Strengthening Australia's cyber security regulations and incentives: Submission

About Vaultron Technology

Vaultron Technology is an inspired group of innovative business and information technology professionals focused on robust cyber security through a sustainable 'Business Partnering' approach rather than the traditional "react out of fear" approach.

Using a proven suite of cyber security and privacy tools, extensive industry knowledge and insight, Vaultron Technology is able to empower sustainable data and privacy security for our clients.

Vaultron Technology is more than just a consultancy supplier. As an expert Cyber Security and Privacy firm, Vaultron specialises in the provision of "hardened" ITC that are ideal for environments where privacy and cyber security are a top priority such as education and healthcare.

At Vaultron we specialised in servicing the 100,000 plus small to medium enterprises with the sensitive Healthcare sector with a predominate focus on Cyber Security Auditing and Assurance.

Executive Summary

The below, in no particular order or level of importance, is a high-level summary of the recommendations made by Vaultron to the Government. Note further details on each point can be found in the response in detail sections following the summary.

- Change the Government and industry messaging to move away from an excessive and unhealthy focus on Threats to focusing predominately on organisation's Vulnerabilities.

  For example at Vaultron we use the following messaging for small business clients:

"Focus on Controlling your Controllables. You only have control over your vulnerabilities not the threats. Decisions made in reaction to threats come from a place of fear and are rarely good decisions, whereas, decisions made from well informed, data driven, vulnerability audits is from a place of being in control."

- In our opinion the current regulatory environment needs to evolve with the following key principles:
    a. All standards are to be mandatory – little to none should be voluntary. Voluntary standards when it comes to compliance is like asking a citizen to pay voluntary taxes. They are just not followed.
    b. Adopt a clear Risk Based approach to Cyber Security. This is based on the principles laid out by the Australian Cyber Security Centre and Australian Standard and International Standard AS/ISO 31000.
    c. Move away from the unenforceable, confusing, inefficient "reasonableness" model and move towards a more prescriptive standard.
    d. Clearly identify that Software as a Service companies have a significantly higher risk and duty of care to provide cyber security so must have their own regime.
    e. Develop a clear mandatory transparency disclosure regime such as a mandatory public "Trust Centre" which covers the core elements of: Transparency, Privacy, Cyber Security and Compliance disclosures.
    f. Implement a robust compliance regime such as the issuing of infringement notices / fines rather than warnings or mediation.
    g. Implement mandatory Cyber Security Insurance for high-risk industries to guarantee consumer protection.

- There is a drastic need to shift from training and awareness to mandatory practical applications of cyber security to ensure adequate controls are in place, operational and effective.

- For small to medium entities that choose to not perform a health check audit and a data breach occurs, then penalties and compensation would attract a mandatory 10 times multiple increase to account for the negligence and lack of taking reasonable steps to appropriately protect data and systems. Ignorance would no longer be an acceptable excuse.

- The approach and scope of an IT Health Check engagement in our opinion must include the following elements:
    a. Health checks must be mandatory for those dealing with sensitive data.
    b. Includes an IT systems vulnerability assessment – can only be performed using specialised software
    c. Includes a Website vulnerability assessment – can only be performed using specialised software
    d. Includes an Internal Process and Policy review – can be performed using questionnaires. Incapable of being performed using computer assisted auditing techniques (CAATs).
    e. Includes Cyber Supply Chain Due Diligence on critical inputs e.g. Software as a Service and Internet of Things. These due diligence assessments identify High Risk suppliers to the business.

- It be made a mandatory compliance requirement for an entity to either perform an independent Health Check audit or ISO 2700 audit in order to gain Cyber Security Insurance. No health check – no insurance. It would be expected that a Health Check to be performed and attested to annually.

- Create a new Quantum Safe Economy department mirrored on the UK National Quantum Technology Programme to prepare Australia for the future in Quantum safe processes and policies.

- Mandate annual cyber security training for Directors of listed companies in high risk or sensitive data.

- Ban the use of use of self-filled questionnaires as a proof of compliance. Based on international and Australian standards, compliance must utilise some element of independent testing on actual assets to prove beyond reasonable doubt that those controls are in place, operational and are effective.

- Mandate that all large and high-risk businesses must create Trust Centre's on their website covering the four fundamentals of trust – Transparency, Privacy, Cyber Security and Compliance.

- Change the Office of Australian Information Commissioner approach away from the ineffective mediation and education compliance to extensive compliance enforcement including the ability to issue infringement notices with on-the-spot fines.

- Prosecution for deliberate falsification or misleading, deceptive or unconscionable conduct about an organisation's cyber security.

- Make Directors or Business Principles personally liable for Cyber Security incidents to high risk and sensitive data. Similar to the Health, Safety and Environmental legislation that makes Directors personally liable for incidents in those areas of social responsibility.

- Create the "Wall of Shame" similar to the United States HIPAA / HITECH website known as the Office for Civil Rights (OCR) portal for cyber breaches that affect over 500 individuals.

- Revoke Government taxpayer funding (i.e. either direct or indirect funding) for uncompliant entities. For example, banning the payment or integration of Medicare rebates to uncompliant healthcare software companies.

- Give the OAIC powers to issue infringement notices / on the spot fines to any organisation that provides a "Trust Badge" for IT security when that organisation is unqualified or negligent to do so. For example, General Practice (GP) accreditation companies accrediting and declaring to patient's GP practices are IT / Cyber accredited or safe when clearly, they are not.

- Regulate the Cyber Security Insurance Industry.

- Elimination of the Australian Privacy Principle 8.2(b) cyber security supply chain loophole.

- Protect small to medium businesses from Cyber Security Investment Asymmetries. As big business utilises free cashflow to invest and make itself more resilient to attacks, Threat Actors are likely to turn their attention to the more vulnerable and weaker and underinvested small to medium enterprises.

- Avoid the "Set and Forget" approach to digital technology by implementing strategies such as mandatory cyber security audit timeframes.

- Create access to the Small Claims Tribunals in the Privacy Act similar to those in the Fair Work Act.

- The Government review the application of section 82 of the Health Insurance Act 1973 on Healthcare organisations (e.g. healthcare software companies or

providers) that fail to adequately assure that their Cyber Security is at the appropriate levels.

- Take a "Licence to Operate" approach to cyber security in line with other social responsibility laws e.g. Environmental Laws, Health and Safety Laws, Fair Work Laws. Lack of compliance with Cyber Security regulations would result in an organisation no longer able to operate in that industry of field.

- The assertion that being Essential Eight compliant is too difficult is in our opinion an absolute fallacy and just another excuse used by businesses to be non-compliant. We not only perform these tests regularly but also make them effective and affordable. An example extract of one of our reports is attached.

RESPONSE IN DETAIL

Chapter 2: Why should government take action?

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

As one of Australia's leading cyber security and privacy experts that focuses solely on servicing the highly sensitive healthcare industry with over 100,000 small to medium businesses, we can provide feedback directly from our thousands and thousands of customers that these are the factors preventing the adoption of cyber security best practice in Australia:

Factor 1 – Attitude: Naivety - It just won't happen to me.

