STRATEGIC INSIGHTS

ASPI

Australia’s next cybersecurity strategy

Views from *The Strategist*

150

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Gai Brodtmann, Peter Dutton, Rachael Falk, Fergus Hanson, Nigel Phair, Lesley Seebeck

Introduction: Australia’s cyber strategy, version 2.0

Fergus Hanson, 10 September 2019

Back in 2016, Australia launched a new national cybersecurity strategy. The strategy covers a four-year period to 2020, and given the changes in the security environment, an update is now clearly warranted. To that end, the government has just released a discussion paper to kick off the public consultation. The closing date for submissions on the discussion paper is 1 November.

To complement the public submission process, ASPI’s International Cyber Policy Centre is initiating a public debate on what should be included in the next cybersecurity strategy. Contributions will be compiled into a report that we will deliver to the Department of Home Affairs to inform the strategy’s development.

Image: iStock.com/Urupong.

February 2020

The overarching themes are what the strategy should focus on and how the government can achieve maximum impact in a resource-constrained environment.

The last strategy had 33 initiatives and a funding package of $230 million for four years. That was a huge number of initiatives and a pretty modest budget given what was proposed. The next strategy needs to be a lot more focused, given significantly greater resourcing seems unlikely.

There are, of course, lots of things that could be included in the strategy, and the government's discussion paper poses plenty of questions for contributors to explore. But to kick things off, I wanted to propose three areas of focus.

The first is the safety of physical systems as we connect more and more of them to the internet. We're rapidly shifting from a world that connected things that couldn't physically hurt us if compromised (like phones, laptops and PCs) to a world where we're connecting lots of things that could seriously injure or kill us if compromised (cars, machinery, aeroplanes). We've already seen several near misses at factories and fatal crashes involving driverless cars (although not yet due to a malicious cyber compromise).

Injuries and deaths from cyberattacks will dramatically increase political attention. But in the case of social media companies, we've seen how problematic it can be to retrospectively regulate in a hurry, especially when it involves writing new legislation over the weekend. A top priority for the strategy has to be narrowing down the types of systems that pose a real risk of causing injury and/or death and ensuring a high level of cybersecurity for those connected devices (noting the many pitfalls of regulation).

The second proposal is to make greater use of the government's procuring power to drive improved standards within government and for firms that sell to government. There are several ways the government could do this. It could, for example, mandate minimum cybersecurity standards in its tender documents (at present, it mostly doesn't do this)—for example, when purchasing new hardware and software for the public service.

It could also mandate that contractors that sell to government meet minimum cybersecurity standards themselves. At present, there's lots of potential for contractors to handle government data using less secure systems. The Department of Human Services has done some good work leveraging its purchasing power to extend the secure supply chain, and the Australian Prudential Regulation Authority's draft standard on information security looks at extending obligations on regulated entities to third parties.

The third proposal is to expand the scope of the rules for mandatory reporting of data breaches. There are two key aspects to this. First, the law needs to be expanded beyond personal data to breaches in general. At present, a company could lose all of its intellectual property without any obligation on it to disclose what in reality would be a major breach. Companies also don't need to disclose a breach that affects their customers (for example, in the case of Cloud Hopper, it seems that at least some managed service providers did not notify their clients that they had been compromised).

One argument commonly used against compulsory disclosure is that notification laws could perversely discourage companies from searching for breaches. But that's the situation that exists already—compromises are rife, security is poor, and it's past time for direct measures that ensure all organisations take security seriously.

The second change to the law that's needed is the imposition of fines. At present, there's no incentive for some sectors to respond to the current 'name and shame' tactics. Without fail, every quarter, the health sector is the worst offender under Australia's notifiable data breach scheme. Even though data on people's health is the most sensitive information anyone holds, the sector has no incentive to improve because consumers have no choice but to go to their doctors and hospitals and there is no single brand on which consumers can target their frustration. So bad behaviour persists. Fines would help sharpen the focus on dealing with this current failure.

That is by no means an exhaustive list. The government's paper poses 26 questions to start the discussion. Over the coming weeks, we look forward to hearing a wide range of views.

For print readers, the original post with live links is at https://www.aspistrategist.org.au/australias-cyber-strategy-version-2-0.

Cybersecurity strategy should focus on corporate Australia

Nigel Phair, 27 September 2019

Image: iStock.com/matejmo.

The Australian government is developing the next cybersecurity strategy to protect Australians from cyber threats. The current version was launched in 2016 and, while novel for its day, was largely underfunded when considering the task ahead. It's now time to learn the lessons from that experience.

Every organisation uses technology—in service delivery, product development, manufacturing and a multitude of other instances. However, many organisations don't fully appreciate how tech-heavy they actually are. One of the cybersecurity sector's biggest issues is to get organisations to undertake basic risk management processes and develop an understanding of what technology means to them. It is there that the next strategy should focus. Getting corporate Australia to take ownership of detecting and deterring cyber attackers targeting their organisations is where the rubber needs to hit the road.

