A RESPONSE TO 'STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES'

Submission by Julie Garland McLellan, Greg Porter, Angus M Robinson, and Peter Slade

1ST September 2021

Strengthening Australia’s Cyber Security Regulations and Incentives

Context for this Submission

This submission has been prepared by several directors associated with a networking group (Gordon Directors’ Group) interested in professional development and with an interest or background in ICT development, particularly cyber security issues.

The group has reviewed the discussion paper ‘Strengthening Australia’s cyber security regulations and incentives - An initiative of Australia’s Cyber Security Strategy 2020’ and has decided on the section of the document which is thought to be of most relevance to directors i.e., the first nominated action, ‘**set clear minimum expectations’**, and to respond to all of the first 10 questions set out in the document.

Executive Summary

In considering the proposal to set clear minimum expectations for dealing with cyber security issues as it applies for directors of companies and organisations, it needs to be recognised that the director community is broad and diverse and extends well beyond the scope of public and SME companies. Directors are now facing a substantial digital transformation of the operations of their organisations where their principal assets of data and information are increasingly subject to an ever widening ‘attack surface’ and vulnerabilities relating to IT system integration. Cyber security needs to be seen as a business issue, not just an IT issue, and directors need to have access to expert information to enable them to fulfil their responsibilities and duties. In essence all data or more importantly information needs to be covered by the existing Privacy Act, 1988 (as amended). This would be an unequivocal and broadly reaching scope. If private information is collected and stored, then the Privacy Act should cover it regardless of technology, sector, or type of data. There is no doubt that directors should have more responsibility for business disruption and losses because of cyber breaches. Any realistic approach to address cyber security concerns must be mandatory as self-governance has been shown time and time again not to work, and to do nothing is negligent. However, any legislation that might be considered would need to be a structured approach with multi-levels to cater for small, medium, and large enterprises.

Overview

The current environment has several characteristics that should be considered in any framework impacting the governance of cyber security.

The principal ones are:

1. the ‘attack surface’,
2. increasing integration and consolidation within organisations, technical complexity,

3. the growth in connectivity between traditional IT (business systems) and industrial technology (OT/IoT), and
4. the agility of attackers to find new methods of penetrating the defences of organisations and to reinvent themselves constantly.

Let’s consider these in turn.

1. **The attack surface is the extent to which any attacker has access for their use.**
    a. While there have been some large attacks in the past, there has been a significant increase in large attacks in the past three years.

    b. Consider the following:

    - Maersk (disruption – global network, applications and data destroyed, 2000 servers rebuilt, network rebuilt, 49,000 PCs rebuilt, cost US$400M part of NotPetya attack on Ukraine).
    - Merck (details never made public but cost US$870M although we do know part of their production facilities impacted, currently suing insurance company for US$1.3B; Insurance company claiming ‘Act of War’ exclusion as part of Notpetya attack on Ukraine).
    - JBS (Brazilian meat processing conglomerate hit by ransomware halting production in Canada, USA, and Australia for one week plus; believed to have paid US$11M ransom).
    - Hydro (Nordic aluminium company had to rebuild 22,000 PCs globally, production capability impacted also; cost of US100M?).
    - Stadler (German train manufacturer business disrupted).
    - Colonial Pipeline (infrastructure supplying 45% of petroleum products of the East Coast of the USA; disruption for over a week, ransom of US$5M paid, part of which was recovered by the FBI).
    - Toll Group (Two global outages within a couple of months, two months to recover, extensive review of security implementation of a 12-month program to increase security).

    c. Why are these large global companies failing? The common characteristic of these companies is the size of the attack surface. Were they all a ‘house of cards’ waiting to fall? Why did many of them have to rebuild their infrastructure, systems, and processes from scratch? Clearly, something fundamental in their risk analysis when the failure is so large.