Australian businesses, particularly small to medium businesses, still think and hold the naïve attitude that cyber criminals only attack large companies and government organizations like banks, the stock exchange or Government agencies. They hold the belief that: "I'm too small for them notice me."

In reality Cyber criminals rarely target any specific organizations they instead are opportunistic. Just like fishing they spread their nets as wide and as far as they can in the hope they trap an unsuspecting victim regardless of the victim's background.

As large corporations and governments invest in more and more sophisticated cyber defenses, cyber criminals are turning their attention to small more complacent organizations to satisfy their criminal schemes.

This leaves small and medium business vulnerable as big business protects themselves with billions of dollars in cyber security investment the opportunistic nature of cyber criminals is to pick on the weak and the vulnerable – this is now small to medium businesses.

Factor 2 – Attitude: Set and Forget

Australian Businesses still do not realise that digital transformation is always dynamic and one of the fastest transforming environments in the world today. Moore's Law dictates that the digital world is completely transformed within 24 months / 2 years.

However, businesses have a "Set and Forget" approach to cyber security. They feel that they set it up once and it remains static with no need to change it. There is a lack of understanding that cyber security is a dynamic approach which requires constant vigilance and checking.

The Australian Information's Security Manual sets out in its controls that each IT environments should be reviewed / audited at a minimum every 24 months – obviously inline with Moore's scientific law that of digital transformation taking place every two years.

Factor 3 – Over reliance and misconceived communication from Government Organisations on Cyber Security Awareness Training and IT Policies.

Cyber Security is not about awareness training or IT policy it is completely about actual action plans and real controls being put in place.

The Office of Australian Information Commission sets out 170+ components to be data secure all of which are required to be **regularly tested or reviewed**. Awareness training and policies is only 2 of these 170 components. This means when you do awareness training you are only 1% compliant to the OAIC cyber security reasonable actions for data protection.

To use an analogy - Would it be acceptable if you had a virus (e.g. COVID 19) and went to a medical provider and all they provided you was some awareness training and a policy on social distancing and hand washing?

Of course not, the expectation would be that the medical professional would give you the awareness training, **plus** do a practical assessment or test, **plus** a treatment plan to eliminate the virus, **plus** follow up at the end of the treatment plan to recheck that the treatment plan was effective.

Cyber Security is no different. It is why they use the term Virus when describing malicious code. Not only does a computer virus act like a human virus but the treatment and prevention plans are exactly the same.

It is the physical testing and diagnostic action plans and treatment of any identified deficiencies that make a business safe – not awareness training.

There is a drastic need to shift from awareness to mandatory practical applications of cyber security.

Factor 4 – Cost avoidance and Cost mitigation: I am a for profit business, why would I spend money on something I am not mandatory required to do so.

Business is about profit, it is not about social welfare. It is so much so that in the Australian Corporations Act it makes it clear that a Director must act in shareholders best interest to maximise profit.

By not making cyber security mandatory in a clear form or worst, not having any adequate enforcement regime is like asking a citizen to voluntary pay additional income tax and question why no one is paying it.

Good profit-oriented businesses by their very nature are designed for efficiency and to eliminate all unnecessary costs. This is why these cost types are called “compliance” costs. Just like Taxes, Health and Safety, Environmental and Workers Compensation, Cyber Security needs to form a part of a mandatory “Compliance” costs and should be required as a “licence to operate”.

Factor 5 – Lack of knowledge on financial impact: Cost benefit analysis of Preventive measures vs Reactive Measures

There is not enough appreciation and education of the principal reason Privacy By Design and Security By Design has been adopted by almost every western society in the world including USA, Canada, the European Union and the United Kingdom.

Privacy and Security By Design is highly more efficient and cost effective as a preventive measure versus the alternative reactive approach.

While prevention does have some upfront compliance costs such as hardware or software implementation and audit of controls, these costs are far smaller than the reactive costs of crisis management, incident investigations, legal class actions / law suits, loss of business and most importantly loss of reputation and insurance premiums.

More emphasises is required on the financial Cost vs Benefit of being Preventive Vs Reactive.

Factor 6 – Business hates the principle based reasonable approach to cyber security.

Businesses do not have the time, resources, or effort to figure out what is reasonable. It wastes their time and resources. They just do not care about this approach to cyber security compliance as this approach is highly inefficient, confusing, costly to figure out and inconsistent.

Businesses just simply want to be told directly:

a) what is best practice
b) what to do.
c) when to do it

Business like and want this approach as it is by far the most efficient and the most cost-effective approach. This approach also allows businesses to easily delegate to responsible persons, set clear agenda's and policy and clearly communicate to stakeholders on their progress and confirm that all compliance has been implemented.

Factor 7 - Over reliance and lack of understanding on unlawful cyber security insurance

Australian businesses, particularly small to medium business, do not understand the difference between Cyber Security risk elimination vs Cyber Insurance risk transference.

However, what is most concerning is the high number of insurance companies marketing their insurance to cover not only cyber security business cost events but also civil and peculiarly penalties e.g. Government fines. This is highly unethical and also unlawful under the Australian Corporations act.

This is the equivalent of an insurance company advertising Environmental insurance to cover Environmental regulator fines so that a corporation could continue to pollute at will knowing that any government penalties would be covered by insurance.

Australian businesses do not recognise or properly understand that good Cyber Security eliminates or mitigates the risk of an incident altogether whereas insurance merely transfers the risk to another entity for a price / premium – With insurance the risk still remains in place and the potential for damage to their business or their innocent customers data is still very real.

There is also the lack of understanding that in the long run risk elimination is by far cheaper for business, Government and the economy than risk transference.

Factor 8 – Unhelpful and incorrect advice from unqualified professionals.

Cyber Security is a specialised area of IT which requires specialised qualifications and knowledge.

Cyber Security audit and assurance is an even a further specialised area is more akin to accounting auditors then IT professionals. So much so in the Unites States they specifically have banned IT professionals from authorising cyber security audits and instead have mandated that only Certified Practicing Accountants are allowed to sign off on their America gold standard SOC 2 / SAS 70 cyber security audits.

What is even worst is the concept of “self-help” or “self-testing” advice. We don’t ask medical patients to self-diagnose, we don’t ask commuters to road worthy their own car, we don’t ask airline passengers to fly their own commercial airplanes. No, we get experts in those fields to provide the appropriate service. Cyber Security and Cyber Security assurance is no different – it needs to be performed by qualified professionals.

Factor 9 – Australian Federal Government financially rewards and pays over $36 billion of taxpayers money per year to private organisations to be non-compliant with Cyber Security laws.

The Australian Healthcare sector accounts for close to 25% of Cyber Security incidents in Australia, the highest of any sector within Australia. With over 90% of Healthcare businesses being non-compliant with the Australian Privacy Act 1988 including Australian Privacy Principle 11 – Data Security, this is set to rise.

