Cyber security skills of company directors – ASX 100

Introduction

There are many expectations and requirements to being a modern company director. The cyber resilience of the organisation they govern is just one part of the role. To achieve this, company directors need to be asking management the tough questions (and be competent enough to know what answers to expect) surrounding their organisations understanding of cyber risk, the investment in creating and monitoring controls, and rehearsed scenarios to be better equipped should a cyber security incident take place. Company directors need to assess cyber security, just as they would any risk, making competent decisions to understand the nature of the risk and how their level of (under) investment in cyber security controls will impact customers and stakeholders.[1]

This analysis is of the company directors of the ASX 100 stated knowledge of cyber security and/or technology in general. This knowledge is gleaned from data provided on ASX 100 company websites and LinkedIn profiles of individual directors. The ASX 100, is a list of the largest and most liquid companies and accounts for 82.73% of the All Ordinaries Index.[2] The ASX 100 Index is Australia's premier large capitalisation equity index[3] and is chosen due to the economic significance they play within the Australian economy.

The Online Threat Environment

Pervasive cyber attacks are one of the most crucial factors threatening the Australian economy. Cybercrime costs the Australian economy $42bn per year[4] and impacts all organisations large, medium and small. The threats range from highly sophisticated state-sponsored attacks, through to phishing, ransomware and business email compromise. Cyber incidents caused huge impacts on Australia's central government and other essential services including healthcare, education, energy, banking, and critical infrastructure providers, and so forth.

Organisations of all shapes, sizes and market sectors are at risk from cyber attack. There have been various cyber attacks toward ASX 100 companies causing privacy breaches and economic impact on the country, with 38 ASX listed companies having been exposed to cyberattacks over the past 10 years. This includes AMP, ANZ Bank, Bluescope Steel, Commonwealth Bank, Fairfax media, Telstra and Wesfarmers[5]. In 2021, The ANZ bank was hit by a distributed denial-of-service (DDoS) cyber attack for a couple of days effectively blocked legitimate requests. In late 2021, Coles, Westpac, and AMP companies were exposed to a significant data breach by hackers. Attackers accessed sensitive customers' data that likely were the goal of ransom[6].

---

[1] Phair, N. *Cybercrime in Australia: 20 years of in-action* (2021)

[2] MarcusToday. *The ASX 100 Made Simple*. [https://marcustoday.com.au/2020/02/the-asx-100-made-simple/]

[3] ASX. *Capitalisation Indices*. [https://www2.asx.com.au/investors/learn-about-our-investment-solutions/indices/types/capitalisation-indices]

[4] Phair, N. N 1.

[5] ABC NEWS. [https://www.abc.net.au/news/2020-05-15/bluescope-steel-cyber-attack-shut-down-kembla-ransomware/12251316]

[6] https://www.webberinsurance.com.au/data-breaches-list

With over 300,000 cyber attacks in Australia in 2021[7], company directors need to factor this growing crime trend into their broader risk management policies and processes.

The Australian Cyber Security Centre has provided an advisory for all Australian organisations to urgently adopt an enhanced cyber security posture.[8]

> Following the attack on Ukraine, there is a heightened cyber threat environment globally, and the risk of cyber attacks on Australian networks, either directly or inadvertently, has increased.[9]

The Role of a Company Director

Company directors are responsible for oversight of the activities of the organisation. Specifically they need to comply with legal obligations under the *Corporations Act 2001*.

> As a director, you must be fully up-to-date on what your company is doing, including its financial position, question managers and staff about how the business is going and take an active part in directors' meetings.[10]

Company directors need to focus on governance, strategy and risk of the organisation. Cyber security falls into all three of these categories. Cyber security governance refers to the part of enterprise governance which addresses the organisations dependence on the online environment in the presence of adversaries.[11] Cyber security is not a technical issue, it is a whole of enterprise issue. The cyber security governance program therefore needs to dovetail into the organisations existing governance regime and provide assurance that cyber security strategies are aligned with and support business objectives, are consistent with applicable legal requirements, and provide assignment of responsibility.[12]

Cyber security strategy is the high-level plan of how an enterprise will secure its information assets. Similarly to governance, it needs to be part of the organisations overarching strategy. A good cyber security strategy should focus on preventing cyber attacks whilst also preparing an organisation to respond to any attack which may occur. The development of a cyber security strategy will depend on many factors including the industry the organisation operates in and the cyber security maturity of the organisation.

Cyber security risk management is the key component of a company directors knowledge and activity when creating a resilient organisation and protecting its information assets. Cyber risk management is the process of identifying, analysing, evaluating and addressing the online threats facing an organisation. Similarly to governance and strategy, cyber risk management needs to dovetail into the whole-of-organisation risk management framework. It is this process where a company director needs specific knowledge and understanding of the cyber threat context which the organisation operates in.

