

Submission to 2023-2030 Australian Cyber Security Strategy
From Cybercy Pty Ltd

Opening Remarks

There is a profound challenge for small organisations such as Cybercy in penetrating into government and federal departments to find an interest, or openness, to test novel or different approaches and so include additions to current methods to address the cyber security challenges faced by Australia. There is a sense that the nature of the problem to be fixed, has been defined.

Improving access channels into policy and decision makers will be critical to enabling a broader more open examination of whether current methods are effective in reducing cyber risk or if innovative approaches are worthy of testing and verifying. "If the only tool you have is a hammer everything looks like a nail."

It appears that nobody in an organisation thinks that cyber security is their responsibility. Senior executives thinking that those with functional responsibility have this covered, those with functional responsibility believing that senior executives are making informed risk decisions about cyberthreat. Once you enquire of the general workforce there is a pervasive view that *"they have it covered, at least I hope so."*

It is Cybercy's experience when talking to senior executives and raising this matter that there is a referral to the cyber security team. On speaking with the cyber security team it is Cybercy's experience that they are referred to executive decision makers about trailing innovations in the realm of cyber.

There are exceptions to this and our experience in Department of Defence may be instructive.

About Cybercy®

Cybercy® Pty Ltd welcomes the opportunity to make this submission to the team that is developing Australia's cyber security strategy looking to 2030.

Cybercy is an Australian Registered start-up with an international network. Services have been delivered to selected clients in Australia, the United States and the Middle East.

In 2022 Cybercy conducted a successful pilot in the Australian Department of Defence. Defence (CLOG) has sought options from Cybercy to extend this program to facilitate a broader cultural change in Defence with respect to cyber culture.

Defining the Problem

Cybercy (Cyber Literacy) is to the online world that literacy is to spoken and written language and numeracy is to mathematics, arithmetic and quantitative reasoning. Cybercy is a corpus of knowledge and behaviours that allows people to develop and apply digital thinking and reasoning strategies in their everyday activities.

In their introduction to the Cyber Security Strategy Discussion Paper, the Expert Advisory Board (EAB) note that by 'cyber' they mean:

" . . . the conduit by which all Australians can engage in a wide range of activity such as shopping, banking, work, education and healthcare."

The word ‘conduit’ does not adequately capture the extent to which people live their lives in the online world. The online world may provide a means of getting from ‘a’ to ‘b’ virtually, a conduit, if you will. However, the online world is much more. It is a major part of the experiential world in which people live, work and play. It is an indispensable part of life. It helps to define who we are and are not and what we believe, value and trust and what we do not – something much larger than a mere conduit.

We think that the language used to describe the online world is vital to our understanding of how, not just to survive, but to thrive within it and how to relate this experience to our experience of the real world. From the perspective of the human psyche the online/real world distinction is artificial and does not apply. People live in a holistic environment in which the real and virtual blend into one whole.

Much of the Discussion Paper, either explicitly or implicitly, seeks technological and regulatory solutions to problems that, since the internet was invented, have been defined largely in these terms. Somewhat sadly, the human dimension has been pushed to the back. Even in the Discussion Paper, we have to wait until Page 21 to find a small section with the heading, Community awareness and victim support. One section to cover two related but quite different points indicates to us that the proposed strategy, might itself be founded on a deep misunderstanding of the problem that the strategy seeks to address. And, to quote from medicine, incorrect diagnosis leads, by definition, to incorrect treatment.

Conventional approaches to cyber security, as noted already, seek technological and regulatory responses, which we know, at the macro level do not work. The chart below provides compelling evidence. It highlights at a global level the challenges faced by organisations as they try to address the cyber challenge (in these data the challenge uses the proxy of cybercrime). Simply put, current prevention measures are not diminishing the cyber problem.

