RESEARCH INTO THE PREVALENCE AND QUALITY OF CYBER DISCLOSURES

AZETS

Department for
Science, Innovation
& Technology

Contents

Introduction

Azets UK was commissioned by the Department for Science, Innovation and Technology (DSIT) in January 2023 to carry out research into the prevalence and quality of cyber disclosures in the annual reports of large and very large[1] organisations. The research supports DSIT's aim to better understand the quality of current cyber disclosures. The publication of the research was deferred so that it followed the conclusion and subsequent publication of the non-financial reporting review call for evidence outcome, led by the Department for Business and Trade (DBT) in collaboration with the Financial Reporting Council (FRC).

Background

The National Cyber Strategy[2] sets out an ambitious vision for the UK to be a leading global cyber power. Pillar 2 of the Strategy sets out objectives to build a resilient and prosperous digital UK, a vital part of which is to better understand cyber security risks. The 2021 Comprehensive Spending Review committed £2.6bn of investment to deliver the National Cyber Strategy, to ensure that the UK is at the forefront of improving cyber resilience of public bodies and UK businesses. DSIT is responsible for delivering outcomes from the National Cyber Strategy that relate to the resilience of businesses and organisations across the UK.

One of the drivers for companies enhancing their cyber resilience is the demand from stakeholders for greater transparency on how they manage digital security risk. This is largely down to how fundamental governance of digital security risk is to an organisations' business continuity, as well as its competitiveness. Investors are a key business stakeholder that would benefit from greater transparency provided by companies. Better quality disclosures on how digital risk is governed would enable them to better assess the opportunities and risks originating from the approach each company takes and therefore make more informed investment decisions.

The Financial Reporting Council (FRC) is the UK's regulator for the accounting, audit and actuarial profession and is also responsible for corporate governance in the UK. In August 2022, the FRC produced their Digital Security Risk Disclosure[3] report which outlines better practice relating to disclosure of digital security risk. The FRC report defines digital security risk as: "the operational, financial, reputational and stakeholder risks caused by cybersecurity threats, including the risk of major data breaches arising from internal lapses". The report focused on FTSE 350 companies and identified that investors and other stakeholders would value better quality disclosure of digital security risk-related considerations. DSIT recognises the excellent insight this report provides as well as the

[1] As would have been defined in *The Draft Companies (Strategic Report and Directors' Report) (Amendment) Regulations 2023.*

[2] Cabinet Office (2022). National Cyber Strategy 2022. National Cyber Strategy 2022 - GOV.UK (www.gov.uk)

[3] FRC Lab. (2022). *Digital Security Risk Disclosure* (Issue August). https://www.frc.org.uk/getattachment/b23698f9-a587-4222-b32a-b947dd7b3300/FRC-Digital-Security-Risk-Disclosure_August-2022.pdf

need to perform further research to establish a comprehensive picture of current practices across large and very large organisations.

The FRC report also contains considerations for audit committees to support their assessment of the quality of disclosures on digital security strategy, governance, risk, and events (incidents) within annual reports. The purpose of these is to promote better quality disclosures on digital security risk within annual reports. The considerations are primarily aimed at audit committee members, however they are also directed at internal reporting and risk teams to encourage better disclosures to address questions from audit committee members. As a result, there may be some overlap in the potential considerations discussed within the FRC report, and the actions identified in this study. The FRC report has therefore been referenced throughout the analysis of this research where appropriate.

Purpose

Azets' research has been commissioned to establish (a) how prevalent current reporting is; and (b) how effective current reporting on digital security risks is. This work will help DSIT to better establish a baseline on the prevalence and quality of current cyber security reporting in the annual reports of companies.

Scope of research

The primary focus of the research was on reviewing annual reports of 250 very large companies i.e. £750m turnover and 750 employees or more. This is referred to as the 'main sample' herein.

The research also included a control sample of 50 large companies which have at least 500 employees and £500m turnover and up to, but not including, either 750 employees or £750m turnover. This is referred to as the 'control sample' herein.

The purpose of including a control sample is to allow DSIT to assess the difference in reporting prevalence and quality between large and very large companies.

A number of interviews have been held as part of the research, all of which were from individuals representing companies in the main sample. The purpose was to gain qualitative insights on the perceived benefits and barriers of including cyber disclosures within annual reports, including the reasons behind organisations reporting or not against cyber security within their annual report. The interviews were held with individuals in a senior cyber security role e.g. Chief Information Security Officer.

Relevant legislation, regulation and guidance

The table below sets out some of the main sources of legislation, regulation and leading practice that applies to companies when producing annual reports. Whilst it is not an exhaustive overview of current reporting requirements and leading practice, the below have been considered as the most relevant to this research:

Source	Companies impacted	Cyber disclosure requirements
Companies Act 2006[4]	All UK companies	Provides the legal basis for the content of company annual reports. S.414C(2)(b) of the Act sets out the need for companies to include details of their principal risks and uncertainties. The Act does not prescribe cyber security risks (or any other risk) as a mandatory disclosure requirement. The FRC has produced guidance[5] on what information should be included within the Strategic Report section of an annual report. This sets out guidance on reporting on principal risks, an example of which is cyber security risk.
UK Corporate Governance Code 2018[6]	Commercial companies	Applicable to the commercial companies category on the London Stock Exchange's Main Market. To comply with elements of the UK Listing Rules these companies must apply the Principles of the Code and comply with, or explain against, the Provisions. Requires reporting on: ● Board Leadership and Company Purpose ● Division of Responsibilities ● Composition, Succession and Evaluation ● Audit, Risk and Internal Control ● Remuneration

[4] The Companies Act 2006 is the piece of legislation that serves as the main source for company law governing the UK. Companies Act 2006 (legislation.gov.uk)

[5] Financial Reporting Council 2022. Guidance on the Strategic Report. Strategic Report Guidance_2022 (frc.org.uk)

[6] UK Corporate Governance Code 2018 is a set of standards governed by the Financial Reporting Council that are applicable to the commercial companies category on the London Stock Exchange's Main Market UK Corporate Governance Code | Financial Reporting Council (frc.org.uk)

Source	Companies impacted	Cyber disclosure requirements
		The Code Provisions address reporting on principal risks but they do not prescribe reporting on cyber security risks (or any other specific risks). Companies covered by the Code are required to provide details of governance in excess of what the Companies Act 2006 demands.
The Companies (Miscellaneous reporting) Regulations 2018[7]: (Corporate Governance arrangements reporting only)	Private (UK incorporated) companies with more than 2,000 employees; and/or a turnover of more than £200 million, and balance sheet of more than £2 billion.	Large companies are required to include a corporate governance statement in their directors' report explaining the governance arrangements applied by the company to secure trust and confidence among stakeholders and benefit the economy and society in general. The Regulations ask companies which, if any, code or governance standards they follow.
Wates Principles[8]	As above	The Wates Principles offer companies a framework to report against these regulations, and the government supports adoption of these Principles. Whilst the Principles do not cover cyber specifically, Principle Four on Opportunity and Risk requires that a board establish oversight for the identification and mitigation of risks. Specifically, it outlines responsibilities of the board in establishing an internal control framework with clearly defined roles and responsibilities for those involved; reporting frequency; and escalation points.

[7] The Companies (Miscellaneous Reporting) Regulations 2018. The Companies (Miscellaneous Reporting) Regulations 2018 (legislation.gov.uk)

[8] Financial Reporting Council. 2018. The Wates Corporate Governance Principles for Large Private Companies. Wates-Corporate-Governance-Principles-for-LPC-Dec-2018.pdf (frc.org.uk)

Source	Companies impacted	Cyber disclosure requirements
Financial Conduct Authority: Disclosure Guidance and Transparency Rules sourcebook[9] (DTR)	Those regulated by the Financial Conduct Authority	The FCA Handbook contains the Disclosure Guidance and Transparency Rules sourcebook. DTR7 sets out corporate governance reporting requirements. For example: ● DTR7.1 sets out the requirements for audit committees and their functions. ● DTR7.1.3(2) requires that the audit committee (or equivalent) "*monitor the effectiveness of the issuer's [entity's] internal quality control and risk management systems and, where applicable, its internal audit, regarding the financial reporting of the issuer [entity], without breaching its independence*". ● DTR7.2.5 requires listed companies to set out within their corporate governance statement *"…a description of the main features of the issuer's [entity's] internal control and risk management systems in relation to the financial reporting process."*

The disclosure requirements of the Quoted Companies Alliance (QCA) Code were not considered relevant to this research as they are primarily applied by small and mid-sized quoted companies.

Acknowledgements

DSIT and the report authors would like to thank those who participated in this research, including those who participated in interviews, and shared data, knowledge, and feedback to help inform this research.

[9] Financial Conduct Authority. 2023. FCA Handbook: Disclosure Guidance and Transparency Rules Sourcebook (DTR). FCA Handbook - FCA Handbook

Methodology

Annual Reports

Identifying the population of companies

The population of companies was identified using a company search database which uses Companies House as a data source, to run a search based on the required parameters. This produced an output of all companies which met the required criteria.

The table below outlines the legal status by which companies were filtered, and whether they were included or excluded from the population:

Legal Status Category	Included / Excluded from population
PLC	Include
Private Company Limited by Guarantee Without Share Capital Claiming Exemption from Using the Word Limited	Include
Private Limited	Include
Private Limited Company Without Share Capital	Include
Private Unlimited	Include
Private Unlimited Company Without Share Capital	Include
Other	Include, with manual process to identify if companies should be included in the population
Limited Partnership	Exclude
Company converted / closed	Exclude

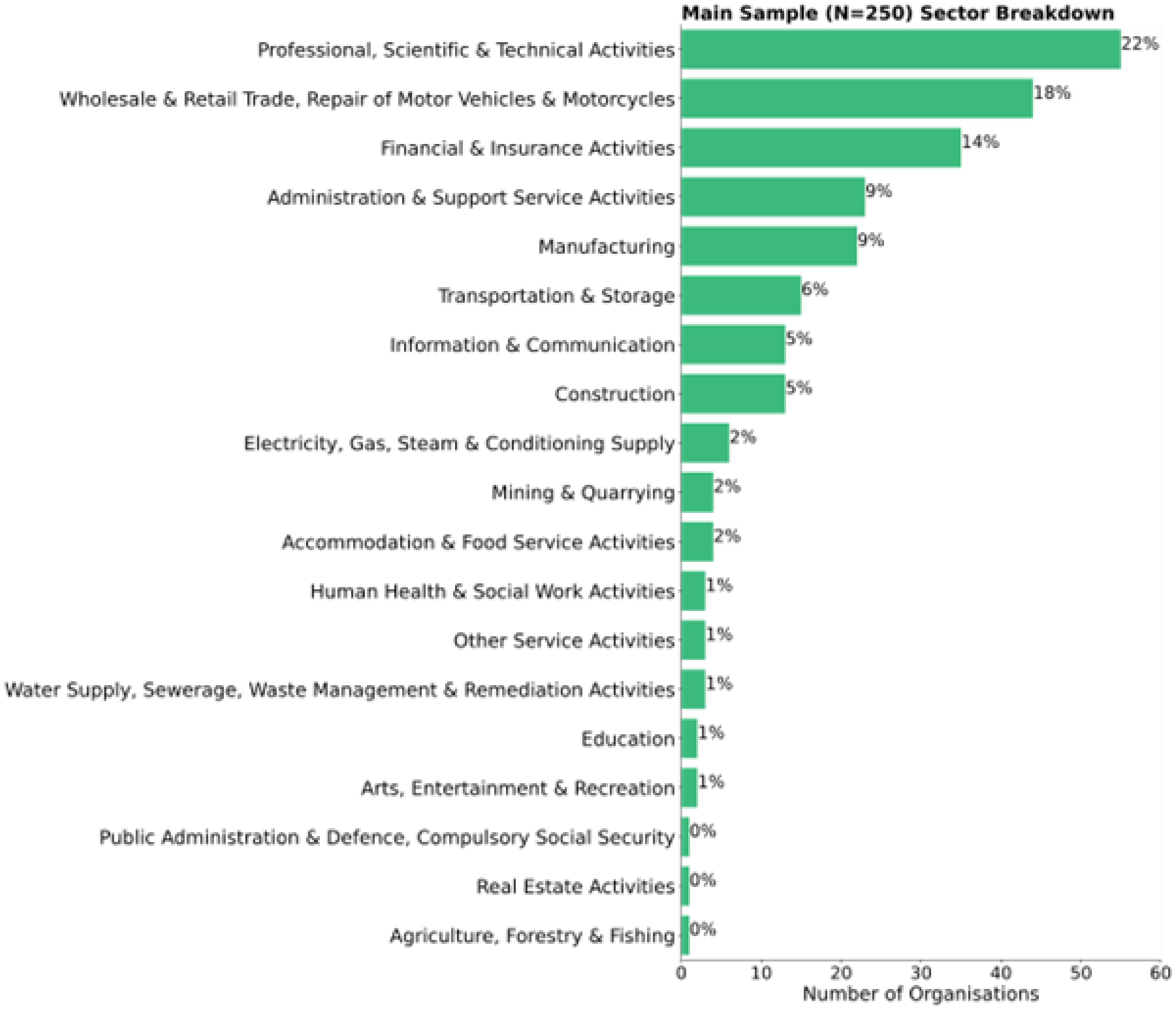
Main Sample

A sample of 250 organisations was identified from the population of 801 which met the criteria for the main sample.

The distribution of the main sample of organisations was stratified based on sector to be representative of the population of companies which met the main sample criteria, within 1%

variance. This is not representative of the entire UK business population. Organisations were selected at random from the corresponding sectors.

