# A guide to managing data security and privacy at board level

Legal & General
INVESTMENT MANAGEMENT

2020 | A guide to managing data security and privacy at board level

# Why focus on data security and privacy?

EU regulations such as GDPR, implemented in May 2018, have improved the protection of European data subjects' rights and clarify what companies that process personal data must do to safeguard these rights. The Securities and Exchange Commission in the US has also focussed on market disclosure, breach notification and internal controls relating to data breaches. Some companies which hold large volumes of individuals' personal data, such as financial services, utilities, large retailers and travel companies, may additionally be subject to industry-specific regulations.

The Information Commissioner's Office ('the ICO') has the power to fine companies up to 2% of their worldwide turnover and has been proactive in recent cases of data leaks. For example, the ICO fined British Airways £183.39 million for GDPR infringements following an investigation into their handling of personal information, which demonstrated poor security arrangements at the company when it came to login, payment card, and travel booking details, as well as names and addresses.

The ICO has also fined, among others, Cathay Pacific for failing to protect customer data as their systems were not deemed to be sufficiently robust; EE for sending customers direct messages without their consent; and Uber for failing to protect customers' personal information during a cyber attack. The UK and US jointly found there has been a significant rise in attacks during the Covid-19 outbreak.[1]

LGIM wishes to invest in companies for whom compliance with data and privacy laws and regulations underpins management activities in this area. We will therefore look for evidence that boards, in particular their Non-Executive Directors (NEDs), have afforded this topic an appropriate level of oversight.

Risks to data security and privacy from cyber attacks, hacking or theft are a major technological threat facing most businesses. Network security breaches, damage to IT infrastructure and theft of personal data and commercially sensitive information are omnipresent risks that pose a significant financial and reputational threat to companies. It is important for shareholders to know that they are investing, through LGIM, in companies that are taking appropriate steps to protect their assets and reputation. Through defining, establishing and monitoring such standards we can show investors that we share their concerns and are proactively responding to them and raising standards.

1. https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf]

# The role of the board

Data security and privacy present material risks for shareholders, debt holders and customers. LGIM therefore relies on company boards to ensure that appropriate data security measures have been put in place and that a suitable amount of time is spent considering internal capabilities in this area. This includes testing the vulnerability of the business to the data loss or theft, incorporating both commercially sensitive and proprietary data.

We recognise that companies may be reluctant to talk publicly about their data security qualities or objectives. In contrast to other environmental, social and governance ('ESG') issues, a common agreement as to what 'good' corporate board standards look like may be hard to achieve.

We agree with UN PRI's view[2] on the vital role of governance when it comes to responding to cyber risks:

> "To demonstrate that cyber security is an organisational priority, companies should establish board oversight of the issue. Boards have a role in ensuring that cyber security considerations [...] drive strategy and shape broader business decision-making. To enable this, board members should receive quality management information and be well-informed so that they can sense-check the adequacy of cyber security programmes, and challenge management actions where appropriate. This does not mean that the board should be involved in the day-to-day technical and operational issues. However, it must set expectations and have confidence that operational, financial and strategic resilience tied to cyber security is in line with those expectations."

2. UN PRI - UN Principles of Responsible Investing.
https://www.unpri.org/engaging-on-cyber-security-results-of-the-pri-collaborative-engagement-2017-2019/5680.article



2020 | A guide to managing data security and privacy at board level

# Practical steps

In satisfying their risk oversight function with respect to cyber security, boards should evaluate their company's preparedness and action plan for a possible cyber security breach. Cyber risks should be monitored on the risk registers of companies, resulting in having controls in place to help mitigate the risk. This will start with identification of the company's mission-critical data and systems. The cyber incident response plan must identify critical personnel and responsibilities that cover procedures for containment, mitigation and business continuity. It is essential to be proactive about defending the company, including the use of tools such as continuously monitoring the 'Dark Web' to ensure there are no data leakages and to collaborate with other companies and share best practice to support each other against the attacks. The National Cyber Security Centre board toolkit is a useful resource which boards should consult.

If a board or its risk committee does not have any NEDs with the specialist skillset to provide meaningful management challenge, it should consider having a separate advisory board and accessing consultancy expertise to provide independent judgements. However, overall responsibility for privacy and security should not sit with a nominated person but instead with a committee to reflect the board-level risk. The committee should have a remit to look at how often tests are conducted, whether escalation procedures are clear, and how responsible persons are expected to react. Cyber policies which protect the company's information should be as familiar to the board as accounting policies. Additionally, we believe it is best practice to ensure that cyber-preparedness factors form part of the executives' Key Performance Indicators.

