AN FTI CONSULTING REPORT

Building Effective Cybersecurity Governance

Evolving Board oversight and reporting to address increasing stakeholder scrutiny of cyber risk

Executive Summary

Digitalisation has changed the way companies operate and given rise to a rapidly evolving set of risks that companies face and must prepare for – cybersecurity risks. The increasing prevalence of cyber attacks, notably ransomware, coupled with declining availability of cyber insurance, is leaving companies increasingly exposed to the often-significant impacts of a cybersecurity incident. There is naturally a short-term financial cost - research from IBM[1] reveals that the average total cost of a ransomware breach in 2022 is $4.54 million- but reputationally the impact of an incident may be longer lasting.

Aware of how companies are increasingly exposed to cybersecurity, governments, regulators and investors alike are increasing pressure on organisations to improve their cybersecurity measures, increase transparency around disclosures, and build governance and management structures that demonstrate cybersecurity is a priority at the top levels of the organisation.

Ensuring oversight structures are in place at board level is a key feature of cyber governance. As a material risk affecting companies, boards are increasingly held accountable for ensuring the executive team is taking appropriate steps to mitigate the risk of a cybersecurity attack, and also ensuring the organisation responds appropriately in the event of an incident. Often, boards have little to no experience in this field, and whilst the dynamic nature of cyber risk means that board members are not expected to be cyber experts - though there is merit to having expertise on the board - they are expected to be able to challenge management on this topic and inform shareholders on the measures in place to mitigate the impact of cybersecurity incidents.

For many companies, the Chief Information Security Officer (CISO) is the executive with accountability for cyber risk. With investors and regulators pushing for greater oversight at board level, the CISO will need to communicate cyber risk and metrics in terms that resonate with the board, and governance structures will need to prioritise engagement with the CISO on cyber risks.

Cybersecurity is also increasingly part of investor and proxy advisor scrutiny of companies. Our research indicates that investors now consider cybersecurity a key priority - with cyber attacks consistently cited as the most important concern or risk area for investors. Allied to this, the world's major asset managers are providing more detail on what they expect in terms of disclosure – including a desire for detail on the structures in place to manage cyber risk, but also the number and scale of cyber incidents affecting a business.

How companies communicate their governance of cyber risk to investors is therefore increasingly important. When announcing proposed SEC rules on cybersecurity disclosure, SEC Chair Gary Gensler stated: *"I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."* This emphasises a lack of transparency around cyber risk and incident disclosure; and a clear indicator that regulation is only going one way.

In evaluating the regulatory environment; reviewing the heightened focus of the investment community; and considering the benefits of greater transparency, our view is that there may be merit in companies approaching cybersecurity in a manner similar to how the Task Force on Climate-related Financial Disclosures (TCFD) approaches climate risk. This is built around four pillars and will enable companies' boards and investors to acknowledge the risks posed by cybersecurity in a more holistic manner covering i) Governance; ii) Strategy; iii) Risk Management; iv) Metrics and Targets.

Ultimately, a combination of regulation and demand for greater transparency will mean a step-change in disclosure for companies. However, there is likely to be a clear benefit – financially and reputationally – for companies who are first movers and adopt a more proactive approach to governance and oversight of cyber risk and disclosure.

Introduction

The World Economic Forum has ranked cybersecurity as one of the top five global risks[2] and has called on companies to incorporate cybersecurity considerations into their ESG risk management. With the growth of cybersecurity threats, and the significant increase in the number of ransomware and malware attacks, cybersecurity remains at the top of the risk register for many companies. Despite increased awareness, a cybersecurity incident continues to be a costly affair, with research from IBM estimating that the average total cost of a ransomware breach in 2022 was $4.54m.[3]

With the increasing digitalisation of businesses, remote working, and the changing geopolitical landscape, as well as the increase in volume and severity of cyber attacks, companies' risk management practices and effective oversight of cyber and technology are becoming subject to increased scrutiny from investors, while regulators continue to accelerate the implementation of necessary oversight frameworks. Companies that fail to implement proper governance on cybersecurity or use appropriate tools and metrics will be considered *"less resilient and less sustainable"*, WEF said.

Cybersecurity State of Play

An Ever-Expanding Threat Landscape

The year 2021 was unprecedented in both the scale and impact of cyber attacks. Much attention was, justifiably, on ransomware and was driven by high-profile attacks conducted by professional cyber-crime groups with the skills and resources to infiltrate large organisations and state infrastructure. Ransomware prevalence continues to increase year-on-year, but took a significant jump in 2021 when it increased by 13%[4] - an increase equivalent to the previous five years combined.

The proliferation of ransomware has been facilitated by the 'Ransomware as a Service' business model where developers sell their strain of ransomware to affiliates, in exchange for a cut of the profits. The use of double extortion (threatening the release of data) and triple extortion (making threats to other stakeholders such as employees and customers) has also raised the stakes for organisations responding to an incident.

The shifting geopolitical landscape of 2022 has also meant that businesses have found themselves in the crosshairs of not only cyber criminals, but also nation state actors[5] conducting cyber attacks alongside traditional military activities. Hacktivists[6] have also targeted organisations for ideological reasons, for example those continuing to do business in Russia. As we enter a period of "cold cyber war", concerns around potential attacks on so-called mission critical industries - such as industrials, financials and utilities - have heightened significantly, as the broader and systemic impacts of these attacks take on a new dimension.