The sectors used are based on the UK Standard Industrial Classification (SIC) code[10] for each company, which is used by Companies House to provide a description of the company's nature of business. The breakdown was as follows:



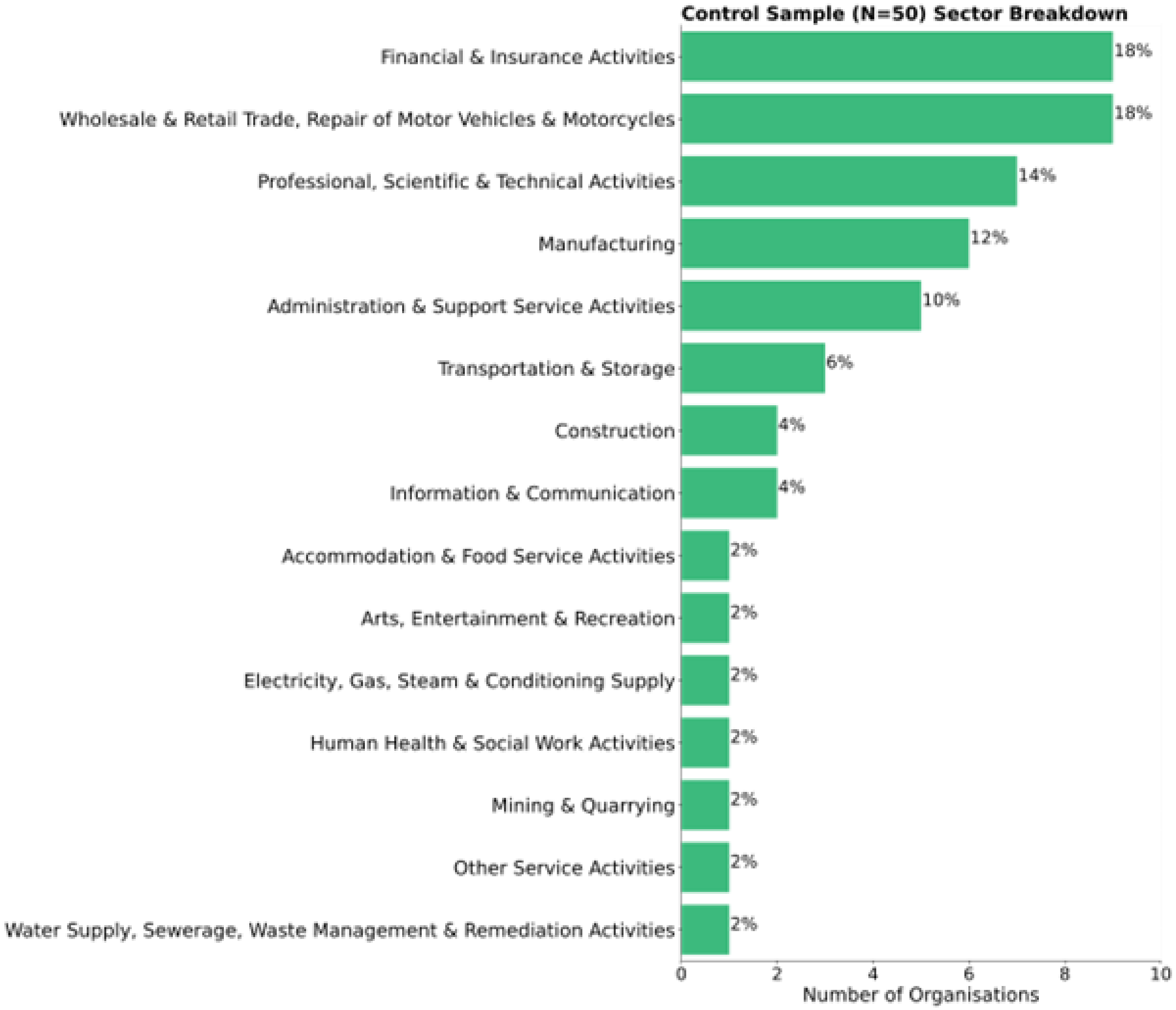
In some cases, detailed reviews of annual reports or Companies House identified grounds for exclusion e.g. the company ceased trading. In these instances, a replacement company from the same sector was identified from the initial population record, to allow the sample to remain statistically representative of the population.

Control Sample

[10] Companies House. 2018. Standard Industrial Classification of Economic Activities (SIC). Standard industrial classification of economic activities (SIC) - GOV.UK (www.gov.uk)

A sample of 50 companies was identified from the population of 450 companies which met the criteria for the control sample.

In line with the main sample, the distribution of the control sample of organisations was stratified based on sector to be representative of the population of companies which met the control sample criteria, within 1.11% variance. Organisations were selected at random from the corresponding sectors. The breakdown was as follows:



Assessing Company Annual Reports

Each annual report was downloaded from the company website where possible, to allow for application of digital search tools to look for key search words (Annex A).

Where the company annual report was not available on the company website, the report was downloaded from Companies House and manually searched.

Each annual report was then assessed using the Quality Assessment Framework (Annex B) to identify which areas of cyber security the company reported against, and to what level.

Data Validation & Quality Assurance

Various data validation and quality assurance steps were undertaken to ensure that the analytical output was fit-for-purpose.

A process was undertaken to verify the quality of data collected by validating the year of the annual report to be 2021 or later, and confirming that the company number on annual reports downloaded from company websites matched the company number in the report lodged with Companies House.

Quality assurance activities were also undertaken to confirm that the data was complete prior to undertaking analysis activities.

Azets also conducted a second, independent quality review on 30% of both samples to confirm the accuracy of assessments using the Quality Assessment Framework as a reference. A small number of differences were noted between the original score and independent review score. Where this was the case, these were highlighted and subject to independent moderation. The results of the review process provided sufficient confidence that there was no requirement to increase the volume of peer reviews.

Interviews

A number of interviews were held as part of the research, with individuals representing companies in the main sample. The purpose of the interviews was to obtain qualitative, detailed insights on the perceived benefits and barriers of including cyber disclosures within annual reports. Interviews focused on understanding what areas companies would be more or less comfortable reporting on. Explanations were sought to understand the rationale for assertions.

The interviews were conducted using a standard set of questions, which are set out in Annex C, with individuals holding a senior cyber security role, e.g. Chief Information Security Officer, in their respective organisation.

Literature Reviews and Desk Based Research

Literature reviews and desk-based research was conducted to identify similar studies which are publicly available. The results were used to compare and contrast statistics and findings highlighted from this research with other similar research. Additionally, reviews of past research were used to inform methodologies, using lessons learned to incorporate known effective techniques into this research.

Sources used for literature reviews were limited to those published within the last five years. Main sources used included:

Researcher	Year	Title of Study	Scope of Study
FRC	2022	Lab Report: Digital Security Risk Disclosure	UK
Eijkelenboom, E.V.A., & Nieuwesteeg, B.F.H	2021	An analysis of cybersecurity in Dutch annual reports of listed companies[11]	Dutch listed companies
Wavestone	2020	How mature are annual reports of the FTSE 100 regarding cybersecurity[12]	FTSE 100, UK
ICAS	2020	Cyber and data disclosures in annual reports[13]	UK
EY, & CPA Canada	2020	CPA Canada and EY: Cybersecurity Disclosure Report[14]	Canada
US Securities and Exchange Commission	2018	Commission Statement and Guidance on Public Company Cybersecurity Disclosures[15]	US

[11] Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. Computer Law and Security Review, 40, 105513. https://doi.org/10.1016/j.clsr.2020.105513

[12] Pouchet, F., & Springate, O. (2020). How mature are annual reports of the FTSE 100 regarding cybersecurity? (Issue July). https://www.wavestone.com/app/uploads/2016/06/Wavestones-FTSE-100-Cybersecurity-Index-2020-Annual-Reports-–-EN.pdf

[13] ICAS. (2020). Cyber and data security disclosures in annual reports (p. 1). https://www.icas.com/professional-resources/corporate-and-financial-reporting/financial-reporting/cyber-and-data-security-disclosures-in-annual-reports

[14] EY, & CPA Canada. (2020) CPA Canada and EY: Cybersecurity Disclosure Report. ey-cpa-cybersecurity-report.pdf

[15] US Securities and Exchange Commission. (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Commission Statement and Guidance on Public Company Cybersecurity Disclosures

Interpretation of Findings

How to interpret findings

Quality Assessment Framework

To provide an objective and consistent method to assess the quality of cyber disclosures within annual reports, a Quality Assessment Framework was created (Annex B).

The framework sets out six key cyber themes:

- Strategy
- Governance
- Risk Management
    - Risk Recognition
    - Policies and Procedures
    - Assurance
- Cyber Incidents
    - Planning
    - Response Capabilities
- Supply Chain
- Cyber Skills and Training

Two of these themes were further broken down into sub-themes, due to their broad coverage. Risk Management was broken down to cover the three key aspects in its lifecycle – recognition of risks, the policies and procedures put in place to mitigate risks and finally, assurance of a company's approach to managing risk. Cyber Incidents was also broken down to cover the two key aspects in its lifecycle, how the company plans for a cyber incident and the company's ability to respond to an incident.

The Quality Assessment Framework sets out criteria for assessing the quality of cyber disclosures for each theme. The quality levels are defined in the table below:

Quality Reporting Level	Description
No Reporting	There is no mention of the theme.
Basic Reporting	Reporting is limited.
Core Reporting	Reporting is of reasonable quality.
Enhanced Reporting	Reporting is of high quality.

Criteria for assessing each theme against the defined reporting levels is detailed in the Quality Assessment Framework in Annex B.

How to interpret charts

The sector breakdown charts in the Methodology section of the report show the number of companies for the x-axis, as small percentages meant this data would be lost if using percentage as the x-axis.

The x-axis of all other charts throughout this report shows the percentage of companies that disclose or their quality of disclosure. The corresponding sample number is given by n=sample number.

As referenced in the Quality Assessment Framework section above, six themes are reported against, two of which have been broken down to include sub-themes. For reporting on these two themes, averages were used to calculate the quality of the disclosure.

How to interpret sectoral analysis

Sectoral analysis was undertaken to identify the difference, if any, in quality and prevalence of cyber disclosures between sectors. Due to the small sample sizes in some sectors, analysis was only made on those sectors which included at least 10 companies, so as not to skew the data due to small sample sizes. As such, sectoral analysis is also only performed on the main sample.

How to interpret qualitative data

Interviews were conducted with senior cyber or digital security personnel within large and very large companies. This provided qualitative data to supplement the quantitative data and to provide insights into the perceived benefits and challenges of including cyber disclosures within annual reports. Insights from interviews and individual responses are shared throughout this report to support the research. However, these examples are not intended to be statistically representative.

Data Limitations

The results of participant interviews may be affected by bias due to the voluntary nature of the interviews. This may have resulted in those who were more positive or negative about cyber disclosures taking part in the interviews.

Control sample results may be affected by the small sample size. Only 50 companies were included in the control sample for a population size of 450 and therefore the results may not be an accurate representation of the wider population.

UK Standard Industrial Classification (SIC) codes were used to identify sectors for each company. As there is a large number of sector classifications, this resulted in relatively small sample sizes for certain business sectors, meaning the analysis of correlation between business sector and quality of cyber disclosures is limited.

Key Findings

High prevalence yet low quality of Risk Management disclosures resulting from Companies Act 2006 requirements

The prevalence and quality of information varied across samples and sectors, however where disclosures were made, these were most often due to cyber security being recognised as a key risk to the business and therefore was referenced within the “Principal Risks” section of the annual report e.g. as part of Cyber Risk or Business Continuity Risk. This is most likely due to the requirements of the Companies Act 2006 which applies to all UK companies and sets out the need for companies to include details of principal risks and uncertainties within their annual report. This most likely explains why Risk Management was the highest disclosed theme (75%).

Despite the high prevalence of disclosures for Risk Management, only 5% of companies in the main sample achieved enhanced reporting levels. Although a large number of companies provide a short statement to confirm that risk management processes are in place, or reference cyber security as a key risk to the business, most provide limited information on areas such as how risk is managed, the presence of an Information Security Management System or the assurances received over risk mitigation controls. This suggests that companies are most likely to disclose the minimum information required to comply with the Companies Act 2006 requirements or do not understand what high quality disclosures would consist of for this theme.

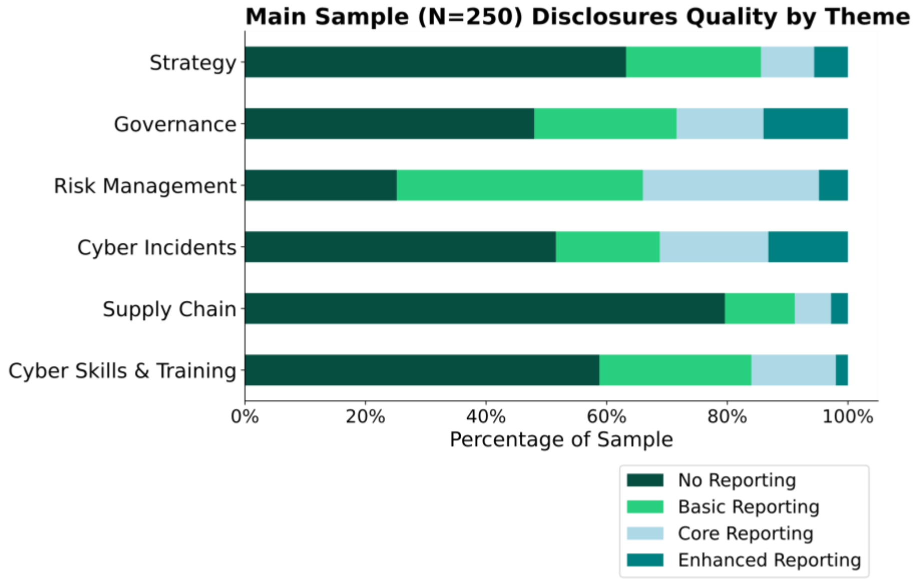
High prevalence and quality of Risk Management and Governance disclosures for listed companies reporting against the UK Corporate Governance Code requirements

Listed companies[16] must comply with governance reporting requirements of the UK Corporate Governance Code, which include, for example, reporting on the activities of audit and risk committees as well as the board. As 25% of the main sample were listed companies, this is likely the reason why there was a high prevalence of Risk Management disclosures.

