Issues affecting company directors in relation to cyber security

Bathurst Lecture 2022

By David Gonski AC

All of us are familiar with instances of cyber security breaches and problems, both in our day to day lives and also in the broader context of the operations of our world.

So important has the issue of cyber security become, that in April of this year, the Australian government urgently advised organisations to adopt an enhanced cyber security posture. They warned of a 'heightened cyber threat environment globally' and an 'increased risk of cyber attacks on Australian networks, either directly or inadvertently'.

The threat is pervasive and persistent. Sadly the question concerning cyber breaches has become not 'if' but 'when'.

In 2021 an Australian organisation suffered a cyber attack every eleven seconds, costing the Australian economy an estimated $42 billion per year [1].

As cyber criminals profit from successful attacks, they continue to invest in technologies, artificial intelligence and machine learning that enables them to grow in sophistication and improve their capabilities to undermine the cyber defences put in their way.

Boards of directors, executive leadership teams, policy makers, regulators and legal systems generally, need to continue to mature and evolve their understanding and governance of and investment in, cyber risk management and enforcement.

Cyber security has now become a national security and corporate imperative.

The recent amendments to the Security of Critical Infrastructure (SOCI) Act demonstrate the evolving regulatory approach to protecting our critical assets and the pivotal role the private sector must now play in relation to our national security. Cyber incidents pose one of the most significant threats to Australian organisations[2] and the SOCI Act recognises this 'shared responsibility'[3] between government and private sector entities.

Protecting our nation's critical infrastructure, our digital assets and the privacy of our employees, customers and citizens, comes with a tremendous, and exponentially increasing cost. In a comprehensive 2020 study in the UK, cyber security spending was noted to have risen 58% to £121 billion over the last five years. Over the same five-year period, security breaches in the UK have increased by 67% and business leaders continue to identify disruption from cyber attack as one of the top five growing risks [4].

It has become clear that simply spending more money is not the solution. The game needs to be changed.

To ensure that key decision makers within an organisation are well equipped to manage cyber risk, both the law (including the enforcement arms of the government and the courts) and our risk management and governance practices, must continue to mature and evolve.

In this lecture, I want to focus on company directors, and in particular how the balance between obliging directors to suitably focus the resources of their corporations on reducing the risk of cyber breaches on the one hand, and placing them in the impossible position of ensuring that these breaches never occur on their watch on the other, is now and potentially should be properly balanced for the benefit of all.

To do so, I will briefly consider the present legal obligations placed on directors and then set out some suggestions for improvement.

I should emphasise that neither I nor really anybody, knows all the answers. But I hope that I can contribute through this lecture to providing some ideas of how to improve the situation and also start useful thinking on some of the issues which are perplexing in this area at this time.

Legal and regulatory environment in relation to company directors and cyber security

The current regulatory framework governing cyber security and cyber risk in Australia is fragmented.

At the moment, cyber security laws are a patchwork of conduct-specific and sector-specific rules and regulations.

In the context of cyber security and risk, businesses are regulated by the Australian Competition and Consumer Commission (ACCC), Australian Securities and Investments Commission (ASIC), the office of the Australian Information Commissioner (OAIC) and the Commonwealth Director of Public Prosecutions (CDPP).

If this isn't enough, listed entities are, in relation to this matter, also subject to ASX rules, and financial services entities are governed by APRA. Australia's critical infrastructure assets are regulated by the department of home affairs' critical infrastructure laws.

With different cyber security obligations being administered by a suite of authorities, a number of commentators have noted that it is clear that Australia has a legal and regulatory environment in need of streamlining in this area[5].

Without pretending to still be a practising lawyer, let me outline a few of the provisions that company directors have to consider in relation to the question of cyber security.

> *[Mr Gonski then addressed: directors duties under the Corporations Act, in particular the duties contained in ss 180 and 181; the ASX Listing Rules, in particular 3.1 superscipt as '6' requiring disclosure; ASX corporate governance principles; ASIC and APRA's requirements; the recent case ASIC v Ri Advice superscript as '7'; and the Australian Government's approach including recent legislative reform].*

Where does this leave directors?

