Mitigation
ICS Risk is managed through a structured ICS Risk framework comprising a risk assessment methodology and supporting policy, standards and methodologies which are aligned to industry best practice models.

In 2021, the ICS RTF was extended to include ICS end-to-end Risk Management and Governance and an enhanced threat-led risk assessment.

The Group CISRO function monitors compliance to the ICS framework through the review of the ICS risk assessments conducted by Group CISO.

All key ICS risks, breaches and risk treatment plans are managed under Group CISRO oversight and assurance. ICS Risk posture, Risk Appetite breaches and remediation status are reported at key Group, business, functional and country governance committees.

Governance committee oversight
At Board level, the Board Risk Committee oversees the effective management of ICS Risk. The Group Risk Committee (GRC) has delegated authority to the Group Non-Financial Risk Committee (GNFRC) to ensure effective implementation of the ICS RTF. The GRC and GNFRC are responsible for oversight of ICS Risk posture and Risk Appetite breaches rated very high and high. Sub-committees of the GNFRC have oversight of ICS Risk management arising from business, country and functional areas.

At a management level, the Group has also created the Cyber Security Advisory Forum, chaired by the Group Chief Executive Officer, as a way of ensuring the Management Team, the Group Chairman and several non-executive directors are well informed on ICS Risk, and to increase business understanding and awareness so that business priorities drive the security and cyber resilience agenda.

Decision-making authorities and delegation
The ICS RTF defines how ICS Risk Management will operate within the Group. The Group CISRO delegates authority to designated individuals through the ICS RTF, including second-line ownership at a business and function level as well as regional or country level The ICS RTF defines the levels of approval required for different risk ratings.

The Group CISO is responsible for implementing and operating ICS Security Risk Management within the Group, leveraging Business Heads of ICS to extend ICS risk management into the businesses, functions, countries and Information Asset and System owners to comply with the ICS RTF, policy and standards.

Monitoring
The risk assessment is performed by Group CISO to identify key ICS risks, breaches and weaknesses, and to ascertain the severity of the Risk posture.

The Risk postures of all businesses, functions and countries are consolidated to present a holistic Group-level ICS Risk posture for ongoing ICS Risk monitoring.

During these reviews, the status of each risk is assessed to identify any changes to materiality, impact and likelihood, which in turn affects the overall ICS Risk score and rating. Risks which exceed defined thresholds are reviewed with Group CISRO for approval and escalated to appropriate Group governance committees.

Monitoring and reporting on the ICS Risk Appetite profile ensures that performance which falls outside the approved Risk Appetite is highlighted and reviewed at the appropriate governance committee or authority levels and ensures that adequate remediation actions are in place where necessary.

Stress testing
The Group's cyber resilience testing approach entails:

- The Group CISRO is responsible for risk based, intelligence led, scenario driven assessments that simulate the actions of real-world cyber adversaries targeting the organisation. This layered testing approach is used to validate the effectiveness of the measures taken to prevent, detect and respond to cyber threats targeting our critical business.
- Group CISO is responsible for supporting control improvement and risk reduction by emulating cyber attacks to enhance the Group's cyber defence capabilities.

Example 8

Although not in the FTSE 100 survey population, The Weir Group PLC clearly disclosed a cybersecurity incident that took place in the year and included their steps to remediate the incident.

Cybersecurity incident
In September 2021, the Group was the target of a sophisticated attempted ransomware attack. On detecting the threat, the Group's cybersecurity systems and controls responded quickly and robust action was taken to protect the Group's infrastructure and data. Forensic investigation, in conjunction with cybersecurity experts, produced no evidence that any data had been exfiltrated or encrypted.

As a result of the incident, the Group took the decision to temporarily remove access to Windows-based PC's and to isolate and shut down IT systems, including the Group's core financial reporting systems, while the threat was assessed. In the days following the incident, processes began to safely restore systems and bring applications back online in a progressive manner and in order of business priority. From a financial reporting perspective, this did lead to some temporary disruption to regular procedures and impacted the Group's usual internal reporting procedures for a short period.

The Committee were updated in their scheduled October meeting on the impact of the cybersecurity incident on the finance function. This included a detailed review of the processes impacted and the early mitigating actions taken to minimise impact and/or risk. In addition, this outlined short-term re-planning of specific finance processes to allow focus on system restorations, ensuring effective controls and data integrity were maintained. Such early mitigating actions included an immediate tightening of controls over the Group's bank accounts and related banking procedures.

The incident necessitated some re-prioritisation of tasks for finance teams globally. The decision was taken to cancel the second half 2021 Compliance Scorecard process and to introduce alternative targeted controls assurance workstreams, focusing on providing assurance post system restores that there were no gaps in the recording of transactions as a result of the incident. A number of planned internal audits were also deferred.

In terms of additional assurance, the Committee were also presented with an overview of planned inventory counts post the incident, providing good levels of coverage in this specific risk area. We also received a report of the findings from Internal Audit's independent review to confirm that the controls implemented by entities to ensure the completeness and accuracy of data processed during the offline period were adequate. Their review covered heightened risk areas such as payments, inventory and revenue recognition. Tests were performed to confirm that transactions on manual lists were transferred to the ERP system accurately. Additionally, sample testing was performed to confirm the existence of transactions recorded offline, and to confirm that they were approved appropriately. Specific balance sheet reconciliations were reviewed with no exceptions noted. Based on their review and findings, Internal Audit were able to conclude that there were no instances of material breakdowns in controls over the key processes reviewed.

Further updates were provided to the Committee in January 2022. Finally, the Committee received an update in February 2022 which included the results from a self-certification exercise introduced in place of the usual six-monthly Compliance Scorecard process. This involved each company Finance Director completing a standard questionnaire and certifying that appropriate balance sheet rigour had been restored.

frameworks, including IT processes and controls, remained stable and effective. We have also taken assurance from the work of PwC in this area.

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:

Phill Everson
Tel:+44 (0) 20 7303 0012
Email: peverson@deloitte.co.uk

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:

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

William Touche
Tel: +44 (0) 20 7007 3352
Mob: +44 (0) 7711 691591
Email: wtouche@deloitte.co.uk

Deloitte.

Designed by CoRe Creative Services. RITM1078662