LEGISLATIVE COUNCIL

PORTFOLIO COMMITTEE NO. 1

Cyber security

Report 52

March 2021

1

www.parliament.nsw.gov.au

Portfolio Committee No. 1 - Premier and Finance

Cyber security

Ordered to be printed 26 March 2021 according to Standing Order 231

New South Wales Parliamentary Library cataloguing-in-publication data:

New South Wales. Parliament. Legislative Council. Portfolio Committee No. 1 – Premier and Finance.

Cyber security / Portfolio Committee No. 1 – Premier and Finance [Sydney, N.S.W.] : the Committee, 2021. [xi, 77] pages ; 30 cm. (Report no. 52 / Portfolio Committee No. 1 – Premier and Finance)

"March 2021"

Chair: Hon. Tara Moriarty MLC.

ISBN 9781922543097

1. Computer security—New South Wales.
2. Computer networks—Security measures—Government policy—New South Wales.
3. Government information—Security measures—New South Wales.
4. Computer crimes—New South Wales—Prevention.

I. Moriarty, Tara.

II. Title.

III. Series: New South Wales. Parliament. Legislative Council. Portfolio Committee No. 1 – Premier and Finance. Report ; no. 52

352.379 (DDC22)

Table of contents

Terms of reference

1. That Portfolio Committee 1 – Premier and Finance inquire into and report on cybersecurity and digital information management in New South Wales, and in particular:

   a) The number of cybersecurity incidents and data breaches involving NSW Government agencies;

   b) The monitoring and response to cybersecurity incidents and data breaches across the NSW Government;

   c) The policies and procedures underpinning the management of digital information by the NSW Government;

   d) Systems management within NSW Government agencies including outages, backups and cyber security;

   e) The financial costs and other impacts of cybersecurity incidents, data breaches and outages involving NSW Government agencies;

   f) Expenditure on cybersecurity, digital services and digital infrastructure across the NSW Government;

   g) The management of public access to digital information under GIPA and similar processes including coverage of mobile based and online platforms;

   h) Contractual arrangements between the NSW Government and providers of digital services and infrastructure, including:
      (i) Provisions relating to cybersecurity generally; and
      (ii) Reporting obligations and the monitoring of cybersecurity incidents;

   i) The extent and impact of outsourcing of government information systems, including:
      (i) Outsourcing to entities which are owned overseas;
      (ii) The risks involved with outsourcing government information systems.

   j) The support provided by the NSW Government to local councils and other organisations in relation to cybersecurity;

   k) The NSW Government's response to cybercrime in the community generally; and

   l) Any other related matter.

The terms of reference were self-referred by the committee on 6 August 2020.

Committee details

Committee members

The Hon Tara Moriarty MLC	Australian Labor Party	*Chair*
The Hon Robert Borsak MLC	Shooters, Fishers and Farmers Party	*Deputy Chair*
The Hon Ben Franklin MLC	The Nationals	
The Hon Taylor Martin MLC	Liberal Party	
The Hon Adam Searle MLC	Australian Labor Party	
Mr David Shoebridge MLC*	The Greens	
The Hon Natalie Ward MLC	Liberal Party	

* Mr David Shoebridge MLC substituted for Ms Abigail Boyd for the duration of the inquiry

Contact details

Website	www.parliament.nsw.gov.au
Email	PortfolioCommittee1@parliament.nsw.gov.au
Telephone	(02) 9230 2553

Chair's foreword

Between March and April 2020 there was a serious cyber attack on Service NSW. This resulted in the personal information of thousands of New South Wales citizens being stolen.

The committee found that this attack was enabled by practices and systems within Service NSW that did not accord with best practice cyber security measures. Compounding this incident, Service NSW was aware of the risks that led to the attack some 12 months earlier but had not acted sufficiently to address them.

Increasingly, citizens of New South Wales must access government services online. In doing so, they are required to provide their personal information electronically. Citizens also rely on digital and internet connected devices in multiple aspects of their lives and, following the pandemic, regularly connect remotely to government systems in order to work from home. It is clear that the amount of data being stored, accessed and shared online is at an all-time high. These factors make attacks like the one mentioned above both more likely and, if successful, more impactful and damaging.

It is for this reason that proactive, robust and resilient cyber security measures are critical now more than ever. Failing to get cyber security right not only puts citizens at risk, but it undermines trust in government and risks the State's economy and business community.

While the NSW Government has taken some proactive measures to enhance cyber security in New South Wales, there is still much work to be done.

In addition to the important lessons to be learned from the attack on Service NSW, the committee recommends that the NSW Government strengthen its Cyber Security policy; enhance the role and mandate of Cyber Security NSW, ensure the Privacy Commissioner proactively assists agencies' privacy protection measures; and enhance cyber security education for public officials and cyber security professionals.

The committee also makes recommendations regarding mandatory notification of data breaches; sovereign cyber security capability; the security of internet of things; as well as clearer requirements for cyber security standards in agencies.

There are considerable opportunities to provide better support to the public, small business and local councils when it comes to cyber security. The committee notes that a holistic approach to cyber security practices across New South Wales will place the State in a position to leverage the significant opportunities that come with operating safely in an increasingly digital world.

On behalf of the committee, I would like to thank all those who participated in this inquiry either by making a submission or appearing at one of the hearings. I also thank my committee colleagues for their considered contributions to this process and the secretariat for their assistance and support.

Hon Tara Moriarty MLC
Chair

Findings

Finding 1 **30**

That the Service NSW data breach may have been prevented had the agency addressed in a more timely manner previously identified risks regarding its handling of personal information.

Finding 2 **30**

That once Service NSW became aware of the attack, it took too long to notify those impacted by the breach and it also did not provide sufficient information, support and direct assistance to affected people throughout the process.

Finding 3 **30**

That, while Service NSW has taken steps to reduce its dependency on sending personal information via email, it continues to engage in this practice thereby operating in a way that enabled the data breach. The committee urges the cessation of this practice as a matter of priority.

Finding 4 **32**

That the NSW Government lacks any real framework or clear processes within government to properly and expeditiously deal with requests by people in the community for assistance in the event of a breach of their data. People who suffer data breaches are left to their own resources and the existing, unsatisfactory state of the law where very few persons are eligible for relief, assuming they have the financial resources to seek it.

Recommendations

Recommendation 1 **31**

That the NSW Government review the functions of Cyber Security NSW and provide it with a clearer mandate to oversee agencies' cyber security progress and ensure their compliance with the NSW Cyber Security Policy.

Recommendation 2 **31**

That the NSW Government move Cyber Security NSW from within the Department of Customer Service to the Department of Premier and Cabinet to provide it with more independence from service delivery agencies and increased visibility and authority.

Recommendation 3 **32**

That the NSW Government review the responsibility and resourcing of the Privacy Commissioner so that the office can be more proactive in ensuring government services and systems are designed and delivered with stringent privacy protections.

Recommendation 4 **32**

That the NSW Government urgently address the matters identified in Finding 4 and implement a framework or clear process within government to properly and expeditiously deal with requests by people in the community for assistance in the event of a breach of their data.

Recommendation 5 **32**

That the NSW Government work with industry and the education sector to develop a cyber security skills framework that includes:

- the provision of a comprehensive and regularly reviewed cyber security training regime for all NSW Government employees
- the requirement for cyber security professionals within NSW Government agencies to be accredited in recognised cyber security certifications
- the provision of adequate tertiary cyber security qualifications to meet government and industry demand.

Recommendation 6 **51**

That the NSW Government review its Cyber Security Policy to provide clarity around mandatory standards and set a benchmark that all NSW Government agencies must adhere to.

Recommendation 7 **51**

That the NSW Government work with industry to determine the most appropriate model for cyber security standards for both NSW Government agencies and cyber security businesses within New South Wales.

Recommendation 8 **51**

That the NSW Government investigate avenues for it to improve the security of Internet of Things devices, particularly those adopted or deployed by its agencies.

Recommendation 9 **52**

That the NSW Government urgently establish a mandatory data breach notification scheme applicable to all NSW Government agencies and its contracted service providers.

Recommendation 10 **52**

That the NSW Government develop a strategy to enhance sovereign cyber security capability which includes building the industry, establishing principles for procuring services onshore and working with agencies to identify what data should be stored offshore.

Recommendation 11 **62**

That the NSW Government:

- provide further financial support to local councils to enhance their cyber security capabilities
- develop a plan in consultation with Local Government NSW to ensure local councils meet the cyber security standards identified for NSW Government agencies.

Recommendation 12 **62**

That the NSW Government develop a strategy to improve the cyber safety of citizens that includes:

- education and awareness measures
- consumer protection measures
- advice and support services.

Conduct of inquiry

The terms of reference for the inquiry were self-referred by the committee on 6 August 2020.

The committee received 28 submissions and three supplementary submissions and held two public hearings at Parliament House in Sydney.

Inquiry related documents are available on the committee's website, including submissions, hearing transcripts, tabled documents and answers to questions on notice.

Chapter 1 Background

This chapter provides background information to the inquiry by explaining cyber security and why it is important as well as setting out the current cyber risks and the cyber security landscape in New South Wales. It also discusses the role of the NSW Police Force in responding to cyber crime and securing its own systems.

Understanding cyber security

1.1 Cyber security protects citizens, businesses, and governments against cyber threats. To understand cyber security, it is useful to first set out the threats that cyber security seeks to guard against.

Cyber threats

1.2 Cyber threats range from the theft and malicious use of personal or sensitive information to attacks on systems designed to disrupt services or prevent them from functioning. It can also include the inadvertent, or otherwise, unlawful disclosure of someone's personal and sensitive information; breaching their privacy.

1.3 The Information and Privacy Commission NSW explained that cyber threats can take a variety of forms including:

- crypto-mining
- data breaches
- distributed denial of service (DoS) attacks
- hacking
- identity theft
- malware
- ransomware
- web shell malware
- phishing attacks
- spoofing.[1]

1.4 The Australian Government's Cyber Security Strategy 2020 identified the following more large scale, sophisticated and rapidly evolving cyber threats:

- nation states and state-sponsored actors and criminals exploiting Australians by accessing sensitive information and for financial gain

[1] Submission 14, Information and Privacy Commission NSW, p 2.

- criminals using the dark web to buy and sell stolen identities, illicit commodities, and child exploitation material, as well as to commit other crimes.
- encryption and anonymising technologies allow criminals, terrorists and others to hide their identities and activities from law enforcement agencies
- cyber criminals taking advantage of the fact that Australians are more connected than ever before.[2]

1.5 The Australian Cyber Security Centre highlighted the increasing risks of cyber attacks and explained what it sees as the most common methods:

> Malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, and sophistication. Phishing and spearphishing remain the most common methods used by cyber adversaries to harvest personal information or user credentials to gain access to networks, or to distribute malicious content. Over the past 12 months the ACSC has observed real-world impacts of ransomware incidents, which have typically originated from a user executing a file received as part of a spearphishing campaign.[3]

1.6 Professor Vijay Varadharajan, Global Innovation Chair, Professor Cybersecurity, University of Newcastle noted the increasing sophistication of cyber attacks and that state actors will increasingly use these attacks for strategic gains:

> In the future, this trend will continue with the threats becoming more automated, more intelligent, and disruptive and even more destructive. Nation-state actors are likely to push the envelope and use cyberattacks against critical infrastructures to achieve greater strategic effects than through traditional means.[4]

1.7 Many inquiry participants highlighted the role of human error in cyber threats. For example, the NSW Information and Privacy Commission said that as many as 95 per cent of successful online hacks come down to human error.[5]

1.8 This view was supported by the Office of the Australian Information Commissioner who said that breaches often occur when an employee sends information to the wrong person or clicks on a link that results in the compromise of user credentials.[6]

1.9 While not all cyber threats amount to cyber crime, inquiry participants advised that this form of crime is a significant threat facing the community and there is no such thing as immunity from cyber attacks.[7]

[2] Australian Government, *Australia's Cyber Security Strategy 2020*, p 6, viewed at: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy.

[3] Australian Cyber Security Centre, *Annual Cyber Threat Report: July 2019 to June 2020*, p 4, viewed at https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020.

[4] Submission 15, Professor Vijay Varadharajan, p 2.

[5] Submission 14, Information and Privacy Commission NSW, p 2.

[6] Submission 18, Office of the Australian Information Commissioner, p 5.

[7] Evidence, Professor Vijay Varadharajan, Global Innovation Chair, Professor, Cybersecurity, University of Newcastle, 29 October 2020, p 4; Submission 6, NSW Auditor General, p 4.

1.10 Palo Alto Networks discussed the prevalence of cyber crime, noting that 'close to one in three Australians were victims of cyber crime and that the Australian Cyber Security Centre (ACSC) receives a report of cyber crime every ten minutes'.[8]

1.11 Dr Bruce Baer Arnold, Associate Professor of Law at University of Canberra proffered that cyber 'incidents are as likely as death and taxes',[9] while Mr Tony Chapman from Cyber Security NSW explained that 'no digital system or service can be guaranteed to be secure'.[10]

1.12 Mr Chapman further explained that it is 'not a matter of if incidents will occur but when and how much their impact, harm and spread can be reduced through prevention, preparedness, early detection, response and recovery'.[11]

Cyber security

1.13 Understanding the threats and the scale or prevalence of these cyber threats, provides important context as to the need for cyber security. The Australian Cyber Security Strategy 2020 outlined the importance of cyber security as a fundamental part of everyday life:

> Cyber security allows families and businesses to prosper from the digital economy, just as pool fences provide peace of mind for households. Cyber security needs to be a fundamental and integrated part of everyday life, enabling Australians to reap the benefits of the internet safely and with confidence.[12]

1.14 Similarly, the NSW Auditor-General described cyber security as 'technologies, processes and controls that are designed to protect IT systems and sensitive data from cyber attacks'. It also explained that cyber security consists of:

- threat identification
- protection
- detection
- response
- recovery of IT systems.[13]

1.15 Discussed in more detail in the next section, NSW Government agencies are required to assess their cyber security hygiene against eight mitigation strategies identified by Commonwealth Government's Australian Cyber Security Centre. These mitigation strategies, known as the Essential Eight, provide useful descriptions of the types of measures that combine to build a strong cyber security posture. These measures aim to prevent, identify and respond to data breaches and cyber threats and are:

[8] Submission 26, Palo Alto Networks, p 5.

[9] Submission 16, Dr Bruce Baer Arnold, p 3.

[10] Evidence, Mr Tony Chapman, Chief Cyber Security Officer and Executive Director, Cyber Security NSW, 3 February 2021, p 20.

[11] Evidence, Mr Chapman, 3 February 2021, p 20.

[12] Australian Government, *Australia's Cyber Security Strategy 2020*, p 7.

[13] Submission 6, New South Wales Auditor General, p 4.

Essential Eight

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening – block flash, ads and Java and disable unneeded features
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Daily backups.[14]

1.16 Active Cyber Defence Alliance described the concept of identifying an attack and recovering from it quickly as 'cyber resilience' which means 'the ability to continue to remain in safe functional operation during an attack and the ability to recover quickly if function is impaired.[15]

1.17 Participants also highlighted that cyber security is a continuous process. Ms Michelle Price from AustCyber warned that 'the game of cyber security is ongoing and the arms race is getting pretty sharp'.[16] This sentiment was also captured by Professor Varadharajan who described cyber security as a journey:

> … it is worth mentioning that it is not a one-off thing. It is a journey, it is a process. We have to do this continuously. Also it is worth mentioning that there is no absolute security in the sense that these attacks will change, there are dynamic changes in attacks, so we have to be vigilant continuously.[17]

A snapshot of cyber security in New South Wales

1.18 Inquiry participants provided evidence regarding the current cyber security landscape in New South Wales. This section provides a background for many of the key issues and themes regarding cyber security in New South Wales which are addressed throughout the report.