2. Increasing integration and consolidation, technical complexity

a. The pressure to integrate and consolidate in the IT world is enormous, both by IT itself and from suppliers who see it as simple and desirable!! However, this complexity increases complexity, and the cyber-attack surface becomes larger leading to greater business disruption. This is especially true when integrated with production/industrial processes and poorly defended IoT devices. Once inside the companies referred to above, the attackers had access to almost the whole company. One assumes there was little segmentation at the company, central business systems, and at the networking levels. Implementation of segmentation at these levels would have reduced the attack surface and reduced the business impact.

b. Although these examples are from big and global business, there are other examples where small companies such as air conditioning firms lose all their systems and data and must recreate their systems and data from 'ground zero', requiring many resources and disrupting their businesses

3. Traditional IT and OT/IoT

a. There is a whole industry of security products for traditional IT and increasing associated costs depending on what level of security you purchase and commit to. These have varying degrees of effectiveness but still have weaknesses. There is also a lack of expertise required to use those tools.

b. On the other hand, OT/IoT and industrial technologies have very poor security, having been designed and built without the same security intent as traditional IT. They often use very old operating systems or bespoke ones because of the nature of the devices and processes. There is very little security expertise and tools in this important area.

4. Agility of attackers

a. Malicious attackers are constantly looking for new methods of intrusion without detection. More recently they are using other parties to attack organisations through either third-party products (e.g., SolarWinds, Microsoft) or through managed service providers (MSPs).

Other Issues

- Too many people have access to data they don't require to do their job.
- Too much seduction by technology and suppliers selling solutions to problems that are not the most pressing.
- Niche development of software adding to complexity.
- Architecture Design?
- Faulty software and architecture that is opaque and poorly communicated.
- CISOs being held responsible for breaches when they have limited control over vulnerabilities and breaches.
- Non elastic pricing from suppliers to enable multiple instances of implementation reducing the attack surface.
- Future technology – quantum computing.

Summary

- Security is everyone's business.
- All infrastructure, systems and processes contain faults and vulnerabilities, so organisations need to act as though they have already been breached.
- The Board is accountable for security. Everyone else in an organisation is responsible. ASIC makes this clear (ASIC Report – 429).
- Reduce Attack surfaces – should reduce cyber insurance cost which can then be used to increase security programs.
- Organisational segmentation to reduce attack surface
- Separation of IT and OT/IoT.
- Ultimate security is to have capability to rebuild the business from 'ground zero', especially required for SMEs.
- Ultimate security is to perform a comprehensive and all-inclusive vulnerability scan/check. Every risk is analysed for probability, impact, and mitigation cost. Decisions regarding vulnerability mitigation – ignore, accept, or pass on, need to be fully documented.

It is against these concerns and observations, that our submission has been written and should be read.

Responses to Questions Posed in the 'Call for Views' Document

1. What are the factors preventing the adoption of cyber security best practice in Australia?

What is cyber security best practices?

- How to establish across a diverse environment when the speed of change is large.
    - Cyber criminals are learning to quickly adapt to the fast-changing environment and using more diverse range of tools to exploit organisations.

What are the factors preventing effective adoption?

- Cyber security is a business issue, not just an IT issue; in many cases it is seen as an IT issue and this on its own creates openings for intrusions.
- Increasingly dynamic and complex cyber environment; the level of expertise to understand this is not present in all but a few organisations.
- The increasing number and type of appliances and services.
- Increasing complexity of technology layers.
- Integration and consolidation are building larger attack surfaces.
- High maintenance of increasing complexity of infrastructure and systems
- Lack of expertise.
    - Poor certification/education of IT/Cyber professionals i.e., anyone can be called an expert.
- Limited visibility of Third-Party security.
    - Increasing targeting of MSPs by attackers
    - Organisations are buying a service not a technology provider.
- Lack of willingness to accept that threats exist; it will never happen to me!
- Lack of willingness to accept that my business is vulnerable; again, it will never happen to me!
- Lack of security protocols in industrial environments and linkages to business systems; industrial environments have very poor security and the interface between business and industrial systems needs to have the best security or complete separation if disruption to operations is to be minimised.
- SMEs access to cyber security advice is limited due to
    - Knowing who to call,
    - Expense of security (even through a third party), and
    - Lack of prioritisation.

2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

Cyber security is not viewed as an in-scope requirement for government intervention. The complexities are so great that any attempt to intervene would just create a greater confusion. It would be difficult to compare supplier products as each product has its own idiosyncrasies and points of difference. It is difficult to enforce suppliers to educate their customers in the functionality of the product as each consumer will have disparate requirements.