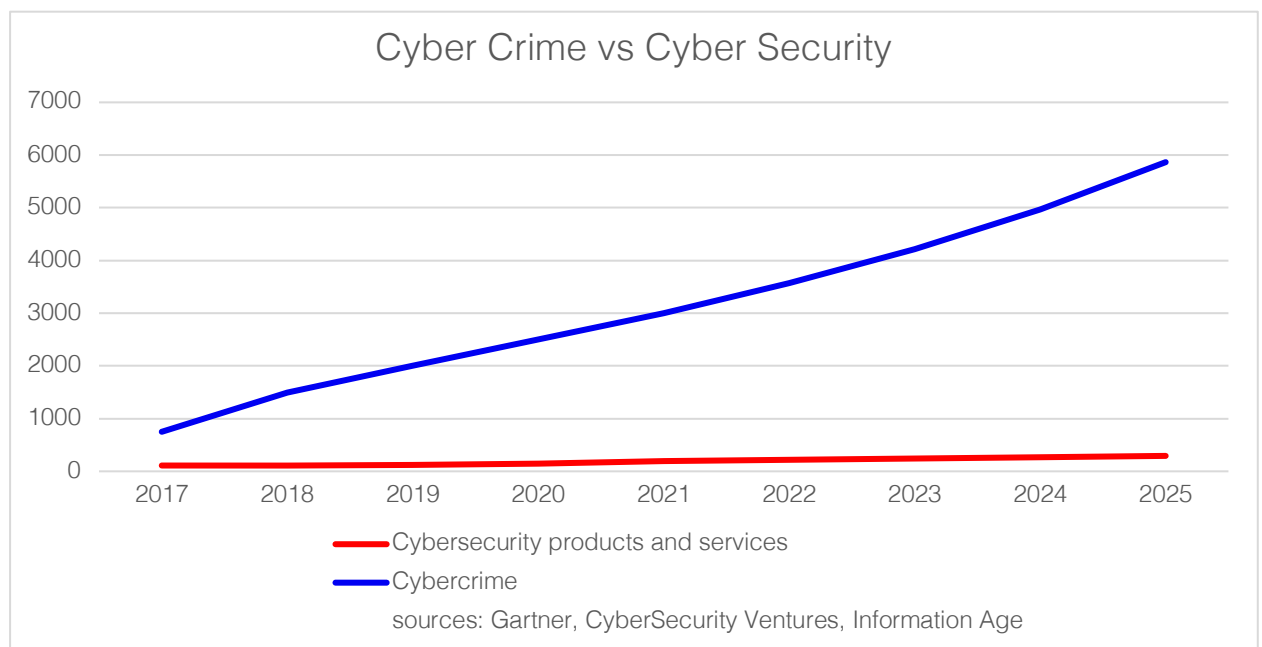


Table 1. Reported global earnings from nefarious cyber activity vs global expenditure on cyber security products and services.

These data are supported by anecdotal conversations. The Head of Cyber at the World Economic Forum told us at Cybercy that leaders are “asleep at the wheel of

the things they need to address in cyber". An Australian official, charged with global cyber security negotiations, said that the problem keeps getting worse and we need everyone to understand cyber in a new way and all the things that impact it, we all need to be more vigilant in our engagement in the digital world.

In essence, no matter how much we spend on conventional solutions, profits from cybercrime are increasing disproportionately. This is not to say we should not continue with conventional cyber security investments and approaches. It is to say that until humans are provided the means to recognise and respond to threats in the online world, at the human level, we will be fighting, at all levels of society, a losing battle.

The internet has become a ubiquitous element of the human environment and experience at such speed that humans have not had time to adapt – to develop the necessary cognitive, aural, visual and reasoning skills to function safely and confidently in the online world. We struggle to recognise danger and threats, and even when we do, we are sometimes confused as to how to respond. The deeply ingrained fight or flight mechanisms that have served us so well as individuals, as communities and as a species in the real world, simply do not work, at least not yet, in the online world.

Cyber Literacy (Cybercy)

How does Cybercy[®] address the problem?

We start with the premise that the overwhelming majority of people are good in a moral and ethical sense. They do not set out to do harm either to themselves or to others. Nor do they set out to harm organisations and institutions such as their employers or companies on which they depend. Most people would be troubled if they learnt that their online behaviour, either through an act of omission or commission, had created a vulnerability that a malfeasant actor might later exploit.

Through a series of steps, we then educate and train cohorts of individuals about the cyber world – it's design, how to recognise dangers and threats, how to identify, mitigate and manage risks and how to behave online in a safe and civil manner as, overwhelmingly, we do in the real world.