A simple answer to the question posed above is, no doubt – very worried.

I don't have the magical answer to this concern, but as a director of many companies, I set out below some issues where I do have strong views and which I believe many listening to me today would also.

I express these by raising some questions.

How does a board of directors gain the insight and expertise that seems to be required in relation to cyber security?

This issue is discussed often between directors and in many other fora.

Many believe that putting an expert in cyber security on their board is an excellent solution.

In its favour, whenever the board meets, there would be somebody who is well versed in the area and can at least ask the right questions of management and indeed of their fellow board members.

Making such an appointment to the board would on its face respond to what a recent Australian institute of company directors' research study concluded. It concluded that

although cyber security awareness is one of a number of responsibilities for directors, there were unfortunately significant skill gaps around cyber security awareness and resilience among ASX 100 company directors. The study analysed 798 director positions (including managing directors and non-executive directors) across all ASX 100 companies. Of these, 707 were non-executive director positions and the research focussed on this cohort. Some of these directors sat on more than one ASX 100 board.

The study 8 (superscript) found that of these non-executive directors, less than 1% had cyber experience and only 16% of directors had general technology experience. On the face of it, 80% of boards have neither cyber nor technology background, and only 4% of their directors have an information technology (IT) background.

This concept of having an expert on the board, is a logical one. However, it suffers from a number of drawbacks.

Having an expert on a board can be dangerous. It can make the remaining board members complacent and indeed dependent on that expert. It can also cause problems between the board and management. Rare is the expert who can sit passively as management outlines their plans in his or her area, and not make their feelings felt without ruffling feathers. This of course does not mean that management should be left to be precious in this area, but problems could arise and particularly where management have taken expert advice in the area and the board member has a strong and differing view.

There is also a concern as to the independence of an expert sitting on the board over time. Clearly they start with great experience, but unless they are actively involved in that area outside of that company, over time, they can appear to be totally knowledgeable but instead be somewhat out of date and in some circumstances dangerous.

There is no doubt that introducing some understanding of technology and/or information as part of a board skills matrix, could be useful. Indeed, the AICD research found that in 2020 38% of all boards were introducing just that.

However, ultimately in my view, a director must be a 'generalist' first. If they happen to have expertise in an area on top of that, it would be desirable for them to know that they are appointed not just for their expertise/specialisation, but for what they bring generally to the board.

A better solution than introducing a specialist to the board may be to give the role of following developments and information on cyber risk to the board risk committee (and if a separate board risk committee doesn't exist, to the audit/risk committee) and to place on that committee the experts that can be found either as permanent members of that committee or as consultants to it. The committee being charged with this role can give the necessary focus to it and obtain the outside input that may be required and desirable. The minutes of these meetings, together with the explanation from its chair should feature, as is normally the case, at each relevant board meeting.

This, together with the following, in my view, would provide a better solution in this difficult area.

In addition, the board itself could: –

1. Seek to familiarise itself and its various members on the generalities of the cyber security problem. This can be done by having cyber security as an update regularly at board meetings, and as an item of education – say at least once a year – when a couple of hours are spent with an outside expert, hearing what is happening and what developments are taking place. Board members should be encouraged to take steps to familiarise themselves with the issues, including attending AICD (Australian Institute of Company Directors) updates on cyber, or indeed the relevant courses that organisation makes available.
2. Getting the whole board involved every year or two in a simulation, I have found to be extremely useful. Not only does this highlight what deficits the board may have in understanding what is going on in this area, but also it highlights how personalities around the board table will react to a difficult situation. At the very least, a simulation can show to board members what the procedures will be and contest whether the policies and procedures are easy to find, easy to follow, and from the simulation itself, adequate. It underscores the fact that the way the company handles the situation may be as important if not more so than the situation itself. There are many organisations who run and/or will arrange these simulations and I have found do it both professionally, and, scarily, very realistically.
3. Board members should regularly be sent updates on what is happening, not just in the company but generally in the area of cyber security and breaches thereof. Often non-executive directors sitting on the board can and should be, encouraged to bring 'war stories' in this area to the board

table. Sharing them with their fellow directors and also management, can certainly assist a corporation in getting ready. It is one of the strengths of the non-executive director model that without breaching confidences, directors can bring experiences to the table from elsewhere.