In tandem with this heightened threat activity, organisations are also seeing their attack surface widen as a result of accelerated digitalisation, increased online activity and complex digital supply chains. This means that risks facing organisations are expanding and constantly changing, while the sophistication with which external actors can carry out attacks is growing.

Regulators and investors are increasingly aware of this growing cybersecurity risk and how costly an incident can be from a business, financial and reputational standpoint, and are putting measures in place that will force businesses to implement appropriate cybersecurity oversight, and consequently hold their boards and senior executives accountable.

Availability and Affordability of Cyber Insurance

In recent years companies had been relying on cyber insurance to manage the fallout from a cybersecurity incident. However, greater incidence of cyber attacks, in particular ransomware, combined with rising ransom demands have led to a greater volume of insurance claims.

Insurers have raised prices[7] in response to the increase in claims, with insurance company Marsh reporting[8] that the price of cover in the fourth quarter of 2021 grew by 130% in the US and 92% in the UK, and grew by a further 110% in the US and 102% in the UK in the first quarter of 2022. The increase in claims has been so severe that many insurance companies are limiting their cover or simply no longer providing cyber insurance. In August 2022, Lloyds of London issued a bulletin[9] to its members stating that, from 31 March 2023, due to the systemic risk to the insurance markets posed by cyber policies, all newly written standalone cyber policies must exclude liability for losses arising from any state backed cyber attack.

Stricter Regulatory Environment

It is against the backdrop of increased prevalence and severity of attacks that governments and regulators continue to increase pressure on organisations to improve their cybersecurity posture while also increasing transparency through greater cybersecurity disclosures. Non-compliance with regulation can be costly for businesses; the cost of a data breach in particular is over 50% higher[10] for organisations with a high level of compliance failures. These increased costs are primarily the result of fines, penalties and lawsuits.

Europe

Cybersecurity regulation in Europe is focused primarily on personal data protection and maintaining the integrity of critical infrastructure, systems and services. GDPR, which covers the handling of personal data and notification of data breaches in the EU is well established and, for the most part, well understood. Its implementation has served to highlight companies' responsibilities as custodians of personal data. The Network and Information Security (NIS) Directive has also provided cybersecurity and notification requirements for digital service providers and operators of essential services such as health, transport, and financial services since 2018. With the ever-changing nature of cyber risks and their increased frequency and sophistication, the EU Parliament approved the NIS2 in December 2021, which will update and replace the existing NIS directive by the end of the year and will cover sectors *"that are critical for the economy and society"*. The policy is being designed with the objective of strengthening existing measures and streamlining reporting from companies. The UK is also widening the scope of its NIS directive to include a broader set of industries.

In addition, the imminent Digital Operation Resilience Act (DORA) will increase the disclosure and reporting requirements for the financial services sector and their third-party providers in the EU.

US

US regulators have focused on the materiality of incidents, with the SEC providing guidance since 2018 that cyber attacks represent existential business risks and may have

a material impact, warranting disclosure. In March 2022, the SEC expanded on this and proposed new rules[11] that would make incident disclosure mandatory for public companies. Under the new rules, companies would have to report material cybersecurity incidents within four days of discovery.

In addition to incident disclosure, the proposals also address cybersecurity oversight stating that the regulations would require companies *"to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy"*. The proposals devote a whole section to cybersecurity governance outlining disclosure requirements related to board cybersecurity oversight and expertise, management's role and expertise in managing cybersecurity risk and how cybersecurity risk is considered in relation to business strategy, risk management and financial oversight. Details shared by the SEC following recent settlements have also revealed the level of scrutiny currently being placed on cybersecurity incidents. The failings outlined in the settlements include:

- Delays in notifications to investors
- Lack of internal disclosure processes and controls leading to inaccurate statements from senior executives
- Written security policies which weren't implemented in practice
- Misleading language, inaccuracies, and omissions in notifications

Although these proposals are still in the consultation phase, it is abundantly clear that the SEC sees cybersecurity as a significant risk to businesses. Companies will not only be assessed on the structures that are in place to manage and oversee cyber risk but also how they respond in the immediate aftermath of an incident.

Corporate Governance and Cybersecurity

The growth in cyber risk has led to increased awareness and higher expectations around cybersecurity issues, with businesses evaluated on their preparedness, resilience and how they respond in the aftermath of an incident. While businesses need to get the basics right and have a clear understanding of their disclosure obligations at both a market and industry sector level, regulators and investors also expect boards to implement a governance structure that prioritises cybersecurity. Appropriate governance is seen as key to both mitigating risk, responding to cybersecurity incidents and demonstrating preparedness.

The proposed new SEC guidance on cybersecurity risk management, strategy, governance and incident disclosure rules will increase boards' accountability for cyber risk. As the proposals will require that material incidents be reported within four days, companies will need to quickly assess the full impact of an incident. In order to meet these strict requirements, and avoid sanctions, boards will need to have a full understanding of their cyber risk and the potential financial impact of an incident, prior to it occurring. Many companies had been relying on cyber insurance to manage elements of their risk exposure, but with providers increasingly limiting their coverage, companies are effectively self-insured for the majority of costs associated with a cyber incident.

This new risk environment combined with regulations that are demanding transparency and accountability, accompanied by increasing pressure from shareholders to better understand how cyber risk is being mitigated, means that a spotlight is now being cast on the role of board directors in the oversight of cyber risk.