This perceived conundrum is something for market forces to manage. Either the consumer becomes better equipped and more knowledgeable regarding requirements versus offering or they rely on an external body. This is where a Special Interest Groups (SIG) or professional bodies such as the ACS (Australian Computer Society), AUScert or AISA (Australian Information Security Association) or lobby groups such as AIIA (Australian Information Industry Association) need to petition technology providers to elucidate their offerings and supply equipment that has clearly defined capabilities. There are already requirements under the Australian Consumer Law that a product sold should be fit for purpose.

In the end consumers need to be more sophisticated in their selection of technology, for example, farmers do not purchase tractors that are not fit for purpose. They will research and seek guidance on farming equipment and use their experience to make the correct decision. So too, must consumers of IT equipment.

3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?

Where do people obtain advice and guidance for Cyber Security?

Privacy, Data Protection and Cyber Security considerations and regulations overlap and vary by industry and State (e.g., Health Records and Information Privacy Act 2002 (NSW) (HRIPA)), not to mention the Crimes Act.

Many standards exist across technology and the implementation of systems and processes (e.g., ISO 270001), while many governance organisations provide guidance in many areas of security (e.g., APRA, ASIC, Governance Institute).

For example, APRA Prudential Standards and Prudential Practice Guides for Cloud Computing include the following.

1. CPS 231 Outsourcing;
2. SPS 231 Outsourcing;
3. HPS231 Outsourcing;
4. PPG 231 Outsourcing;
5. SPG 231 Outsourcing;
6. CPS 232 Business Continuity Management;

7. SPS 232 Business Continuity Management;
8. CPG 233 Pandemic Planning;
9. (draft) CPS 234 Information Security;
10. CPG 234 Management of Security Risk in Information and Information Technology; and
11. CPG 235 Managing Data Risk.

NIST (National Institute of Standards and Technology) is a US based organisation that many countries and organisation look to for the provision of standards, particularly with respect to security, and at an organisational level adopt most of those standards.

So, what constitutes Australia's current regulatory framework? Despite many years in the technology and information processing business, it is difficult to find a single (or several, for that matter) source(s) of truth that is digestible and coherent to security technicians and other people responsible for security. There are even fewer sources suitable for company directors who may have limited IT skills.

A recent scan of the ASIC and ACSC websites illustrate the growth in guidance and advice. APRA clearly have a regulatory role in the areas under its control. It seems a 3-dimenensional matrix would illustrate how laws, regulations, standards, and advice are applicable in each industry and jurisdiction!!

Additionally, there are many voices across government who speak about cyber security e.g., ASIC, APRA, ACSC, ASD, Home Affairs, Foreign Affairs (cyber ambassador?) etc.

People responsible for security have enough trouble keeping up with the technical aspects of the threats and associated actors, let alone the regulations applicable to their situation.

4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

Who are company directors?

In Australia there is no requirement to receive a level of education, or achieve a level of sophistication, before starting a company. Any entrepreneur who starts a company as founder is likely to be the director of that company. Although people running businesses should understand their obligations, these need to be kept in a way that is easy to access and understand, to ensure that the entire commercial system can work.

These sole directors of small businesses are often totally focused on the product or service, and reluctant to spend any time on compliance or governance arrangements. As they tend to use only their own resources, they do not see the point in protecting other people's capital. However, as Storm Capital [1] showed, these companies can have a major impact through the damage they can cause to clients, and or investors.

[1] Storm Capital was pushed into administration by the CBA in 2009 and eventually became a $1 billion corporate failure that lost many investors' life savings.

As a company grows, it is normal for sole directorship to transition to a rudimentary board. However, there is still no requirement for formal education, or any governance expertise in the directors of large public organisations.

Privately-owned 'for profit' businesses

In the private sector, it is quite common for the founder to be joined on the board by family members and or trusted retainers, such as lawyers, and accountants. Whilst the lawyers and accountants may bring specific skills and insights to the governance duties, they are frequently conflicted by the value of their consulting relationship with their client, which, in their minds, often exceeds, and frequently nullifies the value of their duty to the company itself, which should be the overriding concern of a company director.

A good example of this would be the board of Napoleon Perdis. Although this company had grown to become a globally recognised brand name within its industry, the board remained heavily influenced by the founder and his family. The almost inevitable demise of the organisation was to a large extent due to the inability of this small group of untrained company directors to comprehend the needs of a company of the size that theirs had grown to become.