4. Management and the board at strategy meetings and the like, should be encouraged to spend time talking about the issue – preparedness for the inevitable is only one part, the other part is using it as an opportunity for all to bring their combined knowledge and capacities to ensure that their corporation is as ready as it can be.

Should directors have available to them, a defence similar to the business judgment rule?

As can be seen, from what I have already said, the obligations on directors in this area are immense. This gives rise to the question of whether some sort of 'safe harbour' or 'business judgment' rule defence should be sought and given to directors. By this term I refer to rules which, if adhered to, provide an excuse or exemption to the obligations otherwise placed on the director.

The advantages of such are obvious. First, it may remove a developing deterrent to potential excellent candidates joining boards of directors. Without such a safety valve, increasingly potentially good board candidates are preferring to become advisory board members only or stick to non-listed entities. Second, depending on how the safe harbour is drafted, it can assist in directing how the board should handle these matters and give some further insight into what is expected of them.

Many in this room will be more aware than I am of how safe harbours or business judgment rules have been rather ineffective in Australian law and have been the subject of long term debate. Indeed, in the 20-plus years since the Australian business judgment rule was included in the Corporations Act, it has only been sucessfully utilised twice. This is for a number of reasons including that it can only be used as presently drafted, to defend against an allegation that a director has breached their duty to act with care and diligence and can only be used to protect a 'business judgment'. Court decisions have confined the scope of activities that are within the meaning of 'business judgments'. Further, the requirements for the rule to apply to a particular business judgment are difficult to satisfy.

It is with this background that one questions whether a safe harbour specifically as a defence in the area of cyber security is not now warranted.

Other countries have made some inroads in developing statutory cyber security defences.

Although there are substantial variations between the relevant defences, all the defences have one thing in common – they all require evidence of compliance with either a particular cyber security standard/framework, or a standard/framework which is 'reasonable'.

In America, Ohio was the first state to pass the cyber security affirmative defence in 2018. Connecticut and Utah recently adopted their acts in 2021. All three statutes generally encourage companies to develop and maintain a cyber security program that conforms to industry standards.

The laws enacted in Connecticut and Utah are generally modelled on the Ohio statute. The Ohio statue provides 'affirmative defence' to companies with a prescribed written cyber security program that deals with tort claims arising out of a data breach. If proven by the company, this safe harbour would bar tort claims asserted against it. The defence applies only to tort claims related to allegations that the company failed to implement reasonable security controls. To evoke the affirmative defence, the company must 'create, maintain and comply with a written cyber security program' that meets the following requirements:

1. The program must have administrative, technical and physical components that protect personal or restricted information.
2. The program must meet one of the enumerated frameworks to the extent that the available approaches apply to the given entity and its information; and[9]
3. Where a company models its program after one of the enumerated frameworks and that framework is amended, the company must reasonably conform to the amended guidelines within one year. This requirement provides a grace period while also ensuring that companies stay up to date on industry standards for their cyber security programs.

I note several states of America have proposed similar safe harbour laws. Specifically Georgia introduced legislation in 2021 which provides an affirmative defence to cyber security liabilities and provides a 'reasonable' framework that takes into consideration the size and complexity of the company and the sensitivity of the information protected.

I believe that directors should seek and welcome the introduction in Australia of a cyber security safe harbour provision.