The Australian Government pays approx. $36 billion per year in Medicare payments to the Healthcare sector (either directly or indirectly) despite legislation laws within the Health Insurance Act 1973 at section 82 that states Medicare should not be paid to organisations that knowingly, recklessly or negligently engage in conduct that constitutes inappropriate practice by the practitioner.

There is a growing argument that failure to implement appropriate Cyber Security would amount to knowingly, recklessly or negligently engaging in inappropriate practice under section 82 of the Health Insurance Act 1973. There are also growing calls for Medicare payments to be revoked from organisations, including healthcare software companies, that fail to adequately assure that their Cyber Security is at the appropriate levels.

We ask the Government – Why would a sector with the highest number of cyber security incidents in the whole of Australia want to change its approach when it regularly gets subsidised, rewarded or encouraged by the Government to the tune of ~$36 billion a year to continue in its approach?

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

Negative Externalities and Information Asymmetries are a very real and significant problem within the Australian ICT industry which the Government needs to take immediate action on.

At Vaultron, we provide a Healthcare Cyber Security service where we conduct due diligence assessment and reports on over 60 commonly used Health Care software companies that handle millions of patient data every day.

We have found that over 90% of these software companies are non-compliant with the Australian Privacy Act including Australian Privacy Principle 11 – data security. The Office of Australian Information Commissioner does little to nothing to clean up the industry.

When approaching these uncompliant entities we are constantly being deflected or straight out told that the software company's self-interest outweighs any need to provide details on Cyber Security and Privacy.

Also in June 2021, rsearchers at Macquarie University's Department of Computing analyzed over 20,000 health apps for Android in Google Play finding the vast majority to be uncompliant. https://www.bmj.com/content/373/bmj.n1248

Researchers also discovered that over 28 percent of the apps in their sample provided no privacy policies and even when privacy policies were declared, the researchers found that around half of the apps were not compliant with what was stated. A total of 15,838 health apps in Google's Play store were analyzed in detail, with their privacy practices compared to a random sample of over 8000 non-health programs. The results of the investigation showed that almost nine out of ten health apps contained code that could potentially collect user data.

What is also extremely alarming is that per Australian Data Breach statistics, the Healthcare Sector makes up almost 25% of all reported breaches clearly showing that this sector is in desperate need of further regulation as industry bodies are clearly failing to come close to adequate self-regulation.

With global Governments around the world having placed controls in place almost 20 years ago to eliminate Negative Externalities and Information Asymmetries (e.g. Sarbanes Oxley, SOC 2 audits and ISO 27001), Australia is embarrassingly now a laughing stock for its lack of cyber security maturity and action.

The Government needs to act as businesses and industries are putting everyday Australia's at risk.

Negative Externalities and Information Asymmetries can easily and cost effectively be completely eliminated through the simple adoption of an Independent audit regime such as the one currently used in the Unites states based on SAS 70 or SOC 2 audits or the current international recognised independent audit regime is ISO27001 which has also been adopted as part of the official Australian Standards. https://www.standards.org.au/standards-catalogue/sa-snz/other/it-012/as--iso-slash-iec--27001-colon-2015

The Australian Information Security Manual also has numerous controls for organisations to follow such as independent audits and reviews to be conducted on developed software code and penetration testing to be conducted every 24 months.

Small businesses can also easily fall into this regime by conducting basic independent Essential Eight Health Check audits. Vaultron conducts these audits for small business at a cost of merely $145 per device and can be completed within a couple of hours.

The misconception that being Essential Eight compliant is too difficult is in our opinion an absolute fallacy and just another excuse used by businesses to be non-compliant. We not only perform these tests regularly but also make them effective and affordable.

Also a contributor to the Negative Externalities is the Australian Privacy Principle 8 and section 16C of the Australian Privacy Act loop hole. Section 16C makes Australian suppliers liable for cyber security incidents on personal data transferred or processed overseas. However, there is a disgraceful loophole in Australian Privacy Principle 8 where a company may disclose their way out of this liability. We see companies use this loophole every day and send Australian data overseas without proper due diligence that that overseas operator is operating at the level expected and leaving Australian consumers without recourse on damages. The Australian Government should immediately move to eliminate this destructive loophole to Australian consumers.

Chapter 3: The current regulatory framework

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

The current major strength with the Australian regulatory framework is that all major relevant pieces are there already. Rather than a complete rebuild of the regulatory framework there is only a need for improving and consolidating. For example

a) There is already a Federal accepted legislation that is well understood and is able to be used to regulate this space e.g. The Australian Privacy Act 1988 including APP 11.
b) There are numerous Australian adopted Cyber Security Standards already in place.
    i. Australian Standard / ISO 27001
    ii. Australian Information Security Manual
    iii. ASD Essential Eight

The biggest limitations

a) Lack of any effective compliance and enforcement regime. The Office of Australian Information Commissioner is woefully underfunded for the enforcement and compliance requirements and follows an ineffective and substandard approach of mediation and education.

   Imagine the state of Australia's environmental and health and safety status if it took purely a mediation and education approach rather than a compliance and enforcement. Why do we act surprised when the same rigours are not applied to Cyber Security with few organisations following the standards?

   In order for any standard, code, regulatory framework to be effective it **MUST** have a rigorous and widely used enforcement and compliance regime.

b) Lack of clear and cohesive code or standard for organisations to follow depending on their Risk profile. The concept of "Reasonable" or "Principle" based is extremely poorly managed, almost impossible to enforce and open to unlimited interpretation and outrageously complicated for a non IT professional to remotely understand or apply. It is also highly inefficient, expensive and lacks clarity making it impractical for profit driven businesses and economies to implement.

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

In our opinion the current regulatory environment needs to evolve with the following key principles:

- All standards are to be mandatory – little to none should be voluntary. Voluntary standards when it comes to compliance is like asking a citizen to pay voluntary taxes. They are just not followed.
- Adopt a clear Risk Based approach to Cyber Security. This is based on the principles laid out by the Australian Cyber Security Centre and Australian Standard and International Standard AS/ISO 31000.
- Move away from the unenforceable, confusing, inefficient and frankly useless "reasonableness" model and move towards a more prescriptive standard.
- Clearly identify that Software as a Service companies have a significantly higher risk and duty of care to provide cyber security so must have their own regime.

- Develop a clear mandatory transparency disclosure regime such as a mandatory public “Trust Centre” which covers Transparency, Privacy, Cyber Security and Compliance disclosures.
- Implement a robust compliance regime such as the issuing of infringement notices / fines rather then warnings or mediation.
- Implement Cyber Security Insurance for high-risk industries to guarantee consumer protection.

Refer below diagram for summary of recommendations in practice.