There are many aspects of the online environment affecting Australian governments, the private sector, non-profits and individuals that could be covered in the 2020 strategy. However, it should focus on doing a few things very well. One of these is get corporate Australia to do the simple things first, and that starts with understanding the cyber risk and taking a strategic view.

The constant rise in ransomware attacks, phishing attacks, and compromises of business email systems is a clear indicator that the corporate sector needs help—Australian businesses reported more than 5,800 such scams in 2018, a 53% increase compared with the previous year. The government should put its resources into assisting Australian businesses to harden themselves against being targeted, with the view to other jurisdictions becoming the 'low-hanging fruit' for international cyber criminals.

Fortunately, we have the opportunity for a running start. The most recent version of the *Australian government information security manual*, released earlier this month, uses a risk management framework based on the guidance issued by the US National Institute of Standards and Technology. The manual focuses on implementing cybersecurity principles in a maturity model—a concept that relies on continuous improvement to obtain a desired state.

Too often, organisations see cybersecurity as binary, with a focus on achieving compliance with a particular standard or framework. The next strategy should focus on providing resources (and by that I mean holding their hands) for corporate Australia to implement the recommendations in the information security manual that are relevant to their business requirements and to their sector (with guidance from the appropriate regulatory authority for that sector).

A good first step is to determine the organisation's risk appetite and level of risk tolerance. Without this strategic overview it's hard to put meaningful resources into tactical and technical cybersecurity measures. Cyber risk should be a category assessed by a company's risk and audit committee just like all other risks, and the relationships between risks should be recognised. Responsibility for managing cyber risks should be clearly defined, and reporting should be done through a chief risk officer, not the chief information officer role that many organisations opt to assign it to.

As the Australian Institute of Company Directors suggests, organisations should establish a formal process to ensure cyber risk is regularly monitored and reviewed, so that it remains relevant to the company's needs and reflects current regulatory requirements and risk committee best practice.

An important input to the risk management process will be resources to help organisations defend their staff and networks through 'blue teaming', which aims to identify malicious tactics, techniques and procedures and execute response strategies for them. This needs to be a combination of technical capabilities, such as intrusion-detection systems, and human capabilities, such as analysing intelligence. While it's important to conduct penetration testing, putting too much focus on 'red teaming' to imitate attacks against an organisation is not the answer.

The 2020 cybersecurity strategy shouldn't seek to boil the ocean. Ransomware, phishing and business email compromises are remarkably untechnical cyberattacks, yet pose the greatest issue for Australian businesses. Creating and providing resources to make Australian organisations resilient to cyber threats will be key to success.

For print readers, the original post with live links is at https://www.aspistrategist.org.au/cybersecurity-strategy-should-focus-on-corporate-australia.