Policy context

1.19 The NSW Government advised that it has:

- established the dedicated agency 'Cyber Security NSW' within the Department of Customer Service,
- invested $240 million to improve cyber security in agencies

[14] Australian Cyber Security Centre, *Essential Eight Explained*, June 2020, viewed at https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained.

[15] Submission 17, Active Cyber Defence Alliance, p 8.

[16] Evidence, Ms Michelle Price, Chief Executive Officer, AustCyber, 29 October 2020, p 25.

[17] Evidence, Professor Varadharajan, 29 October 2020, p 3.

- released a cyber security policy in February 2019 for all NSW Government agencies to implement
- been working to update its Cyber Security Strategy, which was initially due for release in late 2020, but is now scheduled for release in the first half of 2021.[18]

1.20 In February 2019, the NSW Government released the NSW Cyber Security Policy which applies to all NSW Government agencies. It describes the policy as 'a risk based policy based on the National Institute of Standards and Technology (NIST) cyber security framework'. The policy outlines the mandatory requirements to which all NSW Government departments and public service agencies must adhere to, to ensure cyber security risks to their information and systems are appropriately managed.[19]

1.21 The Cyber Security Policy requires all agencies to:

- strengthen cyber security governance
- identify their most valuable or operationally vital systems or information (“crown jewels”)
- strengthen cyber security controls
- develop a cyber security culture across all staff
- work across all of government to share security and threat intelligence
- implement a whole of government approach to cyber incident response.[20]

1.22 The policy also sets out the roles and responsibilities of key agency decision makers including for Chief Executives, Chief Information Officers, Chief Information Security Officers, Cyber Security NSW and the Chief Cyber Security Officer.[21]

1.23 In addition to this policy, the NSW Government also advised that it is in the process of updating its 2018 NSW Government Cyber Security Strategy.[22] The new strategy will replace the NSW Cyber Security Strategy 2018 and the NSW Cyber Security Industry Development Strategy, combining them into one overarching cyber security strategy for New South Wales. It notes that this recognises the connection between a strong government cyber security posture and a strong cyber security industry.[23]

1.24 The NSW Government noted that there are a range of other policies and initiatives that relate to New South Wales agencies' management of data and cyber security. These include:

- the procurement framework which sets out requirements for managing customer data, security, data breach, privacy, audit and reporting

[18] Submission 10, NSW Government, pp 2 and 6; Answers to questions on notice and supplementary questions, Department of Customer Service, received 2 March 2021, p 11.

[19] Submission 10, NSW Government, p 2.

[20] Submission 10, NSW Government, p 3.

[21] Submission 10, NSW Government, pp 2-3.

[22] Submission 10, NSW Government, p 2.

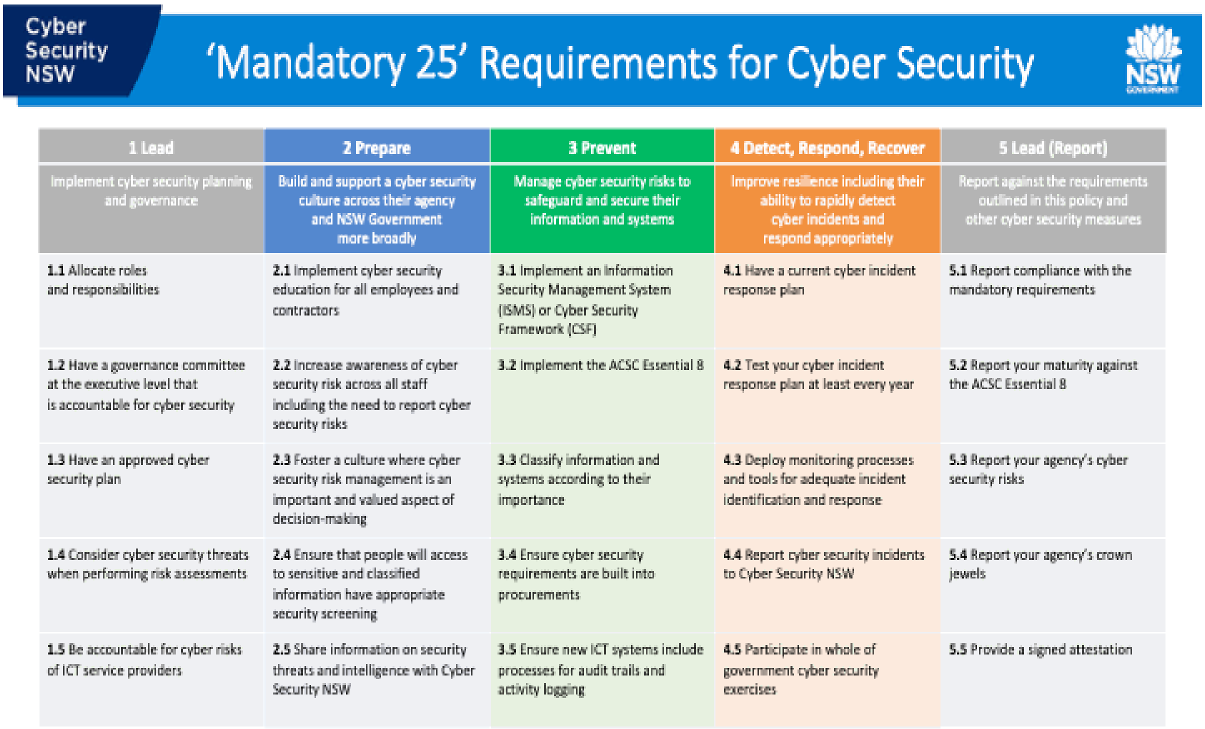
[23] Submission 10, NSW Government, p 2.

- data centre reform – requiring agencies to relocate remaining data centre and computer room infrastructure from current facilities into Government Data Centres and where appropriate consume services through the Government Data Centres marketplace or other suitable cloud services
- Information Management Framework, Cloud Policy, Smart Infrastructure Policy, Artificial Intelligence Strategy and Ethics Policy and Information Classification, Handling and Labelling Guidelines.[24]

1.25 Further, the NSW Government explained that its policy mandates 25 requirements that all NSW Government agencies must implement and report against. It also requires agencies to implement and assess maturity against the Australian Cyber Security Centre's Essential Eight risk mitigation controls, which were detailed earlier in the chapter.[25] Mr Chapman from Cyber Security NSW indicated that for the first time in New South Wales, government agencies are now required to annually assess their cyber security maturity.[26]

1.26 The policy states that agencies must provide a yearly report to their cluster Chief Information Security Officer, or Cyber Security NSW, on their compliance with this policy in a format provided by Cyber Security NSW by 31 August each year.[27] Figure 1, from the NSW Cyber Security Policy sets out the 'mandatory' requirements, that agencies must assess themselves against. Implementing the Essential Eight, is shown at 3.2.

Figure 1 Mandatory requirements from the NSW Cyber Security Policy



Cyber Security NSW

'Mandatory 25' Requirements for Cyber Security

1 Lead	2 Prepare	3 Prevent	4 Detect, Respond, Recover	5 Lead (Report)
Implement cyber security planning and governance	Build and support a cyber security culture across their agency and NSW Government more broadly	Manage cyber security risks to safeguard and secure their information and systems	Improve resilience including their ability to rapidly detect cyber incidents and respond appropriately	Report against the requirements outlined in this policy and other cyber security measures
1.1 Allocate roles and responsibilities	**2.1** Implement cyber security education for all employees and contractors	**3.1** Implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF)	**4.1** Have a current cyber incident response plan	**5.1** Report compliance with the mandatory requirements
1.2 Have a governance committee at the executive level that is accountable for cyber security	**2.2** Increase awareness of cyber security risk across all staff including the need to report cyber security risks	**3.2** Implement the ACSC Essential 8	**4.2** Test your cyber incident response plan at least every year	**5.2** Report your maturity against the ACSC Essential 8
1.3 Have an approved cyber security plan	**2.3** Foster a culture where cyber security risk management is an important and valued aspect of decision-making	**3.3** Classify information and systems according to their importance	**4.3** Deploy monitoring processes and tools for adequate incident identification and response	**5.3** Report your agency's cyber security risks
1.4 Consider cyber security threats when performing risk assessments	**2.4** Ensure that people will access to sensitive and classified information have appropriate security screening	**3.4** Ensure cyber security requirements are built into procurements	**4.4** Report cyber security incidents to Cyber Security NSW	**5.4** Report your agency's crown jewels
1.5 Be accountable for cyber risks of ICT service providers	**2.5** Share information on security threats and intelligence with Cyber Security NSW	**3.5** Ensure new ICT systems include processes for audit trails and activity logging	**4.5** Participate in whole of government cyber security exercises	**5.5** Provide a signed attestation

[24] Submission 10, NSW Government, pp 7-9.

[25] Submission 10, NSW Government, p 3.

[26] Evidence, Mr Chapman, 3 February 2021, p 20.

[27] NSW Government, *NSW Cyber Security Policy*, Updated version, February 2020, pp 3-4.

1.27 In addition to the mandatory requirements, the NSW Government advised that, under its Cyber Security Policy, agencies must appoint staff to roles that cover a broad range of cyber security activities and that these roles range from key leadership positions to line areas and third parties.[28]

1.28 It explained the governance arrangements in respect of cyber security, including:

- the Secretary of the Department of Customer Service gives effect to its Cyber Security Policy through a whole-of-government circular which sets out compliance requirements[29]
- The ICT and Digital Leadership Group comprises senior executives from across all clusters. It considers and endorses cyber security policy, and reviews agency cyber security reports with the Cyber Security Senior Officers' Group (cyber security leaders from across government) to identify common concerns and areas for improvement.[30]

1.29 A number of participants discussed the Government's digital transformation agenda and the impact on cyber security in New South Wales. The Information and Privacy Commission NSW outlined the growth in online government service delivery and the need to address increased risks. It noted that 'maintaining and enhancing the cyber security capabilities of the public sector is vital to protecting the security of its information assets'. [31]

1.30 Professor Varadharajan similarly expressed this view, stating that: 'it is vital that the NSW Government agencies going through digital transformation processes … take every security precaution that is possible to reduce the probability of such occurrences'.[32]

1.31 Palo Alto Networks highlighted the increasing amounts of data and services being moved online by Government and pointed to the criticality in ensuring security:

> In the course of the last year, we have seen the NSW Government move more and more data online, from digital drivers' licenses, to an online death notification service, to the provision of online school enrolments. However, as the NSW Government moves these services and data online, it is critical that they are secured.[33]

1.32 AustCyber and Local Government NSW echoed these views and outlined that public agencies are attracting increased attention because of the amounts of personal data they hold.[34]

1.33 Relevant to the increase in online service delivery, some inquiry participants discussed the importance of government maintaining the trust and confidence of its citizens by ensuring their data is secure. Participants noted that cyber attacks can erode this trust in government,

[28] Submission 10, NSW Government, pp 3-4.

[29] Submission 10, NSW Government, p 4.

[30] Submission 10, NSW Government, p 4.

[31] Submission 14, Information and Privacy Commission NSW, p 1.

[32] Submission 15, Professor Vijay Varadharajan, p 2.

[33] Submission 26, Palo Alto Networks, p 1.

[34] Submission 3, AustCyber, Attachment: Supplementary Report; Modelling the impact of COVID-19 on Australia's digital economy, p 36; Submission 2, Local Government NSW, p 1.

particularly for the victims of attacks.[35] This matter will be discussed further in chapter 2 when considering the Service NSW data breach in March and April 2020.

1.34 Further, participants noted the importance of cyber security for the New South Wales economy. The Australian Information Security Association stated that 'a strong local cyber security and information technology sector is vital for the long-term success of the NSW economy'.[36] Ms Michelle Price from AustCyber also spoke about the growing nature of the cyber security industry and noted that over 50 per cent of Australia's sovereign cyber security companies are currently located in New South Wales'.[37]

NSW Police Force and cyber crime

1.35 Deputy Commissioner Hudson provided information regarding the NSW Police Force approach to cyber crime. He said that in the last year, there was over 12,000 incidents reported to the NSW Police Force, and this figure is growing by 7 to 8 per cent each month. He provided additional information regarding these statistics and how many incidents relate to attacks on Government systems:

> … out of the 12,700 cyber incidents over the past 12 months, less than 10 per cent of those are cyber-dependent crimes, which is an attack on a system. Most of them are cyber-enabled crimes. So, fraud or identity theft—those traditional crime types that are just facilitated through the use of a computer or the internet. Of the matters reported to us, the rate of cyber incidents targeting government agencies would be quite small.[38]

1.36 On notice, the NSW Police Force provided the following breakdown of cyber crime in New South Wales in 2020 by type:[39]

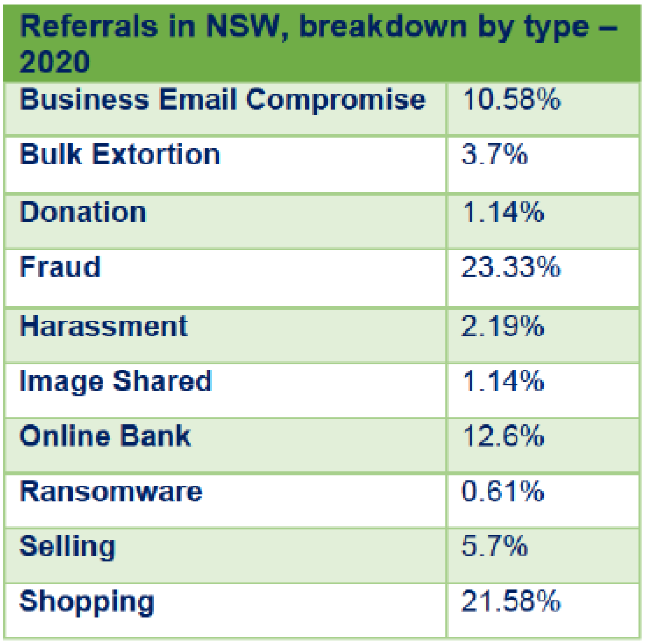
[35] Submission 9, Vault Cloud, p 5; Submission 28, Ms Claire Falkingham, p 1.

[36] Submission 24, Australian Information Security Association, p 9.

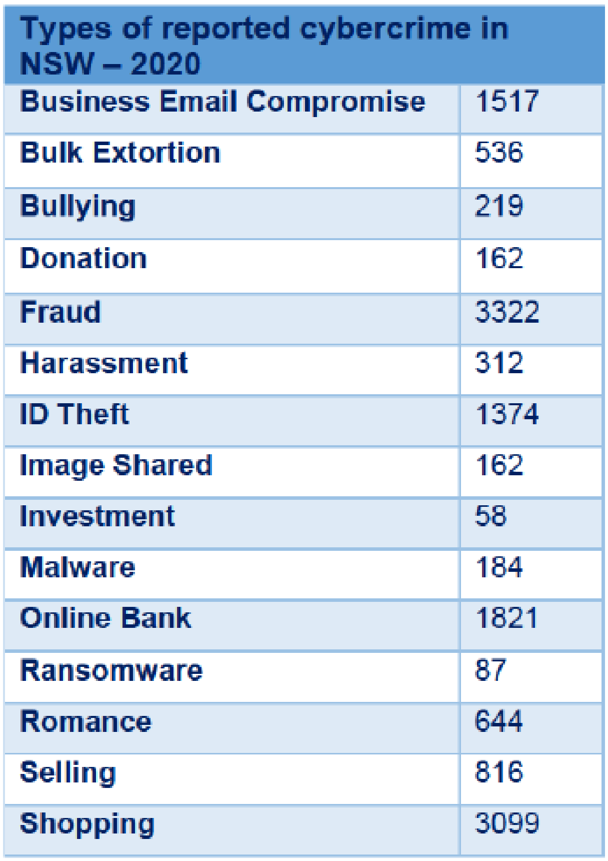
[37] Evidence, Ms Price, 29 October 2020, p 21.