We recommend a new standard regime similar to the one outlined in the below table:

Risk				Risk Elimination	Frequency of Compliance	Risk Transference / Consumer Safe Guard	Solutions	Transparancy Reporting
Type	**Maturity**	**Data Sensitivity**	**Example**	**Minimum Cyber Security Standards**	**Independent Cyber Security Checks**	**Cyber Security Insurance**	**Available in Market Today**	**Information Asymentric Disclosures**
Non Software as a Service - Regular Products and Services	Small Business <$3m turnover	Non Sensitive	Corner Store	Critical 4 of Essential Eight	Mandatory Every 24 months	Voluntary Insurance	Yes	Public Declartion of Compliance Check on Website
		Sensitive	Medical Practice	Essential Eight	Mandatory Every 24 months	Voluntary Insurance	Yes	Public Declartion of Compliance Check on Website
	Large Business >$3m turnover	Non Sensitive	Large Retailer	Choice of Customised ISO 27001 or Essential Eight	Mandatory Every 24 months	Voluntary Insurance	Yes	Public Declartion of Compliance Check on Website
		Sensitive	Financial Institution	Full ISO 27001	Mandatory Annually	Mandatory Insurance	Yes	ISO 27001 Audit Report Published on Website
	Critical Infrustructure	Both Non Sensitive / Senstive	Utilities Company	Full ISO 27001	Mandatory Annually	Mandatory Insurance	Yes	ISO 27001 Audit Report Published on Website
Software as a Service (SaaS)	Start Up < 5 years in operation	Both Non Sensitive / Senstive	Medical Software Provider	Compliant to ISM for Software Development Compliant to ISM for Crytogrophy	Mandatory Ongoing	Mandatory Insurance	Yes	Public Declartion of Compliance Check on Website
			Medical Software Provider	Prior to Launch - Independent White Box Audit	Once Off	Mandatory Insurance	Yes	Independent White Box Audit Report published on website
			Medical Software Provider	At Launch - Indepednet Penetration Testing 1	Once Off	Mandatory Insurance	Yes	Penetration Test Audit Report Published on Website
			Medical Software Provider	24 Months post launch - Independent Penetrtion Test 2	Once Off	Mandatory Insurance	Yes	Penetration Test Audit Report Published on Website
			Medical Software Provider	48 Months post launch - Independet Penetrtion Test 3	Once Off	Mandatory Insurance	Yes	Penetration Test Audit Report Published on Website
			Medical Software Provider	60 Months post Launch - Independent ISO 27001 Compliance Audit	Once Off	Mandatory Insurance	Yes	ISO 27001 Audit Report Published on Website
	Mature > 5 years in operation	Both Non Sensitive / Senstive	Medical Software Provider	Every 24 Months - Independent ISO 27001 Compliance Audit	Mandatory Every 24 months	Mandatory Insurance	Yes	ISO 27001 Audit Report Published on Website

Chapter 4: Governance standards for large businesses

Question 5: What is the best approach to strengthening corporate governance of cyber security risk? Why?

The best approach to strengthening corporate governance of cyber security risk is to

1) Implement a mandatory transparency disclosure regime founded on the principles of a "Trust Centre". These "Trust Centres" must cover all relevant disclosures covering the core topics of: Transparency, Privacy, Cyber Security and Compliance.

   By leveraging off the already established principles disclosing a Privacy Policy on an entities website as set out in the Australian Privacy Act 1988 APP 1, it is recommended new disclosures that expanded to cover the elements of Cyber Security, Transparency and Compliance including compliance with relevant Cyber Security standards such as AS/ISO 27001 and or the Australian ISM and Essential Eight.

   Examples of quality Trust Centres in the world today can be found at:

   https://www.microsoft.com/en-au/trust-center
   https://www.atlassian.com/trust
   https://www.sap.com/australia/about/trust-center.html
   https://www.cisco.com/c/en/us/about/trust-center.html

2) For publicly listed companies a mandatory disclosure is requirement is made within the companies Annual Report and governed by the Australian Corporations Act. This is similar to other required disclosures about Environmental impacts, Health and Safety and other critical risk disclosures.

3) All other business entities in Australia conduct relevant independent cyber security audits in line with their relevant risk profile. All independent audit reports are to be deemed public documents requiring publishing and disclosure on the entity's website including "White Box Audits" and "Penetration Testing" audits again inline already with transparency reporting of Australian Privacy Principle 1.

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

Providing cyber security awareness training to small and medium organisations should ensure that ongoing cyber security awareness is there to assist them in understanding their security responsibilities – in particular their mandatory responsibilities.

However, in the realm of Cyber Security, awareness training is completely useless and ineffective without the actual implementation of controls and testing that those controls are actually in place, operational and effective.

To use an analogy - Would it be acceptable if you had a virus and went to a medical provider and all they provided you was some awareness training and a policy? Of course not, the expectation would be that the medical professional would give you the awareness training, **plus** do a practical assessment or test, **plus** a treatment plan to eliminate the virus, **plus** follow up at the end of the treatment plan to recheck that the treatment plan was effective. Cyber Security for small and medium businesses is no different.

Therefore, it is critical further support is provided to help small to medium businesses to allow them to audit their systems and then implement actual controls. Due to the specialised nature of Cyber Security and IT, these audits and remediation of vulnerabilities must be done by suitably qualified organisations and not self-service.

To use another analogy – self service in Cyber Security is like asking passengers to pilot commercial airliners. Absolutely crazy and bound to end in disaster. Again Cyber Security is no different. Cyber Security is a highly specialised area requiring years of training and expertise and utilisation of specialised tools. It is not something that should be handled or dealt with by unqualified individuals who would either make their systems more insecure or worst, allow an entity to falsely think they were secure when they are not.

We don't let home handymen perform DYI electrical work, or dare I say it – Pink Batts, because of the risks – why would the Government find this acceptable for Cyber Security?

In addition, there needs to be extra funding for small to medium businesses to combat the highly likely impact of Cyber Security Investment Asymmetries. As big business has the luxury of utilising free cashflow to invest and make itself more resilient to cyber attacks, the Threat Actors are now likely to turn their attention to the more vulnerable and weaker and underinvested small to medium enterprises. Therefore, added financial support is required to increase small to medium

enterprise investment in cyber security to ensure they do not become the easy targets.

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

Yes – education and awareness need to be focused more on **auditing** of IT controls and to **identify vulnerabilities**.

In addition, a particular focus needs to be on ensuring controls are actually put in place and are tested to be operational and effective. Cyber Security is in no way a theoretical area of compliance. It requires actual physical action and senior business leaders need to know that they are responsible and accountable for any inaction.

We also recommend a change to the messaging to move away from excessive focus and awareness on Threats to focusing more on Vulnerabilities. At Vaultron we use the following messaging for business clients:

> "Focus on Controlling your Controllables. You can only control your vulnerabilities not the threats. Decisions made in reaction to threats come from a place of fear and are rarely good decisions, whereas, decisions made from well informed, data driven, vulnerability audits is from a place of being in control!"

Chapter 5: Minimum standards for personal information

Question 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?

Put simply – yes the Privacy Act would be appropriate.

In our view it is critical a cyber security code is placed under and would be effective in the Privacy Act. The reasons for this are:

1) The Privacy Act has been in effect for over 30 years and is well known and understood.
2) The Privacy Act already includes Cyber Security elements such as Australian Privacy Principle 11 and is already providing authority in this space.