It's time to reboot Australia's cybersecurity strategy

Rachael Falk, 4 October 2019

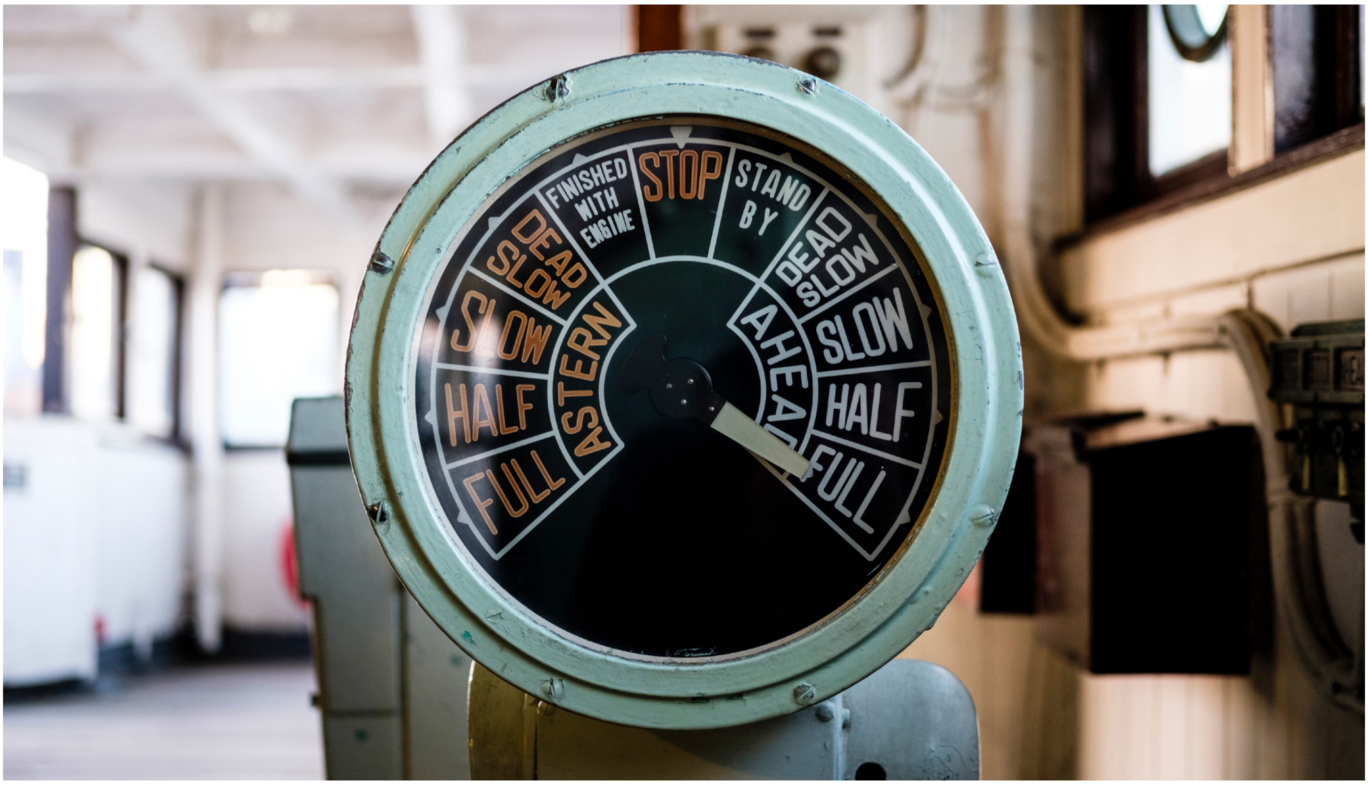

Image: iStock.com/Tsuji.

Australia's 2020 cybersecurity strategy needs the input of all Australians—from individuals to academia, business, community associations and regulators. The government has issued a discussion paper calling for views, asking Australians to contribute to shaping Australia's future and making our 2020 strategy world-leading. The closing date for submissions is 1 November 2019.

It's time for a reboot and time to bring everyone into the discussion.

Cybersecurity is a concept that's not well understood. Frequently it gets tangled up with buzzwords like artificial intelligence and blockchain. More often than not, it's seen as a scary realm with intangible consequences. So, while everyone has heard of data breaches (and the millions of victims of some of those breaches), many people struggle to work out what the actual loss is.

Consumers aren't alone in that. Australia's courts don't recognise damages like anxiety and emotional harm that may come with identity theft or romance scams. Those losses are very real.

In the business world, the picture in the boardroom (in 2017 at least) appears patchy. Only 45% of companies who responded to the ASX 100 cyber health check survey said that they were confident or very confident in their ability to detect, respond to and manage a cyber intrusion. That statistic suggests that a majority of companies are feeling overwhelmed and underprepared.

All the while, many assert that the government should do more. Yet, when pressed, they often can't define what it is the government should actually be doing.

Government action in the cybersecurity sphere, in a public sense, is often described as having an effective strategy coupled with legislative and regulatory settings that are favourable to innovation and unlocking all that this connected world brings—while ensuring there are serious consequences for those who fail to keep our personal data safe.

Cybersecurity awareness for every single Australian is a tough sell. The risk is intangible, cybersecurity insurance is offered as some sort of magical solution, and we have legislation that appears to include fines that have never been imposed in relation to recent breaches.

For the average person, it's easier to just switch off. 'Quiet Australians' are used to getting on with the job and prefer not to be drawn into things that are overly contested or seen as niche issues.

However, we all have a vested interest in getting cybersecurity settings right—from protecting our personal information, to thinking about what kinds of jobs will be around in 2025, to ensuring the integrity and safety of critical infrastructure.

In April 2016, the government released a cybersecurity strategy covering the period to 2020. It was ambitious and tried to tackle many of the big-ticket items you would expect from government. It spanned everything from government partnerships with industry and academia, to better preparedness of our networks and systems to detect and respond to cyberattacks, and (of course) growth and innovation.

It also set the goal of raising the cybersecurity awareness of every Australian. In my experience, that is truly a massive undertaking.

In 2019, the government has rightly recognised that it's time for a cybersecurity strategy 'reboot'. The discussion paper released in September is a forward-looking document that's about ensuring Australia is well positioned for the future.

The language is inclusive and invites views on a wide range of questions. Home Affairs Minister Peter Dutton, whose portfolio includes cybersecurity, writes in the foreword, 'I encourage all Australians to have a say in this discussion paper—from small businesses to large corporations, tech experts to interested individuals.'

Cybersecurity impacts us all—from the personal data we're required to share in order to obtain services, to the critical infrastructure that we rely on every day to go about our lives and the companies that use and store our data when they don't always need to.

Strong cybersecurity must be seen as a mandatory part of doing business, irrespective of whether that business is conducted by a government department, a university or a small company.

