6 Cyber Security Standards You Need to Know About if You Are a Company Director or Board Member

Sean Field, Special Counsel, Maddocks, provides an overview of the cyber security standards that all Company directors and officers should know about.

INTRODUCTION

By now there can be no doubt that legal obligations on company directors and officers under the Corporations Act to discharge their duties with care and diligence extend into the field of cyber security.

In its Cyber Resilience: Health Check (ASIC Report 429) (the **Report**) the Australian Securities and Investments Commission (**ASIC**) has clearly articulated its position on cyber security and directors' duties, stating that:

- it considers board participation important to promoting a strong culture of cyber resilience;[1] and
- a failure to meet obligations to identify and manage cyber risks may, if you are a director or officer of a company, result in you being disqualified from your role.[2]

As a director or board member, how can you satisfy yourself that you have taken sufficient steps in this regard?

This article provides:

- a concise guide to 6 Cyber Security Standards which you should know about; and
- a six point cyber security check list.

Familiarity with the 6 Cyber Security Standards will:

- give you a basic grasp of cyber security issues in your organisation; and
- allow you to have appropriate conversations with and to ask the questions that need to be asked of your line management with responsibility for IT and cyber security.

The accompanying "Six Point Cyber Security Check List" is intended to provide a high level entry point for Company Directors and Board Members to design strategies to meet their legal obligations in relation to cyber security.

THE 6 CYBER SECURITY STANDARDS

Number 1:
Australian Signals Directorate's Top four mitigation strategies to protect your ICT system[3]

The Australian Signals Directorate (**ASD**) is the Commonwealth's peak advisory body on cyber security.

Its 2012 publication, *Top four mitigation strategies to protect your ICT system,* the ASD sets out four cyber security strategies which it says, if implemented, can address up to 85% of targeted cyber intrusions. These strategies are a subset of a wider suite of ASD's published cyber security strategies.[4]

Number 2:
The Australian Government Cyber Security Operations Centre's Questions Senior Management Need to be Asking about Cyber Security[5]

The Cyber Security Operations Centre (**CSOC**) **is** a joint agency under the responsibility of the Commonwealth Attorney-General and the Minister for Defence.

The CSOC suggests that senior management should be asking the following questions:

- What would a serious cyber incident cost our organisation?
- Who would benefit from having access to our information?
- What makes us secure against threats?
- Is the behaviour of our staff enabling a strong security culture?
- Are we ready to respond to a cyber security incident?
- Has the organisation applied ASD's top four mitigation strategies? (see Number 1, above).

Number 3:
ASIC's Cyber Resilience: Health Check (ASIC Report 429)

For directors and officers of corporations and other ASIC regulated entities, this guidance [ASIC's Cyber Resilience: Health Check (ASIC Report 429)] from the regulator should be compulsory reading.

1 ASIC *Cyber Resilience: Health Check (ASIC Report 429)*, (19 March 2015) available at <http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf> 1, 29

2 Ibid 38.

3 Australian Signal Directorate, *Top Four Mitigation Strategies to Protect Your ICT System* (2012) available at <http://www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf>

4 Australian Signal Directorate, *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details* (2014) available at <http://www.asd.gov.au/publications/Mitigation_Strategies_2014_Details.pdf>

5 Australian Government Department of Defence Cyber Security Operation Centre, *Questions Senior Management Need to be Asking about Cyber Security* (August 2012) available at <http://www.asd.gov.au/publications/protect/senior_management_questions.htm>

The Report contains a number of "Health Check Prompts" which provide useful guidance as to the questions directors and officers can ask in assessing their organisation's awareness of and preparedness for cyber security issues.

The Report notes that:

- for listed entities, a cyber attack may need to be disclosed as market-sensitive information; and
- cyber risks may need to be disclosed in Product Disclosure Statements.[6]

Number 4:
The Office of the Australian Information Commissioner's Guide to securing personal information – "reasonable steps" to protect personal information[7] (**the OAIC Guide**)

The Privacy Act 1988 (Cth) requires regulated entities to take such steps as are reasonable *in the circumstances* to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure (Australian Privacy Principle (**APP**) no. 11).

But what constitutes "such steps as are reasonable in the circumstances"?

The OAIC Guide provides useful information in this regard and should be read in conjunction with the other documents referred to in this article.

Number 5:
The Payment Card Industry's Data Security Standard (DSS): Requirements and Security Assessment Procedures (the **PCI Standard**)[8]

If your organisation processes card payments, it should comply with the PCI Standard.

If your organisation outsources card payment processing, your outsourced service provider should comply with this Standard.

Number 6:
ISO/IEC Standards

The International Organisation for Standardisation (**ISO**) and the International Electrotechnical Commission (**IEC**) publish a number of standards used across the IT industry, including specific standards relating to IT security.

The key IT and cyber security standards are the ISO 27000 series.

These are highly technical and detailed publications and it is not suggested that directors and officers become experts in these standards and their implementation.

However directors and officers can ask whether their organisation, suppliers to it and third party products and services are compliant with applicable ISO/IEC standards such as ISO 27000.

Such compliance will not be necessary or appropriate in all cases but to ask these questions may serve as a useful prompt for a discussion with your IT manager or CIO about whether you, your suppliers and third party products are or should be ISO/IEC compliant.

CONCLUSIONS

1. Your organisation's most basic (but arguably not sufficient) cyber-security strategy must include the following:
   a. implement ASD's top 4 cyber intrusion mitigation strategies;
   b. implement the other ASD published strategies, as applicable;
   c. in respect of any of the ASD strategies that are not implemented, ensure that your organisation has a clearly documented audit trail of the reasons why it decided not to implement a particular strategy. That documentation should include an appropriate risk analysis;
   d. ask CSOC's six questions of your IT manager or CIO – are you happy with the answers you get?;
   e. apply ASIC's "Health Check Prompts" to your organisation – what do the outcomes tell you about your organisation's cyber-preparedness?;
   f. if your organisation collects, stores, handles or processes personal information, ask whether it meets the standards set out in OAIC's Guide;
   g. if your organisation processes card payments, ask whether it and its service providers comply with the PCI Standard;
   h. ask whether your organisation, its suppliers and third party products meet ISO/IEC standards, if applicable/appropriate?
2. The 6 Cyber Security Standards referred to in this article and the Six Point Check List below are by no means exhaustive. This article is intended as an introductory guide to allow the non-technical director or officer to ask the right questions of those with managerial responsibility for IT and cyber security.
3. We have not, for example, discussed above the publications put out by the Australian Prudential Regulation Authority (**APRA**). While APRA's publications are aimed particularly at the banking, insurance and superannuation industries, they are of relevance to a wider audience[9].

SEAN FIELD is a Special Counsel at Maddocks, specialising in technology law, intellectual property and M&A transactions in the technology sector.

6 ASIC, see above n 1, 1.

7 Office of the Australian Information Commissioner, *Guide to Securing Personal Information – Reasonable Steps to Protect Personal Information* (January 2015) available at <https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf>

8 PCI Security Standards Council, *Data Security Standard: Requirements and Security Assessment Procedures* available at <https://www.pcisecuritystandards.org/document_library>

9 See for example APRA's *Information Paper: Outsourcing Involving Shared Computing Services (Including Cloud), Prudential Practice Guide CPG 234 – Management of Security Risk in Information and Information Technology and Prudential Practice Guide CPG 235 – Managing Data Risk.*