Who is responsible for better cybersecurity?

Image from my lecturing in Cybersecurity Training

Executive summary

I have worked within the government for many years in the program delivery of innovation policy and would make an individual submission. The cybersecurity environment is fast changing and it is important for any organisation to be able to quickly scan this environment for both opportunities and threats. I have seen how policy needs to be translated into programs and good policy good programs are the preferred solutions. These programs sometimes create good opportunities to protect against threats. My role with the government was to keep an eye out for these opportunities and to alert companies of these opportunities. Some opportunities were real and others offered false hope.

I then moved into teaching business and IT students at TAFE and university level the systems based units, such as WHS, EMS. These were based on a simple loop PDCA to improve the current position to meet the vision of the organisation. I taught future CEOs how to spot these opportunities. I then moved more into cybersecurity both teaching and writing articles about this environment and would like to present some individual observations on how to better improve the cybersecurity of businesses based on this diverse background.

The examples will describe the Australian situation but can be adjusted to suit other countries. The why is the need for better cybersecurity, the what is better training and the how is to use inter discipline Committees. In the conclusion I mention Images of Organisation which shows the theory behind Committees.. One point is that the Australian Industrial Research & Development Board (I was an Assistant Director with DIST) taught me it that Boards have different points of view. Our Committees which in turn formed the Board each had CEOs from industry, each expert in their field with their individual approaches to opportunities. Companies work the same way with cybersecurity Committees reporting to the Board. My recommendation is that these Committees have legal, technical, marketing etc have the expertise to navigate the cybersecurity maelstroms if they have the correct training. The above image was part of a cybersecurity unit where I used the image of an umbrella to show protection. Boards must understand if their umbrella is able to protect the organisation from threats.

Background The need for improvements in cybersecurity.

The Strengthening Australia Cybersecurity Regulations and Incentives report is looking at possible solutions and has various comment points to improve policy.

The focus of the report is seeing where there are gaps in the frameworks. To make matters easier I have addressed the following two questions.

Seeking your views

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

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

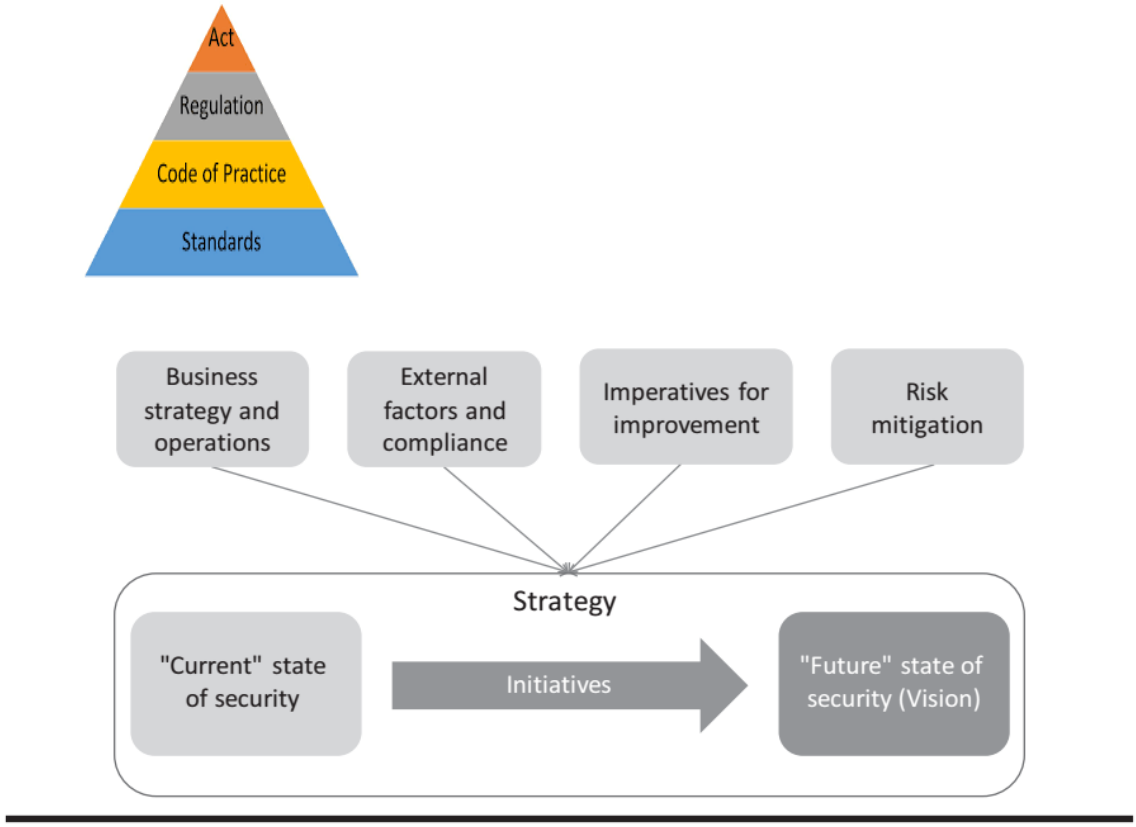
Strengthening Australia's cyber security regulations and incentives