As a by-product, prevalence of Governance disclosures were also high. Analysis found that prevalence of governance disclosures were higher for listed companies (92%) compared to private companies (39%). Disclosures on governance for listed companies were also found to be of higher quality. 52% of listed companies in the main sample achieved core or enhanced reporting for governance, compared with 20% of private companies.

[16] In July 2024 the Financial Conduct Authority (FCA) updated its Listing Rules, including the categories under which securities are listed on the Official list. As a result, there was a change in the companies required to follow the UK Corporate Governance Code. Previously, the Code applied to premium listed companies. Going forward, companies which need to follow the Code include all those listed in the commercial company category or the closed-ended investment funds category.

Low prevalence of high quality disclosures



Disclosures were most often found to be of a basic level across the majority of themes. The theme achieving the highest percentage of enhanced disclosures was Governance, however, this was still only 14% of the main sample. In fact, Governance and Cyber Incidents were the only two themes in which at least 10% of the sample achieved enhanced disclosures.

High quality disclosures on Cyber Incidents despite low prevalence

In some instances, themes which had a lower prevalence still achieved relatively high quality disclosure levels. This was the case for Cyber Incidents in which only 48% of companies in the main sample provided disclosures on this theme. However, disclosures were often of a higher quality, achieving a higher percentage of core (18%) and enhanced (13%) reporting, than other themes.

Disclosures are lower in prevalence and quality

Of the six themes analysed in the main sample, Supply Chain achieved the lowest percentage of disclosures (20%) within annual reports. The research found that although many company reports discussed their supply chain, most referenced non-cyber security aspects such as responsible sourcing of materials, sustainability and how they combatted the risk of modern slavery.

Disclosures were also found to be of lower prevalence or quality in three other themes:

- Low prevalence of disclosures were found for Cyber Incidents Planning (34%)
- 41% of companies disclosed that they offered cyber security training
- 14% disclosed that there is responsibility for cyber at a board level

These results suggest that there is a lack of disclosure within annual reports. This suggests organisations lack an understanding of why disclosing these activities would be valuable to stakeholders, a lack of demand for this information from stakeholders, or organisations have decided to prioritise other areas in relation to that particular annual report based on their materiality assessment.

The prevalence and quality of disclosures across themes are not consistent for each sector

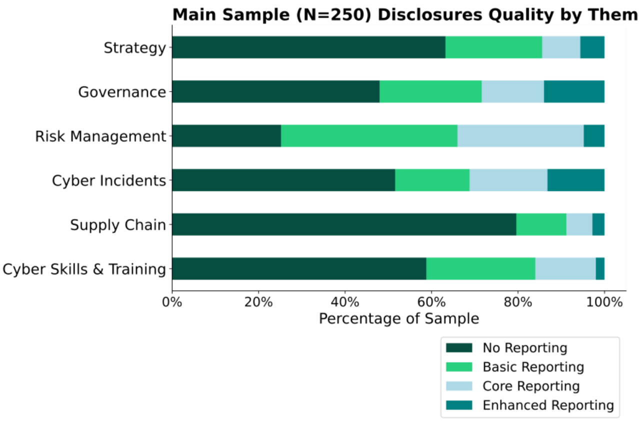
Where certain sectors were seen to have higher prevalence or quality of reporting for one theme, this was not reflected across all themes. For example, companies in the Information and Communication sectors were found to have higher quality disclosures for Risk Management than other sectors, and more prevalent disclosures for Supply Chain than other sectors. However, companies in this sector also had lower quality disclosures for Cyber Incidents compared to other sectors, despite having nearly the same prevalence of disclosures.

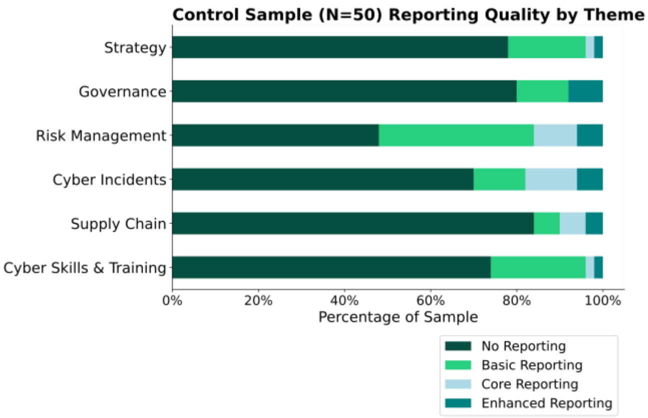
No one sector was shown to have higher prevalence or quality of disclosures across all themes. This suggests that although sectors may be better at disclosing for some themes, this will usually be because it is a theme that they see as key information for their stakeholders that should be disclosed, rather than disclosing high quality information across all cyber themes.

Consistently higher prevalence and quality of disclosures were seen within the main sample compared to the control sample.

Prevalence of cyber security disclosures for the main sample were higher (77%) compared to the control sample (56%).

The main sample also achieved higher quality disclosures than the control sample, as evidenced by the charts below:

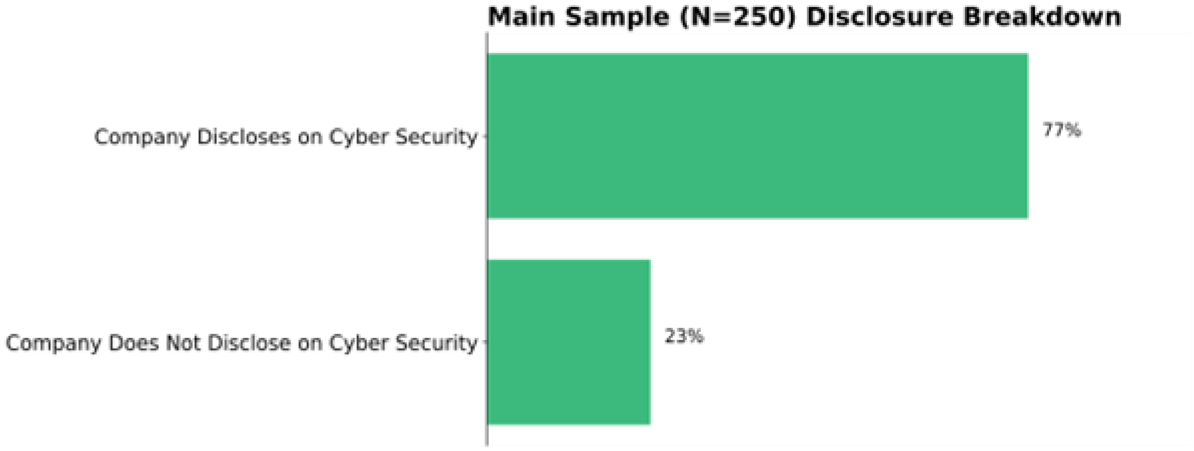




The higher prevalence and quality of disclosures for the main sample could be due to the lower proportion of listed companies in the control sample than the main sample; 11% and 25% respectively. The requirement for listed companies to comply with the UK Corporate Governance Code means that they have to provide wider disclosures on areas including governance, audit, risk and internal control. Companies that are bound only by the requirements of the Companies Act 2006 need only report on principal risks and uncertainties when considering the reporting of cyber risk.

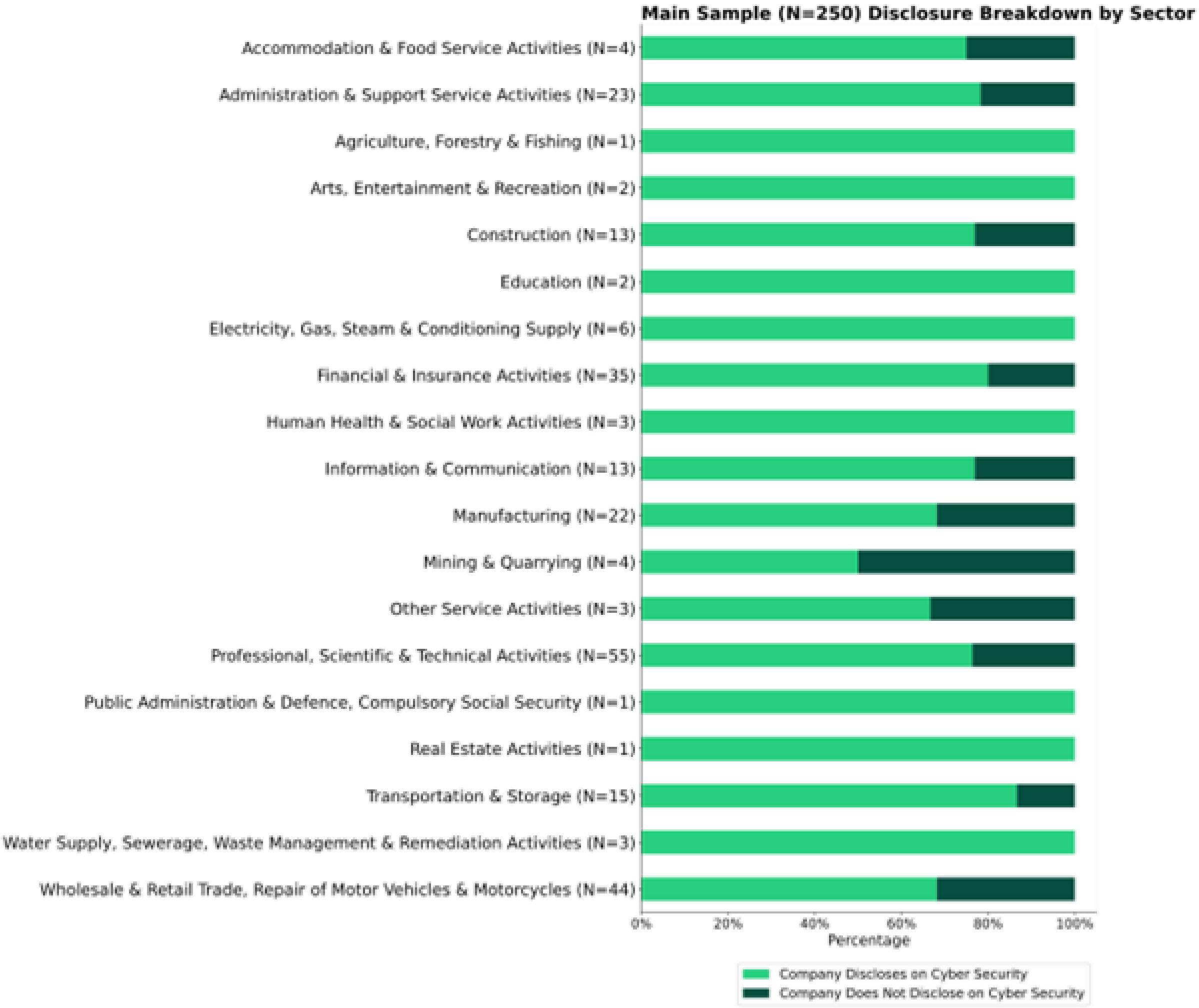
Prevalence of Reporting

General Findings



Research found that 77% of companies within the main sample made cyber disclosures either directly within their UK annual report or by cross-referencing a group-level report. The volume and quality of information disclosed varied, however, disclosures were due to cyber security being recognised as a key risk to the business and therefore was referenced within the “Principal Risks” section of the annual report.

Sectoral Analysis



In the main sample, the 250 companies represented 19 sectors. In some cases, only one or two companies were included from a sector. Therefore, to avoid small sample sizes skewing the results, sector based analysis has only been undertaken where there are at least 10 companies for that sector in the sample.