We should all have a view on cybersecurity. After all, this is about our data and the security of the systems and everyday connected things that we rely on. It's also about our future, about calling boardrooms to account, and about realising our shared ambition to make Australia the safest place to do business online.

It is time for quiet Australians to find their voices.

For print readers, the original post with live links is at https://www.aspistrategist.org.au/its-time-to-reboot-australias-cybersecurity-strategy.

Australia’s 2020 cybersecurity strategy: defining the mission

Gai Brodtmann, 1 November 2019

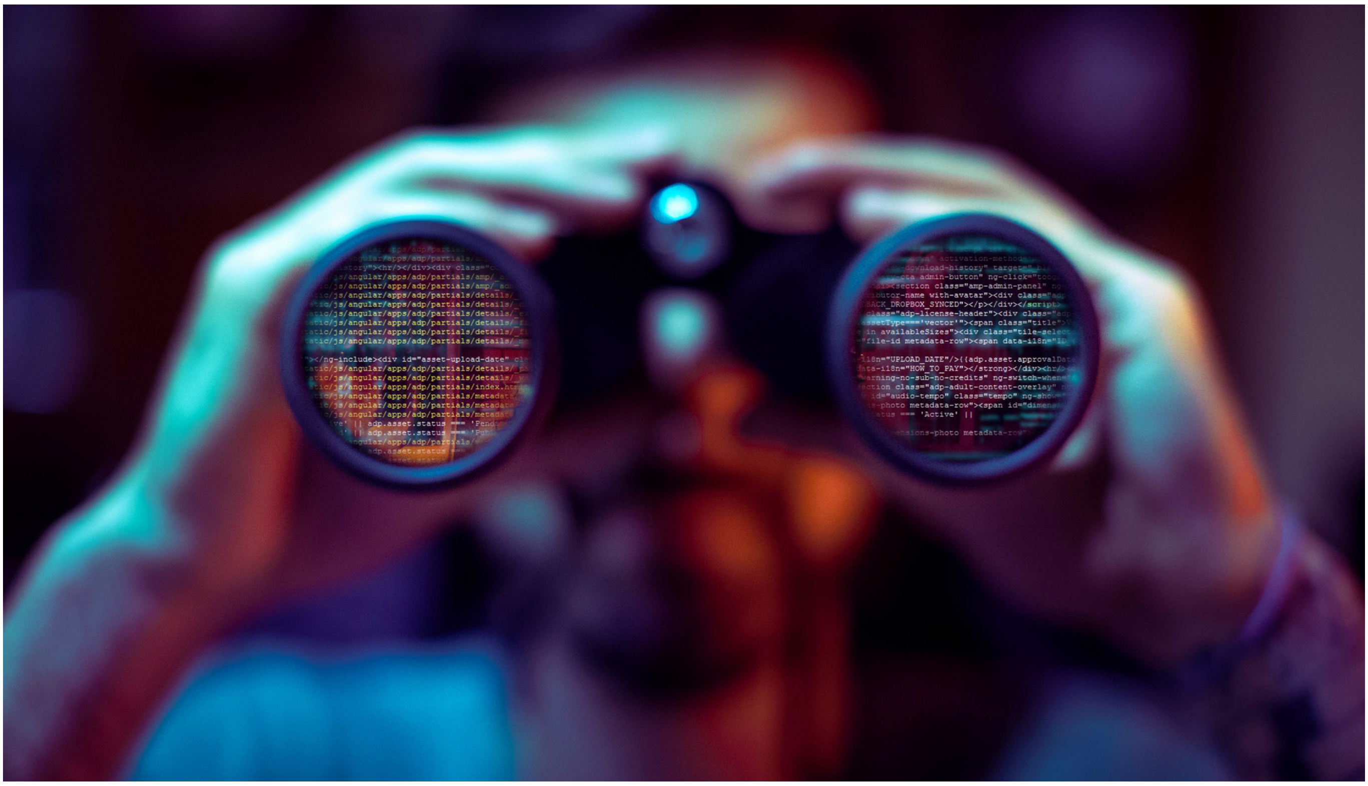

Image: iStock.com/Marco_Piunti.

Three summers ago, I was walking with my husband along a South Coast beach when we noticed a woman diving into the surf with her two teenage children. From where we stood, it was obvious they were heading straight into a rip. They were 500 metres from the flags. Close enough to have walked there with ease. But far enough away to drown before help arrived.

The mother managed to keep her feet and grab her daughter. However, her son was carried away from the beach, so she followed him into the water. To my horror, my husband ran across the beach and followed them in.

I stood and watched as all three were swiftly washed away from the shore. Luckily, the boy and his mother could both swim, but they were fighting against the current. My husband was calling for them to swing across the beach and out of the rip. Fortunately they did, so this story has a happy ending. Everyone survived, but it could have ended in tragedy.