In saying this, I do note that some question the fairness of safe harbour provisioning. This is based on the contention that the onus shifts from the plaintiff/prosecution to the defence with a safe harbour provision. They argue would it not be better for those having to prove the offence to also have to prove that the safe harbour provisions do not apply. I see the logic in this argument, but note a shift in onus is not as bad as not having the provision at all.

From my point of view also, I would welcome the requirement for any new safe harbour exception being potentially that the corporation has met designated public standards (to which I will refer below).

The absence of a safe harbour provision undoubtedly will leave the interpretation of the fairly onerous provisions placed upon directors difficult to fathom in an area that is growing quickly.

Is there therefore any utility in requiring Australian companies to comply with particular cyber security standards?

There is a lot of debate over whether having regulated standards is good or bad.

The major argument in favour is that a standard allows a corporation (and in this instance its directors), to know what is expected of them as the standards will hopefully clearly set out the minimum requirements needed to be achieved. Standards can also provide a clear path for organisations to formally attest they are compliant, and provide opportunities for peer to peer benchmarking.

However, being compliant with a standard does not, of itself, make an organisation secure.

The argument against, generally focuses on the phrase above – minimum requirements. Those who don't believe in standards believe that they become the minimum and that unless they are actively changed and kept up to date, they actually reduce the compliance in the sector as people aim for that minimum rather than going way beyond it.

I should note, that those arguing against the standards also see amendments to standards as often running behind in time and developments in the market, and sometimes being able to be delayed or changed by vested interests.

At the moment, there are various cyber security standards in existence, and in addition to differing views on whether one should have standards there are differing views on which of these are superior.

For example, the Australian signals directorate states that if a company undertakes the following mitigation strategies it will be addressing up to 85% of targeted cyber intrusions:

1. Use application whitelisting to help prevent malicious software and unapproved programs from running;
2. Patch applications such as java, pdf viewers, flash web browsers and Microsoft office;
3. Patch operating system vulnerabilities; and
4. Restrict administrative privileges to operating systems and operations based on user duties.

However, some cyber publications report different statistics and different strategies as being more effective. There are also some counter parties who require that entities they do business with comply with other particular standards.

It is worthy of a debate as to whether standards should be legislated and indeed if so, who will approve these standards, how will they be kept up to date and how will they interrelate with current directors' obligations. In the latter case, should this be achieved through safe harbour provisions, or more directly.

There is no doubt in my mind that there are standards and standards! Standards which are too specific will not over time assist in protecting all of the interests that need protecting. However, standards that are too 'woolly' may also give rise to the same problem and indeed may give rise to the vagaries of interpretation which to some extent remove the benefit of having standards in the first place.

Perhaps naively I feel that there is room here to establish an ongoing body that is charged with prescribing for the benefit of directors – not necessarily for the experts who actually run and advise the corporations – what are the standards that directors should at a minimum seek to achieve with the intended use of those standards at the very least in a safe harbour provision. I should add that the market place can play an important role in getting directors to do more than minimum standards, particularly if consumers etc place importance in the safety of their information and the dangers of delay in supply from cyber interference.

For completeness I should note that in the absence of standards or indeed in harmony with them, the concept of a handbook for directors would be very useful. I understand the AICD and the cyber security CRC are working together to publish one.

Is cyber insurance the solution for reducing directors' liability?

I start with the obvious comment that insurance can in certain circumstances lessen the financial pain that a company or its directors suffer as a result of an event covered by their insurance. It does not however cover the reputational side and so I believe it is clear that insurance should be seen (particularly in this area) as a potential part of assistance, but not a total solution. Establishing preventions and defences to the occurrence of the event before it occurs undoubtedly is the best solution.

In the world of insurance, cyber policies are a relatively new offering. In Australia, the market remains relatively immature, though it is growing, while in the United States, cyber insurance is far more established.

Like traditional insurance policies, cyber insurance generally covers first and third party losses. The policies generally cover a range of costs including those related to business interruption, legal representation, theft or fraud, incidence response, victim compensation, extortion or ransom demands, system remediation and regulatory infringements.