An initiative of Australia's Cyber Security Strategy 2020 p16

(https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf)

The situation

The program which I would like to see implemented is training in the field of cybersecurity management. This is the Board room level of business. A separate article on cybersecurity management is available from myself. It was published in Hakin magazine in 2021. The diagrams below show the process of this transformation in the Boardroom. For strategy to be successful the external factors (attractiveness for an attack) and compliance (acts, regulations, Codes of practice and standards) must be understood.



Information Security Governance Andrej Volchkov CRC Press p76

Acts, regulations, codes of practice and standards.

I taught Workplace Health & Safety (WHS) and Environmental Management Systems (EMS) at TAFE for many years using a CMS to show how the system side of these regulations work. They use a Plan Do Check Act loop to ensure improvement by feedback (system component). Under Australian Law the WHS has an Act while the EMS does not have any legal compliance requirements in Australia. In the WHS field there is a foreseeability concept. If a common man (or woman) can see the outcomes then the company is liable for damages. The EMS does not have the same legal standing. If there is an environmental impact then there is less liability.

An EMS is a voluntary management tool, which aims at the improvement of an organization's environmental performance through an integrated and systematic approach to dealing with environmental issues. Firms and other types of organizations have been implementing environmental management systems for more than two decades. They may design their own EMS or alternatively, may follow the guidelines laid down by third parties, such as the International Standard Organization's ISO14001 standard or the European Union's EMAS regulation. In 2015 more than 300 000 companies operated environmental management systems certified according to the ISO14001 standard, while more than 4400 firms followed the principles of EMAS

Environmental Management Systems—History and New Tendencies. Available from: https://www.researchgate.net/publication/315849235_Environmental_Management_Systems-History_and_New_Tendencies [accessed Jul 25 2021].

In 1993 the European Commission produced a regulation on environmental management and auditing with the Eco-Management and Audit Regulation (1836/93/EC). This included the Eco-Management and Audit Scheme (EMAS).

The point which I would make is that Acts are the top of the compliance triangle, then regulation, then code of practice and lastly at the bottom of the compliance stack, standards. There are various cybersecurity codes of practices (frameworks) such as NIST, Mitre. These are adopted by various companies but again no agreement. The WHS is a must know while the EMS was a nice to know situation.

The Australian situation for laws and regulations regarding cybersecurity is well covered in Australia: Cybersecurity Laws and Regulations

https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia.

This should be a textbook for training in the legal position for cybersecurity management.

Unauthorised access is the main area taught in cybersecurity as pen testing requires clear approval before any test. There are various strategies that you can use to protect an organisation.

So, for a strategy I would first look at my defence measures which are legal.

3. Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There are presently no laws in Australia which prohibit the use of a Beacon or near-field communication technology.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There are presently no laws in Australia which prohibit the use of Honeypot technology or similar autonomous deception measures.

Honeypots are allowed. This gives me a clear legal strategy. So as part of my defence strategy in cybersecurity management I need to know my legal position.

Push or pull? Carrot or Stick?

Do you push with Acts or pull with their need to protect data? Do you fine the directors for non compliance – the stick or give carrots in the form of incentives such as a tax incentive for money allocated to cybersecurity? The reason that business is less protected than it should be is that cybersecurity management is not considered as a field in itself. There are three motivations which hackers use to attack, fear, greed and sex. These are powerful and social engineering is getting better and better. There was a recent case where the university cybersecurity sent out a phishing email offering vaccination against Covid. The university had a phishing response around 40-50

Just before 3pm, UofA Chief Operating Officer, Bruce Lines, formally apologised to staff for the email, calling it 'totally inappropriate and in the worst possible taste'. Lines pinned the blame on the IT Department, which 'generated and approved' the exercise.