[38] Evidence, Deputy Commissioner David Hudson, Investigations and Counter Terrorism, NSW Police Force, 3 February 2021, p 40.

[39] Answers to questions on notice and supplementary questions, NSW Police Force, received 4 March 2021, p 5.



Referrals in NSW, breakdown by type – 2020	
Business Email Compromise	10.58%
Bulk Extortion	3.7%
Donation	1.14%
Fraud	23.33%
Harassment	2.19%
Image Shared	1.14%
Online Bank	12.6%
Ransomware	0.61%
Selling	5.7%
Shopping	21.58%



Types of reported cybercrime in NSW – 2020	
Business Email Compromise	1517
Bulk Extortion	536
Bullying	219
Donation	162
Fraud	3322
Harassment	312
ID Theft	1374
Image Shared	162
Investment	58
Malware	184
Online Bank	1821
Ransomware	87
Romance	644
Selling	816
Shopping	3099

1.37 Against this backdrop, Deputy Commissioner Hudson provided information about the Cyber Crime Squad which has grown from 12 to over 60 staff since 2017. These staff are not just technical experts, but are detectives as well:

> Our Cybercrime Squad…from its infancy in 2017 when it was part of the fraud squad…we created a standalone unit—staffing in that unit since that time has grown from 12 to 65, along with a lot of technical capability that we bring with that. I think we are the largest standalone cybercrime unit in Australia, including the AFP, and we have got some very smart people in that unit. I think, importantly, they are not just technical experts; they are detectives as well. So there is a mixture of those—unsworn technical experts, sworn technical experts and some very smart detectives.[40]

1.38 The NSW Police Force advised that there are now 68 staff in the Cybercrime Squad, 60 sworn officers, of which 58 are detectives. The squad consists of the following three units:

- Cyber Enabled Investigations – Criminal investigations
- Cyber Dependent Investigations – Criminal investigations
- Advanced Capability Unity – Technical experts.[41]

[40] Evidence, Deputy Commissioner Hudson, 3 February 2021, p 38.

[41] Answers to questions on notice and supplementary questions, NSW Police Force, received 4 March 2021, p 6.

1.39 Deputy Commissioner Hudson explained that reporting of cyber crimes occurs in many ways, with the majority coming through the Commonwealth system, ReportCyber. However, he still believes the reporting numbers are low:

> The majority of reports that are made to the New South Wales police come from a Commonwealth system, ReportCyber, which has had a soft launch. … We are receiving several hundred reports per month through that system, as well as other conduits: through our community portal and through our face-to-face at a police station reports. There are a number of different avenues for people to report crime. Having said that, we believe the reporting rate is quite low. It is always difficult to investigate a volume crime type, which this is becoming, when you only have part of the picture of it.[42]

1.40 The NSW Police Force advised that there were 14,572 reports of cyber crime though ReportCyber in 2020. There were also seven cyber-related crimes reported by the NSW Government in 2020, including the Service NSW data breach.[43]

1.41 Deputy Commissioner Hudson identified the NSW Police Force's own systems as an example of those at risk of attack and said they had 58 significant attacks last year, but none were successful. He further noted that at one point there was up to 200 phishing attacks per week on its systems.[44]

1.42 In response to questions regarding the age and security of the NSW Police Force database, Computerised Operational Policing System (COPS), Deputy Commissioner Lanyon noted that, after many years, it was still in the process of being updated.[45]

1.43 COPS was originally implemented in 1994 and in 2013/4, $44.8 million was allocated for the 'COPS modernisation program'. To date $39.55 million of this budget has been spent which covers costs associated with upgrades to the COPS system, its venture with Accenture and the pivot to a new system, Integrated Police Operating System (IPOS). The NSW Police Force advised that since 2018, $22.6 million in recurrent and $1.26 million in capital funding has been expended to determine a viable solution and commercial partner for IPOS. This includes procurement engagements, due diligence, contract negotiation and award process.[46]

1.44 During evidence Deputy Commissioner Lanyon advised that a further estimated $1 billion is required to implement the new platform.[47] He agreed that the system was antiquated, but expressed the need for taking the time to get the new system right.[48]

[42] Evidence, Deputy Commissioner Hudson, 3 February 2021, p 40.

[43] Answers to questions on notice and supplementary questions, NSW Police Force, received 4 March 2021, p 4.

[44] Evidence, Deputy Commissioner Hudson, 3 February 2021, p 39.

[45] Evidence, Deputy Commissioner Hudson, 3 February 2021, p 35.

[46] Answers to questions on notice and supplementary questions, NSW Police Force, received 4 March 2021, pp 2-3.

[47] Evidence, Deputy Commissioner Malcolm Lanyon, Corporate Services, 3 February 2021, p 35.

[48] Evidence, Deputy Commissioner Lanyon, 3 February 2021, p 37.

1.45 Deputy Commissioner Hudson agreed with the proposition that if organisations are going to trust the police to investigate cyber security breaches, they need to be satisfied that the police have proper cyber security controls in place.[49]

Committee comment

1.46 The committee understands the importance of cyber security in New South Wales and that proactive, robust and resilient cyber security measures are critical now more than ever.

1.47 The committee notes that the increase in digital delivery of government services means that the amount of data being stored, accessed and shared online is at an all-time high.

1.48 Further, citizens are being asked to hand over their personal information to agencies in digital environments while also looking for governments to protect their privacy and safeguard their data. We acknowledge that with this digital transformation, the threats of cyber crime, cyber attacks, data breaches and privacy invasion are real and appreciable.

1.49 While cyber threats are not distinct to New South Wales, the landscape in which the state operates places it in a unique position. The committee acknowledges the existing measures by NSW Government to be cyber secure, however we also are concerned that a failure to get cyber security right in New South Wales represents a significant risk to the State's economy, businesses and community, and will affect public trust in Government.

1.50 Conversely however, ensuring sound cyber security practice across NSW Government agencies will place the State in a position to leverage the significant opportunities that come with operating safely in an increasingly digital world.

1.51 Chapters 2, 3 and 4 contain recommendations to the NSW Government for improving cyber security in New South Wales across its agencies, industry, local government and the public.

1.52 Further, the committee notes the work of the NSW Police Force to both ensure its own systems are updated and secure as well as efforts to combat cyber crime in the community. In this regard, the committee considers the age of the NSW Police Force's main database a concern and hopes that efforts to move to a new, more secure system are realised as soon as possible. In addition, the committee recognises the challenges associated with investigating cyber crimes and believes that a continued focus on ensuring the NSW Police Force has adequate resources and skills base to deal with these complex crimes is essential.

[49] Evidence, Deputy Commissioner Hudson, 3 February 2021, p 42.

Chapter 2 Service NSW data breach and the approach to cyber security by NSW Government agencies

This chapter begins by examining the concerning large scale data breach of Service NSW customer records that occurred in March and April 2020. The chapter then considers whether there are opportunities to strengthen the management of cyber security within NSW Government agencies, including educating and upskilling government employees. In considering these factors the committee will also examine work conducted by the New South Wales Auditor-General and Information and Privacy Commission.

Service NSW privacy breach

2.1 In May 2020, the NSW Government announced that it had experienced a targeted phishing attack on 47 staff email accounts, containing personal information of customers of Service NSW. Further investigation revealed that 3.8 million documents had been stolen, compromising the personal information of 186,000 people. At this time, Services NSW reported that 'cyber attacks occur daily' but that they are often able to intercept them.[50] The number of affected people has subsequently been reduced to 104,000 following further investigations.[51]

2.2 This attack was the result of multi-factor authentication not being activated on staff accounts and the significant volume of information that staff were sharing over email.

2.3 Many participants provided evidence regarding these cyber attacks and the response by Service NSW.

2.4 In its December 2020 review of Service NSW's handling of personal information, the New South Wales Auditor-General provided a detailed description of the attacks. This summary provides useful background:

- in late March to early April 2020, Service NSW suffered two cyber security attacks in relatively short succession. In mid-April 2020, Service NSW engaged a cyber security consultant after concerns were raised that an employee's email account was used to send an email to 2,725 Service NSW users, including content indicative of phishing attempts
- analysis found that it was an external actor using a malicious phishing campaign that mimicked an Office 365 warning email, prompting Service NSW employees to visit a fake Office 365 login page which solicited the user’s Service NSW credentials
- as a consequence, 47 staff members had their email accounts accessed without authorisation. Service NSW originally reported that this cyber attack had resulted in the breach of around five million documents, of which around 500,000 were likely to

[50] Service NSW website, *Service NSW cyber incident*, viewed at https://www.service.nsw.gov.au/cyber-incident.

[51] Service NSW website, *Service NSW cyber incident*, viewed at https://www.service.nsw.gov.au/cyber-incident.

contain personal information. Service NSW also reported that around 186,000 NSW residents had been affected by the cyber attack

- on 16 December 2020, Service NSW issued a statement that, while analysis is still ongoing, it now estimates that fewer people may be affected by the breach.[52]

2.5 The Auditor-General noted that even if the estimate of affected people is revised, the impact of the breach has nevertheless been serious, and the processes in Service NSW need significant improvement.[53]

2.6 Mr Damon Rees, the Chief Executive Officer of Service NSW, described the cyber attack on his agency as 'deeply disappointing' and said that they are doing 'everything that we possibly can to support any customers that may have been impacted'.[54] He said that he first became aware of the cyber incident in mid-April and then it took his agency approximately 3 weeks to verify the incident.[55]

2.7 On notice, the Department of Customer Service advised that:

- it first alerted Minister Dominello's office to the breach and potential customer impacts on **5 May 2020**
- this conversation immediately followed receipt of a report from Crowdstrike, a forensic security firm engaged to conduct a preliminary analysis of the incident, into the estimated scope of the breach, and the commencement of a preliminary plan by Allens, an internal commercial law firm engaged to provide legal advice and forensic investigation, to analyse the 47 inboxes on 4 May 2020
- Minister Dominello's office was contacted on **12 May 2020** ahead of the formal briefing the next day.
- once the magnitude of the breach was realised, a formal privacy briefing was held at 10.00 am on **13 May 2020** attended by the Minister, DCS Secretary Emma Hogan, SNSW CEO Damon Rees, DCS Chief Operating Officer Stephen Brady, and GCISO Greg Wells, other senior staff along with the privacy advisors Information Integrity Solutions
- a follow-up briefing was given to Minister Dominello on **18 May 2020** by Mr Rees.[56]

2.8 Mr Rees also explained to the committee the way in which his agency notified those impacted. He said his agency notified affected individuals 'via registered person to person mail'. The letters contained personalised information and guidance on how to manage the risk. He explained that notification took longer as Service NSW wanted to notify only once a complete picture to the

[52] New South Wales Auditor-General, *Special Report: Service NSW's handling of personal information*, 18 December 2020, p. 7, viewed at https://www.audit.nsw.gov.au/our-work/reports/service-nsws-handling-of-personal-information.

[53] New South Wales Auditor-General, *Special Report: Service NSW's handling of personal information*, 18 December 2020, p 7.

[54] Evidence, Mr Damon Rees, Chief Executive Officer, Services NSW, 3 February 2021, p 21.

[55] Evidence, Mr Rees, 3 February 2021, p 21.

[56] Answers to questions on notice and supplementary questions, Department of Customer Service, received 2 March 2021, p 1.

customer could be provided.[57] Mr Rees advised that they have successfully notified 70 to 80 per cent of the affected people.[58]

2.9 Mr Rees further advised that Service NSW established a specialised team to provide support to those affected by the breach:

> The hypercare team is a team that was stood up within Service NSW. They received specialty training around privacy and how to support people that may have been impacted by a privacy breach. They were the dedicated team that we put in place to handle or to support customers that had been impacted by this cyber attack.[59]

2.10 The committee heard from members of the public impacted by the data breach. One participant spoke about the impact upon him and his family, which is exacerbated by the unknown of how or when their personal information might be exploited or what danger they may face as a result.[60]

Case study – A family's personal information stolen from the Service NSW system[61]

In September 2020, a member of the public was contacted by Service NSW and told that data pertaining to him and his family members had been stolen after its system was hacked six months earlier. He expressed concerns about the impact on him and his family given the amount of their personal data stolen. He was told that the hackers had taken his and his wife's birth certificates, the registration of their children's birth, drivers licences and Medicare cards. This information is extensive and provides information about his family's location, images of their faces, their signatures as well as details about their occupations.

Without knowing the motivation of the hackers or being able to see where their personal records have ended up, he holds serious concerns for the safety of his family. He fears the worst; child trafficking or abduction, noting these to be highly lucrative criminal industries.

He has also spent significant time trying to deal with the issues and get the necessary support. He has made a complaint to the Information and Privacy Commission NSW, in which he raised that, despite the Auditor-General highlighting concerns with cyber security in New South Wales six months earlier, the data of his family was stolen, thus endangering their lives. He believes that Service NSW has failed to protect his privacy, despite the warning.

Ultimately he wants to know what the NSW Government will do to ensure the safety of his family.

2.11 The member of the public also explained that when he was first notified of the breach, he received unsatisfactory information. He indicated that the letter he received was very ambiguous regarding what data had been compromised and he had to follow up with Service NSW to get exact information'.[62]

[57] Evidence, Mr Rees, 3 February 2021, p 21.

[58] Evidence, Mr Rees, 3 February 2021, p 27.

[59] Evidence, Mr Rees, 3 February 2021, p 24.

[60] Submission 27, Name suppressed, pp 1-3; *In camera* evidence, Witness A, 3 February 2021, pp 1-5, published by resolution of the committee on 19 March 2021.

[61] Submission 27, Name suppressed, pp 1-3; *In camera* evidence, Witness A, 3 February 2021, pp 1-5, published by resolution of the committee on 19 March 2021.

[62] *In camera* evidence, Witness A, 3 February 2021, p 2, published by resolution of the committee on 19 March 2021.