3) The Privacy Act is a national Act rather than a state-based Act providing national uniform approach.
4) The Privacy Act has the ability to implement and enforce any noncompliance with the Cyber Security code.
5) Cyber Security and Privacy have a high amount of correlation and synergy as they both relate to the protection of data and information.

However, there are a number of key elements that a Cyber Security code would need evolve from the current APP 11.

- Move away from the unenforceable, confusing, inefficient and frankly frustrating "reasonableness" model and move towards a more prescriptive standard
- All standards are to be mandatory – little to none are voluntary. Voluntary standards when it comes to compliance is like asking a citizen to pay voluntary taxes or voluntary adhere to a speed limit. They are just not followed.
- Adopt a clear but easily effect Risk Based approach to Cyber Security. This is based on the principles laid out by the Australian Cyber Security Centre and Australian Standard and International Standard AS/ISO 31000.
- Clearly identify that Software as a Service companies have a significantly higher risk and duty of care to provide cyber security so must have their own regime.
- Develop a clear mandatory disclosure regime to combat Information Asymmetries such as a mandatory public "Trust Centre" which covers Transparency, Privacy, Cyber Security and Compliance disclosures.
- Implement a robust compliance regime such as the issuing of infringement notices / fines rather than warnings or mediation. Put simply if there is no enforcement there will be no compliance.
- Implement Cyber Security Insurance for high risk industries to guarantee consumer protection.

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

A risk based approach should be undertaken in line with AS/ISO 31000 and the internationally and government policy of adopting a Privacy By Design approach.

Small business must meet the Critical four of the Essential Eight mapped to the following ISM controls. Vaultron Technologies can currently do an audit of IT assets for this for $145 per asset.

Critical Four of the Essential Eight:

i. application control
ii. patching applications
iii. restricting administrative privileges
iv. patching operating systems

Software as a Service providers have a significantly higher risk and duty of care to customers so must perform and show public transparent confirmation of the following :

i. Prior to launch – Independent White Box Audit on all software code
ii. At launch – External Independent Penetration Test 1
iii. 24 months post launch – External Independent Penetration Test 2
iv. 48 Months post launch – External Independent Penetration Test 3
v. 60 months post launch – External Independent ISO 27001 audit or ISM audit

We recommend a new standard regime similar to the one outlined in the below table:

Risk				Risk Elimination	Frequency of Compliance	Risk Transference / Consumer Safe Guard	Solutions	Transparancy Reporting
Type	**Maturity**	**Data Sensitivity**	**Example**	**Minimum Cyber Security Standards**	**Independent Cyber Security Checks**	**Cyber Security Insurance**	**Available in Market Today**	**Information Asymentric Disclosures**
Non Software as a Service - Regular Products and Services	Small Business <$3m turnover	Non Sensitive	Corner Store	Critical 4 of Essential Eight	Mandatory Every 24 months	Voluntary Insurance	Yes	Public Declartion of Compliance Check on Website
		Sensitive	Medical Practice	Essential Eight	Mandatory Every 24 months	Voluntary Insurance	Yes	Public Declartion of Compliance Check on Website
	Large Business >$3m turnover	Non Sensitive	Large Retailer	Choice of Customised ISO 27001 or Essential Eight	Mandatory Every 24 months	Voluntary Insurance	Yes	Public Declartion of Compliance Check on Website
		Sensitive	Financial Institution	Full ISO 27001	Mandatory Annually	Mandatory Insurance	Yes	ISO 27001 Audit Report Published on Website
	Critical Infrustructure	Both Non Sensitive / Senstive	Utilities Company	Full ISO 27001	Mandatory Annually	Mandatory Insurance	Yes	ISO 27001 Audit Report Published on Website
Software as a Service (SaaS)	Start Up < 5 years in operation	Both Non Sensitive / Senstive	Medical Software Provider	Compliant to ISM for Software Development Compliant to ISM for Crytogrophy	Mandatory Ongoing	Mandatory Insurance	Yes	Public Declartion of Compliance Check on Website
			Medical Software Provider	Prior to Launch - Independent White Box Audit	Once Off	Mandatory Insurance	Yes	Independent White Box Audit Report published on website
			Medical Software Provider	At Launch - Indepednet Penetration Testing 1	Once Off	Mandatory Insurance	Yes	Penetration Test Audit Report Published on Website
			Medical Software Provider	24 Months post launch - Independent Penetrtion Test 2	Once Off	Mandatory Insurance	Yes	Penetration Test Audit Report Published on Website
			Medical Software Provider	48 Months post launch - Independet Penetrtion Test 3	Once Off	Mandatory Insurance	Yes	Penetration Test Audit Report Published on Website
			Medical Software Provider	60 Months post Launch - Independent ISO 27001 Compliance Audit	Once Off	Mandatory Insurance	Yes	ISO 27001 Audit Report Published on Website
	Mature > 5 years in operation	Both Non Sensitive / Senstive	Medical Software Provider	Every 24 Months - Independent ISO 27001 Compliance Audit	Mandatory Every 24 months	Mandatory Insurance	Yes	ISO 27001 Audit Report Published on Website

Question 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?

The following sectors and types of data should be covered by a code under the Privacy Act to best achieve outcomes:

- Any industry that typically deals with extensive sensitive data the breach of which can cause harm – e.g. Healthcare sector and Financial sector.
- The Software as a Service industry e.g. Cloud Based Software Providers
- Any mobile phone / tablet apps that collect or deal with sensitive data
- Critical Infrastructure

Chapter 8: Responsible disclosure policies

Question 22: Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

Voluntary guidance has proven time and time again to be ignored and simply not followed.

Disclosure responsibilities must be mandatory. There are massive instances of unethical, non-compliant and abusive corporations and software companies which is due to the disclosure policies being voluntary. To be effective they must be mandatory.

In addition, the Australian Judicial systems (i.e courts) have already ruled that any voluntary standards, particularly those that can cause harm to others, will be treated by the courts as if they are mandatory regardless.

This point is best made clear in the recent Queensland Dreamworld Coroner's report at paragraph 997:

> *It was agreed by the experts, and became obvious during the inquest hearing, that best practice for the TRRR was not followed by Dreamworld,* ***particularly in relation to compliance with introduced Australian Standards designed to ensure the safety of devices. Whether these requirements are mandatory or not is largely irrelevant. Those Standards are the minimum practice that is required. It is the responsibility of those that own and operate high risk plant to ensure that***

the most up to date safety standards, risks and requirements known to the industry are considered and instituted if possible, to ensure the safety of staff
and patrons.

This was certainly not the case in relation to the conduct of Dreamworld as to the management, modification and maintenance of the TRRR. ***Dr Gilmore stated during the expert conclave that should 'best practice' not be followed with respect to safety standards, an owner would do so at their own peril.***

Justice James McDougall – Court of Queensland

It is our view that is clear from this court that when it comes to compliance with Australian Standards that are designed to ensure the safety of devices (including the Cyber Security safety of those devices) then those that own and operate those devices must meet those standards. Attempting to argue that they are not mandatory would be irrelevant. Having a Government organisation declare them to be voluntary would only add unnecessary confusion and create a legal nightmare.