---

[7] ibid

[8] ASD. *Australian organisations should urgently adopt an enhanced cybersecurity posture*. [https://www.cyber.gov.au/sites/default/files/2022-03/2022-02%20Australian%20organisations%20encouraged%20to%20urgently%20adopt%20an%20enhanced%20cyber%20security%20posture_1.pdf]

[9] ibid

[10] ASIC. *Small business company directors*. [https://asic.gov.au/for-business/small-business/starting-a-company/small-business-company-directors/]

[11] MITRE. *Cyber Security Governance*. [https://www.mitre.org/sites/default/files/pdf/10_3710.pdf]

[12] NIST. *Cybersecurity Framework*. [https://www.nist.gov/cyberframework]

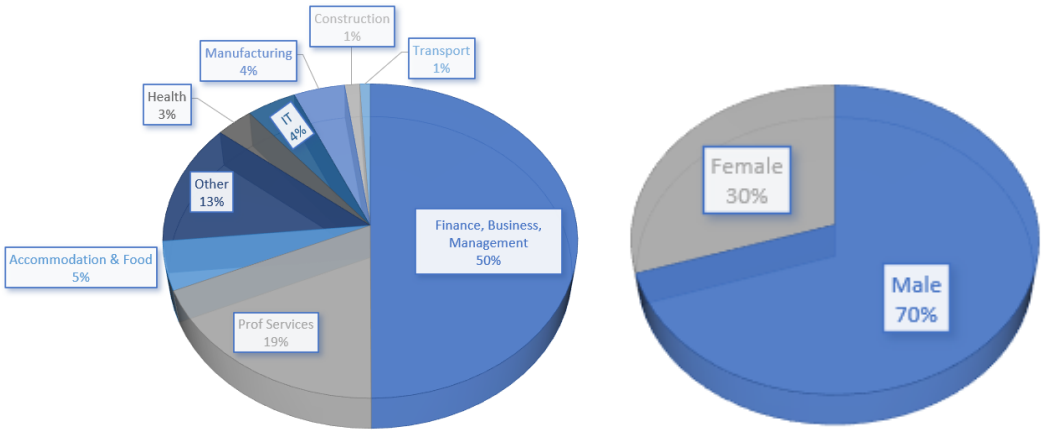

Figure 1. Statistics around ASX 100 Company Directors' Background, Cyber and Tech Skills, and Gender

Analysis

There are 798 director positions (including managing directors and non-executive directors) across all ASX 100 companies. Of these 707 are non-executive director positions. It is this cohort who will be the subject of this analysis. Some of these directors sit on more than one ASX 100 board, leaving only 613 people providing oversight of companies which account for this large majority of Australia's share market capitalisation.

Of the non-executive directors responsible for the overall governance and strategic direction of ASX 100 companies less than 1% have cyber experience and 16% of directors have general technology experience. However, 80% of boards have neither cyber nor technology background, as shown in Figure 1.b. We categorised the skills set and background of ASX 100 directors to nine major categories as can be seen in Figure 1.a. Comparing the skills set and background of directors, we observed that about half of directors have finance, business and management skills and background. However, only 4% of directors have information technology (IT) background. Some other statistics around ASX 100 non-exclusive directors are summarised as follows.

- 0.8% have cyber experience
- 16% have technology experience
- 9% hold an MBA
- 7% hold a law degree
- 0.05% hold an engineering degree
- 55% have a career history in Finance and Management
- On average they sit on four boards
- 30% are female
- The average age (where age could be determined) is 62 years old

In April 2017, the ASX 100 Cyber Health Check Report was released, being a recommendation of the 2016 Australian Cyber Security Strategy. The Health Check was the first attempt to gauge how the boards of Australia's largest publicly listed companies view and manage their exposure to the online environment. The Health Check found 80% of boards expected an increase in cyber risk over the next year or so; 34% of boards had a clearly defined risk appetite for cyber; whilst 43% of boards were confident their company was properly secured against a cyber attack. Interestingly, 93% of

non-executive directors stated their board colleagues take cyber risk very seriously.[13] Meaning there is plenty of words of intent, but no action to back this up.