2.12 Another participant who was also affected by the Service NSW breach, Ms Claire Falkingham, explained the impact of the breach on her life. Ms Falkingham describes a state of complete shock on being told about the breach and was unhappy that she was not informed earlier:

> I was completely shocked when I read this, it was a massive bombshell. I had no indication that this had happened, let alone 6 months prior. My Drivers Licence? That's just about as personal as it gets, that's my full name, address, date of birth, Driver's Licence Number! Leaked, into the hands of unknown Cyber Criminals. I was incredibly shocked and deeply upset on hearing this news. I still am in a state of utter bewilderment.[63]

2.13 Ms Falkingham described the impact of the attack noting the difference with physical crimes: '… when you are the victim of an attack that causes physical injury, people can see those injuries, but with cyber crime, the injuries are invisible, and long lasting'.[64]

2.14 Ms Falkingham was also dissatisfied with the response and support provided by Service NSW following the attack:

> The subsequent, information from Service NSW provided was just empty platitudes, and useless information. In order to assess if my personal details are being used to commit crimes, the process has been completely outsourced by Services NSW, to MyDataCare, which requires the victims of this crime, to enter their most personal Identification documents, online, via 3 separate, outsourced Agencies! Unbelievable in itself, that the Victims of this Cyber Attack would feel safe in doing this![65]

2.15 She went on to explain that the onus is now on her to deal with the fallout and no counselling or support was offered:

> Service NSW have offered the Victims of this Crime no support, instead offering empty advice that goes nowhere, and a veiled apology, whilst firmly placing the onus on each victim to tidy up the mess directly caused by their failings. No responsibility has been taken to offer support or counselling for the victims of this crime.[66]

2.16 Other inquiry participants, although not directly affected, also expressed concerns about the Service NSW data breach, including its response. Dr Bruce Baer Arnold, Associate Professor of Law from Canberra University, was of the view that the Service NSW breach indicates that privacy not being prioritised by the NSW Government:

> Irrespective of the problematical nature of the claim to have 'absolutely enshrined' privacy as a right, the exposure of Service NSW information about some 186,000 people – indicates that privacy is not put 'front and centre' by the Government and by what appears to be a service provider.[67]

2.17 Dr Arnold also expressed concerns regarding the disclosure of the breach and the confusing reference to the 'hyper care' team:

[63] Submission 28, Ms Claire Falkingham, p 1.

[64] Submission 28, Ms Claire Falkingham, p 1.

[65] Submission 28, Ms Claire Falkingham, p 1.

[66] Submission 28, Ms Claire Falkingham, p 2.

[67] Submission 16, Dr Bruce Baer Arnold, p 7.

> In the Service NSW incident that needed to be quicker than four months and without the Minister's obfuscation that the affected people were receiving "hypercare", a term that does not have a legal meaning and in practice appears to be little more than a marketing statement worthy of condemnation by the Committee.[68]

2.18 Mr Tony Vizza from the Australian Information Security Association also raised concerns about the time it took for Service NSW to notify those affected by the data breach:

> I do note that the Service NSW breach has resulted in initially some soul searching around the fact that there was a big delay in letting people who were affected know that they had been affected. I think that it was disappointing from a practitioner's perspective to see that.[69]

2.19 Service NSW has partnered with independent cyber support community service IDCARE to provide an additional level of expert support.[70]

2.20 In discussing how the attacks were possible, Mr Ian Goodwin, Deputy Auditor-General, confirmed 'it is true that information within Service NSW is passed via email and that was subject to phishing attacks'.[71] Ms Claudia Migotto, Assistant Auditor-General noted that this practice of emailing people had previously been identified as high risk some 12 months before the breach occurred.[72]

2.21 As mentioned above, following the attacks, the Auditor-General was charged with conducting a review into Service NSW's handling of personal information. The Auditor-General made eight recommendations for reform, two of which were classed as urgent. In the report, the Auditor-General stated that 'it is unclear why Service NSW did not effectively mitigate this risk prior to the breaches'. It concluded that:

> Service NSW is not effectively handling personal customer and business information to ensure its privacy. It continues to use business processes that pose a risk to the privacy of personal information. These include routinely emailing personal customer information to client agencies, which is one of the processes that contributed to the March 2020 data breach. Previously identified risks and recommended solutions had not been implemented on a timely basis.[73]

2.22 The Auditor-General explained that the breach was also enabled by the lack of multi-factor authentication which, like the sharing of information over email, had also been identified as a risk a year prior to the attacks:

[68] Submission 16, Dr Bruce Baer Arnold, p 7.

[69] Evidence, Mr Tony Vizza, Board Member, Australian Information Security Association, 29 October 2020, p 14.

[70] Service NSW website, *Service NSW notifies customers in relation to cyber incident*, viewed at https://www.service.nsw.gov.au/news/service-nsw-notifies-customers-relation-cyber-incident.

[71] Evidence, Mr Ian Goodwin, Deputy Auditor-General, Audit Office of New South Wales, 3 February 2021, p 3.

[72] Evidence, Ms Claudia Migotto, Assistant Auditor-General, Audit Office of New South Wales, 3 February 2021, p 3.

[73] New South Wales Auditor-General, *Special Report: Service NSW's handling of personal information*, 18 December 2020, p 2.

> The lack of multi-factor authentication has been identified as another key contributing factor to the March 2020 data breach as this enabled the external threat actors to gain access to staff email accounts once they had obtained the user account details through a phishing exercise. Service NSW had identified the lack of multi-factor authentication on its webmail platform as a risk more than a year prior to the breach and had committed to addressing this by June 2019. It was not implemented until after the breach occurred.[74]

2.23 The Auditor-General also reported that the cost of the breach is expected to be in excess of $30 million and this does not include costs associated with remediation or compensation for affected individuals:

> As Service NSW's response to the breach was ongoing at the time of this audit, the full cost of its response was not known. However the agency advised that it is expected to be in excess of $30 million. This amount includes postage, legal and investigative resources, as well as external consultants, vendors, and staff costs. The amount does not include any costs for remediation or compensation that may be required to be paid to affected individuals, including any costs of replacing documents such as the licences or passports of affected individuals.[75]

2.24 Ms Samantha Gavel, the NSW Privacy Commissioner expressed the view that on the back of the Service NSW breach there were some important lessons regarding the level of support that must be provided to people affected by data breaches. She said:

> I think there are some important lessons that are going to come out of this breach. Two that really resonate with me—one is how we look after people when this kind of breach occurs, because it is very stressful and difficult for people when they have a piece of identity information that is compromised. Unfortunately, even though Service NSW did a lot of work to put their hypercare team into place and to have ID care available for people, at the end of the day people actually have to run around and get their new driver licence, get their new birth certificate, tell the police—all those things they have to do, along with everything else and the stress of the breach.[76]

2.25 The Privacy Commissioner also agreed that the remedies available to people following a breach required consideration:

> I think it [remedies] is something that we need to look at because cyber breaches are going to be with us going forward. We are all putting more of our personal lives online. We expect government to be available to us online and cyber breaches are part of that landscape. So, I think these are issues that we really need to consider.[77]

2.26 In discussing the factors that led to the breach occurring in the first place, Mr Rees from Service NSW acknowledged that the multi-factor authentication had not been achieved despite earlier

[74] New South Wales Auditor-General, *Special Report: Service NSW's handling of personal information*, 18 December 2020, p 2.

[75] New South Wales Auditor-General, *Special Report: Service NSW's handling of personal information*, 18 December 2020, p 6.

[76] Evidence, Ms Samantha Gavel, NSW Privacy Commissioner, 3 February 2021, p 16.

[77] Evidence, Ms Gavel, 3 February 2021, p 16.

intentions to do so, however stated that it 'is only one of a range of controls and that control on its own would not have prevented this incident from occurring'.[78]

2.27 Mr Rees also recognised that the sending of personal information via email was high risk and required fixing. When asked whether that practice was still in use he said that it was:

> Right now, yes, there is an ongoing dependency on email. The amount of email that is held is drastically reduced and the security of that platform has been strengthened. But right now, yes, there is an ongoing dependency until the rest of those plans are completed.[79]

2.28 On notice, the Department of Customer Service indicated that a program to enable multi-factor authentication on emails was initiated in 2019/20, but progress was paused due to organisational transformation. It was deferred due to the NSW Bushfire Emergency response and the at-the time need to extend 24/7 customer support to impacted communities.[80]

2.29 The Department of Customer Service also advised that, as of June 2020, Service NSW has implemented an email management initiative to 2,300 frontline staff emails accounts which automatically archives all emails older than 60 days. Emails that have been identified and tagged as containing sensitive information are automatically archived after five days. This has resulted in 92 per cent less data being held in these email accounts.[81]

2.30 Further initiatives identified by the department include the Service NSW Cybersecurity Uplift and Remediation Program and the Service NSW Privacy Program. The Service NSW Privacy Program will address the eight recommendations made by the Audit Offices' Handling of Personal Information report. This includes an urgent focus on options for implementing secure methods of transferring and storing personal information, replacing the need for Service NSW to rely on email and reviewing the privacy provisions detailed in Partner Agency agreements.[82]

2.31 Mr Rees also outlined that Service NSW was undertaking work to reduce the manual handling of information:

> That requires, in many cases, the fundamental digitisation of those processes end-to-end so that the information does not have to be manually handled. It is an important piece of work. It is not a quick or easy or fast piece of work, but that is the work that we are mobilising now with our partner agencies.[83]

2.32 In respect of notifying people impacted by the breach, Mr Rees explained that there were challenges in managing the notification process:

[78] Evidence, Mr Rees, 3 February 2021, p 25.

[79] Evidence, Mr Rees, 3 February 2021, p 29.

[80] Answers to questions on notice and supplementary questions, Department of Customer Service, received 2 March 2021, p 3.

[81] Answers to questions on notice and supplementary questions, Department of Customer Service, received 2 March 2021, pp 2-3.

[82] Answers to questions on notice and supplementary questions, Department of Customer Service, received 2 March 2021, pp 2-3.

[83] Evidence, Mr Rees, 3 February 2021, p 29.

> One of the very difficult things about dealing with this situation has been how to notify. It has been challenged by a couple of things: the first is incomplete information around the customers that are impacted, including contact information for those customers. The second thing we have been very mindful of is how to minimise the risk of scams to customers in our efforts to notify them.[84]

2.33 Mr Rees indicated that when Service NSW did advise the public, it noticed further attempted scams:

> One of the things we observed is that when we did advise the public that we had been impacted by a breach, almost immediately, members of the public were receiving attempted scam calls off the back of that public awareness to attempt to defraud them.[85]

2.34 The Department of Customer Service also advised that, as at 17 February 2021 there have been:

- 94 requests for compensation from citizens whose data was compromised, of which 26 have been remunerated
- 83 requests for reimbursement of costs from citizens whose data was compromised, of which 57 have been remunerated.[86]

2.35 Deputy Commissioner Hudson told the committee that NSW Police Force is investigating the Service NSW breach and that the investigation is ongoing. He described the attack as involving malicious intent amounting to cyber crime.[87]

Responsibilities of Cyber Security NSW and other NSW Government agencies

2.36 In May 2019, Cyber Security NSW was established, replacing the Office of the Government Chief Information Security Office.[88]

2.37 In describing the work of the recently formed office, the NSW Government advised that Cyber Security NSW, part of Department of Customer Services, focuses on enhancing whole-of-government cyber security capabilities and standards, improving cyber incident response coordination and overseeing the development of strategic cyber policies.[89]

2.38 Mr Tony Chapman from Cyber Security NSW described the work of his agency as providing whole-of-government leadership, coordination, advice and intelligence across the NSW Government on cyber security:

> Cyber Security NSW provides whole-of-government leadership, coordination, advice and intelligence across New South Wales government, including to small agencies and

[84] Evidence, Mr Rees, 3 February 2021, p 21.

[85] Evidence, Mr Rees, 3 February 2021, p 21.

[86] Answers to questions on notice and supplementary questions, Department of Customer Service, received 2 March 2021, p 2.

[87] Evidence, Deputy Commissioner Hudson, NSW Police Force, 3 February 2021, p 38.

[88] Digital NSW website, cyber security, https://www.digital.nsw.gov.au/transformation/cyber-security, viewed 3 February 2021.

[89] Submission 10, NSW Government, p 4.

> our local councils, to reduce cyber risks. We coordinate whole-of-government cyber security incident response, including liaison with the Australian Cyber Security Centre and other jurisdictions, by what is known as the National Cyber Security Committee. We set whole-of-government cyber security policies and standards and deliver training, awareness and resilience programs across New South Wales government.[90]

2.39 While noting the role Cyber Security NSW plays, Mr Chapman explained that each government agency is responsible for their own cyber security risks, including 'governance, control, direction and management'.[91]

2.40 Mr Greg Wells, Chief Information and Digital Officer, Department of Customer Service said that decide 'from their perspective what their biggest risks are and what they need to address'. He further explained that while there are mandatory requirements, it is up to each individual cluster to assess their risks and decide what action, if any, is required:

> It is set and mandated across; it is not different per agency. My comment was that it is a risk-based approach that every cluster will take in terms of that same policy and where they see the need for greatest uplift: where there are gaps and where they need to increase capability in those areas. So there are not different policies. It is the one policy with the same 25 requirements across all agencies. Clusters construct from their perspective what their biggest risks are and what they need to address.[92]

2.41 As each cluster is ultimately accountable and responsible for determining their own risks, Mr Wells explained that his agency's role is 'to lift that capability and protection consistently across government'.[93] Further, Mr Wells advised that it is not the role of Cyber Security NSW to know what data each agency collects or where it is stored. Instead, the agency shares intelligence, runs exercises, and builds capability.[94]

2.42 Mr Chapman explained that under its Cyber Security Policy, agencies are now required to 'report what is known as their crown jewels or high-risk assets' to his agency. And that 'for the first time … Cyber Security NSW has a view of what those critical and high risks are across government'.[95]

2.43 Mr Wells indicated that while agencies report what their 'crown jewels' are, Cyber Security NSW does not have a role in understanding where or how this is stored:

> It is not to understand where every cluster's exact data is. We do specifically look, as Mr Chapman said, for reporting around Crown jewels the most important systems and data that clusters hold and run, but it is not specifically to understand every component of that, no.[96]

[90] Evidence, Mr Tony Chapman, Chief Cyber Security Officer and Executive Director, Cyber Security NSW, 3 February 2021, p 20.

[91] Evidence, Mr Chapman, 3 February 2021, p 20.

[92] Evidence, Mr Greg Wells, Chief Information and Digital Officer, Department of Customer Service, 3 February 2021, p 22.

[93] Evidence, Mr Wells, 3 February 2021, p 23.

[94] Evidence, Mr Wells, 3 February 2021, p 33.

[95] Evidence, Mr Chapman, 3 February 2021, p 22.

[96] Evidence, Mr Wells, 3 February 2021, p 33.

2.44 However, Mr Chapman advised that there are plans afoot for his agency to take on more of a compliance role to assist agencies with their risk identification and reporting:

> Cyber Security NSW does have experts within the team that, I guess, sense check and ensure a rigorous approach to that reporting and upon receiving the additional funding will be standing up at a governance, risk and compliance function within Cyber Security NSW to ensure the accuracy of that reporting to us.[97]

2.45 NSW Government advised that in respect of the $240 million investment it has made to enhance cyber security in New South Wales, $180 million is for clusters to access. This investment is for 'targeted cyber security uplift to better manage and address cyber security risks, improve the maturity of cyber security practice in agencies as they implement technical safeguards, and align to best practice standards in the Cyber Security Policy'.[98]

2.46 Mr John Frisken from ISG Consulting expressed concerns about the responsibility for security being handed back to agencies as well as there being too many different, and at times conflicting, policies:

> We think the main problem is that those standards are not being implemented. There are a couple of reasons for that. One is really the devolution of security back into the agencies. There was a stronger presence when we started this process back in 2001. Security in a sense has lost its way. In fact, there has probably been an over-focus on policy. There are now about three or four different policies related to cyber security in New South Wales. It is a very confusing situation. In some of the major agencies, we have found that in fact they conflict with each other and cannot all be implemented. That is one of the main issues that we are seeing.[99]

2.47 Other participants expressed views about the lack of oversight or compliance monitoring with respect to NSW Government agencies' handling of cyber security. For example, Mr Thomas Costa from Unions NSW said that 'there should be a department that should regulate all data across the public sector, and which is responsible for regulating and monitoring breaches but also providing transparency around when those breaches occur'.[100]

2.48 Similarly, Mr Knights and Mr Vizza from the Australian Information Security Association agreed with the proposition that a potential model could be that a central agency sets the standards and compliance regime, but that the line responsibility rests with each individual agency.[101]

[97] Evidence, Mr Chapman, 3 February 2021, p 26.