Therefore, to avoid large amounts of negligence lawsuits and embarrassment to the Government, it is strongly advised the Government makes all standards on Cyber Security mandatory.

Any disclosure requirements must also align with Australian Privacy Act of APP1 and also 2A(d) of Privacy Act.

We also recommend the following controls within the Australian Information Security Manual are also referred to. These controls make it clear that all reasonable disclosure requirements must allow a user to identify a "High Risk" supplier so that an easy and clear decision can be made to stop using High Risk cyber suppliers.

Security Control: 1452;Updated: Dec-20;
Before obtaining components and services relevant to the security of systems, a review of suppliers and service providers (including their country of origin) is performed to assess the potential increase to systems' security risk profile, including by identifying those that are high risk.

Security Control: 1567; Revision: 1; Updated: Dec-20;
Suppliers and service providers identified as high risk are not used.

Security Control: 1632; Updated: Dec-20;
Services relevant to the security of systems are chosen from suppliers and service providers that have a strong track record of transparency and maintaining the security of their own systems, services and cyber supply chains.

We strongly recommend the use and implementation of "Trust Centres" that easily share the disclosure of information. Example of Trust Centres can be found at:

https://www.microsoft.com/en-au/trust-center
https://www.atlassian.com/trust
https://www.sap.com/australia/about/trust-center.html
https://www.cisco.com/c/en/us/about/trust-center.html

It is also recommended that the Australian Government also introduce a Wall of Shame that is similar in approach to the United States HIPAA security breaches through the Office of Civil Rights.

In 2009, the USA HIPAA laws which cover Cyber Security for sensitive data was amended by the HITECH Act. The HITECH Act requires the Secretary of the Department of Health and Human Services to post, on its website, a list of breaches of unsecured protected health information affecting 500 or more individuals. The website is known as the Office for Civil Rights (OCR) portal. The breach list has a nickname in the healthcare compliance industry: The HIPAA Wall of Shame. The reason behind the publication of breach information is to inform the public of data breaches and to provide some detail on what took place giving great transparency and disclosure to the public since 2009.
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

The HIPAA Wall of Shame displays all breaches currently under investigation within the last 24 months. This means that any breach that is submitted, will remain on the HIPAA Wall of Shame for two whole years. The HIPAA Wall of Shame lists breaches by date of submission. For each breach, the following information is provided:

- The name and type of the covered entity
- The covered entity or business associate's state ;
- How many individuals were affected by the breach;
- When the breach was reported;
- The type of breach (i.e., hacking, theft, etc.); and
- The location of the breached information (e.g., email, paper, network server)

Older breaches – those not currently under investigation within the last 24 months – are archived and can be publicly viewed. The archive includes breach reports older than 24 months old, as well as all breaches reported since 2009 for which investigations have been resolved.

This "Wall of Shame" acts as a huge **deterrent or preventative measure** for organisations not to breach the required cyber security regulations of the USA. It is

recommended having such a public disclosure in Australia would encourage preventative compliance vs relying solely on a costly and time consuming reactive court based compliance regime.

Chapter 9: Health checks for small businesses

Question 23: Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

Although a health check program would improve Australia's cyber security, a basic health check is way too simple, ineffective and often performed by unqualified professionals.

Also health checks should not ever be done or performed via self assessments. Self assessments are not only unethical and breach the Familiarity Threat principles but often lead to the false sense of security by uneducated or untrained operators.

An IT Health Check (ITHC) must provide **an independent** assessment of an organisation's cyber security.

To use an analogy: We do not ask passengers to pilot their own commercial airliner – why? Because they are unqualified, do not possess the training and understanding and do not have the relevant experience. To let passengers fly a plane would likely result in that plane being unsafe and crash.

So why would we think it is appropriate for a business owner, unqualified and inexperienced in the highly specialised area of IT cyber security to self-assess themselves and implement remediation strategies? This would likely result in the business being unsafe and have a cyber security incident.

Any healthcheck / audit must be completed by qualified professionals and involve actual testing of assets with the use of Computer Assisted Auditing Techniques (CAATs).

At Vaultron we conduct such tests from as little as $145 per computer – extremely cost effective, completed by qualified and knowledgeable individuals and completed in as little as two hours using computers and Artificial Intelligence to do the bulk of the leg work.

The specialised testing tools we use look for over 50,000 individual vulnerabilities on a single IT asset. No human being is ever capable of performing or knowing all these tests. Only a computer or specialised software is capable of performing these tests.

The approach and scope of an IT Health Check engagement in our opinion must include the following elements:

- Health checks must be mandatory for those dealing with sensitive data.
- IT systems vulnerability assessment – can only be performed using specialised software
- Website vulnerability assessment – can only be performed using specialised software
- Internal Process and Policy review – can be performed using questionnaires. Incapable of being performed using computers
- Cyber Supply Chain Due Diligence e.g. Software as a Service and Internet of Things. These due diligence assessments identify High Risk suppliers to the business.

Once identified, all vulnerabilities are presented in a report that provides clear, measurable results along with effective risk remediation solutions.

Question 24: Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

Yes a small business would benefit commercially for a health check program:

1) Prevention and cost avoidance is far cheaper than the cost reaction to a cyber security incident. Through prevention the following costs can be avoided:
    - Class Action Lawsuits
    - Privacy penalties and fines
    - Damage to brand and reputation
    - Loss of consumer confidence and trust e.g. loss of business opportunities
    - Loss of professional accreditation and licence to operate if dealing with sensitive data or systems
    - Loss of Government contracts or ability to deal with Government organisations

2) Reduced cyber security insurance premiums as health checks can provide assurance of reduced risk therefore premiums should be lower. These health checks could also be used by Insurance Actuaries to calculate risk and provide

cost effect tailored cyber security insurance pricing directly associated with known risk.

3) We at Vaultron can perform a fully conformant small business Essential Eight Health Check audit for $145 and takes approx. 2 hrs. making this extremely affordable.

There are a few additional ways to encourage small business to participate in a health check program:

1) IT MUST BE MANDATORY COMPLIANCE. If it is not mandatory compliance no small business will ever complete it. They will not do anything they do not have to do. We know this from extensive experience and dealing with thousands of small businesses on a daily basis.

2) It must also be made a mandatory compliance requirement in order to gain Cyber Security Insurance. No health check – no insurance. A Health Check must be performed and attested to annually.

   This approach will be great for the economy and cost of businesses. By drastically reducing Cyber Security risk, insurance premiums would also be reduced matching the fall in risk. This would make Cyber Security Insurance significantly more affordable to small business and also provide an added protection to consumers in the event of an unforeseen or “Zero Day” breach.