Expanding Role and Importance of the CISO

Having a dedicated Chief Information Security Officer (CISO), which is separate and distinct from the Chief Information Officer (CIO) role, has become increasingly important with the accelerated digital transformation and associated security risks that the pandemic and geopolitical issues have brought. An empowered and trusted CISO is also essential during an actual cyber crisis when decisions need to be made and communicated quickly, not just to protect operations and reputation, but to avoid future regulatory sanction.

Governance guidelines in the SEC guidance require discussion of the following:

- Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks;
- The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and
- Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

The office of the CISO may have traditionally been seen as an IT function, but the far-reaching implications of a cybersecurity incident mean that cybersecurity must be considered a business risk. Gartner[12] predicts that at least 50% of C-level executives will have performance requirements related to cyber risk by 2026, reinforcing how accountability for cyber risk has shifted from being solely an IT responsibility to becoming a responsibility of business leaders across all segments of a company. These leaders historically may not have factored cyber risk into their decision-making and priorities, and the CISO will therefore need to ensure that these business leaders are equipped with the knowledge and ability to make appropriate risk decisions, as part of the company's broader risk management approach.

This shift, combined with a regulatory landscape that is pushing oversight responsibility up to board level, means that the modern CISO needs to be able to communicate dynamic and fast-changing cyber risks in terms that resonate with both the business and the board. Metrics need to be defined in terms of business and financial impact to reframe cybersecurity as a mandatory investment, not an operational cost. However, a new FTI Consulting survey of 165 CISOs in the US has revealed that 58% struggle to communicate with senior leadership.[13]

Board Oversight

While the CISO plays a significant role in preparing a company's overall cybersecurity strategy, ensuring the adequacy of a company's cybersecurity measures should also be part of the board's oversight responsibilities. Cybersecurity must become part of the recurring agenda at board meetings.

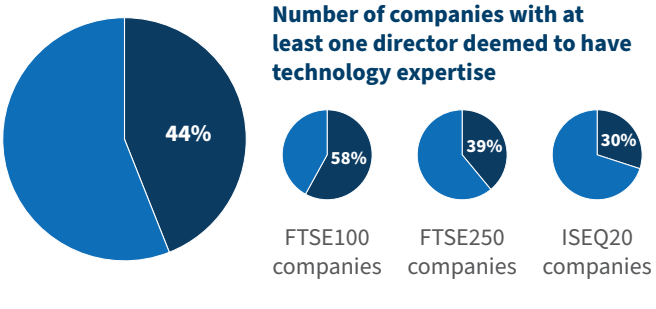
It has been common practice for the cyber risk oversight function to be part of the remit of the board's audit committee. This decision around the most effective oversight structure should be based on each individual company's structure. Further, as institutional investors and proxy advisors increase their focus on cybersecurity oversight, boards – and not just management – should be prepared for regular shareholder engagement on these matters.

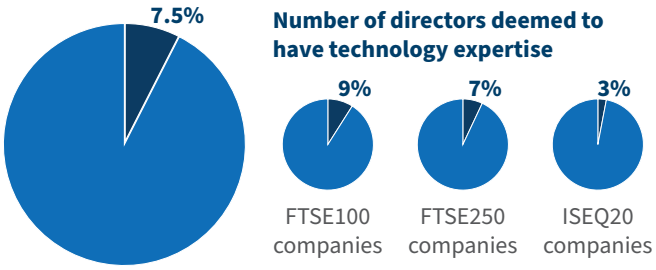
It is critical that the CISO regularly feeds into board discussions in order to communicate the cybersecurity risks that a business faces, and what investments are needed to mitigate those risks, and that the board is prepared to ask pertinent questions about the cybersecurity strategy.

FTI Consulting's CISO survey has revealed that 53% of CISOs believe that cybersecurity priorities are not completely aligned with those of senior leadership. A CISO will often face competing interests from the business and, therefore, it is important that the board helps foster a culture where cybersecurity is prioritised and doesn't lose out to competing interests (e.g., recognising it as an investment not a cost). While the CISO holds the responsibility of designing and implementing the company's cybersecurity programme, it is up to the board to ensure that the appropriate strategy has been developed and implemented by the executive team.

Board Skills

While strong reporting to the board from a CISO or another executive will enhance oversight of cybersecurity risks, much like having deep financial acumen on the board, it is equally important that the board itself has the appropriate expertise and skills to understand cyber reporting and risks. Boards must avail of external industry and other guidance as well as the cybersecurity expertise of fellow directors, third parties and internal resources to effectively oversee the organisation's cybersecurity within an appropriate structure focused on oversight. In a rapidly changing landscape, directors would benefit from continually seeking to expand their own knowledge of this topic.





Indice	2022	2020	Change
FTSE100 Directors	9%	11%	-20%
FTSE250 Directors	7%	8%	-7%
FTSE350 Directors	8%	9%	-12%
ISEQ20 Directors	3%	2%	35%

Data provided by Dilligent

In addition, building relationships internally with stakeholders that are able to provide expertise to guide strategic cybersecurity decisions; seeking out external third-party advisers who regularly report to the board; and implementing periodic audits and/or third-party benchmarking play an important role in strengthening the board's skills in this area. As the understanding around cyber risk grows, many companies have separated the IT and information security teams as part of their governance strategy. Given the frequency and increased risk of facing a cyber attack or a cybersecurity failing, having cyber expertise readily available to the board has become increasingly important. Our previous research, based on 2020 data,[14] indicated that a lack of technology expertise on a board creates a real and meaningful gap in the board's skillset. Based on this data, only 8.5% of directors on FTSE 350 and ISEQ20 indices were deemed to have technology expertise. Looking at 2022 data, this number has come down to 7.2%, with the decrease in the number of directors with technology expertise across the FTSE350, and a 1% increase across the ISEQ20, as detailed in the table.