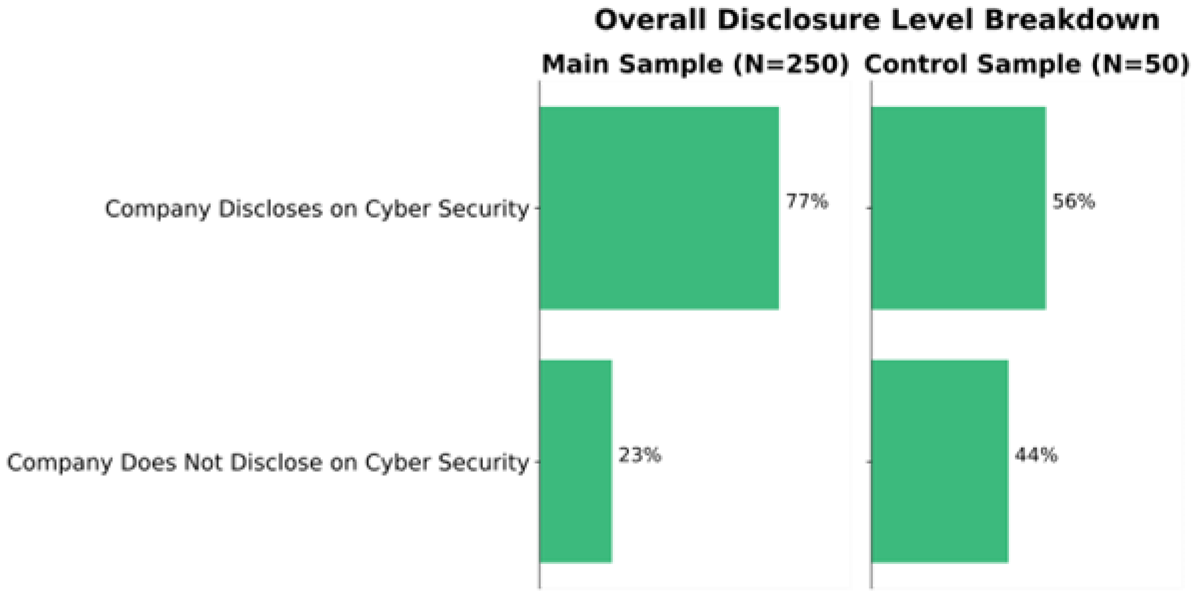
The research has not identified correlation on the prevalence of cyber disclosures within specific sectors. Regulated sectors often, but not always, have requirements to prioritise cyber security or have greater risk management processes and therefore it may be expected that this greater emphasis carries through to public disclosures. For example, it may be expected that companies that are part of UK Critical National Infrastructure[17] (CNI), and those which must comply with the Network and Information Systems (NIS) Regulations[18],

[17] National Protective Security Authority 2023. Critical National Infrastructure. Critical National Infrastructure | NPSA

[18] The Security of Network & Information Systems Regulations (NIS Regulations) provide legal measures to boost the level of security (both cyber and physical resilience) of network and information systems for the provision of essential services and digital services. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

might demonstrate significantly higher prevalence of cyber disclosure within their annual report. However, research found that this is not the case. When filtering the results to focus on sectors which are regarded as Critical National Infrastructure, the research found that 82% of companies in these sectors include cyber disclosures within their annual report whilst 18% do not. This is only marginally higher than the average across all sectors, in which 77% did disclose on cyber and 23% did not.

Comparison to Control Sample



Findings suggest that companies in the main sample (77%) are more likely to include cyber security within their annual report than the control sample, with only 56% of the control sample disclosing on cyber security.

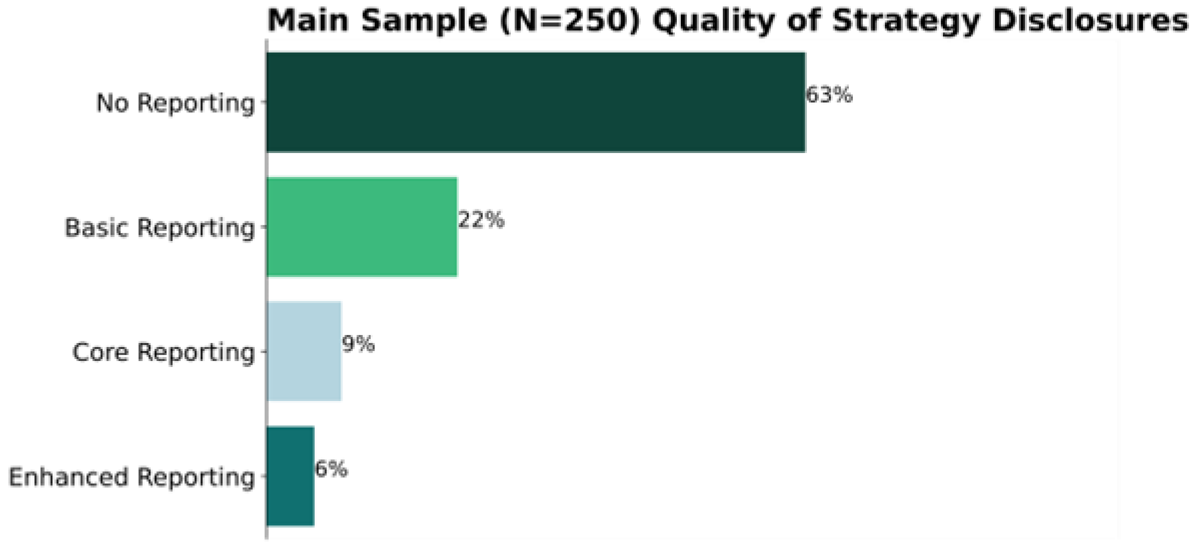
One potential reason for this is that there is a lower proportion of listed companies in the control sample than the main sample; 11% and 25% respectively. The requirement for listed companies to comply with the UK Corporate Governance Code, means that they have to provide wider disclosures on areas including governance, audit, risk and internal control. Companies that are bound only by the requirements of the Companies Act 2006 need only report on principal risks and uncertainties.

This is reflective of other research studies. For example, a research study performed by Wavestone in 2020 on the cyber maturity of FTSE 100 companies shows increased reporting levels when compared to this research. It found that 95% of FTSE 100 companies disclose on cyber security in their annual report, supporting the theory that listed companies are more likely to disclose on cyber security.

Quality of reporting by theme

Strategy

Main Sample General Findings



Low prevalence

Of the six themes analysed, Strategy was found to have the second highest percentage of no reporting for the main sample.

Low quality of disclosures

Most companies that disclosed on Strategy (22%) simply confirmed that a digital or cyber strategy exists or made reference to investment, but with minimal detail. 9% of companies achieved a core level of disclosure and only 6% of companies achieved enhanced reporting for this theme, meaning that companies are currently less likely to set out the importance of the digital or cyber strategy to the overall business model and demonstrate how this strategy is aligned to the wider organisational strategy.

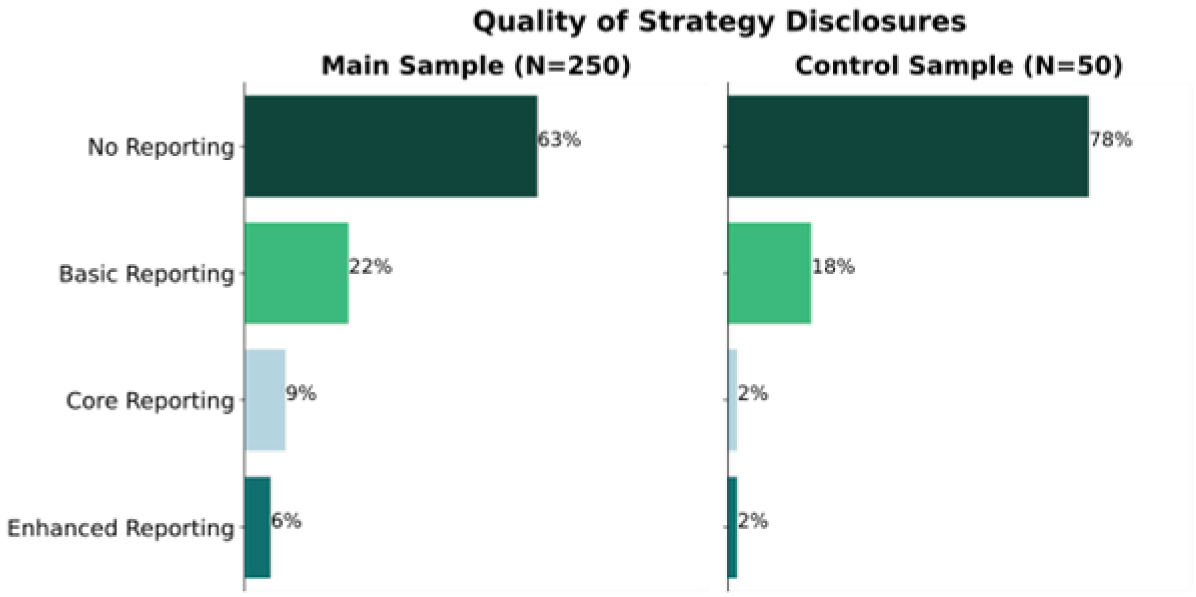
Sectoral Analysis

Only 23% of companies in the Financial and Insurance Activities and Construction sectors disclosed on Strategy. This is lower than the average across all sectors, where 37% disclosed on Strategy.

Some sectors demonstrated higher prevalence of Strategy disclosures than the average. For example, in the Administration & Support Service Activities sector, 48% disclosed on Strategy and in the Information & Communication sector, 62% did so.

No sectors were particularly better at providing higher quality disclosures on Strategy. The percentage of those that achieved core and enhanced reporting levels were in line with the average across all sectors.

Control Sample



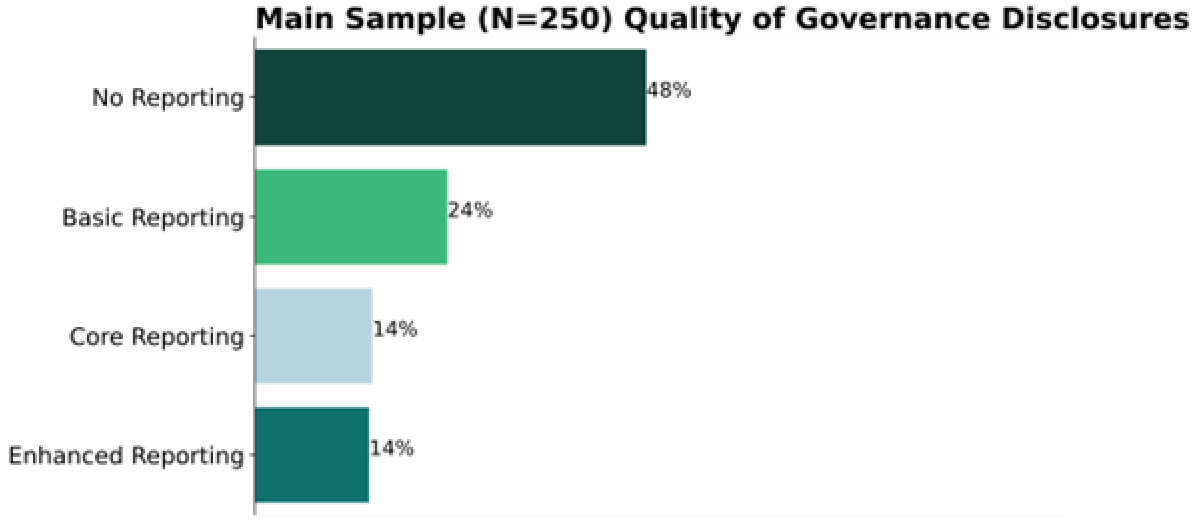
The results found that even fewer of the control sample provided any disclosures on Strategy, with only 22% compared to the 37% in the main sample.

Where companies disclosed on Strategy, most companies in both samples only provided basic reporting, such as confirming the existence of a Strategy but give minimal detail beyond this.

Some companies in the control sample did reach higher quality levels of disclosures however this was consistently lower than the main sample.

Governance

Main Sample General Findings



High prevalence

Governance was the second most prevalent theme, with just over half of companies in the main sample including this in their annual report (52%), compared to those that did not (48%). The research observed more frequent disclosures on governance as a by-product of risk disclosures.

Link between disclosures and legal status of company

Higher levels of prevalence for this theme are likely influenced by the higher proportion of listed companies in the main sample (25%) that are required to comply with governance reporting requirements of the UK Corporate Governance Code. For example, from reporting on the activities of audit and risk committees as well as the board. This is evidenced by further analysis which found that prevalence of governance disclosures were higher for listed companies (92%) compared to private companies (39%).

Disclosures on governance for listed companies were also found to be of higher quality. 52% of listed companies in the main sample achieved core or enhanced reporting for governance, compared with 20% of private companies.

High quality of disclosures

14% achieved core reporting, which in most instances included reference to an Information Security Steering group, or detailing cyber responsibilities within either the risk committee or audit committee report sections.

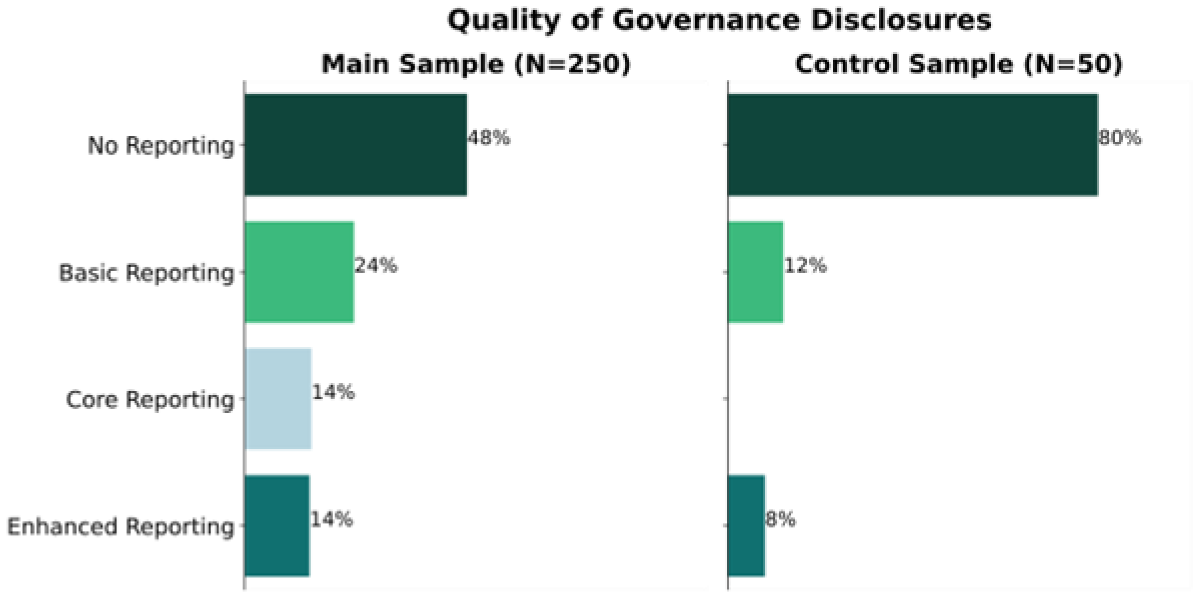
Governance is one of the themes in which the highest number of companies received an enhanced reporting level (14%). Companies detailed ownership at senior levels, explained the governance groups at which cyber is discussed and how this is used to inform business decisions. Research found that companies which achieved this level of reporting referenced roles such as executive responsibilities of Chief Digital and Technology Officers, roles of the Risk Committee and how this feeds into decisions on aspects such as technology advancements.