[98] Submission 10, NSW Government, p 6.

[99] Evidence, Mr John Frisken, Director Professional Services, ISG Consulting Pty Ltd, 29 October 2020, p 33.

[100] Evidence, Mr Thomas Costa, Assistant Secretary, Unions NSW, October 29 2020, p 40.

[101] Evidence, Mr Vizza, 29 October 2020, p 15; Evidence, Mr Stephen Knights, Australian Information Security Association, 29 October 2020, p 15.

Oversight agency evidence

2.49 The committee received evidence from the Auditor-General and the Information and Privacy Commission NSW regarding the way in which NSW Government agencies are implementing cyber security policies and protecting the privacy of citizens.

Auditor-General

2.50 The Auditor-General has undertaken a number of relevant audits in the last few years. These are:

- Detecting and responding to cyber security incidents performance audit, published 2 March 2018
- Report on Internal Controls and Governance 2019, published 5 November 2019
- Report on Local Government 2019, published 5 March 2020
- Integrity of data in the Births, Deaths and Marriages Register performance audit, published 7 April 2020
- Universities 2019 financial audits, published 4 June 2020
- Central Agencies Report 2020, published 10 December 2020
- Special Report: Service NSW's handling of personal information, published 18 December 2020.[102]

2.51 The Central Agencies Report 2020 identified concerns about agencies' approach to cyber security and recommended that: 'Cyber Security NSW and NSW Government agencies need to prioritise improvements to their cyber security resilience as a matter of urgency'.[103]

2.52 During evidence, Mr Ian Goodwin, Deputy Auditor-General also expressed the view that both Cyber Security NSW and other agencies need to improve:

> The Auditor-General recommended for a second year that Cyber Security NSW and New South Wales government agencies need to prioritise improvements to their cyber security resilience as a matter of urgency.[104]

2.53 Mr Goodwin stated that the NSW Cyber Security Policy does not mandate achieving a certain standard like the Commonwealth policy does, but rather it mandates NSW Government agencies to conduct cyber security self-assessments. He said:

> I guess the difference though between the State and the Commonwealth level is that the Commonwealth level mandates achieving certain levels of maturity, whereas in New South Wales we mandate in a self-assessment but not baselining a minimum level to be achieved.[105]

[102] Submission 6, New South Wales Auditor-General, p 1; Evidence, Mr Ian Goodwin, Deputy Auditor-General, Audit Office of New South Wales, 3 February 2021, p 2.

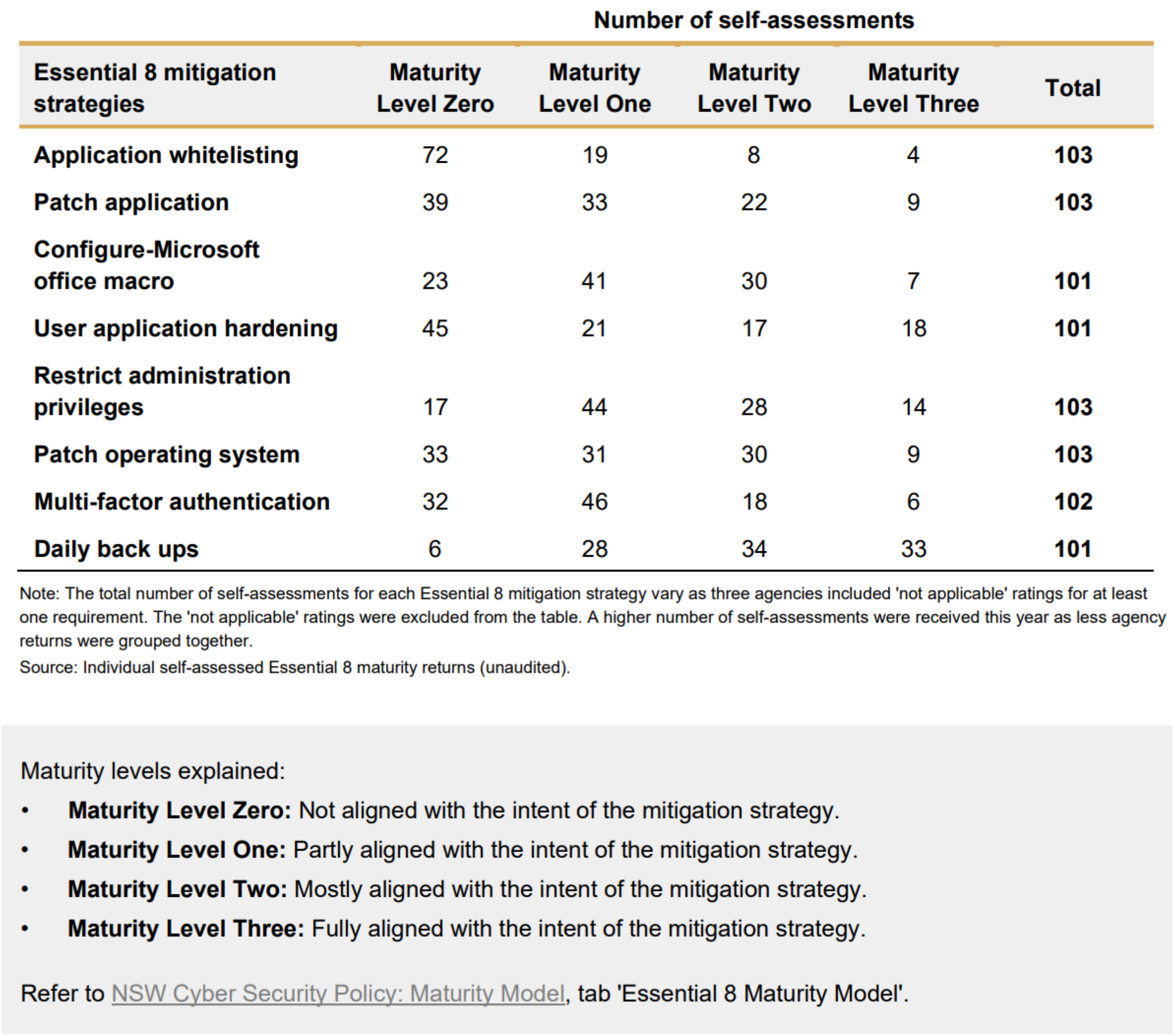
[103] New South Wales Auditor-General, *Central Agencies Central Agencies Report 2020*, 10 December 2020, p 3, viewed at https://www.audit.nsw.gov.au/our-work/reports/central-agencies-2020.

[104] Evidence, Mr Goodwin, 3 February 2021, p 2.

[105] Evidence, Mr Goodwin, 3 February 2021, p 7.

2.54 The Central Agencies Report also stated that 'NSW Government agency self-assessment results show that the NSW Public Sector's cyber security resilience needs urgent attention'.[106] It published the 2020 results of the annual cyber security assessment completed by agencies, in respect of the essential 8 (see figure 2 below).

Figure 2 NSW Government agencies' self assessment results table



	Number of self-assessments				
Essential 8 mitigation strategies	**Maturity Level Zero**	**Maturity Level One**	**Maturity Level Two**	**Maturity Level Three**	**Total**
Application whitelisting	72	19	8	4	**103**
Patch application	39	33	22	9	**103**
Configure-Microsoft office macro	23	41	30	7	**101**
User application hardening	45	21	17	18	**101**
Restrict administration privileges	17	44	28	14	**103**
Patch operating system	33	31	30	9	**103**
Multi-factor authentication	32	46	18	6	**102**
Daily back ups	6	28	34	33	**101**

Note: The total number of self-assessments for each Essential 8 mitigation strategy vary as three agencies included 'not applicable' ratings for at least one requirement. The 'not applicable' ratings were excluded from the table. A higher number of self-assessments were received this year as less agency returns were grouped together.

Source: Individual self-assessed Essential 8 maturity returns (unaudited).

Maturity levels explained:

- **Maturity Level Zero:** Not aligned with the intent of the mitigation strategy.
- **Maturity Level One:** Partly aligned with the intent of the mitigation strategy.
- **Maturity Level Two:** Mostly aligned with the intent of the mitigation strategy.
- **Maturity Level Three:** Fully aligned with the intent of the mitigation strategy.

Refer to NSW Cyber Security Policy: Maturity Model, tab 'Essential 8 Maturity Model'.

2.55 Further, in March 2018, the Auditor-General released a report into the examination of cyber security incident detection and response in the New South Wales public sector. That report concluded that there is no whole-of government capability to detect and respond effectively to cyber security incidents.[107]

2.56 The Auditor-General has also previously made recommendations regarding controls and governance arrangements in place to manage sensitive data in NSW Government agencies. This review found that agencies need to do better at identifying what sensitive data they hold;

[106] New South Wales Auditor-General, *Central Agencies Central Agencies Report 2020*, 10 December 2020, p 17.

[107] Submission 6, New South Wales Auditor-General, p 17.

maintaining an inventory for this data; developing comprehensive data management policies; maintaining a data breach register; and providing ongoing training and awareness to employees.[108]

2.57 The Auditor-General has also undertaken reviews of universities, local government and Birth, Deaths and Marriages data. All of these reviews found opportunities for improvement:

- **Universities** were told to strengthen cyber security frameworks and controls to protect sensitive data. It was found that the number of incidents recorded in 2019 ranged from 2 to 982, with the range being attributed to definitional issues. It also found that on average universities incurred $4.6 million in costs in managing cyber security in 2019.[109]
- It was found that **local councils** lacked a consistent responses and required a cyber security policy to address this. Further, local councils had failed to implement basic elements of governance for cyber security such as a policy or framework.[110]
- While controls existed, gaps in the integrity of **Births, Deaths and Marriages data** controls were identified. Recommendations were made to improve monitoring of user activity, oversight of security controls and controls to prevent distribution of information in the register.[111]

2.58 During the hearing, when questioned about the findings of these reports, and in particular the Service NSW report, Mr Goodwin advised that while the Audit Office has made recommendations warranting attention, he believes that agencies are making progress:

> …we have said that this is an area that needs priority and needs attention, but that does not mean that it is not getting priority and it is not getting attention. It is a journey piece and, in many senses, because of the ubiquitous nature of the risk, it is very hard to get a defined end point and so you are constantly evolving your risk management practices to the constantly evolving threat environment. What I would acknowledge, and I think it is important to acknowledge, is that since the performance audit in 2018 which recommended that there should be a whole-of-government response, there has been a series of government responses.[112]

2.59 Mr Goodwin clarified that in short, cyber security is receiving attention, but it is a complex area that must be considered a priority for the NSW Government.[113]

Information and Privacy Commission NSW

2.60 The Information and Privacy Commission NSW oversees the operation of privacy and information access laws in New South Wales.[114]

[108] Submission 6, New South Wales Auditor-General, p 10.

[109] Submission 6, New South Wales Auditor-General, pp 4-5.

[110] Submission 6, New South Wales Auditor-General, p 9.

[111] Submission 6, New South Wales Auditor-General, pp 6-7.

[112] Evidence, Mr Goodwin, 3 February 2021, p 2.

[113] Evidence, Mr Goodwin, 3 February 2021, p 3.

[114] Submission 14, Information and Privacy Commission, p 1.

2.61 The Privacy Commissioner has responsibility for overseeing and advising New South Wales public sector agencies on compliance with the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*.[115]

2.62 The Information Commissioner has responsibility for overseeing the information access rights enshrined in the *Government Information Public Access Act 2009*. These rights are realised by agencies authorising and encouraging proactive public release of government information; and by giving members of the public an enforceable right to access government information.[116]

2.63 Discussed more in chapter 3, the Information and Privacy Commission NSW advised that it operates a voluntary reporting scheme for when agencies experience data breaches:

> The current voluntary scheme encourages agencies that have experienced a serious data breach to report the details of the breach to the Privacy Commissioner, so that the Privacy Commissioner can assess the breach, provide advice or investigate. Agencies are also encouraged to voluntarily notify people affected by a data breach and provide information about their right to seek an internal review under the PPIP Act in relation to the breach.[117]

2.64 The Information and Privacy Commission NSW advised that once a breach has been identified, it works with agencies to assist them to improve their privacy and data protection measures: 'The IPC engages with agencies that have experienced a serious data breach and provides comprehensive advice to agencies to assist them to improve their privacy and information governance policies, procedures and practices'.[118]

2.65 The submission from the Information and Privacy Commission NSW highlighted the office's work in respect of Privacy-by-Design. It explained the Privacy-by-Design concept as a method of implementing preventative measures which remove or mitigate privacy and security risks:

> Privacy by Design is a methodology that enables privacy to be built into the design and structure of information systems, business processes and networked infrastructure. PbD considers privacy and security requirements from the outset. Implementing preventative measures which remove or mitigate privacy and security risks is more effective to containing costs, managing community expectation and realising policy intent than developing legislative exceptions to privacy laws or redesigning programs or digital solutions after the fact.[119]

2.66 At the hearing, the Privacy Commissioner was questioned about the application of the Privacy-by-Design principle and her office's involvement in ensuring it is factored into new technologies such as the Service NSW app which includes the COVID safe check in feature. Ms Samantha Gavel, Privacy Commissioner advised that the app does not collect location information and noted that privacy protections have been built into the service:

> …the Service app does not collect location information and nor does the COVID check-in feature. Those are important privacy protections that are built into the app.

[115] Submission 14, Information and Privacy Commission, p 1.

[116] Submission 14, Information and Privacy Commission, p 1.

[117] Submission 14, Information and Privacy Commission, p 3.

[118] Submission 14, Information and Privacy Commission, p 4.

[119] Submission 14, Information and Privacy Commission, p 4.

> We have worked with Service on a number of projects, including the digital driver licence, and they have been very aware of the need for privacy by design in those particular projects.[120]

2.67 The Privacy Commissioner explained that information from the Service NSW app will only be passed to NSW Health should it be needed for contact tracing and that it is deleted after 28 days.[121]

2.68 However, the Privacy Commissioner agreed that the Auditor-General had identified deficiencies in the Service NSW Privacy Management Plan. When asked why such deficiencies had been identified by the Auditor-General and not the Privacy Commissioner's office, Ms Gavel explained the limitations of her agency with its broad remit and finite resourcing:

> The IPC is a small agency with a very broad remit and we have quite a number of ways that we engage with agencies and assist them. We have a limited amount of resourcing. We have a particular resourcing envelope and we need to carry out our functions within that envelope. So we really target our resources and our activities on areas where we can have real impact for agencies. We have not been following up with agencies on privacy management plans to ensure that they have updated them. That is something that we will, in light of the Auditor-General's report, be looking at—whether we need to include that into our forward work program. But privacy management plans are a requirement under legislation and agencies need to comply with that requirement.[122]

2.69 Further, the Privacy Commissioner explained that her office consulted with Service NSW on its Privacy Impact Assessment, however, it's not their role to instruct agencies on requirements:

> I have not got the information with me about the consultation that we did, but what I can tell you is that we consulted with Service NSW. We went through their PIA. We went through the security information. As the regulator, part of our role is to consult to assist them to comply with privacy law. It is not to run the ruler over it per se. It is not an audit function in the way that the Auditor-General carries out.[123]

Educating NSW Government employees on cyber security

2.70 The inquiry heard from many participants about the importance of recruitment, training and skill development to ensure people within government agencies have the capability to implement the processes and technology controls required for cyber security resilience.