'While these simulated exercises are a vital part of the University's security activities, more attention must — and will — be given to the subjects of future emails.'

'I offer my deepest apologies to all staff, and to the Adelaide Unicare practices who have been needlessly fielding calls from staff about this issue today.'% but drew a heated response from the their other directors.

https://onditmagazine.medium.com/psych-uni-staff-receive-bizarre-fake-covid-vaccine-email-b85924dade9f

Who was right who was wrong depends on your image of the organisation. Training always works best with actual case studies.

Held to Ransom by Beverley Head was published in the Company Directors magazine in March 2020 (https://aicd.companydirectors.com.au/membership/company-director-magazine/2020-back-editions/march/quick-board-response-could-save-your-organisation-during-a-ransomware-attack). This details the YMCA NSW ransomware attack. The Lessons for the Board Address cybersecurity explicitly in relevant board committees. The Board members can do a cyber awareness course at http://aicd.companydirectors.com.au/education/courses-for-the-director/online/online-education/the-boards-role-in-cyber.

The need for cyber security insurance. The above article discuses how YMCA took out cyber insurance in 2019. Is this a necessary part of business?

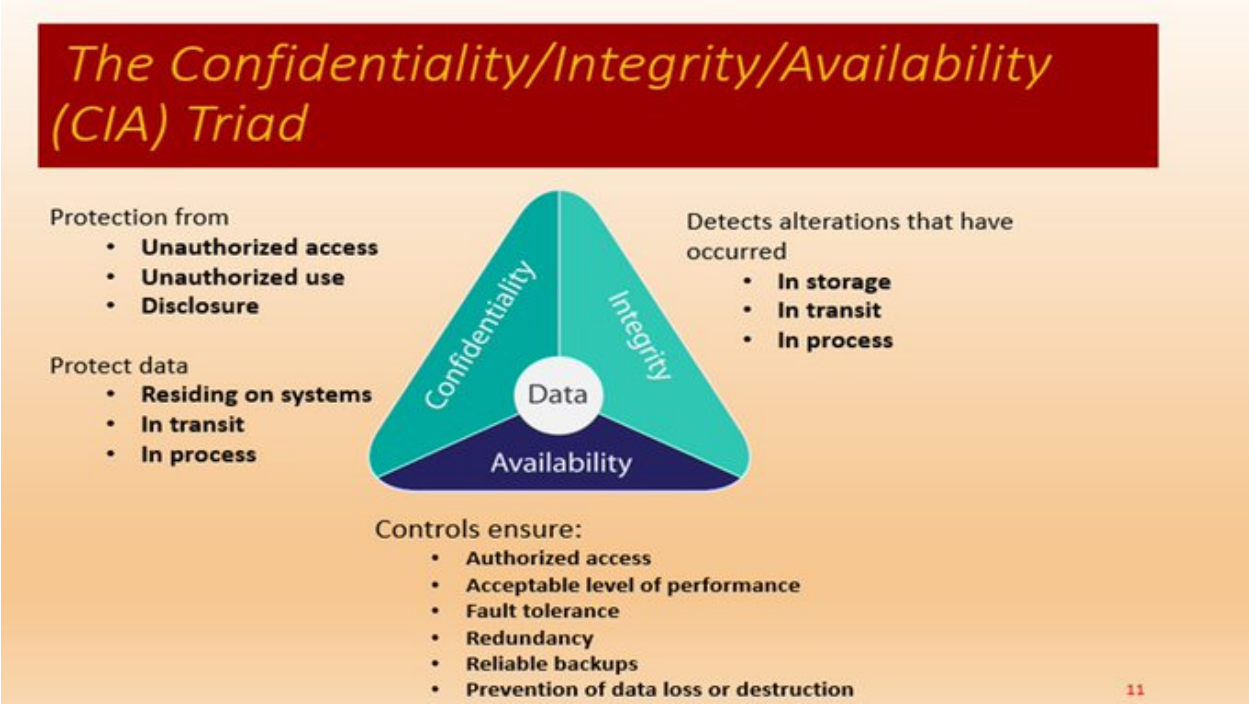
There is little research that documents whether the threat of data security litigation has actually encouraged companies to adopt stronger cybersecurity protections, and companies increasingly are purchasing insurance policies that cover judgments or settlements in data security litigation. Some critics argue that cyber-insurance creates a moral hazard that reduces any incentives that a company might have to invest in cybersecurity.

https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/

The above was taken from a great article Defining Cybersecurity Law by Jeff Kosseff which reviews the arguments for punitive action against directors.