The basis of our program is the IEEE Digital Literacy Standard framework which has eight elements: Use, Identity, Safety, Security, Communication, Emotional Intelligence, Literacy and Rights. Program participants are led through a series of activities, reinforced by online materials and group discussion, to gain insights into their own behaviour that conventional cyber security training, which invariably focuses on compliance and what not to do, simply does not cover. The design of this program has been informed by cybersecurity and tech industry experts, leadership coaching and change psychologists, adult education experts and contemporary film and content experts.

(**note** This is the existing program which is also being developed for online delivery and mass scale education campaigns. Focusing on in person delivery in the first instance builds on theories of change that indicate 4% of a population changing will change a whole population)

Cybercy: Who is Responsible?

In the Pilot we conducted for the Department of Defence, and in our wider conversations, a persistent theme is the sense that cyber security is the responsibility of somebody else. Board members, use their lack of technical expertise to pass the responsibility to the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO). Technical staff, in contrast, argue that the

buck stops in the boardroom because the integrity of any organisation's information system is essential to the organisation's existence. Many individuals view security as a mechanical process to be endured. Passwords need to be invented and remembered and there is an arcane language to be mastered that embraces such terms as Virtual Private Networks, Tokens, Trolls, Phishing attacks and Spam.

Very few people have expressed a view to us that cyber security, safety and behavioural norms in the cyber domain are responsibilities that fall, at least to some extent, on all citizens in their public and private capacities. The cybercy penny has not dropped.

Cybercy and Citizenship

We have a view that cybercy is an essential element of a functioning and strong democracy. In the world before computers, each citizen had one persona. Such documents as were made and kept about us, such as medical records, were held on file cards and often destroyed when no longer needed. Private correspondence, letters, could be filed or just as easily destroyed. In effect, individuals had control of their identity and they knew the extent to which their identity was known to or shared with others. An important corollary is that people generally accepted responsibility for managing their identity boundary. In plain language, they knew who they were.

We contend that this awareness of self is vital to the concept of citizenship. Awareness of self is an essential precursor for participation in society as a citizen, for accepting at least a modicum of responsibility for something and someone beyond ourselves.

The online world is fundamentally different to this past world. We now have numerous identities online. Some are 'ghost' identities, created by software that collects and collates the data that we provide, by definition, as soon as we touch a keyboard or make a call on our smart phones. These identities are constantly refined and used by marketing companies and others to influence our future behaviour. The online world also provides an opportunity for some of us to create false identities and to develop online presences that might be more reflective of who we may like to be or wish we were rather than who we are. These people have, in effect, ceded control of who they are in the online world to that environment with little or no knowledge of how these instantiations of themselves may return to haunt them in years to come.

Citizens who no longer have control of their identities risk compromise at every turn which may affect their capacity to contribute to society as they may have done BC (before computers).

No amount of investment in technology or regulation can address the issues raised above. Cybercy education and training can help and, we would argue, is essential if our society is to take advantage of the benefits of the online world whilst keeping in check the negative impacts of this same, strange virtual world that is an artifact of human ingenuity.

Conclusion

Current approaches to cyber security are not working because, in our experience they are seeking technical and regulatory answers without adequately acknowledging and addressing the profoundly human dimension of safe and acceptable behaviour in the online world.

We need to shift the understanding and attitudes of entire populations. It has been done before in shifting attitudes towards being sun-smart and in attitudes towards


smoking but these were about behavioural adjustments in the real world. With the online world we are dealing with modifications to the entire environment in which we live, work and play. The new environment has emerged rapidly, over two generations and the adaptive mechanisms, notably those associated with safety, security and civil behaviour have yet to emerge.

Cybercy is an attempt to accelerate the acquisition of adaptive behaviours across society at the level of individual citizens. Everybody has an element of responsibility for their online conduct as they do in the real world. However, these responsibilities do not arise by magic or in a vacuum. They have context and purpose that provide safety, security and social cohesion. The online world has emerged with none of these matters having been addressed and incorporated into our language, habits, customs and behaviour – thus the confusion, the addictive behaviour and the disregard for established social norms on many social media platforms.

Cybercy Pty Ltd encourages the EAB to pay more attention to the human facets of cyber safety and security to the benefit of our society as a whole.

We would be pleased to discuss these matters further with the EAB and others involved in preparing the Cyber Security Strategy.

Glenn Welby
Co-Founder and Principal
Cybercy Pty Ltd
Canberra



13 April 2023