Sectoral Analysis

69% of companies in the construction sector provided disclosures on Governance, compared to the average of 52% of companies across all sectors, suggesting that companies in the construction sector are better at recognising the importance of informing stakeholders about how cyber risk is governed.

Companies in the Financial and Insurance Activities sector did not achieve core or enhanced reporting levels as often as those across other sectors. No companies in this sector achieved core level reporting, compared to the overall average of 14%, and only 3% achieved enhanced level reporting, compared to the overall average of 14%. This could be partly due to the lower prevalence of disclosures also seen for this sector, in which 43% disclosed on Governance compared to the average across all sectors of 52%.

Control Sample



The research found that there was a significant difference between those which report on Governance in the main sample (52%), compared with the control sample (20%). This is the most stark contrast in reporting between the main and control samples across all six themes.

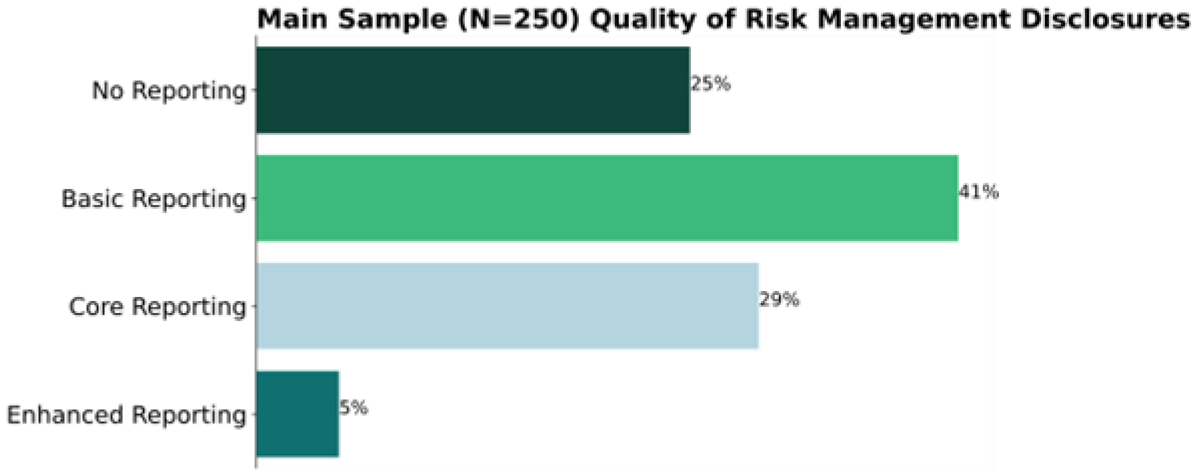
The contrast in reporting between the main sample and control sample could be influenced by the higher proportion of listed companies in the main sample that need to comply with the disclosure requirements of the UK Corporate Governance Code.

However, there were similarities between the main sample and control sample, where companies were disclosing on Governance. Most disclosed basic information such as a short statement to confirm that cyber risk is governed, without detailing further information such as the governance structures in place.

No companies in the control sample obtained core level reporting. This means that where companies in the control sample disclosed on Governance, they either gave basic information or enhanced information such as ownership of cyber at a senior level, discussion of cyber at appropriate governance groups and used the information to inform business decisions.

Risk Management

Main Sample General Findings



High prevalence

Risk management was the most prevalent theme for the main sample out of all six themes. 75% of companies in the main sample provided disclosures on at least one Risk Management sub-theme, compared to 25% that did not.

The high prevalence of disclosures for this theme could be due to company attempts to meet the requirements of the Companies Act 2006, which requires companies to disclose details of their principal risks. This means that if cyber is considered a principal risk for the company, they are required by the Companies Act 2006 to disclose this in their annual report.

High prevalence does not result in higher quality

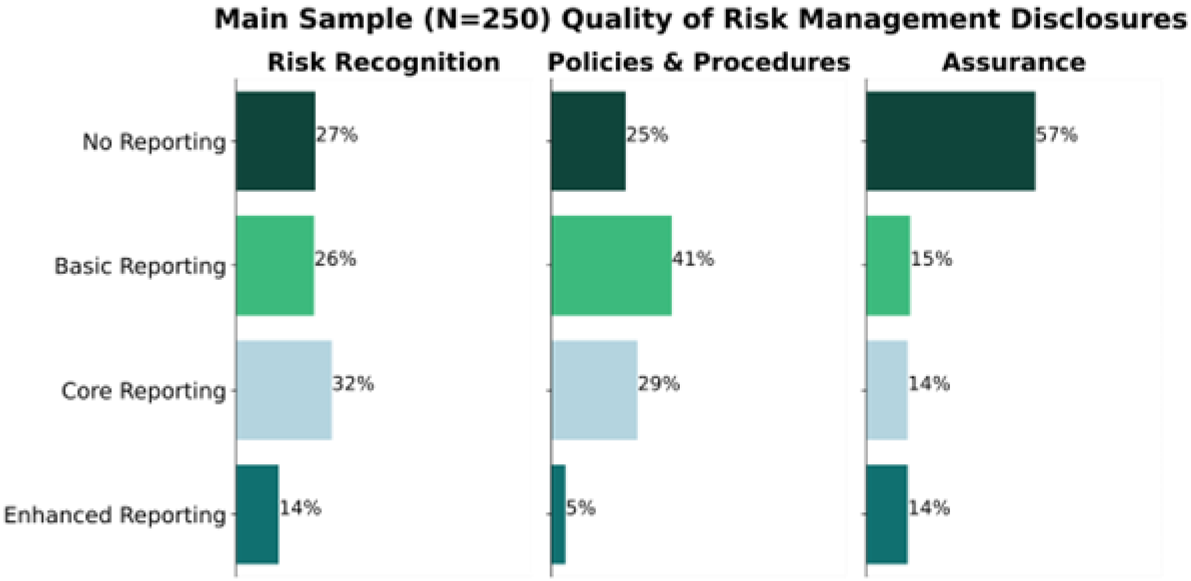
Despite the high prevalence of reporting for this theme, only 5% of companies achieved enhanced reporting levels. Although a large number of companies currently give a short statement to confirm risk management processes are in place, or reference cyber security as a key risk to the business, most provide limited information on areas such as how risk is managed, the presence of an Information Security Management System or the assurances that they receive over risk mitigation controls.

These findings align with those from other research studies on cyber disclosures internationally, which found that risk-related disclosure is a descriptive activity which requires improvement to provide value to key stakeholders. For example, the 2020 Wavestone report found that 95% of FTSE 100 companies acknowledge the impact a cyber attack or incident could have. However, only 44% of those companies expand upon these risks and make specific, contextualised mention of the impacts cyber attacks would have on their business, whilst 51% briefly mention the risk and impact.

The research by ICAS on 12 FTSE company annual reports from 2018 to 2020 also found that all companies identified cyber security and privacy as key risks and described the measures they had taken to mitigate the risk of cyber crime and safeguard data. However, the detail provided by the companies varied, and it was clear that companies were cautious to the extent of the information disclosed on their defences.

Quality of reporting impacted by understanding of cyber

Low quality despite higher prevalence for this theme may be explained by the qualitative information obtained from interviews, in which some individuals suggested that they were concerned that cyber security is too technical to include in annual reports. Specifically, individuals were concerned that bringing cyber into layperson terms can "water it down" and find it challenging to express threat and countermeasures in a way that is "not lost on someone" who does not have a technical background.



Risk Recognition

Most companies that disclosed on Risk Recognition obtained a core level of reporting, which included reference to regular risk assessments and threat intelligence being used to identify risks or confirmed that a risk management framework was in place to escalate risks in line with wider organisational risk frameworks.

In most instances, research found that companies disclosed on their cyber risk by including it as a risk in their “Principal Risks” section, most of which gave a description of the risk and mitigation actions undertaken. 14% of companies in the main sample obtained enhanced level reporting, meaning they demonstrated a clear understanding of their critical assets and provided information about relevant risk mitigations.

A good example of a company that achieved enhanced level of reporting was a water company which showed a clear understanding of the cyber risk to the critical process of providing drinking water, and explained the mitigations it had taken as a result. Many companies that did not achieve enhanced levels of reporting stated cyber risk in generic terms without specifically relating it to their business objectives and critical assets.

Policies and Procedures

Policies and Procedures was the most reported sub-theme, included by 75% of companies in the main sample. Where companies achieved core reporting levels, this was often due to the company referring to an Information Security Management System as part of its risk mitigations section. A small percentage of companies (5%) demonstrated how these policies and procedures met their needs and aligned to different strategic areas and processes. In some instances, companies even explained the role of the board to assess their cyber security policies and procedures to ensure they remain fit for purpose.

There was also a correlation between the prevalence of disclosures for Risk Recognition and Policies and Procedures. This is likely to be similar as most companies included a short statement to confirm that cyber risk management policies, procedures and processes were in place to mitigate the identified cyber security risk.

However, the quality of disclosures was lower for Policies and Procedures than Risk Recognition. This could be explained by findings from qualitative interviews which found that some security professionals are concerned that a company may be seen to be “showing off” if they portray a positive picture of their Information Security Management System and supporting controls and, in doing so, making them a target for attackers. This might suggest why there is a lower reporting quality achieved for sub-themes relating to how the risk is mitigated, such as Policies and Procedures, rather than Risk Recognition.

Assurance

Assurance was the least reported sub-theme, however prevalence of disclosures was still relatively good for this sub-theme, with 42% of companies disclosing on this in their annual report. For those that disclosed on Assurance, the quality of reporting was almost an even split with 15% achieving basic and 14% each receiving achieving core and enhanced reporting. This means that where companies did disclose on Assurance, the information disclosed varied equally from being a basic reference, such as confirming that assurances are obtained, to companies disclosing on both internal and external assurances that have been obtained, and the action that has been taken as a result of these assurance activities.

Most companies that achieved enhanced level reporting referenced a “three lines of defence” model in which assurances were obtained through internal audit teams, external audit teams and security testing such as penetration tests. External assurances are a requisite for achieving enhanced reporting, and accordingly, only 14% of companies in the main sample referenced any external assurance of their cyber risk management. The detail of disclosures for external assurances also varied. In some instances, the company simply stated that external assurances were obtained through their three lines of defence model and the use of an external audit team. Other companies detailed where external assurances were obtained from and how cyber security was incorporated into aspects such as their external audit plan.

The relatively low rates of disclosure of this information may demonstrate a potential reluctance to share these details, there is a lack of understanding of the value of providing these assurances to their stakeholders, there is a lack of demand for this information from stakeholders, or organisations decide it is not to because there is no formal requirement and it is not considered as material.

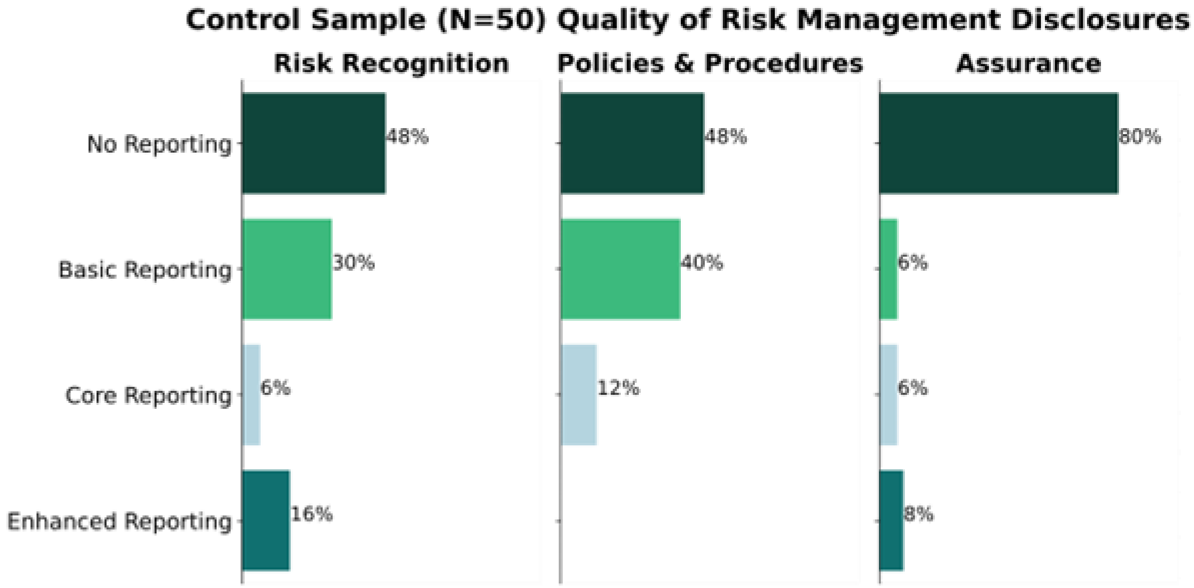
Sectoral Analysis

It was found that companies in the Manufacturing sector are less likely to disclose on Risk Management than companies in other sectors. 36% of companies in this sector did not disclose on Risk Management, compared with 25% of companies across all sectors. It was also found that companies in the Transportation & Storage sector were more likely to disclose on Risk Management with 87% of companies in this sector reporting on at least one sub-theme within Risk Management.