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

The current regulations are often concerned about the C in CIA (Confidentiality, Integrity and Availability).



https://twitter.com/glenn_axelrod/status/1090449316706160643

In short, the existing cybersecurity framework focuses largely on protecting the confidentiality of information for the purposes of protecting individual privacy. However, the laws could be improved to focus more other aspects, including:

(1) integrity and availability;

(2) protecting systems and networks; and

(3) promoting economic and national security interests. Moreover, cybersecurity law could benefit from a more forward-looking perspective with the goal of preventing future incidents, rather than the current focus on penalizing companies for failing to safeguard against previous attacks.

https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/

Sony had an attack which is reviewed against the CIA framework.

Another way of looking at cybersecurity is the Parkerian Hexad. The reason is that attacks based on undiscovered leaks in the code (The case of the Panama Papers is a classic) show the need for a new model.

Parker describes the CIA model as simple and easily and quickly explained to management, information owners and users, and legislative assistants that write our laws. However, we

Parkerian Hexad

are dangerously deceiving them by its simplicity, errors, and deficiencies. The CIA model is simply too simple a concept to secure today's complex networks and it may leave environments susceptible to threats that they are not prepared to handle. Parker aimed to expand the view of security and include people more into the realm of information security.

https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

I would like to support this expansion of the legal framework that is based on the CIA framework to the Hexad framework. The concept of possession of IP might be a good place to start. Breach of confidentiality requires three elements to be proved, not in the public domain, acquired whilst in the course of employment and treated as confidential. An example is a Defence contractor for submarines. The contractor lost owner's IP (design specifications of submarine) as it did not have a secure IT environment. Possession has been shared without consent.

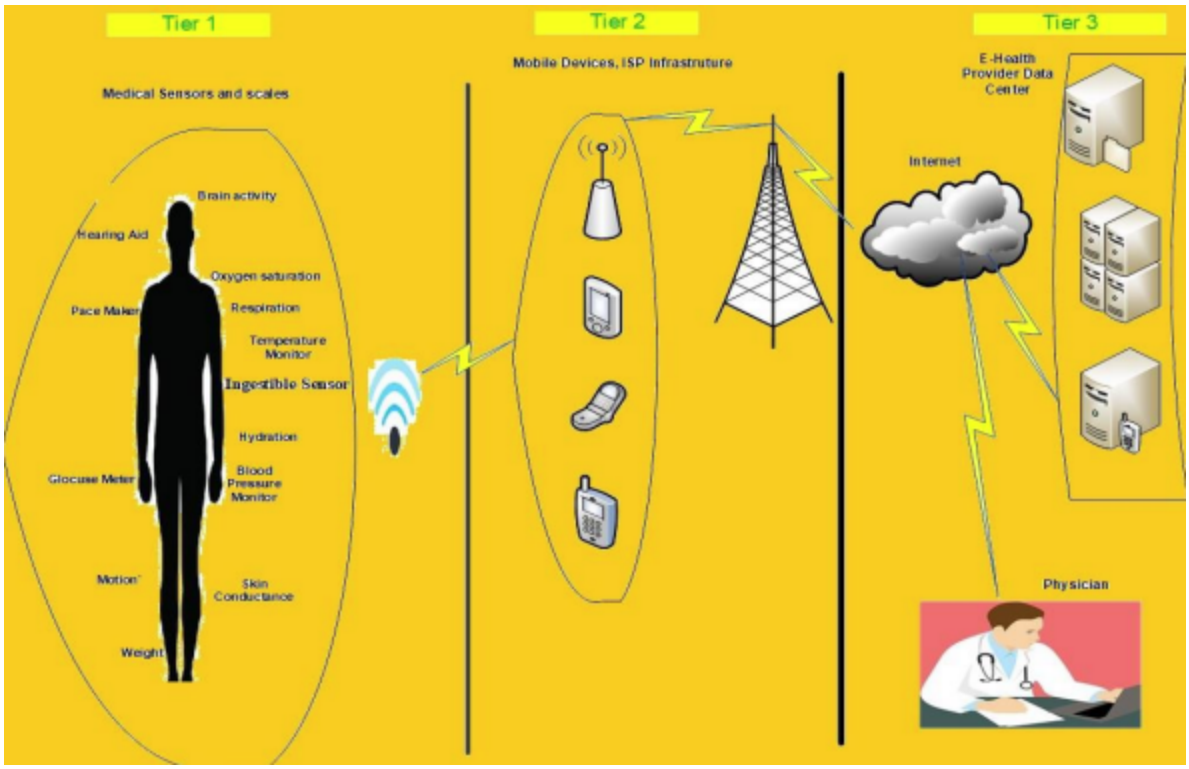
The area of cybersecurity medical IoT was an area of interest to one of my fellow lecturers.