In line with the macroeconomic downturn that has characterised the last two years, the slight decrease in the number of directors with technological expertise on the board of UK and Irish firms between 2020 and 2022 should not be viewed as a decrease in the importance placed on topics of cybersecurity by investors.

Investor Interest

While regulators are attempting to put in place frameworks that will serve to protect investors, some of those same investors are also taking matters into their own hands.

According to the United Nations Principles of Responsible Investment report, the topic of cybersecurity has become increasingly part of investors' engagement agenda, given the potential adverse impact on portfolio valuations and earnings from the legal and regulatory risk associated with cyber incidents. The potential impact on a company's share price, particularly as these incidents become increasingly more likely, is part of investors' analysis of a company, with recent research from HSBC[15] pointing to the fact that 73% of organisations underperformed the market after a ransomware attack. Research conducted by FTI Consulting that surveyed c. 204 institutional investors in 2021 found that cyber attacks are among the greatest concern at the companies in which they are invested. While recent societal and geopolitical upheaval have brought additional concerns to the fore, cyber attacks have consistently remained a top concern for the past two years.

Q. Which of the following do you consider are likely over the next 12 months and concern you about harming companies you invest in? (Please select all that apply)

	Nov 2021	Mar 2021	Aug 2020	Feb 2020
Cyber attack(s) stealing or compromising assets	39%	25%	47%	46%
Major product defect	35%	19%	39%	34%
Litigated against	24%	14%	22%	21%
Embroiled in political corruption	27%	19%	32%	27%
Leak of sensitive internal communications	25%	21%	31%	28%
Political disruption or abrupt policy changes	27%	19%	32%	30%
Victim of fraudulent practices	21%	20%	28%	31%
Impacted by sanctions	14%	20%	21%	21%
Trade restrictions	25%	25%	30%	35%
Embroiled in a regulatory (or other) investigation	13%	17%	16%	14%
Regulatory fine	13%	18%	19%	22%
An operational failure that causes major environmental damage	13%	21%	20%	15%
Major new competitor entering the market	20%	20%	21%	23%
Impacted by disruptive technology	17%	24%	22%	21%
Disrupted by stakeholder activism	8%	19%	18%	12%
Leadership change / transition	16%	20%	24%	25%
A target of aggressive M&A activities	14%	22%	16%	13%
Cash flow issues from bad debt	14%	26%	16%	18%
Carbon pricing	9%	Not asked	Not asked	Not asked
None of the above	6%	3%	3%	5%

Note: research conducted in each period was based on opinions of at least 204 institutions holding over $9 trillion of assets under management

Investor Expectations

As a reflection of the growing concerns and the scrutiny being placed on companies' cybersecurity practices by investors, proxy advisors have incorporated, in their research reports, some additional insights and data points on this topic.

Furthermore, this information has also been incorporated into other third party and rating providers' analysis, with Refinitiv recently announcing the incorporation of third-party cybersecurity data in its risk-focused due diligence reports. Similarly, corporate governance, remuneration, sustainability and cybersecurity tools provider, ISS Corporate Solutions has partnered with another leading technology platform that operationalizes third-party risk, privacy and security. Through this partnership companies will have access to a range of detailed insights and proprietary ratings on their suppliers and third parties' cybersecurity strategy/ practices, to help ensure they are positively contributing to the organisation's reputation and business operations.

In 2021 proxy advisor Glass Lewis announced a partnership with a security ratings company to provide data and insights on cybersecurity in their research reports. The rating provided is based on an assessment of externally available data such as compromised systems, patch levels, and publicly disclosed incidents. Companies are then benchmarked against their industry sector.

The 'ISS ESG QualityScore' rating now also includes several questions related to cybersecurity governance including board cybersecurity expertise, published cybersecurity policies and oversight and details on any cybersecurity breaches that provide a useful framework to better understand a firm's current level of practice.

Stewardship and Cybersecurity

In light of the complexities and the ever-changing landscape of cybersecurity, with regulatory frameworks still catching up, assessing a company's cyber preparedness has become a key consideration for many institutional investors. A Principles of Responsible Investment ('PRI') report[16] found that while companies are increasingly recognising cyber risk, disclosure is not developing at a similar pace. The study found that *"although companies increasingly recognise cyber risks and their impacts, corporate information in the public domain does not assure investors that companies have adequate governance structures and measures in place to deal with cyber security challenges"*. With information at the centre of effectively functioning markets, the cyber space may be a blind spot of sorts.

ISS includes a series of cyber-related questions when determining the ISS ESG QualityScore rating:

- Does the company disclose an approach on identifying and mitigating information security risks?
- What percentage of the committee responsible for information security is independent?
- How often does senior leadership brief the board on information security matters?
- How many directors with information security experience are on the board?
- Has the company experienced an information security breach in the last three years?
- Has the company entered into an information security risk insurance policy?
- Is the company externally audited or certified by top information security standards?
- Does the company have an information security training program?
- How long ago did the most recent information security breach occur (in months)?