As they emerged from the surf, I pointed down the beach and roared at the mother in white-hot rage. ‘Swim between the flags’, I yelled. ‘My husband could have drowned trying to save you and your children because you chose to ignore this warning.’

Australians know the surf as their playground. It is a source of tremendous enjoyment. But bitter experience has taught us it can also be deadly. Which is why we’ve developed a unique national mission where volunteers band together around the country to patrol the beaches and keep us safe.

If you swim between the flags in Australia, the chances you will drown are remote. Test the waters outside the flags and the risk of drowning rises exponentially.

We need to have the same attitude to cybersecurity. We need to develop the same culture of risk management and resilience we impose on the beach. And that begins with defining our national mission.

Since 2016, there's been a lot of activity on the cybersecurity front in Australia. Loads of strategies, policies, advisory groups, action plans, frameworks, dialogues, agreements, workshops and delegations. But I still don't get the sense that we're all pulling together towards a common goal. Because that common goal, and the values and principles underpinning it, hasn't been defined.

So, the starting point for the next strategy needs to be a clear and collectively developed articulation of what we're trying to preserve and protect in cybersecurity, who is responsible for what, and what cyber resilience looks like.

It has to be a unique national mission that will focus the efforts of the nation; guide cybersecurity priorities in policy, standards, legislation, education, training, research, innovation, sovereign capability, and private-sector and public-sector engagement and investment; and embed a cyber-resilient culture in Australia.

We then need to mobilise and empower Australians, particularly individuals and small businesses, to get on board and play their part through an education and awareness campaign modelled on the success of 'Slip, Slop, Slap'.

The campaign would be a call to action to work together to build a 'herd immunity' in cyber resilience by giving Australians the confidence and tools to understand and manage cyber risks. It would aim to encourage Australians to manage their cybersecurity in the same way they manage the physical security of their home or car—to protect not just themselves, but the nation.

The campaign would also provide an overarching frame for the separate efforts currently being conducted by state, territory and local governments and industry and should be led by the Australian Cyber Security Centre.

The next version of the strategy also needs to get the government's own house in order, as a matter of urgency.

Multiple Australian National Audit Office cyber resilience reports over many years have found that just 29% of audited government agencies comply with mandatory cybersecurity standards—even after the Bureau of Meteorology, Department of Parliamentary Services, Australian Bureau of Statistics and Australian National University incidents.

At a time when significant data breaches and cyberattacks are an almost daily occurrence, this is simply unacceptable. These are agencies that hold sensitive and personal data on every Australian and information 'across a range of economic, commercial, policy or regulatory, national security, program and service delivery and corporate activities.'

Government entities must be the 'exemplar' by which others in the community measure themselves. The Joint Committee on Public Accounts and Audit's recommendations of 2017 should be fully implemented now, particularly mandating:

- that every government entity must comply with cyber resilience standards and the Internet Gateway Reduction Program and must complete the annual Australian Signals Directorate cybersecurity survey
- annual reporting on the Commonwealth's cybersecurity posture to the parliament.

The 2020 strategy should also:

- include compliance with cyber resilience standards in the performance agreements of entity heads with hard and fast deadlines
- mandate the appointment of chief information security officers in every government entity and university
- require training on cybersecurity hygiene for parliamentarians and their staff and volunteers and appoint dedicated cybersecurity officers in electorate offices, along the lines of the first-aid officer or fire warden
- include electoral systems in our critical resilience infrastructure strategy
- introduce a data management strategy
- make it a contractual requirement for suppliers to government entities and critical infrastructure, especially in the national security sector, to meet a specified cyber hygiene standard

- review the maturity of the cyber insurance market and assess the suitability of cyber insurance as a mandatory requirement for contracting to government agencies, in line with existing requirements for public liability and professional indemnity insurance
- ensure the Australian Cyber Security Centre provides guidance on, and continuously vets and reports on, technologies being installed in government entities
- establish a Council of Australian Governments cybersecurity subcommittee.

As more and more government services move online, the Australian people are entitled to know their information is being managed and stored according to best-practice standards and processes.

Australians also deserve to know how their hard-earned taxes are being used on our cybersecurity response.

The 2016 strategy was big on 'priority actions', motherhood statements and broad aspirations, but short on detailed, tangible objectives. This accountability and transparency void has made it difficult to assess what results have been achieved and delivered—despite the glowing progress report in the discussion paper—and resulted in duplication and mission creep across some parts of the cybersecurity sector.

The 2020 strategy should therefore include:

- robust and meaningful key performance indicators for every sector, guided by the national mission
- measurable targets, grounded in research and written in plain English
- concrete deadlines with clear milestones, so we can see our return on investment, or not.

The review gives us the chance to take a cold hard look at what has worked, and what hasn't, since 2016. We should make the most of the time to reflect. Because, like the sea that surrounds our nation, the connected world is at once a place of opportunity and threat.