The analysis also identified one sector that produced higher quality disclosures: the Information & Communication sector. 23% of companies in this sector achieved an average of enhanced reporting levels across the Risk Management sub-themes, compared to the average of 5% who achieved this reporting level across all sectors. The section of the report in which this information was disclosed varied. For example, some companies disclosed on their risk within their Principal Risk and Uncertainties section, whilst others included it within the Corporate Social Responsibility section of their report. However, all companies within this sector that achieved enhanced reporting levels referred to a key aspect of their risk as being their ability to maintain and continue services, often stemming from their increased reliance on digital and IT infrastructure. As a result, all companies expressed a concern for their reputation, frequently highlighting “loss of trust” as a potential major impact of their cyber risk.

This highlights that the most probable reason that companies in this sector achieved higher quality disclosures was due to their reliance on digital systems and the reputational impact a cyber incident may have on their organisation.

Comparison to Control Sample



Correlation between Risk Recognition and Policies and Procedures

For both samples, the percentage of companies that did not report on Risk Recognition was very similar to, if not the same as, those that did not report on Policies and Procedures. This suggests that there is a correlation between those that report against these two sub-themes. Where a company does not report against one of the sub-themes, they also tend not to report on the other sub-theme.

Risk Recognition

For Risk Recognition, most companies provided core reporting in the main sample whereas most companies in the control sample provided basic reporting. This means that companies in the main sample are more likely to have higher quality of reporting, and will disclose aspects such as how risks are identified, assessed, and escalated, instead of only referencing that the risk exists.

Policies and Procedures

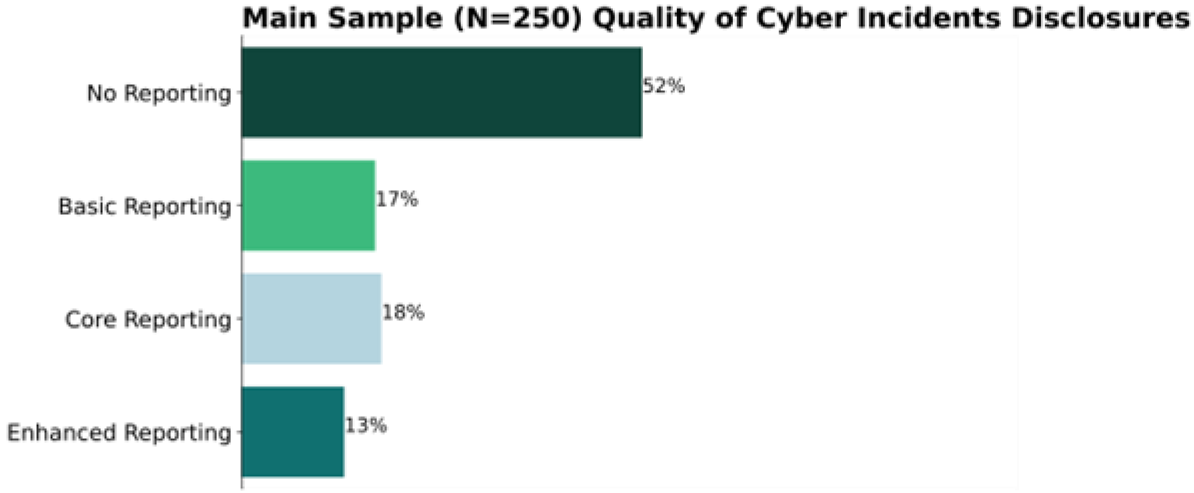
For Policies and Procedures, most companies that disclosed in both samples achieved the same quality of reporting: basic reporting. Research found that the main sample was higher in prevalence for disclosures on this theme than the control sample, but not in quality.

Assurance

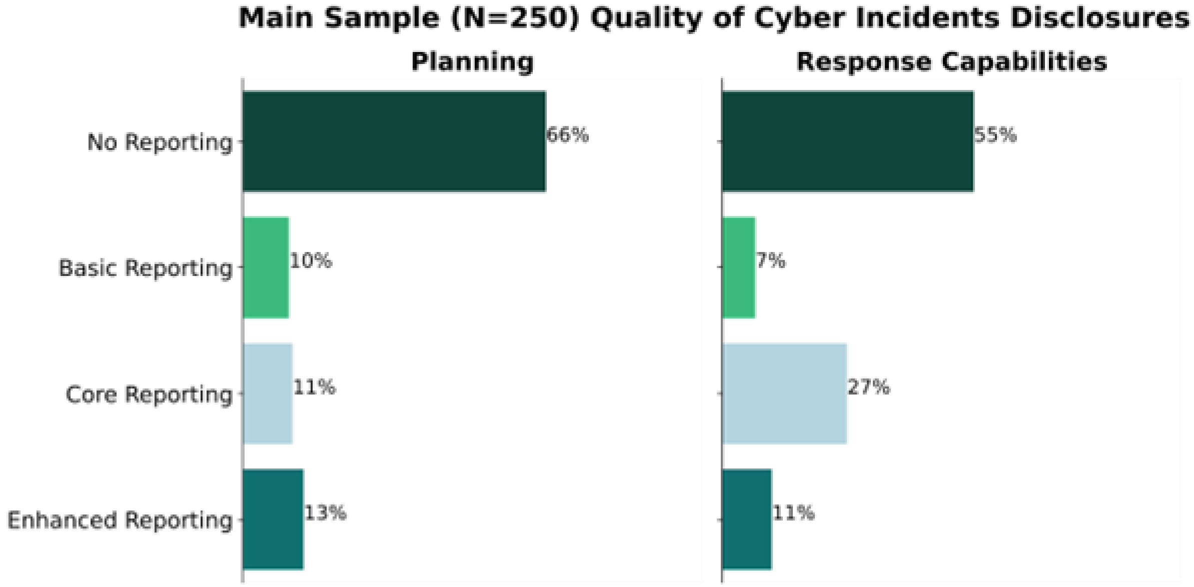
Within both samples it was found that for those companies which disclose on Assurance, the quality of reporting was an even split between basic, core and enhanced levels.

Cyber Incidents

Main Sample General Findings



Cyber Incidents did not have the highest prevalence of disclosures, however where companies did disclose on this theme (48% in total), disclosures are often of a higher quality (higher percentage of core and enhanced reporting) than other themes, particularly within the Response Capabilities sub-theme, as seen in the graph below.



High quality of disclosures across the whole theme

The high quality of disclosures for this theme could be due to a number of reasons. Firstly, where the risk of cyber attacks, incidents, or breaches was identified as a principal risk, the Companies Act 2006 requirement to disclose principal risks likely encouraged companies to disclose incident planning and response information as mitigation of such risk scenarios.

It may also be due to the media attention on this subject, and the level of risk cyber incidents, such as ransomware, pose. This may result in stakeholders having a higher interest in the company's ability to respond to these events, and therefore a higher priority to disclose this information. This would also explain why disclosures are more prevalent and of higher quality for the Response Capabilities sub-theme than Planning.

The high quality reporting for this theme despite the lower prevalence could also suggest that where companies disclose on Cyber Incidents, they often have a more mature understanding of the theme and the importance of including it in their annual report, to provide assurance to investors or other stakeholders that a proactive approach is taken.

Planning

Planning has a higher rate of enhanced disclosures (13%) than other themes, indicating regular testing on incident response plans. However, 66% of companies did not disclose on this sub-theme at all, meaning they did not confirm if they had cyber incident response plans in place, and 21% confirmed that they had plans in place but did not disclose if these were regularly tested. In most cases, disclosures were included as mitigations to risk, being either a cyber risk or business continuity risk.

Response Capabilities

Response Capabilities were more prevalent and of a higher quality when combining both core (27%) and enhanced (11%) reporting, than Planning. This may be due to companies focusing on reactive capabilities rather than proactive planning when managing their cyber attack risk.

Higher quality of disclosures was achieved where companies detailed the response capabilities in place. In most cases, this included backup recovery capabilities and out of hours monitoring. In some instances, companies disclosed that they had suffered an attack in the reporting period, and in minimal cases, the company disclosed the financial impact of the attack and whether they had to claim on their insurance. 11% made specific references to the role of the board in responding to a cyber incident, meaning they achieved enhanced levels of reporting.

Variance of annual report findings to interviews

As stated above, higher prevalence and quality of reporting was identified for Response Capabilities compared to Planning. This differs from feedback that was obtained during interviews, in which some individuals expressed a higher concern about disclosing their ability to respond to an attack, rather than the controls they have in place to plan for an attack.

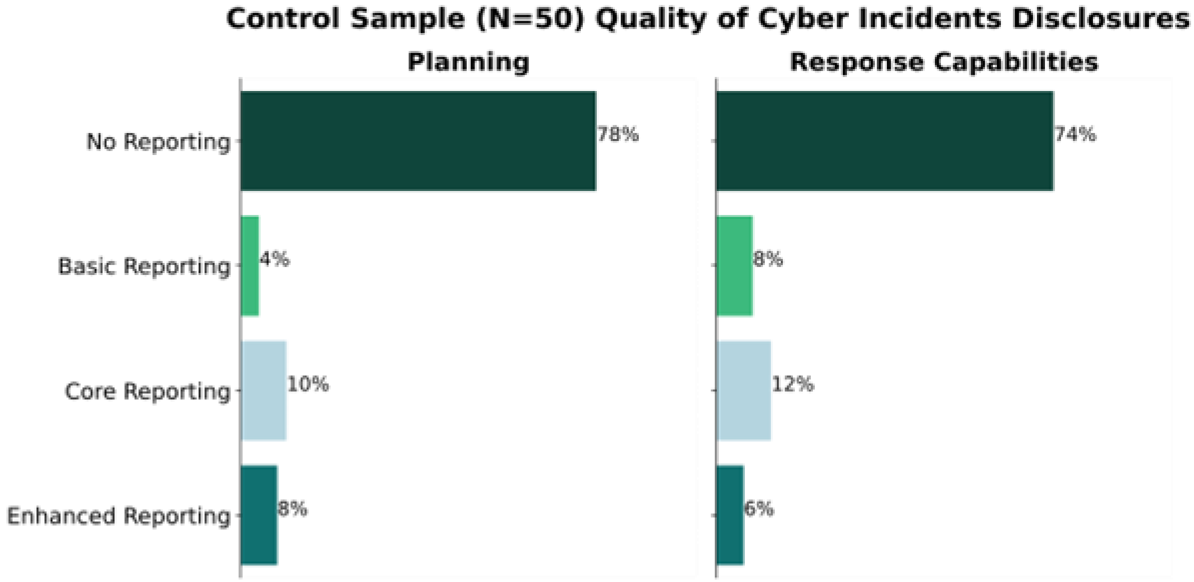
Sectoral Analysis

The Construction sector has the lowest prevalence of reporting on cyber incidents (23%) compared to the average across all sectors (48%).

Companies in the Information & Communication sector were also seen to have lower quality of reporting compared to those across other sectors, despite having almost the same prevalence of reporting (46% disclosing for this sector compared to the average of 48% across all sectors). Only 8% achieved core reporting and 8% achieved enhanced reporting levels compared to 18% and 13% across all sectors, respectively.

Conversely, companies in the Professional, Scientific & Technical Activities were found to have higher quality reporting for this theme with 31% achieving core reporting, and 11% achieving enhanced reporting.

Comparison to Control Sample



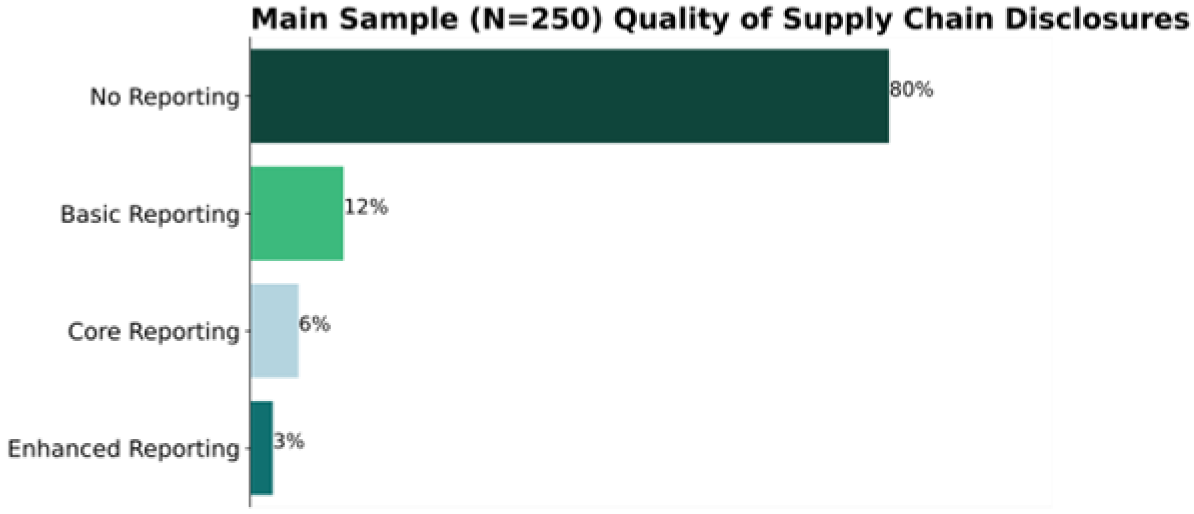
The control sample is less likely to include some form of disclosure for this theme than the main sample. Additionally, the higher quality levels of disclosures found in the main sample were not replicated amongst those that did disclose in the control sample.

Where companies disclosed on Planning, most in the main sample (13%) achieved enhanced reporting whereas most in the control sample (10%) achieved core reporting. This suggests that companies in the main sample are more likely to confirm that incident response plans are regularly tested, whereas those in the control sample simply state they exist.