Figure 2. Comparing the distributions of directors with technology and cyber knowledge among ASX 100 companies

> Just 7% of directors say they clearly understand the cyber security of the broader ecosystem in which the company operates and almost two-thirds (63%) say their understanding of the biggest IT security exposures is limited or non-existent. While only 8% of directors say they have a clear understanding of the key controls in the company's cyber resilience framework.[14]

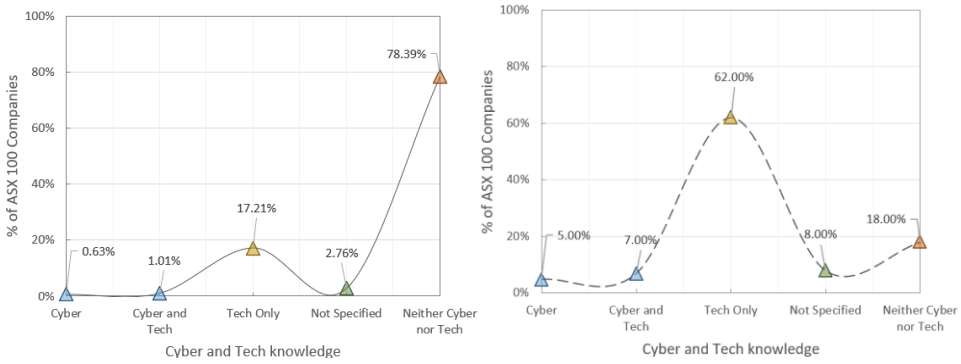

Figure 2.a. represents the distribution of five skills categories among the director board of ASX 100 companies. Figure 2.b. shows the percentage of ASX 100 companies that at least have one director with cyber and technology knowledge. As it can be seen in Figure 2.a, only 0.63% of directors have cyber skills. However, those directors have been distributed into five ASX 100 companies that means only 5% of ASX 100 companies have at least one director with cyber knowledge. Regardless of cyber knowledge, this rate is also very low for technology knowledge of ASX 100 companies, and only 16% of directors have technology only knowledge. Those directors have been distributed into 62% of ASX 100 companies. This rate shows that only 62 companies out of 100 companies in ASX 100 have at least one director with technology knowledge and background. A majority of directors have knowledge in neither technology nor cyber (around 78%). Interestingly, only 18% of ASX 100 companies have neither cyber- nor technology-based directors that can be a target for cyber-attacks and data breaches. However, around 2% of companies remained unspecified based on our analysis.

Cyber security is all about an organisations information assets. Not only do the figures above demonstrate a large proportion of ASX 100 company directors have limited or a non-existent understanding of cyber security, but these figures are exacerbated by 38% of boards not having set a cyber risk appetite, and 20% of boards not having a director with a good understanding of cyber security and no plans to add this expertise.[15]

This report is now five years old and has not been replicated. It would be hard to imagine any improvement. Diversity of background is a key component for a successful board, yet over half of all current AZX 100 non-executive directors having a background in finance and management. Whilst diversity is recognised as a critical component of good governance, most of the effort is targeted towards getting more women on boards (or perhaps more of the same women on boards), rather than also exploring professional background and

---

[13] ASX. *ASX 100 Cyber Health Check Report*. [https://www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf]

[14] Ibid

[15] Ibid

looking for broader career experience. Diversity is recognised as a critical component of good governance with constructive board discussions and decisions requiring a breadth of perspective that by definition is supported by diverse composition.[16]

Many boards receive a yearly cyber presentation by the Chief Information Security Officer, or similar, yet this is a meaningless attribute. If company directors do not know what questions to ask, and more importantly, what answers to expect, then they are merely playing lip service to one of the most important risk components of their organisation. Additionally, the cyber risk environment is so dynamic, it should be a standing agenda item for any Audit & Risk Committee.

For company directors more broadly, in December 2021 cybercrime and data security kept 41% of company directors 'awake at night', specifically the growing cyber risk and changing environment (having grown from 15% in early 2020). Only 8% of company directors strongly agreed that their board has sufficient oversight of cyber security threats.[17]

Those in the 60 – 64 age group account for 5.6% of the population[18], yet it is this narrow group who (on average) are governing Australia's largest 100 listed organisations. This cohort has also not grown up with digital technologies, however limited studies have shown they are adopting to the use of the internet and mobile smart devices.

Overboarding will make it more difficult for company directors to learn new skills, adopt best practises and keep on top of the ever-changing cyber environment. There is no accepted time commitment for an ASX100 board role, needless to say, preparing for meetings, keeping on top of key issues and travel all take time. The cut off for the ASX 100 is a market capitalisation of ~$1.7 billion, organisations of this size and bigger require a lot of time and effort to govern.[19] Yet, with ASX 100 directors holding an average of four company directorships it has to be wondered how they can keep on top of business as usual issues, let alone keeping abreast of new issues such as cyber security.

The Legal and Regulatory Environment

The concept of company director responsibility in cyber security was acknowledged in the 2020 Cyber Security Strategy.

