Responses to specific questions

1. *How are advances in digital technology changing the way you work, your industry, and your community?*

I believe that digital technology is enhancing the way we live – it is enabling us to explore, connect and share information in new ways which is sparking new ideas that can enrich our lives. As a cybercrime expert, I also know that what is created for good can also be used for evil and we need to take this into consideration ant every juncture where technology is designed, implemented and operated.

I do think it is important, however, that we do not just adopt new digital technology for the sake of it. It does need to be useful and serve a purpose and I think we need to get better at measuring how useful technology is. It should provide at least one of the following four outcomes:

1) Risk reduction
2) Operational efficiency improvements
3) A greater return on investment
4) A competitive advantage

2. *What is your vision for an Australia that thrives in a digital economy? Where would you like to see Australia in five, 10 and 20 years' time?*

Australia has long been distant from the rest of the world based on its geography, however, the Internet has been the great equalizer, allowing us to share our thoughts and tap into a vast pool of knowledge only milliseconds away. For more than two decades now, through digital technology we are not isolated. I have seen developing countries leapfrog us in some aspects. They have not had the constant evolution in technology that we have had and that has allowed them to move straight from depositing money by visiting a bank in person to making payments via mobile technology. Essentially, they have skipped the ATM and debit card/credit card technology cycle. Similarly, I have witnessed developing nations develop aggressive plans for building smart cities and are now well beyond the planning phase and into the design phase.

I know, that our population per square kilometre numbers are tiny compared to many nations, and the rugged terrain that separates the east and west coast makes infrastructure costly to implement, but I do believe that if we perform research and development to enhance and embrace wireless technology. I think we can leverage digital technology to compete and excel.

We need to remind ourselves that we are a very capable nation – we have been behind some of the technologies we take for granted now such as the electric drill, refrigerator, ultrasound, black box flight recorder and Wi-Fi. We need to empower the nation to keep innovating over the next 20 years. Australia can not become the next Silicon Valley, but we can be a powerhouse for solving problems that leave others stumped.

3. *What is the role of government in achieving that vision?*

The government needs to play a crucial role in facilitating the research, design and development of new digital technology. It should be encouraging us to solve these problems and it should be enabling us to fund great ideas within Australia, rather than moving to Silicon Valley because that is the only place to get recognition for the work we are doing.

Furthermore, government needs to continue investing in diversity – diversity in gender and culture. This increases our talent pool and enables us to think more laterally about challenging problems worth solving and to come up with innovative yet suitable solutions.

I believe government needs to be more approachable when truly revolutionary ideas that are seeded and nurtured in Australia to create inspiring yet proven results to help spread the word. Failure to do this is forcing talent to go elsewhere and Australian businesses to look elsewhere for solutions to their problems.

I have felt these frustrations myself – my innovation is not in digital technology per se, but in a way to create and sustain a future where the cost of cybercrime is significantly reduced, yet, I wouldn't even know where to begin to make government aware of what I am doing and the profound impact it is having on the large Australian organisations I am working with.

4. What are the key disruptive technologies or business models that you are seeing? What do you predict is on the horizon in five, 10, 20 years' time?

I believe the business models of the future that will thrive will be based around better connecting buyers with real problems with sellers that have fit for purpose solutions. The power will be in being able to match the two through having rich data sets. This is not too dissimilar to the industrial revolution – take supermarkets, for instance. they were the intermediaries connecting sellers of produce with buyers. Where this differs from the models of the future are:

1) The supermarket offers very little value add – they simply present he products on shelves for us to find ourselves. In the future the most effective business models will be those that educate us about the products and services.
2) The supermarket has very little data to help connect us with the ideal product. Loyalty programs enable improved racking f purchases, but imagine being able to recommend products based on knowing our allergies or quirky behaviours such as a greater likelihood to buy products with a blue coloured logo. In the future, the most effective business models will be those that know our preferences, our ailments and past experiences to help steer us in the right direction.

Blockchain, 3D printing, deep learning and DNA sequencing will be key to either providing more data about us or enabling products which can either be tailored to suit us or be manufactured in the convenience of our own homes to explicitly solve the problems we are facing over the next 20 years.

9. What opportunities do we have to build trust and community confidence through resilience to cyber threats, online safety and privacy?