2.71 A number of participants spoke about the three-pronged approach to cyber security; being people, processes and technology. Mr Chapman from Cyber Security NSW captured this by explaining:

> Cyber security risks cannot be mitigated through implementation of vulnerability detection and IT controls alone; it requires a combination of people, process and

[120] Evidence, Ms Gavel, 3 February 2021, p 17.

[121] Evidence, Ms Gavel, 3 February 2021, p 17.

[122] Evidence, Ms Gavel, 3 February 2021, p 17.

[123] Evidence, Ms Gavel, 3 February 2021, p 18.

> technical controls to succeed, which is reflected in our approach to the cyber security policy.[124]

2.72 Mr Tony Vizza a Director from (ISC)^2 also described these three pillars:

- the first pillar is an understanding that **people** are the most essential ingredient in any successful cyber security strategy
- the second pillar is understanding that **process** needs to exist when seeking to implement strong cyber security measures
- the third pillar is **technology**.[125]

2.73 He further explained that the relationship between people and processes is to ensure that people in an organisation possess the right level of skills, knowledge, experience and mindset, otherwise any attempt to create processes that minimise risk will be flawed from the outset.[126]

2.74 (ISC)^2 and the Australian Information Security Association expressed concerns about the 2018 NSW Cyber Security Strategy and its lack of coverage regarding education and training for government employees:

> Another arguable area of weakness of the 2018 NSW Cyber Security Strategy was in its omission of a detailed strategy around cyber security education, awareness, accreditation and qualifications for NSW Government employees.[127]

2.75 Mr Vizza referred to the Commonwealth's Cyber Security Skills Framework and called on the NSW Government to develop something similar:

> …at a Federal level the Cyber Skills Framework that was published in September this year is that reference document. The recommendation in our submission is that the State Government incorporate and adopt that as—to your question around proper role definitions and what jobs cyber security people are meant to be doing and what they should have in terms of knowledge, skills and ability to help them achieve that.[128]

2.76 (ISC)^2 and the Australian Information Security Association recommended an approach to quality training citing the internationally accepted cyber security certification 'AS/NZS ISO/IEC 17024:2012 Personnel Accreditation scheme' as an appropriate standards model for the NSW Government to endorse:

> To ensure that the cyber workforce and skills ecosystem across NSW is trained in globally recognised, quality-assured and industry relevant knowledge, the NSW Government should endorse, promote and adopt the internationally accepted AS/NZS ISO/IEC 17024:2012 Personnel Accreditation scheme. This will ensure that cyber security professionals employed by the state of NSW are accredited in globally recognised cyber security certifications, such as those administered by (ISC)^2, all of which are AS/NZS ISO/IEC 17024 accredited. This will help meet a key theme as

[124] Evidence, Mr Chapman, 3 February 2021, p 20.

[125] Evidence, Mr Tony Vizza, Director, (ISC)^2, 29 October 2020, p 20.

[126] Evidence, Mr Vizza, 29 October 2020, p 20.

[127] Submission 20, (ISC)^2, p 7; Submission 24, Australian Information Security Association, p 7.

[128] Evidence, Mr Vizza, 29 October 2020, p 15.

> described in the 2018 NSW Cyber Security Industry Development Strategy, that being of closing the cyber security workforce skills gap.[129]

2.77 These organisations called for the NSW Government to capitalise on the global demand for cyber security skills, knowledge and experience 'by utilising the vast network of universities, TAFE and private sector providers' in the state to help address the cyber security skills shortage.[130]

2.78 Local Government NSW also noted the skills gap and recommended that the NSW Government addresses this by working with TAFE NSW and registered training organisations to develop cyber security training:

> LGNSW recommends the State Government address skill shortages and impediments to employment by working with TAFE NSW and registered training organisations to develop and deliver accredited training programs in specialist skill areas such as cyber security.[131]

2.79 In response, Mr Chapman from Cyber Security NSW explained that since October 2020 it is now a requirement for NSW Government staff to complete 'cyber security training and daily cyber security hygiene practices'.[132]

Committee comment

2.80 The attack on Service NSW and the subsequent data breach of thousands of citizens' personal data raises significant concern for the committee. The committee thanks those members of the public who were directly impacted for participating in this inquiry and providing their insights into how things could be improved. The committee acknowledges the impact that this experience has had on many people and the stress and trauma that this caused and continues to cause.

2.81 This attack, however, provided many insights into how far reaching a successful attack can be and the important lessons agencies can learn in their endeavors to improve their cyber security posture. The committee was disappointed to hear that earlier warnings to improve data management practices within Service NSW were not heeded and thus enabled the attack. The committee recognises that this is a complicated process and that reforms and system improvements can take time, however the committee urges Service NSW to adopt the recommendations of the Auditor-General as a priority. The committee also encourages the NSW Government to ensure other agencies are not exposed in similar ways.

2.82 Further, the committee considers that in the environment of people being required to provide such significant amounts of personal data digitally to a range of agencies, more support is needed for people who become victim of a data breach, including a review of existing remedies.

[129] Submission 20, (ISC)^2, p 8; Submission 24, Australian Information Security Association, p 8.

[130] Submission 20, (ISC)^2, p 8; Submission 24, Australian Information Security Association, p 8.

[131] Submission 2, Local Government NSW, p 2.

[132] Evidence, Mr Chapman, 3 February 2021, p 20.

Finding 1

That the Service NSW data breach may have been prevented had the agency addressed in a more timely manner previously identified risks regarding its handling of personal information.

Finding 2

That once Service NSW became aware of the attack, it took too long to notify those impacted by the breach and it also did not provide sufficient information, support and direct assistance to affected people throughout the process.

Finding 3

That, while Service NSW has taken steps to reduce its dependency on sending personal information via email, it continues to engage in this practice thereby operating in a way that enabled the data breach. The committee urges the cessation of this practice as a matter of priority.

2.83 Nevertheless, the committee recognises the important work of the agencies involved in cyber security in New South Wales. The committee also acknowledges the significant challenges presented by the cyber threat environment and that cyber security is a complex problem requiring considered and ever evolving solutions, which can take time to implement.

2.84 The committee notes the recent developments to strengthen cyber security in NSW Government agencies including work to update the strategy, the implementation of the 2019 cyber security policy, the creation of Cyber Security NSW and the investment of $240 million for enhancement to cyber security measures.

2.85 However, the committee also notes the multiple findings and repeated recommendations from the Auditor-General and the holds concerns about the adequacy of cyber security across agencies. The committee considers it an urgent matter to bring agencies to a more acceptable position, where there is not several months or years taken to implement recommended improvements. This is particularly critical given the evidence before the inquiry regarding the changing threat environment and constant emergence of new technologies.

2.86 In addition to the developments mentioned above, the committee considers that the role of Cyber Security NSW could be enhanced to provide oversight and more direct input on agencies' cyber security risk assessments and mitigation strategies. The committee recognises that each agency needs to be responsible for its own cyber security, however, there is an opportunity for Cyber Security NSW to have a clearer mandate to ensure agencies are meeting a certain standard. This would seem particularly pertinent in light of the findings of the Auditor-General regarding current levels of cyber security maturity across agencies.

2.87 The committee is of the view that in addition to a bolstered mandate, Cyber Security NSW should move from the Department of Customer Service to achieve increased visibility and authority.

Recommendation 1

That the NSW Government review the functions of Cyber Security NSW and provide it with a clearer mandate to oversee agencies' cyber security progress and ensure their compliance with the NSW Cyber Security Policy.

Recommendation 2

That the NSW Government move Cyber Security NSW from within the Department of Customer Service to the Department of Premier and Cabinet to provide it with more independence from service delivery agencies and increased visibility and authority.

2.88 The committee acknowledges the significant responsibility that the Privacy Commissioner has in ensuring citizens' privacy is not compromised through increased digital service delivery. We have made recommendations regarding a mandatory reporting regime in Chapter 3, however we consider that the Privacy Commissioner should have a more active and hands on role in ensuring systems, processes and data are managed in a way that ensures privacy is upheld. The committee notes the finite resources of the Privacy Commissioner's office. However, as the expert body in managing privacy and ensuring measures are adequate to protect citizens' data, there should be more than a requirement upon agencies to complete a Privacy Impact Statement. Instead, this should be quality assured and signed off by the Privacy Commissioner. The committee considers that the Privacy Commissioner should have a more proactive role, particularly as agencies are increasingly providing services online and the Government is accessing citizens' data now more than ever.

2.89 The committee also notes the report of the Standing Committee on Law and Justice of this House on 3 March 2016 on remedies for the serious invasion of privacy in New South Wales. That inquiry heard evidence from individuals, academics, legal experts, media and arts representatives, as well as from privacy experts including the NSW Privacy Commissioner, with the vast majority of stakeholders arguing strongly for the introduction of a statutory cause of action on the basis that existing legal remedies were inadequate. The bulk of evidence was that the available civil remedies, in particular the equitable action for breach of confidence, was inaccessible, offered a 'poor fit', and failed to offer appropriate remedy to people who suffered a serious invasion of privacy. Stakeholders expressed frustration at the lack of decisive action on this issue, despite several eminent reports recommending a similar course.

2.90 Privacy is an asset. Once it is lost, it cannot be recovered. The impacts of that loss can be devastating. The committee agreed that there is a clear need to ensure better protection of privacy, and to provide adequate remedies to people who experience a serious invasion of privacy. To that end, the committee recommended that the NSW Government introduce a statutory cause of action for serious invasions of privacy, based on the model proposed by the Australian Law Reform Commission in its 2014 report Serious Invasions of Privacy in the Digital Era (see recommendations 3 and 4 of that inquiry).

2.91 The committee notes the NSW Parliament has enacted criminal laws to deal with so-called 'revenge porn' but considers that further action is needed in this area and supports the implementation of the recommendations of the Law and Justice Committee report on remedies for the serious invasion of privacy in New South Wales. The implementation of those recommendations would create a legal framework that would significantly assist those persons who have been the victim of cyber attacks, such as in the cyber enabled attack on Service NSW and the subsequent data breach of thousands of citizens' personal data.

Recommendation 3

That the NSW Government review the responsibility and resourcing of the Privacy Commissioner so that the office can be more proactive in ensuring government services and systems are designed and delivered with stringent privacy protections.

Finding 4

That the NSW Government lacks any real framework or clear processes within government to properly and expeditiously deal with requests by people in the community for assistance in the event of a breach of their data. People who suffer data breaches are left to their own resources and the existing, unsatisfactory state of the law where very few persons are eligible for relief, assuming they have the financial resources to seek it.

Recommendation 4

That the NSW Government urgently address the matters identified in Finding 4 and implement a framework or clear process within government to properly and expeditiously deal with requests by people in the community for assistance in the event of a breach of their data.

2.92 The committee recognises the critical role that people play in any agency's cyber security success. The evidence regarding education, skill development, training and support for staff at all levels and roles within agencies was compelling. As an emerging field and the skills shortage we heard about, there is a requirement to ensure there are adequate qualifications and training within our education systems to produce high quality cyber security professionals. Further, the training and skill development within agencies, is paramount to any robust cyber security strategy. Noting the human element in the attacks and data breaches we heard about, agencies need to invest in upskilling staff and raising awareness about the importance of cyber security and the role each employee can play in prevention and early detection. We therefore recommend that the NSW Government work with industry and the education sector to develop a cyber security skills framework for the state.

Recommendation 5

That the NSW Government work with industry and the education sector to develop a cyber security skills framework that includes:

- the provision of a comprehensive and regularly reviewed cyber security training regime for all NSW Government employees
- the requirement for cyber security professionals within NSW Government agencies to be accredited in recognised cyber security certifications
- the provision of adequate tertiary cyber security qualifications to meet government and industry demand.

Chapter 3 Enhancing cyber security in New South Wales

Chapter 2 looked at the responsibility of NSW Government agencies as well as the 'people' aspects of cyber security, including what can happen when an agency does not get its cyber security right. This chapter examines the process and technology measures that contribute to enhancing cyber security in New South Wales. These include standards, monitoring and reporting and building sovereign cyber security capability.

Standards

3.1 A number of participants discussed the opportunity for standard setting by the NSW Government. This included cyber security standards for NSW Government agencies, standards for the procurement of Information Technology services and standards for the security of Internet of Things; particularly those used by NSW Government agencies. The Internet of Things (IOT) refers to the interconnection via the internet of computing devices embedded in everyday objects such as smart televisions and smart fridges, enabling them to send and receive data.

Standards for NSW Government agencies

3.2 As discussed in chapter 1, the NSW Cyber Security Policy outlines 25 'mandatory' requirements against which NSW Government agencies must assess themselves and report on. NSW Government describe the policy in two ways:

- a risk based policy based on the National Institute of Standards and Technology (NIST) cyber security framework
- it outlines the mandatory requirements to which all NSW Government departments and public service agencies must adhere.[133]

3.3 There was general agreement amongst participants that standards are necessary to improve the approach to cyber security in New South Wales. Ms Michelle Price, the CEO of AustCyber viewed that part of the solution with cyber security rests with having proper standards with which Government must comply.[134]

3.4 Mr Tony Vizza from (ISC)^2 and the Australian Information Security Association agreed and said that 'the adoption of industry standards for the management of information security systems is critical'[135]. He viewed that the 'NSW Government as a leader in that space has an opportunity to come up with standards' and recommended training programs that will help us close the gap.[136]

[133] Submission 10, NSW Government, p 2.

[134] Evidence, Ms Michelle Price, Chief Executive Officer, AustCyber, 29 October 2020, p 24.

[135] Evidence, Mr Tony Vizza, Director, (ISC)^2, 29 October 2020, p 20.

[136] Evidence, Mr Tony Vizza, Australian Information Security Association, 29 October 2020, p 11.

3.5 As discussed in chapter 1, representatives from the Department of Customer Services indicated that the NSW Cyber Security Policy provides a base line or a set of standards. Mr Tony Chapman from Cyber Security NSW said that his agency is responsible for setting 'whole-of-government cyber security policies and standards'. He went on to explain that its policy includes 'Australian-leading cyber security standards' which take a risk-based approach to cyber security.[137]

3.6 However, information from the Auditor-General, including the results of agencies' self-assessments, raised concerns about whether the 25 requirements were mandatory standards that must be met, or simply measures which agencies must report against (see chapter 2 for further details).

3.7 The Auditor-General published the results of last year's agency self-assessment reports which showed that in respect of the Essential 8 'mandatory' requirements, many agencies were not implementing them. The Auditor-General stated that 'completed self-assessment returns highlighted limited progress in implementing the Essential 8'.[138]

3.8 The lack of implementation was also highlighted by Mr John Frisken the Director Professional Services for ISG Consulting, who went on to explain that standards needed some form of independent certification to ensure they are being implemented.[139]

3.9 In addition to the need for standards, participants offered views as to most appropriate model of standards to use in New South Wales and noted that the National Institute of Standards and Technology (NIST) is currently used.