In the past, cyber insurance was often purchased as an add on to standard business liability insurances. However, as the risks posed by cyber threats have increased and evolved, there has been a shift to establish cyber risk as a standalone issue and subsequently a standalone insurance policy. In the US there has been a lot of research into the underwriting processes of US cyber insurance policies and this has indicated a lot of variance. Recently, one of the larger American cyber insurance companies, Resilience, announced new measures that they would implement to bolster cyber security. Resilience said it would now require policy holders to 'meet a threshold of cyber security best practice as a condition of receiving coverage'[10]. This is an indication that a large company is looking to establish standards with the problems that come with those standards as previously mentioned.

This concept of having [a cyber-security] expert on the board, is a logical one. However, it suffers from a number of drawbacks.

The market here remains quite opaque, although it has expanded significantly over recent years. There is no doubt that cyber risk exists that is not explicitly included or excluded in current insurance policies and as a result, organisations may be under the assumption that they are adequately covered when in reality they may not be.

This uncertainty sometimes called 'silent cyber' is a global phenomenon and has prompted the OECD to release its 'encouraging clarity in cyber insurance coverage report' in 2020[11]. In addition, the UK's prudential regulation authority has provided guidance outlining its expectations regarding the management of cyber insurance underwriting risk and recommending companies offer explicit cover for cyber risks and clearly articulate what is not covered[12].

There has also been recent volatility in the cyber insurance market as a result of large ransomware payments, which has had a flow on effect for reinsurance. Globally, cyber reinsurance rates reportedly soared by up to 40% in the 2020-2021 financial year, attributed to a spike in ransomware attacks.

There is also evidence from overseas that ransomware criminals have accessed systems in search of insurance certificates. Insurance perhaps being an appetiser to the criminal and of course the ransom demand being made often accords to the specific amount covered by an insurer.

The question of whether insurance should be taken out is one for the company and its directors themselves. But what is clear is that in looking at the insurance, what is covered and indeed what is excluded, must be carefully understood.

I should also note that some insurers require their own consultants and officers to negotiate with the cyber security criminal should a ransom be sought. This is good and bad. There is no doubt that the insurer will almost always be much more experienced in these negotiations than the party that is the subject of the ransom request. On the other hand, directors may be troubled by having the future of their company (both in terms of the amount to be paid and the time that it will take before normality is sought and obtained) taken out of their hands as part of the arrangements in the policy terms. Indeed, it is a question for another day whether directors can delegate some of these activities to parties outside of their control and still be seen to have acted responsibly and properly.

Is the payment of ransomware demands legal or illegal?

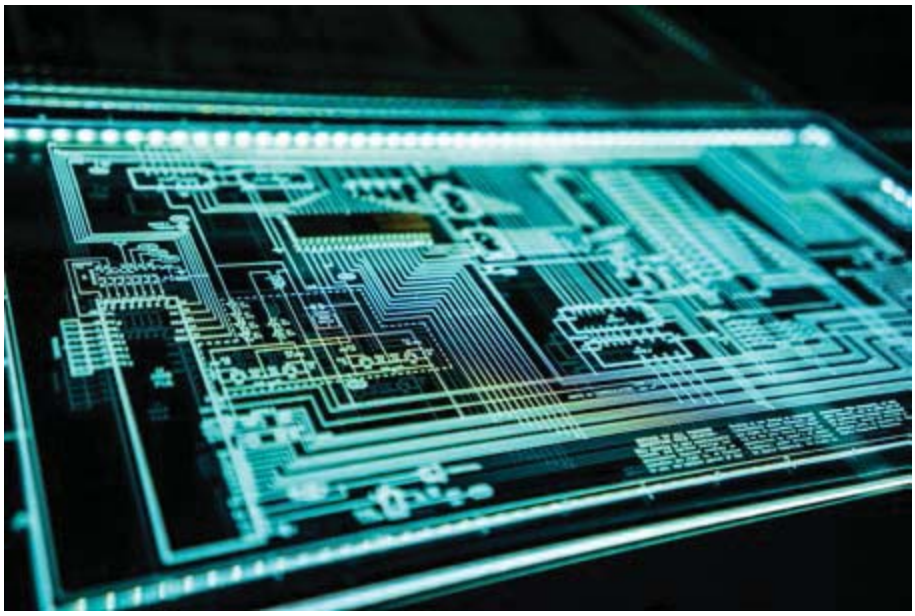
If a company is hit by a ransomware attack and a demand is made, directors are faced with a choice: to pay or not to pay?