Institutional Investors' Perspectives and Updates

BlackRock, the world's largest asset manager, identified in their 2021 annual stewardship report[17] that cybersecurity is a systemic risk, given the data privacy and security risks that can affect personal information, as employees or customers, and also the ripple effect it could have through the broader financial system. In its 2022 voting spotlight report,[18] BlackRock continued to identify data privacy and security as a priority topic for companies and investors alike, in light of the increasing role of technology in companies' business models and interactions with employees, customers and other stakeholders. BlackRock considers this issue in the context of the industry and market of the companies it engages[19] with and seeks to gain a better understanding of how each company is prepared to best navigate this evolving landscape.

> *"From the point of view of a long-term investor, seeking to ensure durable returns for our clients, increased access to personal data by companies comes with material business risks that can impact a company's reputation and their ability to operate. Whereas the global average direct and indirect cost of a single data breach is estimated to be over $4 million in 2021, the financial tail risk associated with a very significant data breach can run to hundreds of millions of dollars. While mega breaches are not the normal experience for most businesses, they can have an outsized impact on consumers and industries[...] Investors, however, can face significant transparency gaps when assessing companies' management of these risks and preparedness for a crisis event. More recently, we have seen efforts to address that gap, with an increased emphasis on regular reporting and transparency on policies and board oversight, which we welcome given the sensitivity associated with the topic as well as the relatively new nature of these risks and regulation."*

Source: BlackRock's Approach to data privacy and security

In its Investment Stewardship Semi-Annual Report[20] in 2020, Vanguard also highlighted the importance of robust corporate governance structures to prevent or reduce the impact of material risks such as cybersecurity in long-term value, as noted:

> *"Ultimately, boards should work to prevent risks from becoming governance failures. We've seen increasing evidence that non-traditional but material risks related to environmental and social topics (such as climate change, cybersecurity, and human capital management) can damage a company's long-term value. If a company's practices, organisational culture, or products put people's health, safety, or dignity at risk, they can pose a financial risk to investors too. Strong oversight practices enable a board to steer a company through unpredictable crises."*

Source: Vanguard 2020 Investment Stewardship Semi-Annual Report

Schroders

While there is no defined method to engage on cybersecurity, Schroders has noted the below questions that guide its engagements on cybersecurity:

1. Is there responsibility for cybersecurity and data privacy at the board and management level?
2. How is the company's technical expertise organised?
3. What training and monitoring of employees and suppliers is in place?

Shareholder Engagement

In addition to reviewing disclosures and third-party ratings, investors have used engagement as a means of gaining a deeper insight into companies' approaches to this material risk, particularly as disclosure requirements are still developing. Companies have shown some

reluctancy to disclose significant detail around their cybersecurity strategies and frameworks, but have, in turn, shown availability to engage directly with their shareholders on their practices. The aforementioned PRI report, also noted that the companies contacted as part of this collective engagement *"were open to private dialogue and willingly made their experts - usually chief information security officers or digital directors (as well as staff from their sustainability and investor relations teams) – available to help investors develop a more comprehensive view of how they are addressing cyber security risks".*

This depth of information, including the combination of backgrounds and insights, would not have been captured in the review of public filings alone, and further highlights the significant merit of shareholder engagement in gaining a more holistic view of a company's approach, and also evidencing the level of interaction between the board of directors and the executive team. As engagement and stewardship on cybersecurity increases, board members will need to be prepared for these conversations. Regular engagement with CISOs and security teams will allow fora greater understanding of the company's cybersecurity status. BlackRock has developed their approach to engaging with companies, particularly those with the greatest potential risk, on data privacy and security and the objectives of their engagement are detailed below:

BlackRock

BlackRock's Approach to Engagement on Data Privacy and Security Engagement:

Materiality assessment

— What is the company's exposure to data privacy and security risk based on its business model, for example from
— the quantity, type and sensitivity of the data it collects (i.e., users vs. customers; individual vs. corporate; private vs. public, sensitive vs. non-sensitive)?
— What are the concrete financial implications to the company related to privacy, data, and cyber security?
— Are there any related regulatory actions taken or anticipated? For a company operating/listing in multiple jurisdictions, how does it manage to comply with multiple data security/privacy regulations?

Board oversight and resources

— How effectively does the board maintain comprehensive oversight and understanding of material privacy and data security risks?
— How are these matters factored into the company's business continuity plan?
— What are the resources dedicated to cyber risk management and why are these considered adequate for the business? Are metrics related to employee training shared broadly with stakeholders internally and externally?
— Does the company use an industry security framework and how do they measure themselves against that framework?
— How does the company identify and address technical and organizational security issues to protect against data security breaches?

Board oversight and resources

— How does the company determine what data is appropriate to collect and balance the use of customers' personal information for revenue opportunities with legal, regulatory, and reputational risks while maintaining customer trust?
— As customers become more aware of the importance and risks associated with their data, how does the company factor in potential shifts in customers' willingness to share their data over the long run?
— How does the company ensure that collected data is used for its stated purpose and that there are no deviations?
— If the company is applying algorithms to users' personal information for targeting purposes, what is the policy to review these algorithms (at both the management level and the board level) to ensure that there is no perceived discrimination based on ethnicity, purchasing power or other demographic categories that might be perceived as sensitive?

Third party management

— In the case of transfer of data to third parties, how does the company ensure that the handling of data is done in a responsible way during the transfer and aligned with the company's protection policies?

