nccgroup
freedom from doubt

Cyber Risk & Security Guidance for Non-Executive Directors

NCC Group

A BOARD LEVEL ISSUE

Cyber security and resilience is a topic that all boards need to contend with due to the impact on governance and legal obligations. Empowering non-executive directors with the knowledge, vocabulary and questions to ensure that organisations have appropriate oversight and posture relevant to the threats they face is critical for good corporate governance in the 21st century.

Risk management, security, resilience and assurance

An organisation's exposure to cyber risk is built and managed using a number of core tenets.

- **Risk Ownership:** Identified individuals within the organisation who are accountable to the chief executive. These individuals are responsible for deciding the acceptable levels of risk as the organisation operates and ensures that threats beyond these levels are mitigated, remediated or escalated.
- **Risk Management:** Individuals and functions responsible for day-to-day operation of the business ensuring that risks are appropriately managed.
- **Security:** The elements that are responsible for mitigating, remediating or managing the threats faced by people, processes, procedures, suppliers and technology to the business.
- **Assessment and Assurance:** The means of assessing and assuring the organisation's level of risk exposure and any mitigation are as expected and performing to appropriate levels.
- **Resilience:** The ability to detect and respond to both internal and external cyber security incidents as part of a business-as-usual steady state.

It is about more than just a technology

Cyber risk and security are often seen as solely a technological problem. The reality is while technology is a key source of risk, and thus poses a security problem, it is neither the sole source nor the solution.

Today's businesses are complex blends of people, technology, processes, procedures and suppliers. This complex and diverse eco-system means that all constituents can all play a role in ensuring or undermining the cyber security of an organisation.

As such it is important that while technology will often be seen as a manifestation of risk and thus needs securing, other elements that can undermine technology security need to be considered and managed.

Threats don't just come from the outside

Cyber security threats are often perceived to only originate externally, but in actual fact they can originate from anywhere in or outside of the business. As such solely focusing on threats of external origin can still leave an organisation exposed to significant risk. A malicious ex employee or a breached supplier holding your organisation's data can be equally if not more impactful, when compared to an external attack.

You can't outsource risk ownership only offset it

Broadly speaking organisations can outsource certain functions or operations but they can't outsource risk ownership. They can, however, offset or transfer risk via insurance and similar mechanisms.

CYBER SECURITY QUESTIONS AS A NON-EXECUTIVE DIRECTOR

Who owns cyber risk within the organisation?

Owner(s) should be clearly identified for cyber risk at an executive level. Often these individuals will own the operations of the business so they can make informed decisions on risk versus reward.

Who manages cyber risk within the organisation?

Manager(s) should be clearly identified for ensuring that the risk owners are appraised with the relevant information to understand what their exposure is while managing to acceptable levels.

Does the board receive regular briefings on the organisations cyber risk and security posture?

Boards should receive several detailed briefings on the cyber risk and security posture of the organisation including summaries of key incidents.

Has the organisation demonstrated an ability to detect and respond to both internal & external incidents?

Cyber security is not a binary state (i.e. secure or not secure) organisations need to be capable of detecting and responding to cyber security incidents as part of a steady state.

Does the organisation know where its critical assets are and are they adequately protected if so?

Organisations that cannot identify or articulate what its critical assets are or where they are located, can similarly not ensure that the associated cyber risk is managed appropriately.

Does the organisation treat cyber risk and security as a blended challenge across people, technology, processes, procedures and suppliers?

Organisations that solely treat cyber risk as a technology problem can often be easily undermined by blended attacks including social engineering (confidence tricks) such as phishing.

How is the level of exposure communicated up to the board?

Organisations often rely on 'Red Amber Green' reporting for cyber risk and security. For a topic so nuanced and complicated this is rarely sufficient. As such the level of reporting expected should be more detailed than this even at board level.

How does this organisation's posture compare with its peers and my other seats?

Organisations that over or underspend are not competitive. By understanding how an organisation compares to its peers based on vertical, size and geography ensures appropriateness and maturity of its cyber risk and security programme.

Do I have confidence there is a sufficient understanding of the problem within the board?

Having confidence in the executive's ability to understand the challenges and opportunities presented is critical. An executive that does not understand sufficiently due to lack of knowledge or insight means they may underestimate the exposure and consequences.

ADDITIONAL RESOURCES

Visit www.nccgroup.trust/cyber-defence-operations for more information and guidance on your cyber security strategy and technical requirements

Blog post: Cyber security and the board

Blog post: How should employers communicate data breaches to employees?

Infographic: Five Cyber Security Myths

Services: Cyber Defence Operations

All of our cyber security research and thought leadership is available at: www.nccgroup.trust/research

ABOUT NCC GROUP

NCC Group is a global information assurance specialist. As the cyber arms race and technology revolution continue to outpace the ability of organisations to cope with the plethora of security, performance and availability issues, we are best placed to help organisations to manage the risk and limit the threat.

We are committed to ensuring that organisations have access to a total information assurance solution that works for them. We assure the protection of your information against malicious attacks and data loss.

Through expert security and penetration testing, forensic services, incident response, compliance advice, vulnerability research and logical and physical audits we will help you to strengthen your position in the cyber arms race.

With the UK's largest penetration testing team and top-level accreditations from bodies ranging from the government's CESG CHECK scheme to the PCI Security Standards Council, we are a trusted advisor to over 15000 clients worldwide.

We are passionate about changing the shape of the internet and making it safer.

Visit: www.nccgroup.trust

Contact: response@nccgroup.trust

Share

www.nccgroup.trust
@nccgroupplc