5.2.5

CYBERSECURITY AND INFORMATION SECURITY OVERSIGHT

Cybersecurity oversight

With increased reliance on digital technologies, cybersecurity has become a significant concern. The Board is responsible for overseeing the company's cybersecurity measures, ensuring the protection of sensitive data and mitigating potential risks.

The key areas of its responsibility are:

1. ***Strategic oversight:*** integrate cybersecurity risks into the overall company strategy and ensure an understanding of how cyber threats could affect the business goals and financial performance of the entire organisation.
2. ***Oversight and accountability:***
    a. Be aware of and understand the key cyber risks. The Board should be informed about the most significant cyber risks the company faces and how management is addressing them.
    b. Monitor cyber resilience: oversee the company's ability to withstand and recover from cyberattacks.
3. ***Board expertise:*** the Board and its designated committee (if any) should have clear ownership of cybersecurity oversight. Board members may seek additional training, if needed, to fulfil this responsibility professionally and effectively.

By actively engaging in these areas, the Board can help the company to mitigate cyber risks and protect its critical assets, ensuring its resilience.

More on cybersecurity oversight can be found in "Cyber-Risk Oversight – Key Principles and Practical Guidance for Corporate Boards in Europe".[18]

Information security oversight

Information security is one of the core elements of corporate resilience, risk management and internal control. It covers the protection of the company's information, systems, data, networks, digital assets and critical technology infrastructure against unauthorised access, misuse, loss, disruption, manipulation or disclosure. It is directly linked to strategy, business continuity, legal compliance,

18 BICG (2020), Cyber-Risk Oversight – Key Principles and Practical Guidance for Corporate Boards in Europe, https://www.bicg.eu/wp-content/uploads/2020/09/Handbook-1.pdf.

customer trust, reputation, financial reporting, personal data protection, intellectual property and long-term value creation. It also supports operational resilience, strategic decision-making and the company's ability to maintain critical services during disruption.

The Board should ensure that the company has a clear information security policy, defined roles and responsibilities, and regular reporting to the Board and/or a relevant Board committee. Management should be able to explain which information assets and systems are critical, what the main threats are, what controls are in place, how incidents are detected and escalated, and how the company would respond to and recover from a serious cyber or information security incident.

Information security oversight should cover at least the following areas:

AREA	WHAT THE BOARD SHOULD ENSURE
Governance	Clear accountability for information security at executive level
Risk appetite	Agreed level of acceptable information security and cyber risk
Critical assets	Identification of critical data, systems, infrastructure, intellectual property, artificial intelligence systems and operational technology
Controls	Appropriate preventive, detective and corrective controls
Incident and crisis response	Tested procedures for detecting, escalating, responding to and recovering from incidents, including communication, authorities' notification and stakeholder coordination arrangements
Business continuity	Alignment between information security, business continuity and disaster recovery plans
Third parties	Oversight of information security risks from suppliers, cloud providers, outsourced services, software dependencies, supply chains and group companies
People	Employee awareness, access controls, training, insider-risk management and information security culture
Legal compliance	Compliance with data protection, cyber, sectoral and disclosure obligations
Assurance	Internal audit, external testing, penetration testing or independent reviews where appropriate
Reporting	Clear, concise and decision-useful reporting to the Board

The Board should receive regular information security reporting. Such reporting should not be limited to technical metrics. It should help the Board understand whether the company is operating within its risk appetite and whether management

is improving the company's resilience. Useful Board-level indicators may include material incidents and near misses, results of cyber exercises, status of critical remediation actions, employee training completion, phishing and social engineering test trends, vulnerability remediation, third-party risk exposure, audit findings, disaster recovery test results, insurance coverage and regulatory developments.

The Board should also ensure that the company periodically tests its information security arrangements. This may include tabletop exercises, cyber incident simulations, disaster recovery tests, penetration testing, supplier-risk reviews and crisis communication exercises. Lessons learned should be reported to the Board, with clear owners and deadlines for improvement actions.

The Board also plays an important role in setting the tone for security culture across the organisation. Information security should be treated as a shared business responsibility rather than solely a technical or IT matter.

Information security risks increasingly arise through third parties, outsourced services, software providers and interconnected supply chains. The Board should ensure that supplier risk management is proportionate to the company's critical services, dependencies and regulatory obligations, particularly where critical operations, data or technology services rely on external providers.

In company group structures, information security policies may be developed at group level. However, the Board of each subsidiary should consider whether group policies are suitable for the subsidiary's own business, systems, regulatory environment, risk profile and stakeholder interests. Group consistency is valuable, but it should not replace the subsidiary Board's responsibility to ensure that the subsidiary has adequate information security governance and resilience.

Effective Board oversight does not require technical expertise from every Board member, but it does require sufficient understanding to ask informed questions, challenge management and support informed decision-making.

The key expectation is that the Board should **oversee, challenge and assure**, not manage technical details. A robust information security framework should give the Board confidence that management understands the company's digital risks, has implemented proportionate controls, can respond effectively to incidents, manages critical dependencies and continuously improves the company's resilience and security culture.

KEY TAKEAWAYS

A. Cybersecurity and information security are strategic risk governance matters, not IT matters. The Board oversees, challenges and assures; it does not manage the technical detail, but it must understand enough to ask informed questions.

B. The Board should ensure that there is a clear information security policy, executive-level accountability, an agreed risk appetite for cyber and information risk, identified critical assets, proportionate controls and tested incident, continuity and recovery procedures.

C. Board reporting should go beyond technical metrics: material incidents and near misses, exercise results, remediation status, training and phishing test trends, third-party exposure, audit findings and regulatory developments.

D. Information security risks increasingly come through suppliers, cloud providers, software dependencies and group companies; supplier risk management must be proportionate to the company's critical dependencies.

E. In a group, each subsidiary Board remains responsible for ensuring that group policies are suitable for its own business and risk profile. The Board also sets the tone for a security culture in which information security is a shared business responsibility.

QUESTIONS FOR THE BOARD

1. *What are our most critical information assets, systems and data, and who is accountable for their security at executive level?*
2. *Is cyber and information security risk included in the company's risk appetite and risk register, and integrated into the strategy?*
3. *Which third-party, cloud and software dependencies could significantly disrupt our critical operations, and how are they overseen?*
4. *Do we understand the risks associated with emerging technologies, including artificial intelligence and automation?*
5. *How often does the Board receive information security reporting, and what were the most significant incidents, near misses or control weaknesses in the last year?*
6. *Have our incident response, business continuity and disaster recovery plans been tested, and were the lessons translated into concrete improvements?*
7. *Do we have sufficient internal expertise and independent external assurance, and are employees and managers properly trained?*
8. *Does the Board itself have sufficient understanding to challenge management on cyber risk, or should it seek training or expert support?*