3) If no health check performed and a data breach occurs, then penalties and compensation would attract a mandatory 10 times multiple increase to account for the negligence and lack of taking reasonable steps to appropriately protect data and systems. This approach is currently implemented and working already in the Commonwealth’s “Fair Work Act”. If an employer deliberately or negligently acts outside of its responsibilities, e.g. fails to pay wages per awards, then the penalties are significantly times higher.

Question 25: If there anything else we should consider in the design of a health check program?

Health Check’s must be done with the following audit approach

1) Full Essential Eight computer assisted auditing technique audit of target assets such as laptops, macbooks, desktops, and servers. Vaultron currently offers

this service for $145 per asset using software used by 50% of the fortune 500 including banks, financial institutions, healthcare and governments. This includes a significant deficiency report. This is easily affordable to small business and takes less than 2 hrs to complete. **Please attached an example extract from one of our reports for a small business.**

2) Must consider sub-contractors and the relationship – making it very clear who is responsible for Cyber Security and who must do a health check. We so often run into issues with a Principle arguing that it is the sub contractors responsibility for cyber security but the sub contractor turning and saying no it is the principle contractor's

3) Due diligence of cyber supply chain suppliers must also be completed.

4) Website developers must provide a vulnerability scan and report for all new websites developed attesting that the work they have performed is at the quality level required.

5) Health Check / Audit / Assessment / Review must be performed by qualified Cyber Security auditors

6) Business Principles e.g. directors, sole traders, partners or trustees must make a statement in their privacy policy that they have conducted an independent health check audit and can attest that they have taken all reasonable steps to remediate gaps.

7) Business Principles e.g. directors, sole traders, partners or trustees must publish in their Privacy Policy a list of their supply chain sub processors including name, country, core function of service and declaration that they have conducted a due diligence and attest that that the sub processor is deemed to not be high risk.

Chapter 10: Clear legal remedies for consumers

Question 26 What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

The Australian Consumer law is predominately designed for end user consumers and does not cover business to business transactions such as those used in a cyber supply chain.

Supply Chain Example: Consumer →Retailer→Software as a Service Provider →Cloud Hosting Service Provider.

What is covered under the Australian Consumer Law is the first relationship between the Consumer and Retailer but there is no protection under the Consumer Law between the Retailer and the Cyber supply chain e.g. SasS provider or Cloud Host.

This creates a large gap in the Consumer Law as it specifically excludes the Business-to-Business supply chain.

We see this weakness on a daily basis as the 100,000 Healthcare Service providers are not able to access these protections from dodgy Software as a Service providers such e.g. Practice Management Software. This is because it is a Business to Business transaction rather then a personal transaction.

The Consumer Law does not adequately deal with the extensive Cyber supply chains.

The most major issue we at Vaultron see is Business to Business Software as a Service providers making misleading, deceptive and unconscionable statements about their companies Cyber Security posture or controls. As this is a Business to Business relationship there is limited remedies.

It would be extremely interesting on how the application of Part2-2 – Unconscionable Conduct of the Consumer Law would apply to the Cyber Security.

At section 21 (4) (a) (b) of the Consumer Law is states in regards to the protections of Unconscionable Conduct:

> *It is the intention of the Parliament that:*
>
> *(a) this section is not limited by the unwritten law relating to unconscionable conduct; and*
>
> *(b) this section is capable of applying to a system of conduct or pattern of behaviour, whether or not a particular individual is identified as having been disadvantaged by the conduct or behaviour;*

It is challenged that Part2-2 – Unconscionable Conduct of the consumer law could potentially apply to traders that deliberately fail to adequately provide Cyber Security when the consumer would expect it to do so.

Question 27: Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

Significant attention and action from the Government must be made to compliance with the Privacy Act and Cyber Security elements.

In our opinion and experience, the compliance actions by the Office of the Australian Information Commissioner (OAIC) are almost useless to non-existent. Massive changes are required to the compliance regimes to allow adequate consumer protections. It is strongly recommended to move towards an infringement penalty regime and abandon the ineffective and resource wasting consultation and mediation type scheme currently in place.

Similar to the Fair Work Act – the Government could look to implement Small Claims Tribunal clauses into the Privacy Act 1988 allowing consumers to access quick and affordable consumer protections. It is also noted that the Australian Consumer Law already allows for consumers to access Small Claims Tribunals.

The Government should also consider the consequences of Misleading and Deceptive Conduct and Unconscionable Conduct outlined in the Australian Consumer Law. We see on a daily basis unethical Australian software companies making false, misleading or deceptive comments about their Cyber Security. For example – claiming they are using best practice encryption however when checked they are actually using outdated / obsolete encryption. It is recommended the Government make sure these companies are held to account for their false and misleading statements.

The Government may also wish to consider giving clear guidance through ASIC for Directors to have a fiduciary duty to maintain adequate Cyber Security for their organisation.

A significant review of the Health Insurance Act 1973 (Medicare Act) of is also required to ensure compliance with section 82.

Currently the Australian Government spends approximately $36 billion on Medicare supplements with the vast majority of that money being allocated (directly or indirectly) to uncompliant and Cyber unsafe Medical Practices or Medical Software

Providers. Ultimately this is causing the Australian Government to reward and incentivise a whole industry with billions and billions of taxpayers money to actively be Cyber Security unsafe, uncompliant with little interest in becoming compliant or resilient.

Chapter 11: Other issues

Question 28: What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?

Quantum Safe Economy – Preparing Australia for the Quantum World

The Australian economy and wider society depend on increasingly advanced technologies. At their core, these digital technologies are governed by the inescapable laws of physics, economics, social norms and advancement.

A new wave of technologies now promises to harness the quantum effects such as superposition and entanglement. Quantum technologies are set to provide much improved capabilities in timing, sensing and measurement, imaging, computing and simulation, and communications. The new technologies, as well as the businesses and services that develop around them, are expected to affect many major sectors including healthcare, defence, aerospace, transport, civil engineering, telecommunications, finance and information technology.

But while this new Quantum Age brings excitement and revolutionary advancement it also brings exponentially unheard-of risk and opportunity for use for destruction and harm not seen since the invention of nuclear energy. **Due to its unique and revolutionary processing, Quantum computing can break and make all current traditional cryptography and cyber security defences useless and obsolete.**

Therefore, there is a need for Australia to begin to act now and start the forward process of developing new and unique way on how to make the Australian economy and society a Quantum Safe Economy.

The United Kingdom has already begun this process by introducing the UK National Quantum Technology Programme https://uknqt.ukri.org/. and other initiatives to make the UK Quantum Safe.

A great Australian based article can be found at https://www.aspi.org.au/report/australian-strategy-quantum-revolution that is written by the Australian Strategic Policy Institute.

We strongly recommend and encourage the Australian Government to implement a new Australian Quantum Safe Cyber Security department that researches and recommends new policies, practices and legislation that will allow Australia to not only embrace the Quantum advances but also protects the economy and society as well. With great Quantum power also brings great responsibility.

Mandatory public disclosure of Cyber Security Supply Chain for industries that deal with sensitive data e.g. Healthcare / Finance

Ask yourself – do you know what practice management software your doctor use? Do you know whether that software is reputable? Do you know whether that software is compliant to all privacy and cyber security requirements for your sensitive healthcare data?