Not for profit businesses

In the 'not for profit' sector, it is very common to find directors who have no corporate or business experience whatsoever. Yet these directors can find themselves volunteering on the boards of sizable organisations in the aged care, disability, registered clubs, superannuation, and other sectors such as community-based organisations.

When these organisations fail the impact is often felt by our most vulnerable citizens. However, this fact does not lead to an investment (or even an awareness of the need to invest) in developing the skills of the directors. Most directors in the sector remain unaware of the requirements to comply with the ACNC Governance Standards and when confronted with the need to meet basic governance requirements express disbelief that this could apply to them. Any funds the organisation generates or receives are preferentially targeted towards the cause, and very little is spent of building the capacity of the organisation or of its board.

Governance aware directors

Only the elite directors are aware of, and invest in improving, their governance capabilities.

When talking to governance institutions such as the Australian Institute of Company Directors (AICD) or the Governance Institute of Australia, it is common for these organizations to talk about their members, and the needs and abilities of their members. However, it is very important to remember that the membership of these organisations is a minute percentage of the number of company directors in Australia.

Most company directors do not think of themselves as governance professionals, or indeed as company directors. They think of themselves as ‘businesspeople’, or in the ‘not for profit’ sector as volunteers serving a cause.

It is of paramount importance that in creating a regime to encourage greater responsibility among company directors for issues such as cyber security, the legislators and regulators are cognisant of the low level of technology and governance education that most directors have. Members of governance organisations might span the small to large business spectrum, but they are still very much an elite.

It is worth noting that in its most recent journal (*Company Director, volume 37, issue 08*), the AICD has included several most helpful and informative articles dealing with cyber security issues specifically i.e.,

- ‘Cybersecurity governance’ by Louise Petschler, page 15.
- ‘Chinks in the Armour’ by Professor Pamela Hanrahan, pp. 26-27.
- ‘Better Watch Out’ by ASIC Commissioner Cathie Amour, page 28.
- ‘Staying Cyber Safe’ by Courtney Brown, pp. 42-43.
- ‘Held to Ransom’ by Damien Manuel, Chair of AISA and Centre for Cyber Security Research and Innovation, page 44.

The ACID has also published in 2018 for the benefit of members *‘The New Governance of Data and Privacy: Moving beyond compliance to performance’* authored by Malcolm Crompton and Michael Trovato.

Hard to reach directors

It is also important to recognise the difficulty of reaching company directors with information about any changes in the requirements placed upon them. Very few directors will read the ASIC website, even fewer will visit the websites of the Governance Institute or the AICD.

Some organisations will be able to be reached through service providers, such as their law firms or their accounting firms. However, reaching every lawyer and every accountant who serves a company board is an equally difficult and onerous task.

Whilst it is common within government circles to conflate ‘start-ups’ with high tech, high growth, family businesses and small businesses, each of these is subtly and fundamentally different from the others.

Within the ‘hi-tech’ sector company directors tend to be highly sophisticated and very aware of E commerce, internet connectivity, and the security risks that these might entail. Within other start-ups, such as service companies and product-based companies, directors are very often unaware of cyber security risks.

Even in relatively large businesses directors are not aware of how to govern and manage these risks. Within some long-standing small businesses, many directors have experienced decades of business without the need for cyber awareness. These directors lack basic cyber security and information technology skill and will frequently declare that they do not need them.

Whilst this blinkered approach to cyber security is frustrating and annoying for regulators and any customers or suppliers or employees who are inconvenienced when the inevitable happens, and a cyber-attack strikes a soft target, it is important that when creating new regulation and legislation we place the burdens of compliance on the people who are better able to carry them and that we do not underestimate the task of reaching and educating the whole director community.

5. What is the best approach to strengthening corporate governance of cyber security risk?

Any realistic approach must be mandatory as self-governance has been shown time and time again not to work, and to do nothing is negligent.

Take any company, the one-man plumbing service, the local bakery or a large corporate. Do directors take cyber security, occupational, health and safety or workplace bullying seriously? To some extent, the answer is yes, although the SME will probably give it a cursory thought.