Collective Engagement Strategies

Another approach to gaining a better understanding of cybersecurity governance across different companies has been through collective engagement strategies, which give investors greater access and insight, but also provides additional scale to influence company practice. Starting in 2019, the Border to Coast Pensions Partnerships, a local government pension scheme fund, and Royal London Asset Management, have conducted a collaborative initiative on cybersecurity, which has allowed them to evolve their understanding of cybersecurity risk and approach, noting the significant value of these interactions: *"an in-depth dialogue rather than increasing general disclosures may be in the best interest of investors"*. Through the different stages of engagement, the initiative has now detailed investors' expectations[21] on this topic, which will guide its individual engagement and voting decisions.

Between 2017 and 2019, the PRI coordinated a global engagement programme on cybersecurity governance, with the participation of 55 institutional investors, representing over $12tn in AUM, covering 53 companies, with a focus on the financial, healthcare, telecommunications, IT and consumer discretionary sectors. The key objectives of the engagement, particularly in line with the limited levels of disclosure, were to:

1. Build investors' knowledge of how their portfolio companies are positioned to manage cyber risk (with a focus on companies' policies and governance structures);
2. Improve the amount and quality of disclosure on cyber risk and governance;
3. Establish investor expectations on what companies can and should disclose regarding cyber risk governance.

While companies' public disclosures have a significant distance to travel, the report notes that companies did make their experts available to investors, to provide a comprehensive view of their approach to cybersecurity, and in turn, these conversations helped investors scrutinise governance practices and discuss expectations on this topic. Furthermore, these dialogues and collaboration have allowed for the development of guidance to investors on how to engage on cybersecurity.

Border to Coast and Royal London Asset Management Approach

MINIMUM EXPECTATIONS:

- Risk identification and oversight at board level
- A nominated Chief Information Security Officer (CISO) with supporting resources.
- Inclusion of cyber covenants in supplier contracts and effective due diligence.
- Inclusion of cyber considerations in inorganic growth strategies including in the due diligence and integration phases.
- Timely disclosure of cybersecurity breaches
- Disclosures about a cyber resilient culture, to include tailored training across the workforce.

ADVANCED PRACTICES:

- Inclusion of information security and cyber resilience in executive compensation KPIs.
- Use of NIST Cybersecurity Framework as a reference for cybersecurity risk management.
- ISO 27000 for all operations.

These are highlighted in the PRI report[22] that sets out various engagement questions shareholders can use to get a better understanding of:

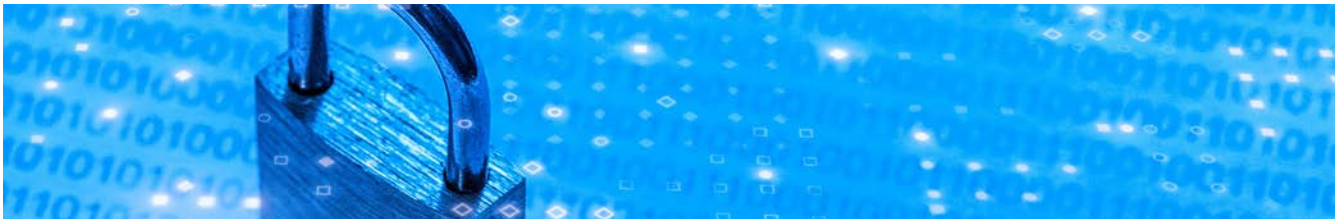
1. Board Oversight, and the governance structure supporting cybersecurity efforts;
2. Ensuring cyber resilience is integrated into overall strategy, and where key priorities are in this regard;
3. Finding common language on cybersecurity and how the information is translated to the board and across the company;
4. Looking beyond technical controls and companies are continuously updating their approach around cyber, and finally
5. Setting disclosure expectations which highlights some key areas where disclosure has been commonly and increasingly implemented.

FTI's Proposed Framework for Cybersecurity Reporting

In order to satisfy growing investor and regulator demands for enhanced cybersecurity governance and oversight, companies, particularly their leadership, will need to be able to clearly and concisely communicate what cybersecurity structures and controls they have in place to its key stakeholders. In fact, when announcing the recently proposed rules on cybersecurity in the US, SEC Chair Gary Gensler stated: *"I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner"*. However, there is currently a lack of guidance and established best practice for how this information should be shared.