This is from this area of research for medical sensors providing medical data.

The CIA Triad composed only of the three elements: Confidentiality, Integrity and Availability, but does not adequately address and satisfy the requirements of ownership and continuity of the medical records and health care systems. Therefore, the Parkerian Hexad model is a more suitable model than the CIA triad, since the Parkerian Hexad model adds three extra elements to the CIA triad: Possession or Control, Authenticity, and Utility

The rational of using Parkerian Hexad model as central structure of this study is that its attributes cannot be broken down into further ingredient; and not overlap with each other

https://www.researchgate.net/profile/Q-Kharma/publication/334184776_Secure_Medical_Internet_of_Things_Framework_based_on_Parkerian_Hexad_Model/links/5df37894a6fdcc28371d8e39/Secure-Medical-Internet-of-Things-Framework-based-on-Parkerian-Hexad-Model.pdf?origin=publication_detail



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

The current regulatory environment is not well known. The problem is that it needs to combine cyber security understanding with compliance to understand risks. I have taught Business Continuity, Disaster Recovery Planning at TAFE level. I have not seen training in business at university level which cover these topics. The clarity of the message is not clear. The nebulous

nature of what is more important from a regulatory viewpoint, loss of data or loss of sole possession of the data. Kevin Mitnick once defended his actions making a copy of IP is not theft as there has been no loss to the owner, they still have their copy.

Conclusion

The article Defining Cybersecurity Law by Jeff Kosseff has many good points:

The coercive and cooperative cybersecurity laws must be harmonious. For instance, if the government determines that medical devices are particularly vulnerable to attacks, it could take a multipronged approach. First, the government could provide companies with the technical guidance to adopt adequate safeguards for the devices, as the National Institute of Standards and Technology ("NIST") often does by developing many cybersecurity controls.

Second, the government could create tax incentives for device-makers to invest in the technology and staff necessary to implement the controls. Third, the Food and Drug Administration ("FDA") could refuse to approve new devices that have not incorporated these controls into new products. Fourth, the FDA could impose heavy fines on companies that do not maintain these safeguards and fix vulnerabilities in existing devices. The government need not choose only one of these options. Rather, all four approaches could achieve a common goal.

The points which I would make are to look at the ability to deliver a workable program. The WHS training is based on an Act and carries legal implications. The Board whose role it is to protect an organisation needs a clear strategy. This is available in the collection of rules and requirements but where they need to understand their risks and legal defences to develop a strategy (one size cybersecurity does not fit all).

Cybersecurity management (covered in another article) is a gap in the training. The best background book to start is a book entitled Images of Organisation by Garth Morgan which illustrates how each discipline sees things differently. These are the technical image, the political image, the financial image etc. Cybersecurity management shows that each viewpoint needs to be understood. For example, in a cybersecurity simulation run by Harvard University, the technical image has a viewpoint "lets monitor the attack to see what they are after" while the legal is to shut down servers as fast as possible.

Cybersecurity management allows those from different disciplines to agree on a path forward. In my opinion the phishing exercise in University of Adelaide was needed to show how to protect from social engineering. A response rate of 40-50% shows a problem.