The vast majority of Australian citizens would say no as there is little transparency from organisations that deal with sensitive data.

Just like other industries e.g. food and agriculture, the supply chain providence and transparency is becoming critical for consumers to make informed decisions. We see how this should be no different for Cyber Security supply chains.

It is therefore recommended a mandatory disclosure regime is implemented by the Government for all organisations that predominately deal with sensitive data e.g. Healthcare / Finance that they publicly disclose the supply chain e.g. Software as a Service providers. This will allow consumers to make informed decisions about utilising that supplier but also allow a sense of public awareness of the use of software companies that are not at the standards expected.

This is currently already performed around the world such as in the European GDPR where they mandate a disclosure of an organisations supply chain / sub processors in the Privacy Policy including the countries that those suppliers are associated with.

How to deal with the Small Mobile Devices and Healthcare Paradox

There currently exists a Paradox between Healthcare and Small Mobile Device Cyber Security.

Healthcare is rapidly facing and embracing digital transformation. It is now highly accepted that the front door to the healthcare system is no longer the front door of

the General Practice Surgery or Hospital Emergency department – it is the patient's mobile phone or mobile device. These devices and technologies are seen to revolutionise and improve patient's health as never has been seen before.

However, it is also well accepted and understood in the Cyber Security realm that mobile phones and mobile devices are the single most unsecure and highly hackable devices ever invented and should not in any way or form be used in or with highly sensitive data such as Healthcare data. This in the technical Cyber Security arena is called "Excessive Inherent Cyber Security Risk".

So, when combining Healthcare and Small Mobile Devices this amounts to a paradox, the Mobile Healthcare Device Paradox. This is because this combination not only revolutionises Australia's healthcare system welfare of its citizens but also at the same time totally destroys the data integrity, privacy and reliability of the patient's healthcare cyber security.

In addition, it can be argued by some, that software and IT developers are prioritising their own commercial interest by unethically and immorally using desperate patients healthcare benefits against the cost of those patients' data integrity and security.

It is therefore recommended a detailed and specific policy is implemented by the Australian Government on how mobile devices such as mobile phones, tablets and their associated mobile apps can be utilised to handle sensitive data industries such as Healthcare and how patient data security and rights can be protected particularly if those patients are vulnerable to exploitation due to their desperate health situations.

Take a United States of America Section 404 of the Sarbanes Oxley Act approach to Cyber Security for Publicly Listed Companies and Critical Infrastructure.

The Sarbanes-Oxley Act of 2002, often simply called SOX, is U.S. law meant to protect stakeholders from deficient or material weak internal controls by corporations. Sarbanes-Oxley was enacted after several major scandals in the early 2000's perpetrated by companies such as Enron, Tyco, and WorldCom.

SOX Section 404 – Management Assessment of Internal Controls:

All USA listed company's annual financial reports must include an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these SOX controls also must be reported. In addition, registered external auditors must attest to the accuracy of the company management's assertion that internal controls are in place, operational and effective.

This Section 404 has a significant impact on USA listed companies Cyber Security as it would be covered extensively in the "internal control" attesting that the controls are in place, operational and effective.

It is recommended a similar style approach is made to Australian Listed companies regulating the testing and disclosure of their Cyber Security internal controls giving all stakeholders of listed companies comfort that all reasonable measures are in place, operational and are effective.

This would in effect make Cyber Security for ASX listed companies a required "licence to operate".

<u>How to deal with new and innovative software and technology companies that have a monopoly or are first to the market – Cyber Security Social Responsibility.</u>

With technology and digital transformation comes great innovation and advancement. But with this innovation and advancement comes also monopolisation and protection of intellectual property. This amounts to a significant imbalance of Cyber Security and Data Security for consumers. It also does not incentivise newly innovative organisations to act ethically or in the interest of consumers data security. This has a tendency to lead consumers down a path that in order to access this great innovation it comes at a cost of their data and cyber security of data. This is due to the natural lack of competition there is no viable other alternatives.

To use an analogy – a newly innovative organisation in the mining industry, before it can even think about beginning mining, it would have to work through numerous environmental and health and safety laws and regulations regardless of the benefits of the innovation. Without that appropriate Environmental compliance, the innovation would be deemed socially unacceptable and not meeting its basic "licence to operate".

Put simply – innovation and advancement should not come at the cost of social responsibility.

However the same rigours we place on other areas of social responsibility such as environmental laws, health and safety laws, employment laws, consumer laws do not seem to be applied to personal data and Cyber Security. It is therefore recommended that the Government implement policies to bring Cyber Security in line with other Social Responsibility laws.

Illegal advertising and unlawful Cyber Security Insurance – Corporations Act

There is a wide lack of understanding or misconception that Cyber Security Insurance is a way to mitigate the cyber risk. Also that Cyber Security Insurance can totally replace Cyber Security preventive controls. This is false. Cyber Security Insurance is **risk transference** and is not risk reduction.

The risk to the consumer remains exactly the same regardless of whether there is insurance or not. Cyber Security Insurance does not stop or prevent an incident or damage occurring. Also, the damage that can be done by cyber incidents, such as reputational damage, can rarely ever be undone, repaired or adequately compensated financially.

In addition, it is widely held that the increased use of cyber insurance over the last decade has been an unfortunate stimulant to ransomware gangs - it has encouraged more attacks as insured victims are often quite willing to rapidly pull the trigger on ransom payments knowing that they will be reimbursed by insurance.

What is extremely concerning is the wide advertising by insurance companies that Cyber Security Insurance is a way to avoid cyber security controls and simply mitigate the risk through insurance. Also, these insurance companies also tend to advertise that their insurance also covers the Government fines and penalties – which is unlawful under the Corporations Act. To use an analogy – this is like a chemical manufacturer being able to extensively pollute the environment because they have some kind environmental insurance that covers Government fines and penalties. Or a taxi driver being able to ignore all speeding regulations because they have an insurance that covers speeding fines. This is immoral, unethical and in our opinion unlawful.

It is highly recommended that the Government puts very clear guidelines and policies in place for Cyber Security Insurance vendors to ensure they advertise and develop products that adequately meet the Australian public's expectations with extensive and harsh penalties for breaches of those rules.

The removal of the overseas liability exemption of the Australian Privacy Principle 8.2(b)

Australian Privacy Principle 8.2 (b) and section 16C of the Australian Privacy Act contain a loophole.

Section 16C makes Australian suppliers liable for cyber security incidents on personal data transferred or processed overseas. However, there is a disgraceful loophole in Australian Privacy Principle 8.2(b) where a company may disclose their way out of this cyber security supply chain liability.

We constantly see companies use this loophole every day and send Australian data overseas without proper due diligence that that overseas operator is operating at the level expected and leaving Australian consumers without recourse on damages. The Australian Government should immediately move to eliminate this destructive loophole to Australian consumers.

Your Sincerely

Ash Runham – Director

Vaultron Technology