We can all enjoy the benefits if we know how to mitigate the risks. But right now too many Australians are walking wide-eyed into a rip.

For print readers, the original post with live links is at https://www.aspistrategist.org.au/australias-2020-cybersecurity-strategy-defining-the-mission.

Cybersecurity: people are not the problem

Lesley Seebeck, 4 November 2019

Cropped image: John Lund/The Image Bank/Getty Images.

Those of us older than a certain age will recall an excellent British television series, *Yes, Minister*, and its successor, *Yes, Prime Minister*: they were required viewing for young and enthusiastic public servants in Canberra.

One of the more memorable episodes, 'The compassionate society', involved a hospital with no patients, though it did have 500 administrators and ancillary workers to ensure things ran smoothly. Not having patients both prolonged the life of the facility and cut running costs, ensuring it was one of the best-run hospitals in Britain.

Unfortunately, we find the same attitudes in other walks of life. The 'socio-technical divide' is a well-known phenomenon in technology. If only people weren't involved, or just did what we told them, we'd have perfect systems.

That also reflects a lot of thinking and commentary around cybersecurity—'people are the problem'. After all, most intrusions and attacks start with people being persuaded or misled into going onto disguised or infected sites, to handover details or otherwise compromise their own systems. One estimate is that 94% of malware is delivered via email—phishing—which requires someone to preview, open and/or click on a link or file. If only people—users, clients, members of the community—didn't do what people naturally do, we'd all have much more secure and efficient systems.

That's muddled thinking.

First, people—thankfully—are messy. They're changeable. They work in a variety of different styles, with different information. They desire both privacy and openness—mediated on their own terms, and with people whom they get to choose. They're impatient, focused, curious, biased, distracted, inspired and sometimes plain lazy. They're driven by motivations that generally have little do with the incentives of engineers and managers who build and oversee systems and data.

They’re also the reason why we build technologies, systems, organisations and institutions to start with—to enable, support, help and entertain. We need more than cybersecurity specialists; we need good people to conceive, construct and care for good, adaptable, human-centred, secure, resilient systems, that account for the people who use or are supported by them.

Technology is inherently reductionist: that it fails to capture the complexity of humans and their systems should be unsurprising. Despite attempts to map ‘personas’ or ‘life journeys’, technological systems will always struggle to keep up—there’s no universal, singular human experience. The fact that systems and system design either neglect or fail to accommodate the messiness of people and their underlying needs is fundamentally a human concern. That’s even more so as those same technologies become increasingly embedded in our daily lives.

Second, the line that ‘people are the problem’ usually applies to the faceless masses. It tends to overlook that systems designers, engineers, managers, vendors and government ministers are also people and no less prone to the same messiness, incomplete decision-making, changeability and biases as anyone else. They make mistakes, too. They respond to their own set of incentives, not necessarily others’, or society’s for that matter. And they tend to build systems that favour their own position and point of view.

Third, the systems themselves that people design, approve and administer are no less flawed. Moreover, there’s a case that the consequential misunderstandings, misinterpretations and misconfigurations are so deep in both practice and theory that everything is broken.

The result is that the whole, inevitably, is deeply complex. Complex systems have a variety of properties that make them unpredictable and less tractable to top-down, centralised control.

In such systems, cause and effect are rarely linear. Simple actions may have extraordinary effect, while massive effort may yield little change. Failures may cascade across systems, which may have networks, dependencies and behaviours previously unsurfaced and so unrecognised by managers, administrators and technical staff.

Systems and stakeholders—and their expectations—co-evolve, so that what worked once or in the last funding cycle, may not do so again. And preventive action may easily create increased rigidity and tension in the system. It may be better to allow small failures—analogous to backburning, for example—if they dilute the prospects for major conflagration or collapse.

In such circumstances, attacking officials for a failure—‘heads will roll’—or blaming the victim does little to encourage staff to learn and to build resilience. Instead, it may well increase the chances of greater systemic failure later. The slow work of building human capability and a systems-level understanding is likely to yield better results than firing staff or micromanaging.

Last, we live in a liberal, Western, free-market democracy. Democracies give preference to individuals and their rights, freedoms and opportunities.

Democracies are being challenged by authoritarian regimes and illiberal thinking, including within the democracies themselves. To many—disillusioned by the failure of democratic government to cope with the turmoil caused by digital disruptions, by inequality, by discrimination and biases, and by failures in corporate governance—a populist, or even an authoritarian or strongman approach, looks attractive. It offers simple and direct action and solutions. The lack of consultation, and of transparency, is seen not as an impediment but as an enabler. And authoritarian systems are often able, at least initially, to generate more immediate and focused outcomes.

But a fundamental strength of democracies is that, by investing in individuals and giving them the freedom, and the ability, to create, build, prosper and take a large measure of responsibility for their own wellbeing, they build both legitimacy and resilience that authoritarian societies lack.

