OCTOBER 2019

Cybersecurity fundamentals for boards

The IoD is a proud partner of New Zealand's Cyber Smart Week which is intended to help people and organisations improve their cybersecurity.

Cybersecurity requires board level attention and responsibility and is not just an IT issue. Given this, it is critical that boards include time on the agenda to discuss their approach to cybersecurity, and constantly assess and reassess their capacity to address cybersecurity threats.

The principles behind cyber-risks are no different to other areas of risk. Boards must grasp the specific risks, determine risk appetite and take actions to deal with cyber-risk.

There are five core principles for boards in their oversight of cyber-risks

1. Take a holistic approach

Boards should approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Understand the legislative environment

Boards should understand the legal implications of cyber-risk as they apply to the organisation's specific circumstances.

3. Access expertise and put cybersecurity on the board agenda

Boards should have adequate access to cybersecurity expertise. Discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

4. Establish a framework

Boards should set the expectation that management will establish an enterprise-wide cyber-risk management framework.

5. Categorise the risks

Board and management discussion of cyber-risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Breach notification

Organisations and people that have experienced a cyberattack can report it to **CERT NZ**, the first port of call in New Zealand for reporting cybersecurity problems (see **cert.govt.nz**).

It is also anticipated that New Zealand will soon have mandatory privacy breach reporting. This has been proposed in the Privacy Bill (before Parliament) requiring organisations to report to the Privacy Commissioner and affected individuals when there has been a harmful (or potentially harmful) privacy breach.

Further resources

IoD/Aura ***Reporting cybersecurity to boards***

IoD ***Cyber-risk practice guide***

FMA ***Cyber-resilience in FMA-regulated financial services***

UK National Cyber Security Centre, ***Cyber Security Toolkit for Boards***