Provision 29 Mythbuster: Focus on Cyber

When considering material controls, it is likely that many companies will attribute one to cyber security. Cyber security is a significant issue for companies, especially those who rely on digital systems and technologies, like AI, to conduct business operations.

Cyber threats continue to evolve as adversaries adapt their methods. Companies should therefore keep their cyber risks, controls and resilience arrangements under regular review, adapting them as the threat landscape and their own exposure change. The FRC has heard concerns from companies that reporting in this area could disclose commercially sensitive information or details that may undermine their security. Companies have also questioned whether a subsequent cyber incident could call an earlier effectiveness declaration into question.

Reporting on cyber, including a declaration under Provision 29, is not a guarantee that a company will not subsequently experience a cyber incident. Nor should reporting be so granular that it discloses the specific technical controls used to prevent or mitigate the harm arising from an incident.

This mythbuster, prepared in consultation with the Department for Digital, Culture, Media and Sport and the National Cyber Security Centre, deals with some of these issues in more detail.

Q. **Information about our cyber controls is sensitive; if we publish details, we are putting the company at risk both commercially and to threat actors – is this what Provision 29 expects us to do?**

A. The declaration should not include commercially sensitive information or specific details of the technical controls implemented to support the company's cyber resilience. However, the board needs to satisfy itself that the company's material controls are effective and explain how it has monitored and reviewed their effectiveness. The declaration focuses on that assurance process and its outcome, rather than the detailed design or operation of individual technical controls.

Q. **Do we need to include disclaimers to mitigate for any unknown risks?**

A. The declaration of effectiveness of material controls is as at the balance sheet date. There is no expectation that you look beyond this in your declaration.

We understand that you cannot plan for or mitigate against unknown future risks in this area, as the landscape can change very quickly. However, companies should consider reasonable changes in cyber risk when designing, monitoring, and reviewing their controls, as boards will understand the landscape within which they are working.

Q. **Do you expect us to provide a guarantee of cyber security?**

A. Provision 29 does not require boards to guarantee total cyber security, nor is it realistic for there to be an expectation that cyber risk can always be eliminated, as a board will not always know the threat that it might be exposed to.

Boards monitor the effectiveness of the company's material controls in place to manage cyber risks and explain how they have done so. Alongside work on Provision 29 companies should have a focus on cyber resilience, which would usually include an assessment of exposure to cyber risk and how resilience is built into business planning.

Q. **Does Provision 29 take into account the difference between a failed material control and changes to the external environment given how quickly cyber risk changes?**

A. We recognise that the board may be sufficiently satisfied that material controls were effective at the balance sheet date, while also recognising that point-in-time assurance does not imply enduring protection.

When the board has determined that a control is effective, it does not mean that the risk is eliminated. There are limitations to controls, which may include internal and external events and uncertainties which sometimes may be outside the company's control.

Q. **Should cyber risk be reported separately from the broader control framework?**

A. We expect boards to provide a description of how they monitor and review the effectiveness of the risk management and internal control framework, a declaration of the effectiveness of material controls as at the balance sheet date, and a description of any material controls that have not operated effectively as at the balance sheet date. Where cyber controls are identified as material, they are included in this.

We welcome cross-referencing to other areas of your reporting if appropriate.

Q. We had a cyber breach; how do we report this?

Provision 29 does not create a separate requirement to report every cyber incident or breach. The focus of the Provision is on whether the board can declare that its material controls were effective as at the balance sheet date.

If the cyber breach indicates that a material control did not operate effectively as at the balance sheet date, the annual report describes at a high level that control failure, the action taken, or proposed, to improve it, and any action taken to address previously reported issues.

Boards should consider the breach in the context of their wider risk management and internal control framework and assess whether it affects their declaration on the effectiveness of material controls. The emphasis is on the effectiveness of the material controls, rather than the occurrence of the cyber incident itself.

A.

Where can we find more cyber risk guidance and support for Boards?

Board members need enough knowledge for constructive discussions with key personnel in their organisation, so they can be confident that cyber risk is being appropriately managed. To support boards in fulfilling this, the UK Government introduced the Cyber Governance Code of Practice which sets out the key actions for Board members to take to govern cyber security risks effectively, detailing their responsibilities and accountability in safeguarding the organisation. The Information Commissioners Office recently set out that they expect organisations that are using or storing personal data, as set out in the UK GDPR, to have implemented the actions in the Cyber Governance Code of Practice.

The Cyber Governance Code of Practice is the foundation of the government's free package of support on cyber governance and should be the first point of reference for board members. It is underpinned by Cyber Governance Training, which helps boards members to strengthen their understanding of how to govern cyber security risks, and the Cyber Security Toolkit for Boards, which supports board members in implementing the actions set out in the Code.

The government has also launched the voluntary Cyber Resilience Pledge which provides a tangible way for organisations to demonstrate their commitment to cyber security, boost their resilience to cyber attacks and differentiate themselves fromtheir competitors.

Get in touch
London office:
13th Floor,
1 Harbour Exchange Square,
London, E14 9GE

Birmingham office:
5th Floor, 3 Arena Central,
Bridge Street,
Birmingham, B1 2AX

+44 (0)20 7492 2300

www.frc.org.uk
Follow us on LinkedIn