What is the one thing in common that really attracts attention of organisations/directors? Answer – the Australian Tax Office (ATO). Everyone in general prepares a return and pays tax. It is a legal obligation that if an individual is not capable of undertaking the work, then accounting expertise is sought and utilised. Every company that is compliant will have their own accountant.

So why is cyber security different? Because it is not regulated and mandated. Make all directors accountable for cyber security consequences and the attitude will surely change. Directors will seek advice as necessary just as with taxation.

However there needs to be a one stop shop for cyber security guidance and frameworks. The ACSC is an attempt to do this however there are too many other departments where information can be found and needs to be searched. They are listed as follows, to name a few e.g.,

1. ASIO
2. Federal police
3. Australian Signals Directorate (ASD)
4. Defence Intelligence Organisation (DIO)
5. Department of Home Affairs

Where does a director turn for factual and documented information on the following issues?

1. Past attacks and lessons learned.
2. Best practice for passwords or how to avoid using passwords.

3. Credential Stuffing.
4. CVEs - Common Vulnerabilities and Exposures.

The use of Google is fraught with pitfalls and inaccuracies hence should not be the first option to seek accurate information. A centralised Australian website/organisation must surely be the repository for control of accurate and informative cyber security awareness.

So, if cyber security regulations are mandated and a central repository is developed where do those directors in need go? As is the situation with income tax, directors could go to the 'one-stop' shop, however there will always that other step needed to engage an external resource, invariably a consultant.

However, unlike a surgeon or auditor anyone can just hang out a shingle and call themselves a cyber security or IT consultant regardless of education, experience, and skillset. This is not a new issue and therefore, along with corporate governance of cyber security risk, it is imperative to develop certification for those calling themselves expert practitioners of cyber security.

Peak bodies such as AusCERT and AISA could be certified/licensed by government and then in turn these bodies become certifiers of consultants. The main group to be targeted would be Managed Service Providers (MSPs) although anyone providing advice would need a level of certification.

Another concern that needs to be addressed is how is cyber security to be legislated. Accounting principles and standards are understood. They can be incorporated in law and policed. How is this achieved with cyber security?

With accounting, organisations need to observe the framework established with compliance being achieved by the organisation itself. With cyber security there is no framework, nor will a static framework be established. The face of cyber security is always changing.

As much as an organisation wishes to comply, it's the external third party, a malicious actor, who is always going to push the limits. So apart from compliance an enterprise will need to battle external forces.

Any legislation would need to consider a structured approach with multi-levels to cater for small, medium, and large enterprises.

According to ASIC, 'cyber resilience is the ability to prepare for, respond to and recover from a cyber-attack. Resilience is more than just preventing or responding to an attack—it also considers the ability to adapt and recover from such an event.'

Therefore, it is this cyber resilience-based approach that is imperative to allow organisations to not only defend against attack however more importantly to recover, learn and evolve from attacks – utilising both personal and third-party experiences.

The types of risks encountered by organisations and their tactics to ensure cyber resilience, will depend on their nature, scale, and complexity. The approach by most will be risk-based. After a thorough analysis of their risk a complex cost benefit analysis will be performed. Not until this analysis is complete will a picture of the risk profile be clarified.

Risk-based and proportionate cyber-resilience management practices need to be developed and continually reviewed to combat the ever increasing and changing cyber-threats. Unknown unknows being the most challenging risk. The status quo or static thinking must be challenged. The concept of 'failure of imagination' must be duly considered and assimilated. If every possible situation has been considered, then something has been omitted.

ASIC encourages enterprises to consider using the NIST Cyber Security Framework to analyse their cyber security risks. The NIST Cybersecurity Framework is a voluntary, technology-neutral, cyber security risk management tool for organisations. Utilising common language to tackle cyber security risk in a cost-effective way based on business requirements, risk tolerances, and resources.

6. What cyber security support, if any, should be provided to directors of small and medium companies?

The current issue is how and where do directors find information.

As discussed in response 5, a central source of truth needs to be established to co-ordinate the various and perhaps disparate government departments that currently exist. This does not necessarily mean the amalgamation or closure of departments rather a single co-ordinated approach that can reach out to subject matter experts as required.

This single body would develop, maintain, and enforce mandated requirements. Just as the ATO is multifaceted with income tax, GST and FBT so would this peak body have a reach into other Departments as necessitated.