Although this question seems simple, the decision involves a myriad of complex considerations.

If the directors determine to pay the demands, the questions that then arise are:

1. Is it legal to do so;
2. Will in fact a payment result in the restoration of the company's access to its systems and prevent disclosure of stolen data; and
3. Will it start an avalanche of further ransomware demands as the criminals then know that that company pays ransoms?

The dilemma for the director is very difficult. On the one hand, the payment of the ransom may see an action against the directors by authorities if any part of it is illegal and in addition, shareholders may sue the directors for failure to act with due diligence etc. On the other hand, if the board determines not to pay a ransom, shareholder action could still occur through class actions and the like, based on losses of profit etc for not paying the ransom.[13]



The policy stance of the Australian Government is not to make ransomware payments under any circumstance. Nevertheless the untested legal environment and lack of clarity draws significant criticism within business circles.

Turning to the first question, namely whether it is legal to make a payment, there is presently no clear prohibition in Australian law against ransomware payments.

However, the actual payment may well be illegal even though such an overall prohibition doesn't exist.

In certain circumstances, making a ransomware payment may constitute an offence for which the company is liable and in turn its directors.

The *Charter of United Nations Act 1945* (Cth) (UN Charter) and *Autonomous Sanctions Act 2011* (Cth) and their related regulations prohibit making funds or assets available to a sanctioned organisations, are set out in the Department of Foreign Affairs and Trade's consolidated list. It is well known that some ransomware participants belong to sanctioned organisations. As a result, there is potential each time a payment is made, that it may be to such an organisation.

A company that is found to have violated Australian sanctions laws may be able to rely on the defence under section 21 (2e) of the UN charter if it proves that it took reasonable precautions and exercised due diligence to avoid the contravention.

It is also possible that a company that makes a ransomware payment could be liable under US legislation in relation to financing terrorist activities. The *USA Patriot Act 2001* has extra territorial reach and it prohibits companies from providing material support to terrorist organisations.

The *Federal Criminal Code Act 1995* (Cth) also makes it an offence to intentionally provide resources that would help a terrorist organisation involved in a terrorist act. This offence operates even if the company is merely reckless as to whether the organisation is in fact a terrorist organisation.

In addition to the above, the money laundering (instrument of crime) offences need also to be looked at. If the funds being paid in relation to the ransomware demand can be seen to be monies used to commit any crime then the person paying the money may be liable for a money laundering offence under division 400 of the *Federal Criminal Code Act 1995* (Cth).

An interesting argument arises here. If it is a crime to extort money in these circumstances, and particularly so if critical infrastructure is involved, does division 400 make it an offence now to pay the ransom as those monies will be used in committing the crime?

There are defences to this division 400, which include that of duress. Accordingly, if the company had a reasonable belief that the ransomware threat would be carried out, unless the payment was made, and there was no reasonable way that the threat could be rendered ineffective in a different way and that the conduct was in fact a reasonable response, then a defence claim may be made.

In addition, a defence of 'self-defence' may be available where the company can conclude that the payment of the ransom is necessary to protect the company's property from destruction, damage or interference.

Finally there is a defence of 'sudden or extraordinary emergency'. It is available if the conduct was carried out in response to a sudden or extraordinary emergency and the payment was the only reasonable way to resolve the emergency.