2020 | A guide to managing data security and privacy at board level

# Assessing quality of oversight

LGIM is likely to be seeking answers to the following questions relating to corporate boards' oversight of cyber and privacy risk, regarding both protection against cyber incidents and mitigation of those that have materialised:

1 **Does the firm have a board-approved cyber security strategy?**

2 **How often does the board or its committees include this risk on its agendas?**

3 **How does the board ensure it has the necessary level of technical insights?**

4 **Does the board explicitly approve the budget required for managing cyber risk?**

5 **What is the quality and depth of cyber and privacy management information provided to the board?**

6 **How does the board ensure that a suitable cyber and privacy culture is in place?**

7 **How does the company identify and protect its critical assets?**

8 **How does the company detect and respond to an incident, recover the business, and learn from the experience?**

9 **When was the last cyber audit and scenario planning exercise conducted? Have the backup and recovery facilities been tested?**

10 **Do the chief information security and data protection officers have a voice in the organisation?**

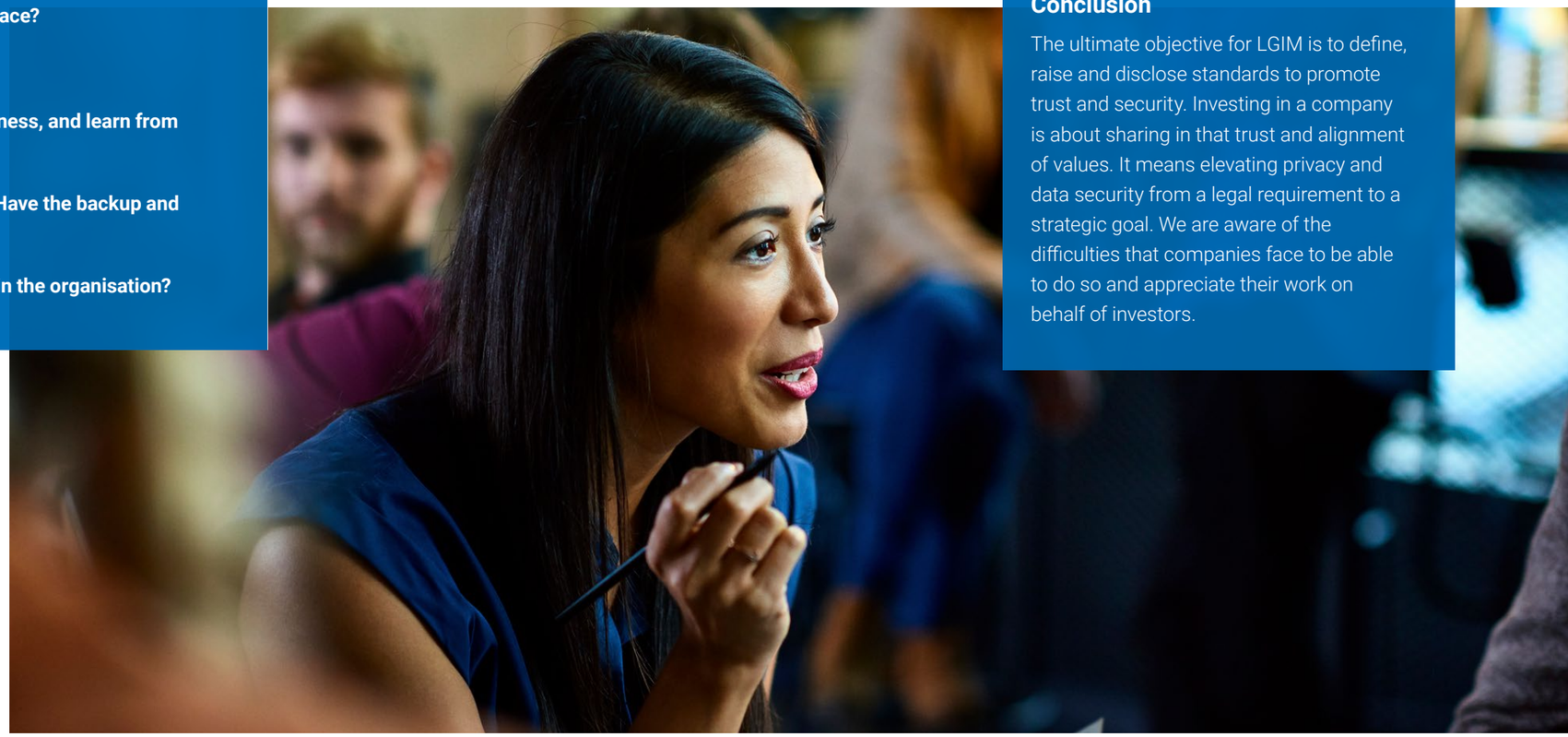
The answers will provide a valuable snapshot of a firm's cyber resilience capability and highlight areas for further development. Directors themselves should be aware that they and those close to them are prime targets for hackers due to the sensitive information they are handling. Therefore, directors need to make sure they are cyber aware (for example, don't use personal email accounts) and follow security protocols from their organisations.

Importantly, we would like to see more disclosure in annual reports about the measures that have been implemented and to what extent the company is continuously learning and improving their cyber risk management practices. During our engagements we have seen great examples of effective prompt management of privacy breaches, which were outcomes of successful collaboration across the firm, and grounded in firm-wide preparedness and thorough prior scenario testing.

Boards should be prepared to explain to shareholders their company's approach to handling the privacy, data and cyber security risks faced by their organisation, and the structures and processes in place to mitigate these risks.

## Conclusion

The ultimate objective for LGIM is to define, raise and disclose standards to promote trust and security. Investing in a company is about sharing in that trust and alignment of values. It means elevating privacy and data security from a legal requirement to a strategic goal. We are aware of the difficulties that companies face to be able to do so and appreciate their work on behalf of investors.



# Contact us


**Important information**

The value of an investment and any income taken from it is not guaranteed and can go down as well as up, you may not get back the amount you originally invested.



CC69082020_GM SEP2020

Legal & General
INVESTMENT MANAGEMENT