Within both samples it was found that Response Capabilities disclosures were slightly more prevalent compared to Planning. Where companies disclosed on Response Capabilities, most in both samples achieved core reporting. This suggests that companies in both samples are more likely to confirm that response capabilities are in place, and what those are, but not necessarily detail the role of the board in responding to an attack.

Supply Chain

Main Sample General Findings



Low prevalence and low quality

Of the six themes analysed in the main sample, Supply Chain achieved the lowest percentage of disclosures (20%) within annual reports. The largest percentage of disclosures for this theme was found to be basic (12%), meaning that where companies did disclose on Supply Chain, most gave a short statement to confirm that processes are in place to manage and review security within the supply chain, but did not disclose what these were. In most cases, basic disclosures meant companies detailing that they had security clauses within contracts and conducting security due diligence during procurement stages.

Although many company reports did discuss their supply chain, most referenced non-cyber security aspects such as responsible sourcing of materials, sustainability and how they combatted the risk of modern slavery.

These findings align to those identified in other research on cyber disclosures in annual reports and on cyber security practices on supply chains. The 2020 Wavestone report highlighted from an international analysis of 250 listed companies, that only 19% of companies included supply chain security within their annual report.

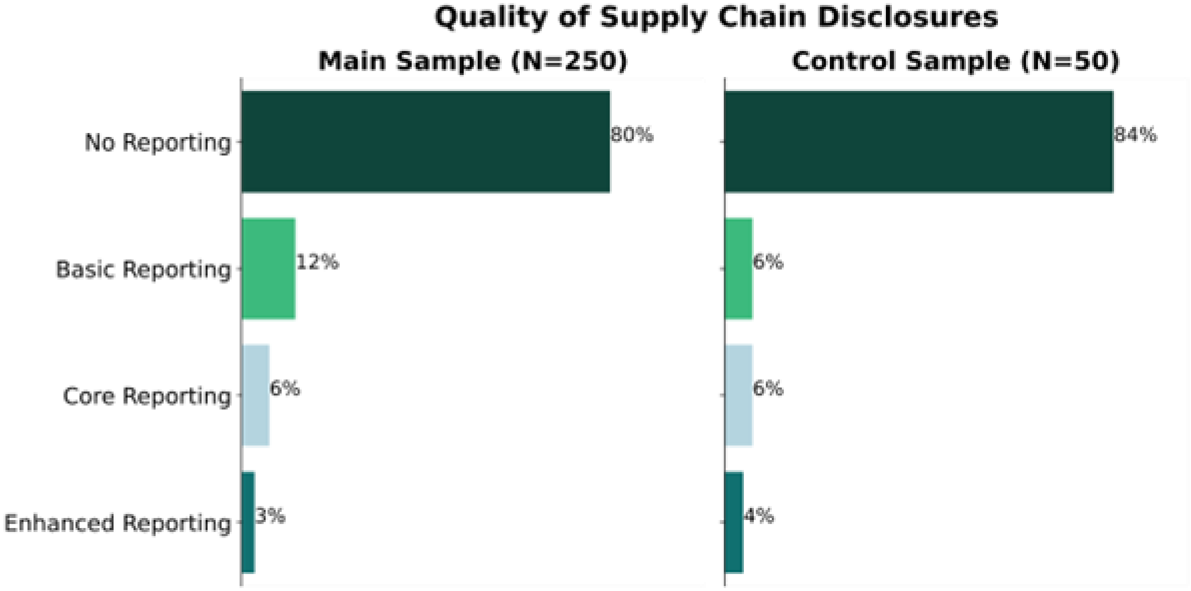
Sectoral Analysis

Sectoral analysis found that companies in the Information & Communication sector are more likely to disclose on Supply Chain than those in other sectors. 38% of companies in this sector disclosed on Supply Chain to some level of quality, compared to only 20% that did across all sectors.

Companies in the Financial & Insurance Activities were less likely to disclose on Supply Chain. 91% of companies in this sector did not disclose at all on this theme, compared to 80% across all sectors.

Analysis showed that the quality of disclosures for this theme where companies did disclose, was largely the same regardless of sector.

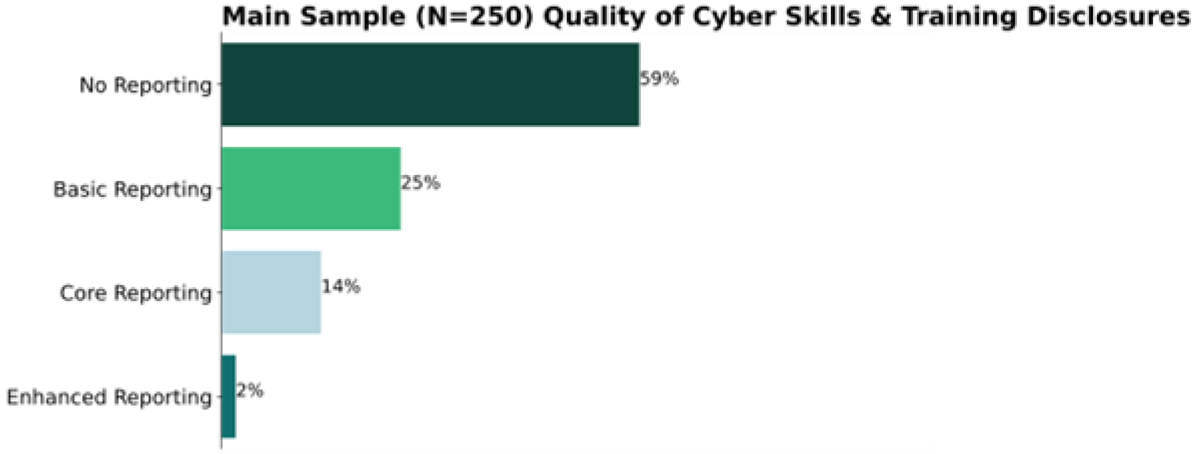
Comparison to Control Sample



A similar percentage of companies did not disclose on Supply Chain for both samples. The percentage of companies that achieved higher quality reporting (core and enhanced) was largely similar across both samples. A higher percentage of companies in the main sample (12%) included a basic level of Supply Chain disclosures than those in the control sample (6%) however this is likely due to the differences in percentage of those which report and do not report, rather than difference in quality of reporting. This suggests that prevalence of Supply Chain disclosures are low regardless of company size.

Cyber Skills & Training

Main Sample General Findings



Reasons for non-disclosure

41% of companies include Cyber Skills & Training within their disclosures, whilst 59% do not. The review of company annual reports suggested that companies are better at reporting on mandated training, such as Health and Safety, and Data Protection Act training.

Low quality of disclosures

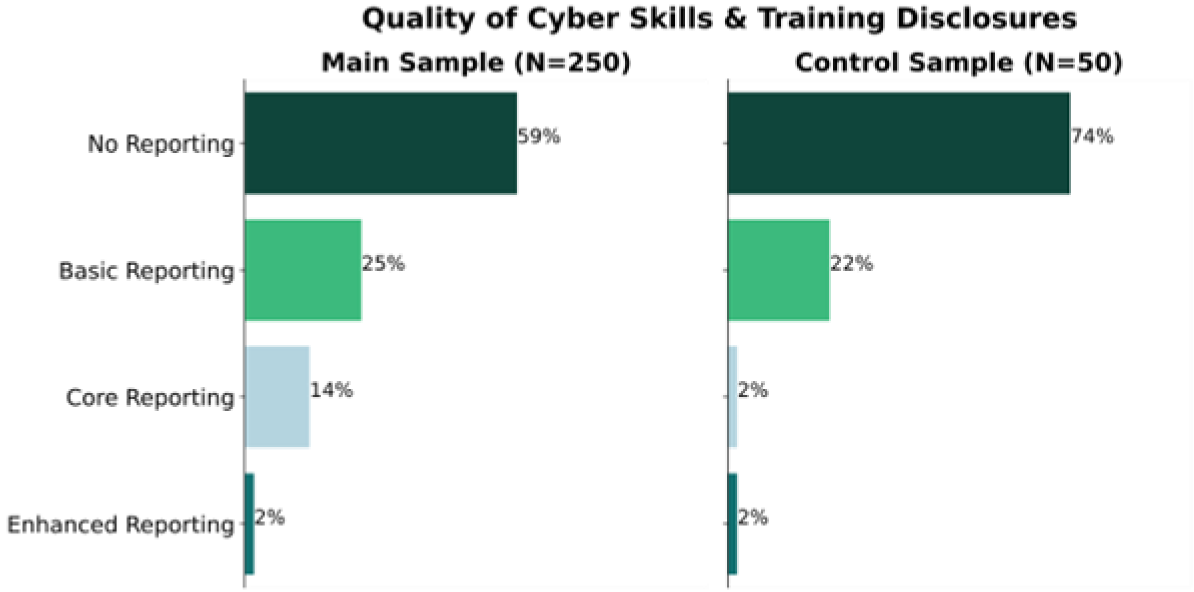
Where companies did disclose on Cyber Skills & Training, the majority of companies (25%) disclosed at a basic level, meaning they made a high level reference to a dedicated cyber security team, or referenced cyber training initiatives. Only 16% achieved core or enhanced disclosures. This means that there were low levels of disclosures by companies on areas such as responsibilities for cyber at board level.

Only 2% of companies provided enhanced reporting, which further detailed aspects such as the cyber skills and capabilities within their company and plans to address skills gaps. This suggests that, where companies do report on this theme, reporting is likely to set out aspects such as company-wide training but there are gaps in disclosing details of dedicated resources, skills capabilities and responsibilities at board or Executive level. Some of these gaps may be explained and backed up by findings from interviews in which some individuals suggested they are happy to disclose a summary of their cyber risk and mitigation controls but are worried about disclosing too many details that could provide valuable information to attackers.

Sectoral Analysis

Sectoral analysis found that companies in the Construction sector are more likely to disclose on Cyber Skills & Training than those across other sectors. 69% of companies in this sector did disclose on this theme, against the average across all sectors being 41%. However, none of the companies in the Construction sector achieved enhanced levels of reporting, with most (46%) achieving core level of reporting. This means that, although companies in this sector recognise the value of including some level of disclosure for this theme, and have higher prevalence of disclosures than in other sectors, it is not resulting in any higher quality of information, evidencing that a higher prevalence of disclosures does not necessarily equate to a higher quality as may be expected.

Comparison to Control Sample



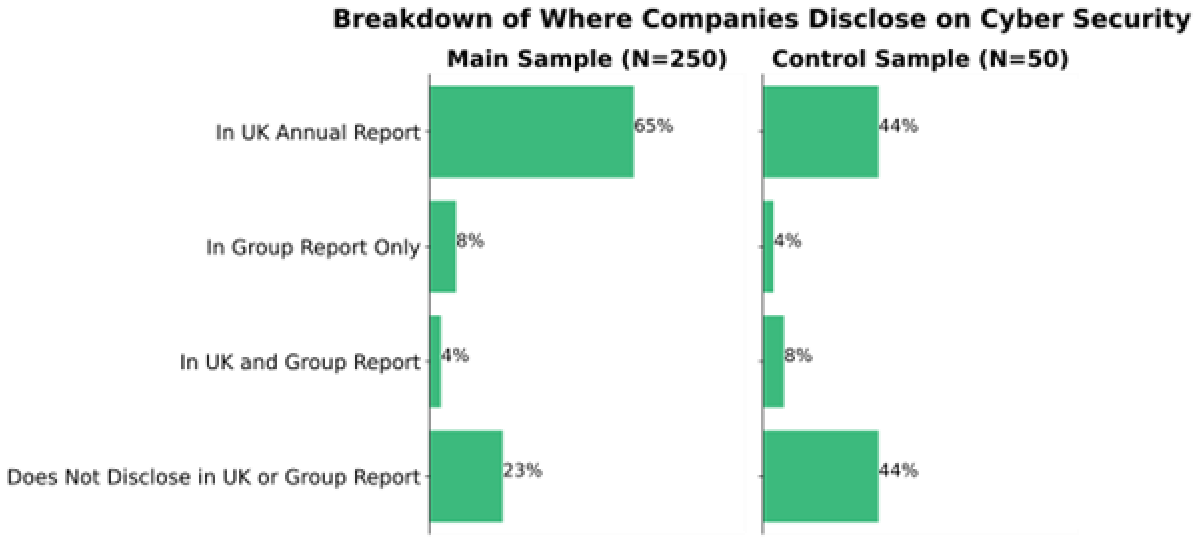
Prevalence of disclosures for this theme were higher for the main sample (41%) compared to the control sample (26%). The quality of disclosures was also higher for the main sample, with 16% achieving either core or enhanced reporting levels, compared to only 4% in the control sample.

Group-Level Reporting

Companies which refer to group-level report

In performing the review of company annual reports, there were occasions where the reporting company was part of a larger group and directed the reader to the group annual report for information on risks, governance, strategy, etc.

To minimise misreporting of disclosures, the results of the review of both the company and group annual reports were recorded. The location of the group company was also documented.



Main sample findings

Most companies disclosed directly within their UK annual report. However, the research found that, where companies did refer to a group level report, these reports were more likely to include higher prevalence and quality of cyber disclosures across all themes. All group-level reports disclosed on at least one sub-theme within Risk Management, compared to the average of 75% across all report types for the main sample. The biggest increase was seen in the prevalence of Governance disclosures, in which 91% of group-level reports disclosed information for the main sample, compared to the average of 52% across all report types. A higher percentage of group-level reports also achieved enhanced reporting for all themes in group reports when compared to the average across all annual reports within the main sample.