Increasingly, that’ll include their online activities as well. In a complex system, government has little hope of ensuring safety and security for all. Technological fixes will be quickly overtaken; social fixes, including legislation, risk impairing people’s ability to look after themselves; and both, imposed with little understanding or consultation, will erode trust, legitimacy, resilience and the government’s own ability to enact change.

The discussion paper released by the Department of Home Affairs on a new cybersecurity strategy raised a multitude of questions—literally. That reflects the sheer complexity of the problem at hand. And if everything is indeed broken, reaching for quick technological or even legislative fixes is likely to add further complexity, increase fragility, increase insecurity and impair resilience.

And so, rather than assuming that 'fixing' cybersecurity and improving safety are matters for the central government—which has stretched resources and fewer levers than it once had to enact change—decision-makers would do well to place citizens at the centre of the challenge, and to ask themselves, 'How can we best help our people to help themselves?'

Now more than ever is the time to double down on our democratic impulses, rather than seeking false shelter in an omnipotent government.

For print readers, the original post with live links is at https://www.aspistrategist.org.au/cybersecurity-people-are-not-the-problem.

Cybersecurity is a national priority for Australia

Peter Dutton, 18 November 2019

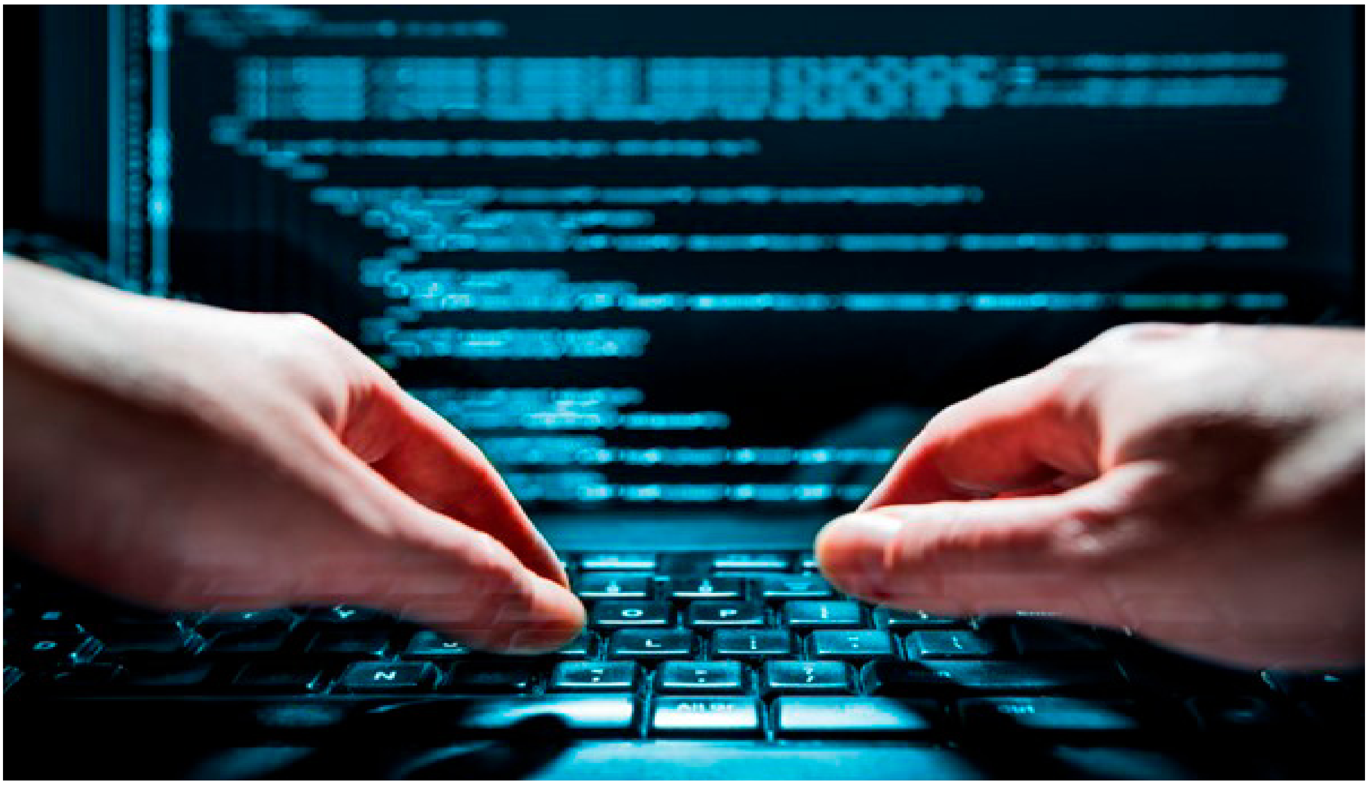

Image: iStock.com/scyther5.