So, the support for small and medium enterprises would be sourced firstly from this central body and its government resources. Though if the requirement was more complex than a series of phone calls then the expectation would be the engagement of an MSP or certified consultant.

This engagement would come at a cost however that should be seen as the cost of doing business just as already discussed is the engagement of an accountant.

7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

The undoubted answer to the first question is a definite YES.

How to do it is a more complicated question.

The scope could involve a large spectrum of organisational and business types, from sole traders, SMEs, NFPs, NGOs, partnerships, large businesses. Some might involve laws and regulations from other countries you may have dealings with. So, US companies may have to deal with the Sarbane Oxley Act, business dealings with European countries will need to examine their potential compliance with GDPR.

The **first issue** then, is to identify who requires education. Is everyone registered somewhere so they can be identified. In the case of directors this might be resolved somewhat when all directors of Australian companies need to be individually registered. Now, it is thought less than 1% of eligible directors are members of the AICD, for instance. Many volunteer organisations are manned by people who ‘help’ operationally but should be seen as responsible directors/senior leaders as they sometimes handle much private information.

The **second issue** is what is the scope of the education. Education now is very sporadic and piece meal, and often delivered by suppliers whose objective is to sell their products in a small part of an organisations cyber defence strategy. The subjects and content will be different for different classes of businesses. Perhaps a central source like ACSC or ASIC could matrix the various requirements across different classes of organisation.

The **third issue** is ‘who to deliver the training’? Well, it could be RTOs given an established curriculum from ACSC or ASIC, or other experienced cyber security organisations and perhaps accredited to deliver different aspects of cyber security and data breach education. Perhaps the Commissioner for Small Business could develop and oversee online courses for individual traders and small business free of charge.

The hardest question of course is how to identify those needing education and how to persuade them that it is in their best interest to do it, when they are probably ‘struggling with crocodiles’ daily.

While many organisations outsource their technology support operations, they think they can outsource the responsibility. Unfortunately, that is not possible as in the event of a disruption, it doesn’t matter where a third-party provider is involved in that breach, the end impact will be the operating organisation itself. You can outsource the operation, but you cannot outsource the responsibility and accountability for the potential impact. Education is required for all business owners, directors and of course, ultimately the consumer.

8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

The six areas we would like to address are as follows:

1. Business Systems
2. Industrial/operational technologies
3. Social Media
4. Consumer/corporate mobile and home devices

5. International Usage of Data
6. Culture

1. Business Systems

a. The guiding principle should be that any person whether they be staff, contractor, supplier, or customer, should only have access to specific personal information to enable them to do the task at hand, and for only the period that information is required.

b. For larger businesses, the systems available largely cater for this, including an audit trail of who had access, what time and duration, what was modified. However, it is frequently the case that people don't have their access privileges changed when they move to different roles, or their access closed when they leave the company.

c. A cyber security code would assist organisations to design their system requirements, implementation, and processes to ensure compliance with the Privacy Act, 1988 (as amended) – the Privacy Act.

d. In practice, this should include a person responsible for privacy being included in the early stages of design and throughout the life cycle of introduction, and after the implementation monitoring the audit system

e. Based on operational experience, project teams need much more education in the Privacy Act, and a Cyber Security Code would be a useful tool to reinforce the principles and privacy requirements

f. For smaller businesses, the situation is not as clear as for large business. The systems are smaller, cover fewer features, and in order to be affordable, they may not have some of the controls of the larger systems. People in small businesses often have multiple functions and therefore have greater exposure to more information about individuals.

2. Industrial/operational technologies

a. This is an area of great concern as has been previously outlined in another question response. For organisations who require work orders to build/process to a customer's requirements, the industrial/process parts of an organisation require certain information which will probably include a customer's address and other details. Security in these areas and indeed the knowledge of the Privacy Act requirements will not be as strong as in the business systems areas of an organisation.

b. The Privacy Act will still apply, and as will the need to educate staff and others (particularly MSPs) is required. A cyber security code would assist here.

c. MSPs may require certification before given access to organisational systems (remembering the breach that occurred at Target in the USA came through an air conditioning supplier!). A Cyber Security Code may be of use here.