Disclosure by location

The research considered the location of group level reporting to identify if a higher prevalence and quality of reporting was seen in specific geographical areas. Group locations included:

- Canada
- France
- Japan
- Jersey
- Netherlands
- Republic of Ireland
- United Kingdom (UK)
- United States of America (USA)

There was no clear correlation between the group location and quality of reporting; however, as only a small number of companies across both samples referenced a group report, the number of groups in these countries was not enough to allow the research to draw formal conclusions on correlation. Literature reviews of similar studies[19] found that regulations relating to the need for organisations to report on cyber security in annual reports have yet to be considered or enforced in many countries, resulting in variations in cyber disclosures across annual reports in organisations internationally.

Comparison to control sample

The control sample found a higher number of companies that did disclose, would refer to their group report (21%) to do so, compared to those that disclosed in the main sample (15%). This suggests that companies in the control sample are more likely to rely on their group or parent company report to disclose cyber security information.

[19] Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. Computer Law and Security Review, 40, 105513. https://doi.org/10.1016/j.clsr.2020.105513

Ramírez, M., Ariza, L. R., Miranda, M. E. G., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. Sustainability (Switzerland), 14(3). https://doi.org/10.3390/su14031390

Conclusions

The research has identified a significantly higher prevalence (77%) of cyber disclosures for very large companies, when compared with the control sample of large companies (56%). However, the quality of cyber disclosures is low, with Governance and Cyber Incidents the only two themes in which at least 10% of the sample achieved enhanced disclosures. This highlights that, although most companies do report formally on some aspect of their cyber security, the quality provided varies.

Higher prevalence and quality of cyber and digital security risk disclosures is most likely driven by existing reporting requirements. From the research, two themes – Risk Management and Governance – displayed higher prevalence disclosures. In the case of risk reporting, this is likely to be directly related to the Companies Act 2006 requiring companies to disclose their principal risks and uncertainties within their annual reports. Governance also had the highest percentage of enhanced disclosures. Better frequency and quality of reporting on governance is likely to be a by-product of wider risk reporting, particularly so for listed companies that must comply with the UK Corporate Governance Code. As set out in the Introduction section of this report, the Code requires more detailed reporting on governance, audit, risk and internal control in the annual reports of listed companies. Cyber security disclosures must strike a balance between transparency and minimising cyber security threats and attacks. During the interviews, senior security management recognised that there was value in enhancing the prevalence and quality of disclosures. However, they also expressed concern on disclosing excessive information in relation to cyber security. They identified that there was a fine line in achieving better quality reporting and placing information in the public domain which, individually and collectively, could be used by cyber security threat actors as the basis of, or to inform, a cyber attack.

A common example of feedback from interviews was that companies recognised the importance of disclosing cyber security as a significant business risk and that it should be recorded as a principal risk in annual reports. They also felt comfortable in disclosing oversight and governance arrangements. However, there was little enthusiasm for disclosing specific details of digital security risks and the mitigating actions being taken. This also extended into disclosing plans to improve cyber resilience through strategy, programmes, or projects.

Feasibility of Impact Evaluation

The research considered the feasibility of conducting a future impact evaluation to assess whether the prevalence and quality of cyber disclosures improves over time.

The research has concluded that the output data could be used as a baseline on the prevalence and quality of current cyber security reporting in the annual reports of very large companies, assuming research:

- focuses on the same key objectives: a) how prevalent current reporting on digital security risks is; and b) how effective current reporting on digital security risks is.

- uses the same Quality Assessment Framework to code the quality of disclosure by theme.
- is undertaken for two samples: the main sample encompassing companies with 750 employees and £750m turnover, or more; and the control sample encompassing companies which have at least 500 employees and £500m turnover and up to, but not including, either 750 employees or £750m turnover.

An impact evaluation should be conducted in line with the HMT Magenta Book[20] which considers questions such as:

- What measurable outcomes, both intended and unintended, occurred?
- Have different groups (e.g. sectors) been impacted in different ways, how and why?

The impact evaluation feasibility study was carried out based on future reporting requirements on cyber resilience being brought forward. A future review on a government intervention would have used a difference in differences to show how the main group changed their reporting relative to the control group.

One challenge of using the difference in differences model is that it relies on the assumption that the outcomes variable for both groups would continue to move in parallel if a policy was not implemented. Future research should therefore consider that factors other than government intervention may influence findings, such as:

- A general increase in awareness and understanding of cyber security across the UK as a result of other initiatives, for example those undertaken as part of the National Cyber Strategy.
- An increase in the number of cyber attacks which occur or receive coverage from media, as these may influence cyber awareness.
- Increase in digital transformation undertaken by companies, resulting in changes to company risk landscapes.

The above factors could be the source of future research to understand whether other non-legislative factors are impacting reporting.

[20] HM Treasury. Last updated 2020. Guidance on what to consider when designing an evaluation. The Magenta Book - GOV.UK (www.gov.uk)

Annex A: Key Search Terms

When searching the company's annual reports, the following key search terms were used:

- Cyber
- Cyber security
- IT Security
- Digital security
- Information security

The following key search terms were used for specific themes:

Theme	Key search term
Strategy	Strategy Approach Strategic Programme Management system Investment Digital strategy
Governance: Roles & Structures	Audit committee Risk management committee Chief Information Security Officer (CISO) Chief Technology Officer (CTO) Head of Cyber Services
Risk Management: Process / Framework	Cyber risk Digital risk Threat (intelligence) Assessment
Risk Management: Policies & Procedures	Policy Policies Process Standard

Theme	Key search term
Risk Management: Assurance	Audit Compliance Assurance Framework Review ISO 27001 SOC 2
Cyber Incidents: Planning	Incident Data breach Attack Playbook Response plan Disaster recovery Business Continuity
Cyber Incidents: Response	Monitoring Backup recovery capabilities Recovery Resilience Security operations Cyber insurance
Supply Chain	Supply chain security Vendor security Supplier security Due diligence Procurement Third party

Theme	Key search term
Skills & Training	Awareness Training Certification Phishing Education

Annex B: Quality Assessment Framework

Each theme or sub-theme was assessed as either having:

- No reporting, meaning there is no mention of the theme;
- Basic reporting, meaning reporting is limited;
- Core reporting, meaning reporting is of reasonable quality; or
- Enhanced reporting, meaning reporting is of high quality.

As this research is focused on the quality of reporting, and not the quantity of reporting, those in the "enhanced" bracket do not need to be reporting on aspects covered within "basic" or "core", unless explicitly stated.

Strategy

Level	Definition
None	There is no mention of a digital or cyber strategy or investment in cyber security.
Basic	Reporting confirms that a digital or cyber security strategy exists or makes reference to cyber security investment, but with minimal detail.
Core	Company has a digital or cyber security strategy or there is reference to the company having a strategic investment plan for cyber security and it sets out how important this is to the business model and generating value, gives an indication of how developed the strategy is and whether there are any associated key performance indicators (KPIs).
Enhanced	Company has a digital or cyber strategy, or it sets out key priorities for strategic investment in cyber security and it sets out how important this is to the business model and generating value. There is clear alignment of the cyber security strategy or investment plan to the wider organisational strategy.

Governance

Level	Definition
None	There is no mention of cyber governance.
Basic	Reporting gives a short statement to confirm that cyber risk is governed, but reporting does not provide detail of how or what structures are in place.
Core	Governance structure (for the board, relevant committees and specific digital or cyber governance groups) are in place.

Level	Definition
Enhanced	There is ownership of cyber at a senior level, and cyber is discussed at appropriate governance boards such as audit committee and executive level meetings, and used to inform business decisions.

Risk Management

Risk Recognition

Level	Definition
None	There is no mention of cyber risk management.
Basic	Reporting gives a short statement to confirm that cyber risk management processes are in place, or references cyber security as a key company risk.
Core	Reporting confirms that regular risk assessments and cyber threat intelligence is used to identify the company's cyber risks or reporting confirms that there is an appropriate risk management framework in place to escalate risks which is in line with the company's wider risk management framework.
Enhanced	The company has a clear understanding of its critical assets and provides information about risk and mitigations relevant to the business at the right level of granularity.

Policies & Procedures

Level	Definition
None	There is no mention of cyber risk management.
Basic	Reporting gives a short statement to confirm that cyber risk management processes are in place, or references cyber security as a key company risk.
Core	Reporting confirms that the company has policies and procedures in place to manage cyber security.
Enhanced	Reporting confirms that the company has an Information Security Management System or procedures in place based on their needs and which links to different strategic areas and processes.

Assurance

Level	Definition
None	There is no mention of cyber risk management.
Basic	Reporting confirms that assurances are obtained but does not give detail as to what those are.
Core	Reporting confirms that internal assurances have been obtained and for what purposes.
Enhanced	Reporting provides a summary of the internal and external assurances which have been obtained during the period. It is clear how the company has taken action as a result of assurance.

Cyber Incidents

Planning

Level	Definition
None	There is no mention of cyber incident response plans or cyber incident response capabilities.
Basic	Reporting gives a short statement to confirm that cyber incident response processes are in place.
Core	Reporting confirms that plans are in place to respond to cyber incidents. For example, the report references an incident response plan or IT disaster recovery or business continuity plans with specific reference to plans for information security or cyber security risks.
Enhanced	Reporting confirms that an incident response plan is in place, regularly tested and linked to the business continuity plan.

Response Capabilities

Level	Definition
None	There is no mention of cyber incident response plans or cyber incident response capabilities.
Basic	Reporting gives a short statement to confirm that cyber incident response processes are in place.

Level	Definition
Core	Reporting confirms response capabilities are in place. For example, reporting mentions out of hours monitoring or backup recovery capabilities. If any incidents have occurred during the period, reporting provides information about the nature of the incident, immediate impacts and summarises actions taken to restore operations and reduce customer impact (where appropriate).
Enhanced	Reporting confirms response capabilities are in place and explains the role the board has in this process or makes reference to senior individuals' representation on crisis management teams. If any incident has occurred during the period, it is clear that lessons learned have been identified and incorporated into current processes. The estimated financial impact has also been quantified if material.

Supply Chain

Level	Definition
None	The company's approach to security supply chain management is not mentioned.
Basic	Reporting gives a short statement to confirm that processes are in place to manage and review security within the supply chain.
Core	Reporting summarises the supply chain management process, which includes aspects such as having security clauses within contracts and conducting security due diligence during the procurement stage.
Enhanced	The company demonstrates that they have a clear understanding of their supply chain risk, and have conducted an exercise in the last year to identify critical third parties within the organisation's supply chain, as well as managing ongoing security due diligence processes.

Cyber Skills & Training

Level	Definition
None	There is no mention of cyber skills or training undertaken within the company.

Level	Definition
Basic	Reporting gives a high level summary i.e. reference is made to a dedicated cyber security team or confirmation is given that all staff members are provided with cyber security training.
Core	Reporting provides confirmation that cyber security training is role specific and that there are dedicated resources in place to manage cyber security. This includes responsibility for cyber at a board level i.e. an expert on cyber on the board. Reporting confirms that the board receives training and how frequent this is.
Enhanced	Reporting confirms that the company has a clear understanding of skills or capabilities and that this informs the training plan and enables the company to deliver on its wider cyber strategy. Reporting also covers how the company plans to address any skills gaps, or acknowledgement of what type of skills are needed for future work in line with planned growth or transformation.

Annex C: Interview Questions

1. Would you consider digital security risk to be a material risk to the company, and why?
2. To what extent do you agree that managing digital security risk has become more of a priority for your company, and why?
3. Does your company embed consideration of its cyber security and digital risk within its environmental, social and governance (ESG) framework?
4. What do you perceive as the benefits of reporting externally on digital security risk?
5. To what extent do you agree that external reporting helps to build cyber resilience, and why?
6. To what extent do you agree that external reporting would help to create a positive cyber security culture a) within your organisation; and b) within the wider UK industry, and why?
7. What do you perceive as the barriers for reporting on digital security risk externally and how do you think these barriers could be addressed?
8. To what extent do you believe that a lack of senior buy-in acts as a barrier for external reporting against cyber security?
9. To what extent do you perceive external reporting on digital security risks to be a risk itself?
10. Is cyber or digital an area which your key stakeholders are interested in? If yes, please explain which stakeholders are interested in this area.
11. To what extent do you agree that reporting on digital security risk demonstrates maturity and builds trust with stakeholders?
12. Are there any other factors that you think need to be considered as part of this research?

Glossary

Term	Description
Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data
Cloud Technology Solutions	Infrastructure, platforms, or software hosted by an external party which is on-demand and is not directly managed by the user or organisation
Control Sample	Sample encompassing companies which have at least 500 employees and £500m turnover and up to, but not including, either 750 employees or £750m turnover
Critical National Infrastructure	Infrastructure considered necessary for a country to function and upon which daily life depends
Cyber Attack	A malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation
Cyber disclosure	Inclusion of cyber security aspects such as strategy, governance, risk management, incidents, supply chain or skills and training, within a company's annual report
Cyber Incident	An occurrence that actually or potentially jeopardises the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies
Cyber Resilience	The ability to maintain required capability in the face of adversity resulting from a cyber incident
Cyber Security	Any processes, practices, or technologies that organisations have in place to secure their networks, computers, programs, or the data they hold from damage, attack, or unauthorised access
Digital Security Risk	Cyber security threats and the risk of significant breaches of data protection obligations
Digital Transformation	The adoption of digital technology where products or services are currently non-digital, or the effectiveness or efficiency of those already digital

Term	Description
Government	The UK government, officially His Majesty’s Government (HMG)
Key Search Term	Exact words entered when searching annual reports
Main Sample	Sample encompassing companies which have 750 employees and £750m turnover, or more
Managed Technology Solutions	Technology solutions which are managed by a third party on behalf of the user or organisation
Response Capabilities	Resources such as people, tools, and processes in place to allow the organisation to respond to an adverse incident
Stakeholders	Anyone with an interest in the performance of a company. For example, shareholders, investors, auditors, customers, employees, and suppliers