3.10 In its submission to the inquiry, ISG Consulting noted its concern about the adoption of the NIST model in New South Wales, as this is out of step with Australia's usual practice of adopting the more familiar European ISO standards.[140]

3.11 ISG Consulting advised that NIST is a North American standard whereas ISO 27001 and IEC 62443 are European. ISO standards have a Plan-Do-Check-Act set of phases throughout all standards, which permits common management systems to be developed across all standard areas. ISG Consulting considered that this leads to enormous cost and efficiency savings for large enterprise who are required to maintain systems for managing multiple standards. It viewed that NIST also has its own set of phases, which while logical, is not is sync with European standards, which Australian Governments and private sectors have traditionally supported. This imposes significant cost and efficiency burdens on large agencies for little or no benefit.[141]

3.12 ISG Consulting further argued that NIST has not been developed within a Certifiable Framework, like ISO standards, and therefore there is no mechanism for legal enforcement by the NSW Government, which is a significant drawback compared to ISO 27001.[142]

[137] Evidence, Mr Tony Chapman Chief Cyber Security Officer and Executive Director, Cyber Security NSW, 3 February 2021, p 20.

[138] New South Wales Auditor-General, *Central Agencies Central Agencies Report 2020*, 10 December 2020, p 17, viewed at: https://www.audit.nsw.gov.au/our-work/reports/central-agencies-2020.

[139] Evidence, Mr John Frisken, Director Professional Services, ISG Consulting Pty Ltd, p 33.

[140] Submission 23, ISG Consulting Pty Ltd, p 4.

[141] Submission 23, ISG Consulting Pty Ltd, p 4.

[142] Submission 23, ISG Consulting Pty Ltd, p 4.

3.13 During evidence, Mr Milton Baar, Director Cyber Security at ISG Consulting Pty Ltd, explained the ISO 27000 standards model and indicated that it is the only standard to which you can be internationally certified:

> There is the 27000 suite of standards and 27001 is the only standard to which you can be internationally certified. If you are certified to 27001 in Australia it is recognised anywhere in the world. It is an information security management standard. All of the others are checklists or guidelines but you cannot be certified to them.[143]

3.1 Mr Baar further described ISO 27001 as a 'cyclic process' that operated to constantly improve practice:

> It is a plan, do, check, act model that you continue forever. It is not an end point … You are literally a hamster on a wheel going around for ever because you never reach the end; you are constantly improving and identifying deficiencies and improving slowly as you go along.[144]

3.2 Mr John Frisken, also from ISG Consulting also viewed that the implementation of the NIST causes confusion and goes against the usual approach in Government of adopting the European standards based on ISO. He said:

> Most standards—almost 100 per cent of standards—that are adopted by government agencies, apart from cyber security, are European; they are based on ISO and take a certain approach to how that is implemented using similar systems. In cyber security we introduced a completely different set, so you have an organisation that is saying that you have to implement NIST because it is a new framework but we have 27001 as well. How do you think an individual agency is going to react to that? They have no idea.[145]

3.3 Mr Frisken viewed that 'we have this really complicated approach at a policy level' in Australia and it is the reason that there are problems with implementation:

> That is probably one of the reasons why there is nothing happening in terms of implementation, because most government departments probably have no idea how to meet that. I would think that is one of the things that needs to be sorted out pretty quickly, to try to simplify that, and get back to a set of standards and policies that can be simply certified against at the moment.[146]

3.4 Similarly, the Australian Information Security Association and $(ISC)^2$ endorsed the adoption of standards aligned with the ISO model. In particular they recommended adoption of the 'ISO/IEC 27000:2018 family of Information Security Management System accreditations, both internally as well as for stakeholders such as suppliers as well as the broader NSW economy'. It viewed that by adopting this recommendation, many of the actions listed in the Action Plan contained in the existing NSW Government Cyber Security Strategy will be met and the NSW Government will lead by example.[147]

[143] Evidence, Mr Milton Baar, Director Cyber Security, ISG Consulting, 29 October 2020, p 39.

[144] Evidence, Mr Baar, 29 October 2020, p 38.

[145] Evidence, Mr John Frisken, Director Professional Services, ISG Consulting Pty Ltd, 29 October 2020, p 38.

[146] Evidence, Mr Frisken, 29 October 2020, p 38.

[147] Submission 20, $(ISC)^2$, p 8; Submission 24, Australian Information Security Association, p 8.

3.5 Mr Vizza, who is a senior lead auditor in ISO 27001, described the flexibility of this suite of standards and the benefits this entails:

> … different organisations can draft their own statements of applicability around what of those controls are applicable to them as an organisation, and that makes ISO very flexible in terms of a standard. That is not to say that you can craft your own very narrow statement of applicability and then say, "I am compliant with ISO 27001." There are steps involved. You need to prove whether those steps that you have omitted actually need to be included as part of your assessment.[148]

3.6 Mr Rupert Taylor-Price from Vault Cloud also raised the issue of different approaches to standards between the NSW and Federal Governments. He said:

> We have found that there are vastly different standards and expectations between Federal and State Government. I would say that the Federal Government is further along the maturity process, partly because they have much more of a national security mandate than the New South Wales Government. That has driven a lot of expertise and maturity in the space.[149]

3.7 Conversely, Ms Michelle Price, from AustCyber, advised that her organisation has been working with NSW Government in respect of standard setting and harmonisation and said that it is about providing a base line across all industries. Ms Price said that her organisation is working with the NSW Government on the basis that it is the 'biggest economy within Australia and the one that was most conducive to understand the complexities of how to do the practice of cyber security well'.[150]

3.8 The NSW Government explained that it is currently undertaking work in respect of standard development and harmonisation. It advised:

> In June 2020, the Minister for Customer Service announced the creation of the Standards Harmonisation Taskforce. The taskforce will harmonise baseline cyber security standards and clarify additional sector-specific standards and guidance. It is a collaboration between NSW Government, AustCyber and Standards Australia. In addition, the taskforce aims to enhance competitiveness standards in the cyber sector for suppliers and consumers and support Australian cyber security companies to seize opportunities globally.[151]

3.9 The Standards Harmonisation Taskforce released its recommendations report in February 2021. The accompanying media release explained that the report highlights priority areas for standards development and that businesses and government agencies are encouraged to review and implement the recommendations in the report to help improve their cyber security policies and increase their cyber resilience.[152]

[148] Evidence, Mr Vizza, 29 October 2020, p 13.

[149] Evidence, Mr Rupert Taylor-Price, CEO, Vault Cloud, 29 October 2020, p 32.

[150] Evidence, Ms Michelle Price, Chief Executive Officer, AustCyber, 29 October 2020, pp 23-24.

[151] Submission 10, NSW Government, p 7.

[152] NSW Government, Media release, *Release of Cyber Security Recommendations Report*, 1 February 2021, viewed at: https://www.nsw.gov.au/news/release-of-cyber-standards-recommendation-report.

3.10 The report sets out the seven key priority sectors as being cloud, defence, education, energy, financial services, health, telecommunications and IoT. The next steps for the taskforce will be to develop an accessible list of cyber security standards for all 7 priority sectors.[153]

Procuring services externally

3.11 Another concern raised by inquiry participants was the lack of NSW Government standards concerning the procurement of external Information Technology services. ISG consulting said:

> In large government departments we still see major short comings in processes for technology procurement which do not place responsibility for vendors to comply with standards nor implement review processes internally to check compliance. In such an environment cyber resilience will never be achieved until basic accountabilities are recognised and processes put in place to monitor them.[154]

3.12 Mr Vizza expressed the view that 'external contractors and third party suppliers to Government should be accredited to some sort of standard' noting that 'ISO 27001 is the appropriate standard'.[155]

3.13 Mr Vizza advised that there used to be a requirement in procurement processes to confirm that a person is ISO compliant, but this appears to no longer be the case:

> We have actually gone backwards. From the latest set of procurement documents that I have seen, which was yesterday, there is mention of, "Are you adherent to the New South Wales Government guideline standards", but there is nothing around the ISO standards.[156]

3.14 Relevantly to the question of standards placed on external providers, the Auditor-General has identified concerns with the visibility some agencies have over the external providers they use for IT services or data management. In respect of Birth, Deaths and Marriages, it was concluded that:

> BD&M has no direct oversight of the database environment which houses the Register and relies on DCJ's management of a third-party vendor to provide the assurance it needs over database security. The vendor operates an Information Security Management System that complies with international standards, but neither BD&M nor DCJ has undertaken independent assurance of the effectiveness of the vendor's IT controls.[157]

3.15 The Auditor-General also identified that most IT service providers are not contractually obliged to report incidents to agencies:

[153] NSW Government, Media release, *Release of Cyber Security Recommendations Report*, 1 February 2021. https://www.nsw.gov.au/news/release-of-cyber-standards-recommendation-report.

[154] Submission 23, ISG Consulting Pty Ltd, p 4.

[155] Evidence, Mr Vizza, 29 October 2020, p 13.

[156] Evidence, Mr Vizza, 29 October 2020, p 13.

[157] Submission 6, New South Wales Auditor General, p 6.

> Agencies advise that IT service providers report cyber security incidents to them, but only two of ten had contractual arrangements which obliged providers to report incidents in a timely manner. Agencies without such arrangements have little assurance that they are advised of all significant incidents in a timely way. Where agencies are not informed of an incident, they cannot act to contain the incident and limit damage to themselves and their stakeholders.[158]

3.16 Active Cyber Defence Alliance raised a different issue concerning the implementation of standards when contracting external providers on long term projects. They expressed the view that the cyber landscape moves quickly, and standards adopted during a tender process can become outdated:

> During these extended timeframes the cyber threat landscape evolves significantly and dynamically, with the result that the cyber security standards and controls, proposed during the tender process, become obsolete, sometimes even before the tender is awarded and the project is delivered.[159]

3.17 The NSW Government outlined in its submission that it has a Procurement Policy Framework that applies to the procurement of goods and services of any kind, and that this is supported by a Procurement Board Direction 2020-02, which mandates the use of the Framework by NSW Government agencies. The Board Direction requires that agencies complete a risk assessment to 'ensure the appropriate use' of Procure IT framework contracts. It also advised that the contract templates have requirements for managing customer data, security, data breach, privacy, audit and reporting.[160]

Internet of Things

3.18 As outlined above, the Internet of Things (IoT) is an everyday item that has had internet connectivity added to it to allow data to be sent and received. The Australian Cyber Security Centre described IoT as including smart fridges, smart televisions, baby monitors and security cameras. IoT devices within homes and businesses generally use Wi-Fi or cellular networks, such as 4G or 5G, to connect to the internet.

3.19 The Australian Cyber Security Centre provides advice online about the dangers of the IoT as devices are often not designed with security in mind:

> Many IoT devices commonly found in Australian homes and businesses have not been designed with security in mind. This has resulted in devices being vulnerable to compromise via the internet. Such incidents can allow cyber criminals unsolicited access to your device and personal data for malicious purposes'.[161]

[158] Submission 6, New South Wales Auditor General, pp 17-18.

[159] Submission 17, Active Cyber Defence Alliance, p 8.

[160] Submission 10, NSW Government, pp 7-8.

[161] Australian Cyber Security Centre, *Internet of Things devices*, viewed at: https://www.cyber.gov.au/acsc/view-all-content/advice/internet-things-devices.

3.20 For example, Mr Vizza noted that very recently there was an incident where solar panels with internet connectivity lacked security and this 'effectively gave a cyber-criminal full access to their home network'.[162]

3.21 Some participants noted the need for the NSW Government to enhance the security of the IoT through standard development. Professor Varadharajan identified this as a priority area due to its significant reach and predicted expansion, such that it will impact almost everyone.[163]

3.22 When discussing cyber threats, Mr Knights from the Australian Information Security Association identified speed to market and the lack of standards as problems with IOT. He said:

> I am talking specifically about the Internet of Things. We are making the same mistakes over and over by not having a minimum standard. Where speed-to-market is more important than security, we should at least set some standards where these mistakes are not being repeated.[164]

3.23 Similarly, Mr Vizza said that from a standards perspective, there needs to be an entry point which sets a minimum standard for entry for IoT devices into the market which is then bolstered over time:

> We want to start with a starting point, allow people to say "This is the hurdle you need to actually reach to get into the market." And from there we can actually refine that and raise the bar over time as we get more sophisticated with how these devices are interacting with our life.[165]

3.24 (ISC)^2 and Australian Security Information Association referred to California having introduced laws to provide security over IoT and called on the NSW Government to either regulate on this matter or advocate for the Commonwealth Government to do so:

> The state legislature of California in the United States has legislated Senate Bill No. 327, popularly known as the '*IoT Security Law*' offering consumers appropriate levels of protection, and the NSW Government should adopt regulations at a state level or pursue the matter through the National Cabinet to promote the adoption of similar regulation at a federal level to ensure IT products are fit for sale to NSW consumers.[166]

3.25 The Australian Information Security Association advised that in October 2019, it surveyed its more than 6,000 members who suggested that 'anyone who is selling technology or technology services should be held responsible for 'enforcing' security standards in what they sell to business and consumers'. They also suggested that 'the Government should be responsible in overseeing the security standards to which technology vendors legislate to enforce compliance'.[167]

[162] Evidence, Mr Vizza, 29 October 2020, p 16

[163] Evidence, Professor Varadharajan, 29 October 2020, p 3.

[164] Evidence, Mr Stephen Knights, Director, Australian Information Security Association, 29 October 2020, p 11.

[165] Evidence, Mr Vizza, 29 October 2020, p 17.

[166] Submission 20, (ISC)^2, p 10; Submission 24, Australian Security Information Association, p 10.

[167] Submission 24, Australian Information Security Association, Attachment A, p 6.

3.26 The NSW Government advised that it has an IoT Policy and it includes data management, security and privacy advice for agencies using IoT enabled devices and equipment.[168] The committee did not receive evidence regarding action that the NSW Government may be taking in respect of improving the security of IoT devices more broadly than the abovementioned policy.

Monitoring, reporting and information sharing

3.27 Another key area of concern raised by participants was the inconsistent and insufficient approach to the monitoring and detection of cyber security incidents and the inadequate reporting once incidents were identified.

Monitoring and detection

3.28 Ms Michelle Price, the CEO of AustCyber, advised that in general it is common for cyber security incidents to go unreported for long periods of time:

> In Australia at the moment the average time from the actual breach through to an organisation knowing that they have been breached is 286 days, and that is often because they do not have sufficient monitoring of their systems and their infrastructures.[169]

3.29 Participants highlighted concerns with the approach by NSW Government agencies to detect incidents. For example, the NSW Auditor-General has found that agencies' incident detection and response ranged from good to poor and has made recommendations aimed at improving agencies' detection activities.[170]

3.30 The NSW Auditor-General found that there is a lack of a whole-of-government approach, leading to poor information sharing between agencies:

> There is no whole-of-government capability to detect and respond effectively to cyber security incidents. There is limited sharing of information on incidents amongst agencies, and some of the agencies we reviewed have poor detection and response practices and procedures. There is a risk that incidents will go undetected longer than they should, and opportunities to contain and restrict the damage may be lost.[171]

3.31 The 2019 NSW Cyber Security Policy included a reference to agencies being required to implement a whole-of-government approach to cyber incident response, and while it is not clear as to the specific requirements upon agencies to monitor and detect cyber threats and incidents, the Auditor-General concluded that 'given current weaknesses, the NSW public sector’s ability to detect and respond to incidents needs to improve significantly and quickly'.[172]

[168] Submission 10, NSW Government, p 9.

[169] Evidence, Ms Price, 29 October 2020, p 25

[170] Submission 6, NSW Auditor General, pp 17-19.

[171] Submission 6, NSW Auditor General, p 17.

[172] Submission 6, New South Wales Auditor General, p 17.