3. Social Media

a. Well, where do we start! The social phenomenon of the last 20 years is one that has shaped and will continue to shape our lives for years to come.

b. The major issues with social media are:

i. The sharing of personal information by people who have no understanding the implications of sharing personal information (such as telling everyone where you are, where and when you are going on holidays etc.).

ii. The fact that the individual or organisation is the product that Facebook, Google etc., sell (i.e., personal information and habits).

iii. The owners of the products such as Facebook and Google, personally don't like privacy constraints.

iv. The users of these products do not understand what PII is, and are oblivious to the threat that such products pose by revealing Personal Identity Identifiers (PII)

v. The privacy controls in these products are hard to understand and generally hard to find. Most people just sign up and use them!!

c. Could such a social platform be subject to a Cyber Security Code? These platforms need to be examined and tackled on a worldwide and governmental basis for any codes to have an impact, and the companies responsible for those platforms would be fighting that every step of the way as their revenue would surely fall.

4. Consumer/corporate mobile and home devices

a. Convenience is the name of the game here. People use devices at home or while mobile principally because of the mobility and convenience of use.

b. However, this convenience comes with risks. Around five years ago it was found that over 90% of doctors in the UK were using their mobile devices to share medical records, discussions, and medical images of their patients with other doctors. This was done without any concern for both security and privacy of themselves and patients.

c. Perhaps, there needs to be a privacy code to govern the use of such devices, and/or the development of specific applications to enable this 'convenience' safely. Undoubtedly, progress has been made in this space.

d. Home usage for work purposes is somewhat more difficult. Often devices are used for both home 'work' purposes (logging in to email, budgeting on a private spreadsheet program, homework by children etc.).

e. Ideally, a Privacy Code would define some precautions on how this might be done through use of end point controls, separate user profiles for work and private, strong WFH technology providing security of work data or even separate devices dedicated to work and private usage.

5. International Usage

a. In their book '*The New Governance of Data and Privacy',* Michael Crompton and Michael Trovato point out the role of data in international business and the importance of privacy laws in each jurisdiction being dealt with. Unfortunately, the privacy laws and data breach legislation in various jurisdictions are all quite different. They compare the Australian provisions of the Privacy Act with the EU GDPR. GDPR provides a much stronger framework than does Australia and provides for expensive penalties for those who fall foul of its requirements, which include companies in Australia who trade with the EU.

b. There seems to be some agreement that the EU GDPR regulations may be adopted extensively outside of the EU, and this should be supported.

6. Culture.

a. It has been stated in our response that 'security is everyone's responsibility'. Similarly, 'privacy is everyone's business' as well.

b. Again, Crompton and Trovato believe that it is the board that 'sets the tone from the top by making respect for privacy one of the entity's core values' and works with the management team to ensure this culture is implemented throughout the organisation.

9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

The Privacy Act was introduced in 1988 to protect the privacy of individuals. This included the regulation of how Australian Government agencies and organisations with an annual turnover of more than $3M, plus some others would manage personal information.

There are 13 Privacy Principles to be considered. The principles govern the way information is to be managed and cover the following aspects.

- The collection, use and disclosure of personal information;
- An organisation or agency's governance and accountability;
- Integrity and correction of personal information; and
- The rights of individuals to access their personal information.

Controls as part of the Privacy Act would need to ensure the three fundamentals of cyber security are duly managed and upheld. Those fundamentals being confidentiality, integrity, and availability (CIA) of information.

The 13 principles need to be analysed against the CIA to ensure all aspects of confidentiality, integrity and availability are categorically covered and unequivocally explained.

The term 'take reasonable steps' really just opens up an excuse for organisations not to comply. Take reasonable steps implies a lack of effort and a lack of due care. The terminology needs to be tightened to enforce a no stone unturned or 'every possible effort' approach. Conversely, it also opens the possibility that boards and directors, who would only be examined against the standard after a breach had occurred, would find it near impossible to mount a defence as the steps that seemed reasonable at the time are, with hindsight, never enough.

So, in summary, the 13 principles need to fully, by incorporation or addition, comply with the CIA triad in the first instance and secondarily to remove the easily achievable or impossible to achieve the terminology of 'take reasonable steps'.

10. What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

In essence all data or more importantly information needs to be covered by the Privacy Act. This would be an unequivocal and broadly reaching scope. If private information is collected and stored then the Privacy Act should cover it regardless of technology, sector, or type of data. If an identity can be established, then the Act must apply.