Firstly, I am pleased to see the word, resilience. In four years of research on what had caused cybercrime to reach pandemic proportions, I discovered that one of the biggest issues is that society has made cybersecurity a goal – it is in fact a goal which can never be achieved. Cyber resilience, on the other hand is achievable, and those companies I have worked with that have rebranded their teams from information security or cybersecurity to "cyber resilience" have had major uplifts in morale and impact in combating cybercrime.

To build trust we need to recognise that cybercrime is not just a technology problem, and that making a technology problems has created cybersecurity. Instead we need to see it as a problem in culture, communications, process, people and technology – and we need to address each of

these in order. Technology should be the piece we do at the end to enable people. Leading with technology has made it a crutch. In essence, we need to shit our technology centric focus on cybercrime to one that is 70% psychology and 30% technology, if we are to build trust and community confidence.

10. What roles should government, business and individuals play in protecting the community in a digital economy?

In short, everyone needs to play a role. Both government and business can do more to protect individuals. Bank do a reasonably good job of helping their customers understand the importance of protecting information. Government and business need to play an important role in educating individuals – customers and shareholders.

Roles that need to be covered can be broken up into five categories:

1) **Responsibility** – this should reside with those who can make decisions at a government or business level
2) **Accountability** – this should reside with those who set strategy and policy at a government and business level
3) **Support** – this is everyone's job. All cybercrime involves humans, whether they are the target or inadvertently impacted. Everyone needs to be equipped with enough knowledge to become the first line of defence. This is similar to the Police Force – they are usually not the first line of defence. It is the citizens who detect that a crime is in progress, or has already occurred and report it to the Police, who then respond. Similarly, we can all play a role in detecting cybercrime and reporting it to the necessary authorities be it ACORN, the Privacy Commissioner, the Police of an appropriate representative in a corporate entity.
4) **Consultative** – this resides with subject matter experts. This could be cybersecurity professionals but not only reserved for them. Cybercrime can have operational, physical, personal, legal, reputational and financial impacts. As a result, this means that fraud experts, psychologists, PR, lawyers, facilities managers and operations managers also can play an import role in offering pertinent advice for developing a strategy for combating cybercrime
5) **Informant** – this resides with those persons whom know what to say and how to say it when communicating about the highlights and lowlights of combating cybercrime. This is likely to be a:
    a. CISO, CSO or CIO when communicating with the directors and executives of a company about the progress being made with respect to risk reduction
    b. CEO or director when communicating with shareholders about progress being made
    c. CEO under the guidance of PR and legal, or a PR expert when communicating with the public following a cyber breach

11. What integrity and privacy measures do we need to ensure consumers can protect their data?

To meet integrity and privacy requirements and allay any concerns around these for consumers, it is important we understand what causes breaches of integrity and privacy and to understand what needs to be done, if despite best efforts, breaches of integrity and privacy do occur.

Six processes are required:

1) Asset Management
   A cyber breach can not happen unless there is information of interest to cybercriminals that they feel is worth targeting. Information does not live in a vacuum, whilst it is an asset, it is stored, processed or transported by other assets, and it is these which are targeted by cybercriminals. Good asset management helps us understand what assets we have and to appreciate which assets are likely targets.
2) Vulnerability Management
   Assets are either create by humans, or are human and therefore imperfect. All assets contain some form of vulnerability and it is these which provide an opportunity for cybercriminals to penetrate an asset. Good vulnerability management helps us understand where these weaknesses lie and which one are easiest to exploit by cybercriminals.
3) Threat Management
   Assets that contain vulnerabilities are subject to threats. Cybercriminals create threats to exploit vulnerabilities. It should be considered though that a threat in and of itself is not dangerous. Only when the threat exploits a vulnerability is it a real danger. Good threat management helps us predict and prevent activities cybercriminals engage in to cause us harm.
4) Incident Management
   When a threat is successful in exploiting a vulnerability it progresses to an attack. An attack signifies that cybercriminals have established a point of entry and this is an opportune time to put a stop to their activities, if not already stopped at the vulnerability or threat stages. Good incident management helps us detect and respond to attacks in progress.
5) Continuity Management
   When an attack has not been responded to quickly enough, this elevates the chances of cybercriminals being able to complete their objectives. At this point the attack has progressed to a breach. Breaches can be of privacy, integrity or availability of information. Good continuity management helps us quickly assess the damage of a breach and recover from it enabling minimal disruptions to the organisation.
6) Crisis Management
   When a breach has occurred, how it is dealt with is critical to minimising the impact to the organisation. Poor handling can increase the costs to the organisation significantly. Cost can be measured in terms of operational, physical, personal, legal, reputational or financial impacts to the organisation. Good crisis management helps us determine and manage the impact to the organisation