Australia's cybersecurity has never been more important to our economic prosperity and national security.

At the same time, there are more cyber criminals and they are better resourced, and state actors have become more sophisticated and emboldened. Australia has been fortunate to avoid a catastrophic national cybersecurity incident so far, but the threat to essential services, the economy and potentially even human life remains very real.

Real threats need real action. Some 65% of Australian businesses have been interrupted by a security breach in the past year, with half of these costing between $1 million and $4.9 million. It's particularly difficult for small and medium businesses to know how to defend against insidious threats like ransomware. Indeed, we know that around half of Australian victims pay the ransom, desperate to get their livelihoods back.

The 2017 'WannaCry' ransomware attack severely impacted the UK National Health Service and many other global organisations. In 2018, the 'NotPetya' malware spread from Ukraine to the Cadbury factory in Tasmania.

Online data breaches are now so common that many in our community treat them as a non-event. But one of the consequences of those data breaches is identity crime, which has impacted one in four of us. The clean-up is usually messy and traumatic, with most identity crime victims reporting a psychological impact.

We cannot be blind to the hostile forces intent on using technological change to exploit our businesses, vulnerable community members and our children, and ultimately undermine our way of life.

It's time to stop, step back and look at this problem with fresh eyes.

Our landmark cybersecurity strategy in 2016 invested $230 million to foster a safer internet for all Australians. But as the cyber threat evolves, so must we. As a nation and a community, we're less prepared than we need to be. That is why the government has committed to delivering a new cybersecurity strategy in 2020.

Government doesn't have all the answers. The complex, intertwined digital world means we need the whole community to provide their views. So we put out a nationwide call for views through a discussion paper, and the responses have overwhelmingly been clear, consistent and compelling.

Your calls for action have been heard. You've asked for more leadership from government.

We need to start by looking at roles and responsibilities, such as the role that balanced regulation and standards can play in improving the baseline cybersecurity of systems that are most critical to the economy and community. Equally, the many views on improving information sharing, supporting small and medium businesses at scale, changing behaviour through awareness, and recognising the importance of cybersecurity skills will shape the new strategy.

The formal call for submissions might have closed, but the conversation is really just beginning.

Cybersecurity has been, and will always be, a collective responsibility between governments, industry and the community. And we need to make sure there aren't gaps or barriers stopping us from working together—legal, technical or otherwise.

Unlike the transport, water and power sectors, the internet is fundamentally shaped by the private sector—not governments. The private sector provides most digital services and holds most of the data.

Government's limited role online means more responsibility for cybersecurity is borne by the private sector. Many digital providers are doing the right thing, and I've seen countless examples of Australian businesses addressing the threat in innovative and creative ways. The next generation of technological solutions are being developed by Australia's world-class cyber industry.

However, when the risk isn't managed appropriately, everyone pays—businesses, governments and the community. Right now we're paying too much, and we're too vulnerable.

Too often ordinary Australians are expected to be their own cyber experts. In addition, the private sector is left to defend our most vital systems from the highest-end threats by themselves. In many cases, government wouldn't know if industry was under attack until after the fact. How many of us are comfortable with this status quo?

While cyberattacks are automated, most of our defences are human. We're fighting a 21st-century problem with a 20th-century mindset.

The way the internet has evolved makes it difficult to tackle cybercrime: anonymity is easy and effective, Australian Federal Police investigations often hit dead ends in international safe havens, and hacking tools are cheap and widely available on the dark web.

The internet has made our lives richer and easier, and businesses more efficient. Australians don't want to turn back the clock. However, they have a right to expect a level of cybersecurity that gives them confidence online.

We've solved problems like this many times before. Australians trust the cars they drive, the water they drink and the medicines they consume. This is because everyone involved in providing these goods and services is accountable for managing risk and consumers understand what they need to do. It's a national priority that we get to the same mature state in the digital world and make necessary changes to protect all Australians—particularly the most vulnerable.

For print readers, the original post with live links is at https://www.aspistrategist.org.au/cybersecurity-is-a-national-priority-for-australia.

About the authors

Gai Brodtmann is a former federal Labor MP for Canberra and shadow assistant minister for cyber security and defence.

Peter Dutton is Australia's home affairs minister.

Rachael Falk is the CEO of the Cyber Security Cooperative Research Centre.

Fergus Hanson is head of the International Cyber Policy Centre at ASPI.

Nigel Phair is the director of UNSW Canberra Cyber.

Lesley Seebeck is the CEO of the Cyber Institute at the Australian National University.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

About Strategic Insights

Strategic Insights are short studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI

Tel +61 2 6270 5100
Fax +61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

facebook.com/ASPI.org

@ASPI_org

ISSN 1449-3993

Australia’s next cybersecurity strategy

Views from *The Strategist*