If information is contained in one of the following platforms, that is provided by way of an example rather than a definitive list, compliance with the Privacy Act needs to be regulated.

- Any type of computer including PC, mainframe, microcomputer, quantum computing;
- Any type of Apple device;
- Any type of Android device;
- Any type of IOT device;
- Any type of OT device;
- Any type of manufacturing device,
- Any type of industrial device;
- Any type of medical device;
- Any type of industrial control system;
- Any type of process control system;
- Any micro-chip-based device or system; and
- Any type of data storage equipment including hard drives, SSD, micro-disks, USB drives to name a few.

In summary, any digital device storing data that can establish an identity must be incorporated into the Privacy Act. The incorporation must be unequivocal and not limited. Regardless of technology, design, sector, or data type an individual's privacy must be upheld according to the principles of the Act and conferring with it the triad of CIA – confidentiality, integrity, and availability.

Summary

There is no doubt that directors should have more responsibility for business disruption and losses because of cyber breaches.

However, there is quite a difference between responsibility for financial and cyber security breaches.

In the case of financial breaches, it is because an organisation or someone within it has not adhered to the rules for what should have been a defined outcome. Accounting and tax laws, and processes are prescribed and known.

In the case of cyber security breaches, the organisation is dealing with something that has inherent faults and vulnerabilities that no one in the organisation may have knowledge of and may also not be in the control of any such breaches.

The size of the breach will be determined by the size of any attack surface open to intruders, and the degree of segmentation of the organisation, infrastructure, applications, and network. Every organisation has a unique set of infrastructure, processes, systems, and operations, and so there will be a unique attack surface for each organisation.

Ultimately, the size of the breach will depend on the design of the organisation, infrastructure, and systems architecture to minimise disruption. The concept of segmentation at organisational, systems and networking levels is gaining momentum but that will come at a cost which needs to be seen against potential losses.

There is probably universal agreement that directors should have responsibility for cyber security breaches; the question really is, 'what criteria are you going to hold them against'. Perhaps, the criteria might be a series of questions that require substantial answers, such as those in ASIC's Report 429. To those questions, the following can be added.

- What measures have been put in place to minimise the attack surfaces (size of potential breach) and disruption to the business of the organisation?
- Are operational technologies able to continue if business systems are compromised?
- In a worst-case scenario, could the organisation rebuild its infrastructure, systems, and data from 'ground zero'?
- Another question requiring resolution is which government organisation should have primary responsibility for the oversight of cybersecurity?

In the USA, operational oversight is the responsibility of CISA while the standards are set by NIST. In Australia, oversight is currently spread over many government departments. It might be easier and more efficient if ACSC is given the responsibility of operational oversight. They currently issue a great deal of good information. So does ASIC. Standards and regulations? While SAA recently updated its standards to make directors more responsible, are they the right body to establish standards and regulations in a dynamic and ever increasingly threatening environment?

Lastly, there needs to be a mandatory breach reporting obligation on organisations and directors, so the business community (and government for that matter), learn the nature of breaches, the size of the breach, the time to contain and recover, the cost and other details. This would enable all organisations to continually learn from those attacked. Obviously, some of the information reported would be commercial in confidence (such as the cost of the breach). The reporting would necessarily need to have categories and thresholds to make the collection efficient (in most organisations if one computer is subject to a ransomware attack, it can usually be fixed by the IT provider within a short period of time).

References

1. The New Governance of Data and Privacy: Moving Beyond Compliance to Performance – Michael Crompton & Michael Trovato, 2018, Published by the AICD, Sydney.
2. ASIC Guidance – Report 429: https://asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf

Authors

Julie Garland McLellan CSP FAICD
https://www.linkedin.com/in/juliegarlandmclellan/

Greg Porter MAICD
https://www.linkedin.com/in/gregporteritclarity/

Angus M Robinson MAICD FAILM
https://www.linkedin.com/in/angusmrobinson/

Peter Slade (Technical Adviser) – 40 years' experience in Australian IT including development, security, networking and managed services with Telstra, Optus, and Fujitsu. Qualifications from UTS and Swinburne - including IT and Cyber Security.
https://www.linkedin.com/in/peter-slade-4864191/

1st September 2021