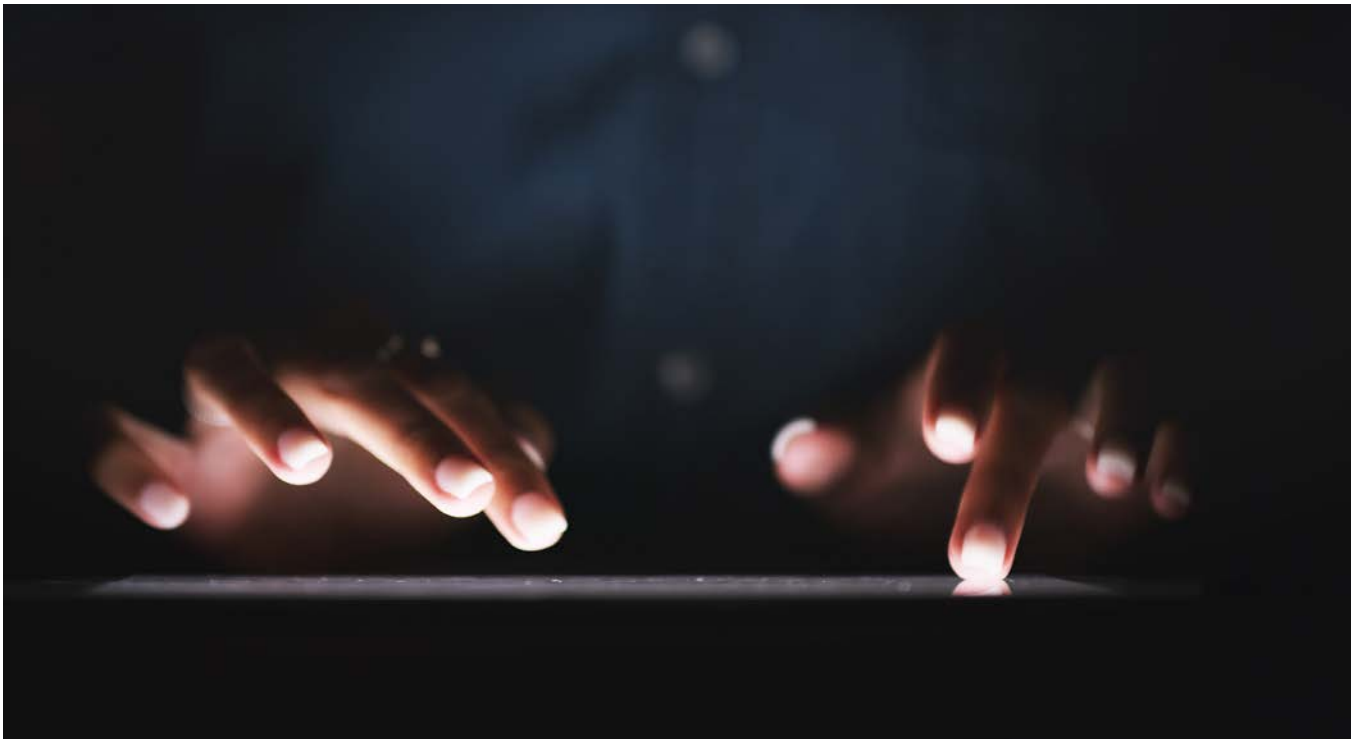
The current state of play with cybersecurity echoes some of the conversations that have taken place in recent years regarding climate and biodiversity, as well as sustainability more generally; and how companies' strategies and impact can be meaningfully communicated to investors. The Task Force on Climate-related Financial Disclosures (TCFD) and Task Force on Nature-related Financial Disclosures (TNFD) were created by the Financial Stability Board (FSB) to address inconsistencies in climate and biodiversity disclosures while, more generally, the Sustainable Accounting Standards Board (SASB) published standards designed to *"enable businesses around the world to identify, manage and communicate financially-material sustainability information to their investors."* There is an opportunity to reflect on the learnings from these disclosure frameworks and apply them to cybersecurity, given their focus on robust governance structures and risk-based approach. Indeed, there are elements of guidance already set out within existing frameworks – SASB and the Global Reporting Initiative ('GRI'), as two examples – which can provide building blocks towards a more specific framework for reporting and strategy assessment. The cybersecurity metrics outlined in the SASB framework provide a clear set of accounting metrics that can provide a meaningful information benchmark for investors on how a company is approaching its cybersecurity risk. As a starting point, it looks at indicators such as the number of data breaches, the percentage involving personally identifiable information, or the number of users affected. For more technology heavy companies, which with growing prevalence of digitalisation has become increasingly more uniform, companies are also expected to describe their approach to identifying and addressing data security risks, and the use of third-party cybersecurity standards is also included. This 'dual approach' provides companies with a structure to disclose their approach to cybersecurity in a more meaningful, quantifiable, and harmonised manner.

We propose a guidance framework below which attempts to address how companies, and the board of directors in particular, can demonstrate oversight of cybersecurity, while also maintaining necessary levels of confidentiality. The framework is based on the recommended reporting structure proposed by TCFD and TNFD, but tailored to reflect the current cybersecurity regulatory landscape, investor focus and the general pressures on businesses. The intention is for this framework to provide a consistent and standardised method, and common language, for the board and security leaders to communicate their approach to cybersecurity to investors and other key stakeholders. Many companies have concerns about disclosing details of their cybersecurity strategy as they believe it may expose them to a potential attack. We believe this framework could allow companies to acknowledge the risks posed by cybersecurity in a more holistic manner without sharing details that could be misused by a cyber threat actor or provide commercially sensitive information publicly. This communication with key stakeholders falls within the scope of the board of directors of a company. This approach could also be used as a diagnostic tool and a conversation starter between the board and cybersecurity teams, helping a company to identify and mitigate the future risks posed by ever-evolving cybersecurity threats. It will also ensure regular and structured engagement between the board and security leaders, which is of critical importance given the dynamic nature of cybersecurity and the threat landscape.