The major difficulty then for the directors when considering how to respond to a ransomware demand is the absence of clear judicial guidance on how courts will interpret and apply the various defences referred to above. Accordingly the payment of a ransom demand could be one that revisits criminal charges on to a company at a later date.

The policy stance of the Australian government is not to make ransomware payments under any circumstance. Nevertheless the untested legal environment and lack of clarity draws significant criticism within business circles where company directors with the best of intentions could face criminal liability for the payment of a ransom.

There is considerable argument in favour of the government legislating to make payment of a ransom illegal, except in the most exceptional circumstances where there is a risk to life. To do so would solve the decision for directors and also potentially mean that demands on Australian companies shouldn't be made as frequently, as those making them will know that no payment can legally flow from it.

Some believe that this will move the demands towards circumstances where there is a 'risk to life'. Others argue that such legislation is too prescriptive and could prevent directors solving a problem quickly and may exacerbate the possibility of losing their systems and/or data. Some also argue that the notification provisions which now exist and to which I referred earlier are a better way to focus attention on the problem.

I believe that this should be debated more fully and that probably the best solution is to prohibit the payments except in designated circumstances, and perhaps to use the panel of experts to which I refer below as a way of assisting when such exemptions should apply.

One other solution to the above question advanced by some is to stipulate in the Corporations Act that a director will not be liable of an offence for 'not paying a ransomware demand', rather than making the payment specifically illegal. This would mean that directors know they have no liability if they decide not to pay and it follows they have bigger liability if they do.

Should there be a cyber disputes panel?

As mentioned previously, the area of cyber security is a very specialised one. In addition, it is an area of much technicality and one which is developing very quickly. Added to this is the often vital need for decisions to be made quickly and any delays in such decisions are incredibly expensive and potentially dangerous to many.

This has made me consider whether there would be virtue in establishing a cyber panel.

The panel could be modelled on the takeover panel, which is a peer review body comprised of part-time members appointed from the takeover advisor and business community. The panel members are specialists in mergers and acquisitions such as lawyers, investment bankers, company directors and other professionals as well as government appointees.

The purpose of the cyber panel would be to make decisions in specified circumstances and obviously to make them quickly, bringing great specialisation and technical knowledge to bear.

A number of examples come to mind of where such a panel could have jurisdiction. The first is to assist in helping the relevant minister to authorise the Australian signals directorate to intervene in the operation of critical infrastructure assets where there is a serious cyber security incident impacting those assets.

The powers the minister has to authorise actions in these circumstances include:

1. Giving direction to a specific entity for the purpose of gathering information;
2. Giving specified directions to an entity to do one or more things to respond to an incident for an entity to take actions; or
3. Requesting an authorised agency (the ASD) to provide specified assistance and cooperation to respond to the incident.

The minister then has step-in powers where an entity is 'unwilling or unable' to comply with a direction or authorisation in relation to a cyber incident affecting critical infrastructure assets. The panel could provide an urgent avenue of appeal to endorse or otherwise whether the minister should step in, in the abovementioned circumstances.

Given the far reaching nature of the minister's powers, and given the judicial review of the minister's decisions are expressly excluded in the legislation, further protection of the legitimate interests of the entity could be provided by allowing the cyber panel power to urgently review the decision of the minister. The benefit of this would be to prevent unwarranted encroachments on the freedom of business made by legislation such as this – i.e., there would be an avenue of appeal previously denied. From the minister's point of view, although he or she would lose the absolute authority that the Act presently gives, they would instead gain the opportunity of outside review on an urgent basis by those equipped to do so in that area, thereby in some circumstances preventing adverse criticism against the minister at a later date.

The cyber panel could also have input in determining whether a ransomware demand can be paid in circumstances where the government in the future comes to the conclusion that ransomware demands should not be able to be paid unless there is risk to life or other mitigating circumstances. The cyber panel could in those circumstances, make the determination on the application by the company involved within a period of 24 hours, or even shorter, and thereby protect the directors and the corporation from breach of that legislation and indeed from claims in respect of their dealings in that regard.