> The Australian Government will also work with businesses to consider legislative changes that set a minimum cyber security baseline across the economy. This consultation will consider multiple reform options, including duties for company directors and other business entities.[20]

Section 180 of the *Corporations Act 2001*, directors have an obligation under civil law to exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise if they:

- were a director or officer of a corporation in the corporation's circumstances; and

---

[16] Harkovirto, M. et al. *The importance of diversity on boards of directors' effectiveness and its impact on innovativeness in the bioeconomy*. [https://www.nature.com/articles/s41599-020-00605-9]

[17] AICD. *Director Sentiment Index Survey 2nd Half 2021*. [https://aicd.companydirectors.com.au/-/media/cd2/resources/advocacy/research/director-sentiment/2021/roymorgan-aicd-appendixreport_2021-2.ashx]

[18] .idCommunity. *Australia Five year age groups*. [https://profile.id.com.au/australia/five-year-age-groups]

[19] ASX100 list. *ASX Top 100 Companies*. [https://www.asx100list.com/]

[20] Australian Government. *Australia's Cyber Security Strategy 2020*. [https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf]

- occupied the office held by, and had the same responsibilities within the corporation as, the director or officer.

Accordingly, if care and diligence is not exercised in relation to a company's cyber security posture and protection of key assets (which includes data), they could be found in breach of the Act.[21]

The Australian Securities and Investment Commission have realised the impact a cyber attack could have on the broader financial system and the need to ensure trust and confidence.

> Depending on the severity, a failure to meet some of these obligations could result in fines, penalties, enforceable undertakings, licensing conditions, or a licence suspension or cancellation. If you are a director or an officer of a company, it may result in being disqualified from your role.[22]

Similarly, the Australian Prudential Regulation Authority has acknowledged the importance of cyber security for their regulated entities stating "stakeholders including Boards of directors (Boards), senior management, shareholders, customers and regulators have heightened expectations for the effective safeguarding of information assets underpinned by an organisational culture that promotes information security."[23]

The 'Centro Case' of 2011, where the Court highlighted the responsibility of all directors to pay appropriate attention to the business of the company, and to give any advice received due consideration and exercise his or her own judgment in the light thereof, is important jurisprudence for all company directors that when discussing information security they should dig deeper to become more informed in their decision making.

Similarly, with continuous disclosure rules and the recent introductions of some safeguards for entities and its officers against civil penalty proceedings where there is a knowing failure to comply or recklessness or negligence.[24] A cyber attack, which reduces or degrades the ability of an organisation to function could have share market price implications and as such would need to be disclosed.

Interestingly, even though some ASX 100 companies have a non-executive director with nominated technology skills, that does not necessarily parlay into cyber security knowledge. Indeed it could be argued they might think they understand cyber security - when in fact they probably don't, as opposed to those directors with no background in either technology or cyber security who would readily admit no knowledge.

Skills Matrix

The best way to address the deficiencies of the ASX 100 with regard to cyber security knowledge and practise is by recognising it in a boards skill matrix. ASX Listing Rule 4.10.3 recommends an

---

[21] AICD. *The board's role in cyber security assurance*. [https://aicd.companydirectors.com.au/membership/membership-update/the-board-role-in-cyber-security-assurance]

[22] ASIC. *Cyber resilience: Health check*. [https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf]

[23] APRA. *Prudential Practise Guide CPG 234 Information Security*. [https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf]

[24] Clayton Utz. *Significant reforms to the Australian continuous disclosure regime are now law: A guide for listed entities and their officers*. [https://www.claytonutz.com/knowledge/2021/august/significant-reforms-to-the-australian-continuous-disclosure-regime-are-now-law-a-guide-for-listed-entities-and-their-officers]

organisation disclose on its website or in its annual report "a board skills matrix setting out the mix of skills that the board currently has or is looking to achieve in its membership"[25]

> For listed entities, it is good governance to disclose the skills matrix or a summary of it. Disclosure will also meet the recommendation in the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* for companies to have and disclose a board skills matrix that sets out the mix of skills and diversity that the board has in place or is looking to put in place.[26]

Interestingly, in 2020, 38% of all boards said they were introducing specialist technology and/or innovation roles to the board skills matrix.[27] Yet, this thinking is yet to parlay into action with respect to the ASX 100.

The adoption of technology by organisations will continue to grow at a rapid pace. In concert with this, is the dynamic role cyber security needs to play to protect the organisation, the data it creates and the people who access it. Since the 'tone starts at the top', having appropriately skilled company directors is a fundamental requirement.

Nigel Phair

Hooman Alavizadeh

---

[25] ASX. *ASX Listing Rules Guidance Note 9*. [https://www.asx.com.au/documents/rules/gn09_disclosure_corporate_governance_practices.pdf]

[26] Governance Institute of Australia. *Good Governance Guide. Creating and disclosing a board skills matrix* [https://www.asx.com.au/documents/asx-compliance/creating-disclosing-board-skills-matrix.pdf]

[27] AICD. *Director Sentiment Index: Research Findings First Half 2020*. [https://aicd.companydirectors.com.au/-/media/cd2/resources/advocacy/research/director-sentiment/final-full-results-pack-pdf.ashx]