FTI's Approach to Cybersecurity Risks and Opportunities and Disclosure

Governance	Strategy	Risk Management	Metrics and Targets
— Is the board directly responsible for cybersecurity oversight? — Does the board understand how cybersecurity impacts upon their collective responsibilities? — Is there appropriate cybersecurity expertise on board? — How often does senior leadership brief the board on cybersecurity? — What percentage of the committee responsible for information security is independent? — What cyber insurance cover is in place?	— Does the strategy clearly outline cyber-related priorities, risks and opportunities? — Does the strategy align to risk management objectives? — Does the strategy articulate the material impact of risks and opportunities on organisation's business strategy and financial planning, and mergers & acquisitions' due diligence? — Does the strategy describe the resilience of the organisation in the face of a cybersecurity incident and post-breach management?	— Are the processes for identifying, assessing and managing cyber- related risk clearly defined and understood? — Are the processes for identifying, assessing and managing cyber-related risk integrated into the organisation's overall risk management? — Do risk management procedures account for internal and external risks, in particular supply chain risks? — Are the cybersecurity threats to the business analysed and understood to ensure defensive efforts are relevant and appropriate?	— Are metrics defined and used to assess cybersecurity risk? — How many incidents have occurred over the past 12 months? — Are defined controls in place that map to the threats faced by the organisation? — Can cybersecurity investments be linked directly to risk reduction, resilience and reliability provided by these investments? — How are employees, partners, vendors and key stakeholders trained and awareness maintained? — Is security culture measured?



Conclusion

Increased threat activity and a rapidly changing insurance landscape, combined with greater stakeholder scrutiny and a stricter regulatory environment, is increasing the pressure on companies to invest in cybersecurity and simultaneously implement governance and management structures that directly address cybersecurity. Regulators and investors alike not only want to see improved incident disclosure, but also want companies to clearly demonstrate that they are proactively addressing cyber risk. With greater accountability being placed on boards and management to comprehensively understand cyber risk and the controls that are in place, there is no longer space for inaction.

There is no one size fits all approach to ensuring boards are in a position to oversee cyber risk and while it is not expected that boards become cybersecurity experts, ensuring that – as a collective – the board is able to effectively engage and, ultimately, challenge the CISO and the company's cybersecurity strategy is an imperative. While it is the executive and operational teams' responsibility to draft and prepare the cybersecurity preparedness plan, the board plays a crucial role in asking the right questions to challenge and test this process, and also in managing the tensions between risk, usability, security and cost. Boards must be fully aware of the infrastructures, processes and people overseeing cybersecurity risk, and have a solid understanding of which parts of their organisation are deemed higher risk, what are the vulnerabilities in its control framework – particularly from a human error perspective – or whether third-party risk has been factored in the analysis. Furthermore, in order to manage the "knowledge" gap between the board and cybersecurity specialists, clear and consistent communication channels and engagement with the executive and operational teams on cybersecurity are key, alongside a clear commitment to continue to develop understanding of the evolution of cyber threats and risks as they relate to the business.

While cybersecurity is today primarily addressed under the governance pillar, it may touch on other aspects of ESG, in particular the social pillar. Cybersecurity incidents can have wide-reaching societal impact when they disrupt critical infrastructure and essential services, while data breaches can cause significant distress for data subjects, with employees often directly impacted. While appropriate cybersecurity governance should be a priority, these governance structures are only laying the foundations for what will likely be broadening scrutiny in future.

ORLA COX
Director – Strategic Communications
orla.cox@fticonsulting.com

HETAL KANJI
Director – Strategic Communications
hetal.kanji@fticonsulting.com

SIMON ONYONS
Managing Director – EMEA Cybersecurity
simon.onyons@fticonsulting.com

[1] https://www.ibm.com/security/data-breach

[2] https://www.weforum.org/reports/global-risks-report-2022/digest

[3] https://www.ibm.com/security/data-breach

[4] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

[5] https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

[6] https://www.wsj.com/articles/nestles-data-leak-shows-war-related-hacktivism-risks-11649151002

[7] https://www.ft.com/content/60ddc050-a846-461a-aa10-5aaabf6b35a5

[8] https://www.marsh.com/uk/services/international-placement-services/insights/global_insurance_market_index.html?utm_source=publicrelations&utm_medium=referral-link&utm_campaign=global-insurance-market-index-q4-2021

[9] https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381 Market Bulletin - Cyber-attack exclusions.pdf

[10] https://www.ibm.com/security/data-breach

[11] https://www.sec.gov/rules/proposed/2022/33-11038.pdf

[12] https://www.gartner.com/en/newsroom/press-releases/2022-02-24-gartner-says-the-cybersecurity-leader-s-role-needs-to

[13] Data not yet published. Research Methodology: FTI Consulting conducted an online survey among n=165 CISOs and those in charge of information security for large organizations across the U.S. between the dates of June 27 and July 5, 2022. For questions related to the research, please contact cyberbrand@fticonsulting.com

[14] https://fticommunications.com/boards-technology-a-gap-in-expertise/

[15] https://www.research.hsbc.com/R/36/PX7wVpdT9rsU?sbtv=036b0bcf-0103-11ed-adc0-005056b635ff

[16] https://www.unpri.org/cyber-security/engaging-on-cyber-security-results-of-the-pri-collaborative-engagement-2017-2019/5680.article

[17] https://www.blackrock.com/corporate/literature/publication/annual-stewardship-report-2021.pdf

[18] https://www.blackrock.com/corporate/literature/publication/2022-investment-stewardship-voting-spotlight.pdf

[19] https://www.blackrock.com/corporate/literature/publication/blk-commentary-our-approach-to-data-privacy-and-security.pdf

[20] https://corporate.vanguard.com/content/dam/corp/advocate/investment-stewardship/pdf/policies-and-reports/2020_investment_stewardship_semiannual_report.pdf

[21] https://www.bordertocoast.org.uk/wp-content/uploads/2022/03/CYBERSECURITY-ENGAGEMENT-FOCUS.pdf

[22] https://www.unpri.org/download?ac=10398