The cyber panel may also have a role to play in relation to standards.

If standards are indeed put together and if it flows that directors who have achieved that minimum standard have some protection through safe harbour or general law – the cyber panel could perhaps be approached where the standards are not clear or where there is a need for a determination of what is required, and indeed meant by the standard, the panel also could be an avenue for extension of the standards in certain circumstances.

The above are just three situations that come to mind in the area of cyber security, and there are no doubt many more.

The area of cyber security develops and develops quickly.

The liabilities of corporations and their directors, established well before the coming of cyber and its related technologies, stand to make directors and corporations potentially liable in many, many circumstances.

One of the biggest risks is that the area is developing so quickly that what directors believe is normal and sufficient at the time of a breach may well be almost totally forgotten in months, if not years later when the dispute concerning that event comes to litigation.

The essence of my message is that this is an area that regulators, lawyers and those practising in the field need to grapple with quickly.

The suggestions I have made, namely:

- as to how directors gain insight and input into their deliberations on cyber;
- the possibility of a safe harbour provision or business judgment rule;
- the need for security standards in the area of cyber;
- the limitations of insurance;
- the need for more definitiveness in the law of whether the payment of ransomware demands is legal or illegal and at the very least, likely to cause liability; and
- the potential need for a cyber panel or some other quick to act and technically enabled legislative panel;

are just some of the ideas that need to be contemplated.

Minds much more involved in the area than mine will no doubt have many more to add.

If focus is not brought to bear on this with some urgency, at the very least, good potential directors will fear getting involved in corporations and, which may be even worse, the fear of liability will result in normal and proper business risks not being taken for the advancement of the relevant corporations. BN

I want to personally and substantially thank Robert Hanley, Joshua Smith, Miriam Kleiner, John Macpherson, Maxine Viertmann and their colleagues at Ashurst for assisting me in trawling through the various provisions relevant to this subject. Their knowledge is very deep in this area, and their interest commendable.

ENDNOTES

1. Phair, n; cybercrime in Australia: 20 years of in- action (2021).
2. ACSC Report.
3. Security Amendment Bill.
4. Debate security: cyber security technology efficacy.
5. Https://www.herbertsmithfreehills.com/latest- thinking/regulatory-enforcement-in-cyber-space- what-have-we-seen-and-what-can-we-expect.
6. Asx listing rules chapter 3.
7. *Australian Securities and Investments Commission v Ri Advice Group Pty Ltd* [2022] FCA 4.
8. Cyber security skills of company directors – ASX 100 research study by Nigel Phair and Hooman Alavizadeh – https://assets-us-01.kc- usercontent.com/4df0558d-5779-0012-00f2- b3fa06d6c950/df25f810-494d-4f8c-b434- 0e65c577dd97/cyber%20security%20skills%20of%20c ompany%20directors_ver%203%20(003).pd.
9. Three US state laws are providing safe harbor against breaches – https://www.cshub.com/security- strategy/articles/three-us-state-laws-are- providing-safe-harbor-against-breache.
10. Underwritten or oversold? How cyber insurance can hinder (or help) cyber security in Australia (cyber security cooperative research centre) – https://cybersecuritycrc.org.au/sites/default/file s/2021-10/underwritten%20or%20oversold%20%20-%20dv.pd.
11. Encouraging clarity in cyber insurance coverage: the role of public policy and regulation, OECD (2020) – www.oecd.org/finance/insurance/encouraging- clarity-in-cyber-insurance-coverage.pd.
12. Encouraging clarity in cyber insurance coverage: the role of public policy and regulation, OECD (2020), p.12 – www.oecd.org/finance/insurance/encouraging- clarity-in-cyber-insurance-coverage.pd.
13. Cyber-security class actions a 'ticking time' bomb for directors – governance institute of Australia – https://www.governanceinstitute.com.au/resourc es/governance-directions/volume-73-number- 10/cyber-security-class-actions-a-ticking-time- bomb-for-directors/.