Exercising good practices with each of these six processes can help all of us protect our data

12. What are barriers for business, particularly small business, in adopting cyber security and privacy practices?

The biggest barriers come in the form of a lack of understanding and that lack of understanding creates fear. Most have awareness that cybercrime is a problem but the lack of understanding stems from poor communications about what cybercrime is and the impacts it can have. This is due to:

1) No common, universally accepted, definition of cybercrime
2) Technologists being left to explain cybercrime – without business context and efforts to break the communications down into simple language, this creates the perception that cybercrime is complex and a technical domain. Of course, cybercrime can be explained in simple language that directors and executives can understand and even feel empowered to play a role in (that's what I do every day)
3) False assumptions that Australian organisations are not good targets – I often share stories about publicly available case studies such as those breach that impacted Distribute.IT, Codan, Maroochy Shire Council, and Red Cross to name a few to highlight that we are just as likely targets due to the speed at which data, and hence cyber attacks can travel
4) False assumptions that cybercriminals don't target small businesses – I often share stories about how we all have information that is valuable; if we didn't we would not have a business that could differentiate itself. I also discuss that the lack of understanding and planning by small businesses for cyber threats makes them extremely vulnerable and even if they do not have millions of dollars of IP to steal, the very fact they have computers is enough to become a launchpad into other more lucrative targets or simply as a means for mining bitcoins

Education is key. I am already investing a lot of my time working with larger companies but would welcome more opportunities to help Australian organisations overcome these barriers and be not only aware, but understanding of the problem.

13. What integrity measures do the Australian Government and the private sector need to take to ensure business-consumer transactions are secure?

Both government and private sector need to exemplify good cyber resilience practices. We need to stop leading with technology and leading with culture, which will in turn influence the ways in which we communicate. Our communications will then enable us to develop the right processes. Our processes will then be able to be performed by people with the appropriate skills; People can then leverage the technology to assist them in combating cybercrime. Technology becomes an enabler, not a crutch, in part of a complete strategy (psychology and technology) in helping Australia create and sustain a future where cybercrime is insignificant.

About me

I am a Father and someone who loves seeing innovative technology enrich our lives, and it is the collision of these two roles that have brought me on the exciting journey I am on today.

My name is Andrew Bycroft and my vision for creating and sustaining a future in which cybercrime is insignificant came about in 2012 when I started thinking about what the future might be like for my daughters when they reach adulthood if we allow cybercrime to continue to worsen. A $2 bottle of milk would cost $120 by 2030 if inflation increased at the rate of cybercrime. Despite having been in the cybersecurity industry since 1994, I knew that technology was just a small part of a much bigger solution that was required if I was to achieve my vision.

In 2017, I am working towards my vision. I founded The Security Artist, a management consultancy built on my personal values of openness, consistency, simplicity and caring to ensure that Australians have access to the very best education and consulting to help them create the necessary culture, communications, and processes and acquire the best people and technology to beat the rising cost of cybercrime.

I am currently working through the first phase of my vision which is where I empower directors and executives of large companies to play a small, but vital, role in beating the rising cost of cybercrime. I do this through delivery of three hour workshops in their boardroom to provide them with the jargon free wisdom they can use to truly understand cybercrime and its impact to their organisations. What's more, I don't charge a cent for these workshops, but do ask that they make a small tax-deductible donation to a charity of their choice.

The next two phases I plan to work with smaller businesses and individuals.

I am a much sought after public speaker, the author of two books ("The Cyber Intelligent Executive" and "Adapt or Die"), and often asked to contribute my opinion on radio across Australia. I am looking to play a greater role in enabling Australia to embrace the digital economy and want to ensure that my daughters live in times when cybercrime is like cholera – once a pandemic but reduced to a level of insignificance

Andrew Bycroft
1300 018 872
0477 999 138
andrew.bycroft@thesecurityartist.com
www.thesecurityartist.com