3.32 The NSW Government advised that in June 2020 it launched the NSW Vulnerability Management Centre in Bathurst which will deliver vital, sector-wide risk management capability and is critical to ensuring enhanced monitoring of at-risk government systems, and early identification and remediation of known vulnerabilities.[173]

3.33 The committee did not receive detailed evidence regarding the specific nature of effective detection strategies. However, the Auditor-General reported that most agencies use an automated tool, although some only undertake monitoring on an ad hoc basis:

> Most use an automated tool for detecting and alerting IT administrators when there is a suspected incident. The tool's coverage ranged from all IT systems in some agencies to just a few in others. Some agencies do not use such a tool and only monitor logs periodically or on an ad hoc basis.[174]

3.34 The committee did hear from the Active Cyber Defence Alliance regarding detection strategies and the need for these to be more proactive. It provided information regarding elevating detection measures from the more traditional passive approach to a more proactive model:

> Today's conventional security strategies mainly focus on passive cyber security approaches using tools, techniques and procedures that seek to prevent and protect against attacks. Although these controls are necessary, they are insufficient against sophisticated adversaries and the demands of rapid response timeframes.[175]

3.35 Mr Andrew Cox from Active Cyber Defence Alliance argued that active cyber defence measures are a more dynamic set of controls to predict and respond to malicious cyber activity:

> By active cyber defence we are referring to cyber intelligence, deception, active threat hunting and lawful countermeasures to give defenders visibility of their adversaries' objectives, methods and identities so that they are no longer fighting blind but can predict, detect and respond effectively to malicious cyber activity.[176]

3.36 Mr Cox explained such measures as essentially creating 'fake computers that look like real computers' that can be placed in any network and will let you know if there is a malicious actor moving around the network. He argued that this is more effective and efficient than human monitoring, which he believed is vital for the critical infrastructure in New South Wales. He provided the analogy that we are currently operating as a 'blind boxer':

> Essentially what is going on is that we are like a blind boxer in the way that passive cyber security works. We have our eyes shut and our ears blocked so our opponent can beat the living daylights out of us. We flail around trying to defend ourselves and once in a while we land a lucky punch. By and large we on a hiding to nothing. If we can open up our eyes and start to see the threat environment—not the generic threat environment that is affecting everybody but what is affecting this or that organisation specifically—and detect activity effectively, then we will have the ability to exact a cost against our adversary and make ourselves a far more hostile target.[177]

[173] Submission 10, NSW Government, p 7

[174] Submission 6, New South Wales Auditor-General, p 17.

[175] Submission 17, Active Cyber Defence Alliance, p 11.

[176] Evidence, Mr Andrew Cox, Member, Active Cyber Defence Alliance, 29 October 2020, p 27.

[177] Evidence, Mr Cox, 29 October 2020, p 27.

3.37 Ms Helaine Leggat, also from Active Cyber Defence Alliance, identified confusing and competing laws as a barrier to the adoption of active cyber defence strategies and advised that this has caused some to question the lawfulness of such strategies, resulting in inaction. She said that there are 'literally hundreds of statutes that deal with issues relevant to cyber active defence' and 'it is difficult to thread all of the requirements together to find out what a person can properly do and we end up stagnant and not responding'.[178]

3.38 Ms Leggat advocated for the simplifying of legal complexity so that active cyber defence strategies can be adopted.[179] She used the analogy of self-defence provided for in criminal law, whereby it is recognised that individuals can take certain steps to prevent unlawful interference with person or property. She advocated for these measures to be applied in cyberspace to protect people to take more proactive preventative measures.[180]

3.39 The Australian Information Security Association, however, advised that its members were not strong supporters of deception or disruptive measures. It advised that 'deploying deception or disruptive technology (honeypots) across the Australian environment, including some small business environments was suggested by only 3.7 per cent of [its survey] respondents' when asked about how governments can create hostile environments for malicious cyber actors.[181]

Reporting

3.40 The committee heard from many participants about the lack of a mandatory reporting scheme for data breaches in New South Wales. Participants were in broad agreement that this is a key requirement to enhance New South Wales' approach to cyber security.

3.41 Unions NSW expressed that the NSW Government must immediately create and enforce mandatory reporting requirements for its agencies.[182] It went on to explain that the NSW Government continues to operate without a mandatory reporting scheme despite its own 2018 Strategy seeking to establish one:

> The 2018 Strategy sought to establish mandatory reporting requirements for cyber incidents with the intention information about such an incident would be disseminated to other agencies to mitigate repercussive or associated harm. However, a September 2020 report by the Information and Privacy Commission NSW demonstrates New South Wales continues to operate without mandatory reporting requirements and instead relies on voluntary reporting schemes.[183]

3.42 Similarly, Professor Vijay Varadharajan expressed concern at the lack of a mandatory reporting scheme and agreed that one was necessary. He further noted that this already existed at the Federal level.[184]

[178] Evidence, Ms Helaine Leggat, Member, Active Cyber Defence Alliance, 29 October 2020, p 28.

[179] Evidence, Ms Leggat, 29 October 2020, p 28.

[180] Evidence, Ms Leggat, 29 October 2020, p 27.

[181] Submission 24, Australian Information Security Association, Attachment A, p 1.

[182] Submission 25, Unions NSW, p 6

[183] Submission 25, Unions NSW, p 6.

[184] Evidence, Professor Varadharajan, 29 October 2020, p 4.

3.43 Participants offered views about the benefits of a mandatory reporting scheme including its importance in improving transparency and public confidence, understanding emerging threats and ensuring lessons are learnt.

3.44 Unions NSW expressed the view that mandatory reporting is necessary to ensure the protection of personal information in the long term rather than having a reactive response:

> The primary concern of Unions NSW in respect to cyber security and data is to ensure the protection of the personal information of people and behavioural data through robust, well-managed regulation. Primarily we are calling for a cyber security strategy which creates and imposes mandatory reporting requirements upon all New South Wales Government agencies in respect of any and all cyber security breaches. We would like this to be a strategy that will build resilience and other long-term proactive protection rather than a just-in-time reactive response strategy.[185]

3.45 Similarly, Professor Vijay Varadharajan expressed that mandatory reporting will 'help to improve the consciousness, awareness and the ability or confidence of organisations to detect and respond' to breaches. [186]

3.46 Transparency was considered by many to be a key hallmark of a mandatory reporting regime. As Mr Costa from Unions NSW offered, without mandatory reporting, 'there is no transparency around when data breaches occur'.[187]

3.47 Ms Michelle Price from AustCyber stated that transparency is at the core of an effective reporting system. She said: 'I think that again when you look at the good models of mandatory notification around the world there is a very key principle of transparency that is the foundation of those systems'.[188]

3.48 AustCyber submitted that it supports a mandatory reporting scheme and openness about the issues identified, as it helps other agencies to have visibility as to the threats so they can take action to protect themselves:

> AustCyber supports governments monitoring and reporting cyber incidents and being transparent about the types of threats, how they are changing and where they are targeted. This information is very useful for understanding the threat environment, how it is changing and helping governments, technology and behavioural practices to improve so all organisations can make the necessary changes to protect networks and develop measures to get ahead of the threats and when they arise respond to them quickly to minimise the disruption.[189]

3.49 In addition to the value of improving transparency, the ability to learn from incidents and responses was also considered vital to continual improvement of the cyber security approach in New South Wales as well as to build public confidence. Dr Arnold discussed the importance of a whole-of-government approach to monitoring and reporting:

[185] Evidence, Mr Thomas Costa, Assistant Secretary, Unions NSW, 29 October 2020, p 40.

[186] Evidence, Professor Varadharajan, 29 October 2020, p 5.

[187] Evidence, Mr Costa, 29 October 2020, p 40.

[188] Evidence, Ms Price, 29 October 2020, p 25.

[189] Submission 3, AustCyber, p 4.

> Stakeholders should be seeing a coherent whole-of-government approach to security incidents in which the community can see that government is 1) acknowledging the existence of incidents and 2) reporting evaluations of the significance of incidents and 3) being seen to learn from those incidents on a proactive basis.[190]

3.50 Mr Vizza from the Australian Information Security Association also expressed strong support for a mandatory reporting scheme and advised that a similar model to the European Union General Data Protection Regulation should be followed in New South Wales:

> I would absolutely support mandatory reporting at a State level and at a local government level, which I know is not required under the Federal mandatory breach notification laws. If the State Government were to implement an arrangement similar to the European Union General Data Protection Regulation [GDPR], I think that would be highly beneficial in terms of that breach reporting as well as ensuring these cyber security and privacy-related concerns for a lot of people in New South Wales would be very much met by incorporating a GDPR standard here in New South Wales.[191]

3.51 The Office of the Australian Information Commission (OAIC) told the inquiry that it operates a mandatory reporting scheme for the Commonwealth Government. Under the Privacy Act, the OAIC has oversight of the mandatory Notifiable Data Breaches (NDB) scheme, which commenced in February 2018. The OAIC explained the 'NDB scheme replaced the voluntary data breach notification scheme that had been in operation at the Commonwealth level since 2008'.[192]

3.52 It also said the NDB scheme sheds light on the causes of data breaches, allowing the OAIC and entities to better understand how they might be avoided and implement prevention strategies. It identified the following additional benefits of a mandatory scheme (as opposed the voluntary one in New South Wales):

- providing clarity for entities as to the kinds of data breaches that need to be notified and expected timeframes for notification
- providing consumers with confidence that they will be advised if their personal information is compromised and more comprehensive and consistent information about data breaches that may affect them and how they might mitigate associated risks.[193]

3.53 The OAIC explained an eligible data breach occurs when the following criteria are met:

- there is unauthorised access to, or disclosure of, personal information held by an entity
- this is likely to result in serious harm to any of the individuals to whom the information relates
- the entity has been unable to prevent the likely risk of serious harm with remedial action.

3.54 It also expressed that careful consideration needs to be given to statutory timeframes for the assessment and notification of data breaches to balance the ability of agencies 'to complete an

[190] Submission 16, Dr Bruce Baer Arnold, p 3.

[191] Evidence, Mr Vizza, 29 October 2020, p 11.

[192] Submission 18, Office of the Australian Information Commissioner, p 2.

[193] Submission 18, Office of the Australian Information Commissioner, p 6.

investigation to assess the level of risk associated with a suspected breach, with the timely notification to individuals so they may take steps to mitigate the risk of harm'. [194]

3.55 The OAIC advocated for any state based scheme to be consistent with the Commonwealth:

> A state-based scheme that aligns with the requirements of the NDB scheme under the Privacy Act would ensure that Australians' personal information is subject to similar protections whether that personal information is being handled by an Australian Government agency or a state or territory government agency, or private sector organisations.[195]

3.56 The Information and Privacy Commission NSW advised that while there is not currently a mandatory reporting scheme in New South Wales, it 'strongly encourages NSW public sector agencies to report data breaches under the voluntary reporting scheme'.[196]

3.57 The Information and Privacy Commission NSW also advised that in 2018 she commenced quarterly reporting of voluntary data breach notifications received from agencies and that during 2019/20 her office received a total of 79 breach notifications, representing an increase of 23 per cent over the previous year.[197]

3.58 Ms Samantha Gavel, NSW Privacy Commissioner, informed the committee that steps are underway to implement a mandatory reporting regime in New South Wales and that she supports the development of this scheme. Ms Gavel also indicated support for the New South Wales model to be consistent with the Commonwealth:

> We consider that the Commonwealth scheme works well in the Australian context. Not to say that we would necessarily mirror it and bring in the same scheme, but there are benefits in having a similar scheme because of the way that we do share information with the Commonwealth.[198]

3.59 When questioned about why the mandatory scheme was taking so long to implement in New South Wales, Ms Gavel provided the following update:

> The discussion paper went out 18 months ago and there was time for the community and agencies to put forward their submissions in relation to that scheme. The submissions were taken in by DCJ and they considered the findings of those submissions. Something that was very pleasing to me as Privacy Commissioner was that the submissions were overwhelmingly supportive of such a scheme. As I said, over the past year or so we have been consulting with DCJ on the form of the scheme. I hope that work is nearing completion but, as I have said, it is for the Government to announce further developments in the scheme.

3.60 Similar to the criteria set out above in respect of the Commonwealth reporting scheme, the NSW Privacy Commissioner discussed her views regarding the 'reporting' threshold as being where there is a serious risk of harm. She explained the threshold as being:

[194] Submission 18, Office of the Australian Information Commissioner, p 3.

[195] Submission 18, Office of the Australian Information Commissioner, p 7.

[196] Submission 14, Information and Privacy Commission NSW, p 3.

[197] Submission 14, Information and Privacy Commission NSW, p 3.

[198] Evidence, Ms Samantha Gavel, NSW Privacy Commissioner, 3 February 2021, p 12.

> … where a data breach results in or is likely to result in a serious risk of harm to the individual—that that breach should be reported to the Privacy Commissioner and also to people who are affected by the breach.[199]

3.61 Ms Gavel was questioned about why this seemingly high threshold is considered the best approach and not the more readily accepted EU model where there must be immediate reporting unless it is unlikely to result in a risk of the rights and freedoms of individuals. Ms Gavel advised that the scheme in New South Wales is not yet finalised and further consultation is yet to take place:

> … the scheme has not been finalised. We are talking about a hypothetical scheme at the moment that we have been working on. When the legislation comes forward for consultation, then everybody will be able to put their views forward on what they think of that scheme, what they think of the model, what they think of the legislation, what they think of the definition for when breaches need to be notified. And that is going to be the appropriate time to put that forward.[200]

3.62 Ms Gavel further explained that she is advocating for a model that provides the best protection to citizens and a model that would capture breaches such as the Service NSW incident:

> I am advocating for a scheme for New South Wales that will protect privacy in New South Wales and protect people in New South Wales, and, in particular, I have in my mind the Service NSW breach. That is the kind of breach where we need to protect people, and the threshold that will be set in the scheme will do that work, and that is what is important.[201]

3.63 Some participants also identified the need for any mandatory reporting scheme to be accompanied by strong governance and guidance to promote a reporting culture.

3.64 For example, Ms Michelle Price stated that agencies should be supported when they are breached, rather than being condemned:

> … breach notification again needs to have some injection of what good looks like. Breach notification should not be taken as something that is a slight against the ability of a company or an agency to be able to do cyber security well … If an organisation … discloses mandatorily that it has been breached and/or compromised, we should have a culture of not sort of throwing bricks at those organisations; we should be rallying around them to help them resolve that situation and learn from it so that we can continue to build the resilience of the systems overall as well as the culture that surrounds it all.[202]

Building sovereign cyber security capability

3.65 The need to support cyber security capability within Australia and to be judicious when considering use of offshore services was a consistent theme raised by participants. However, there was also recognition that sovereignty will not always be necessary or possible.

[199] Evidence, Ms Gavel, 3 February 2021, p 13.

[200] Evidence, Ms Gavel, 3 February 2021, p 14.

[201] Evidence, Ms Gavel, 3 February 2021, p 14.

[202] Evidence, Ms Price, 29 October 2020, pp 24-25.

3.66 The ability to maintain control over data was cited as one reason to keep data onshore. Vault Cloud, an Australian owned and operated Cloud platform, said that outsourcing to foreign entities meant that: 'the NSW Parliament cannot provide NSW citizens assurances or control security, privacy or sovereignty outcomes when the NSW Government provides overseas companies with access to NSW citizen data'.[203]

3.67 Mr Costa from Unions NSW viewed that 'data should be maintained onshore and in-house' and cited control as the reason. Relevantly, Mr Costa said:

> … having data offshore in a jurisdiction where laws and regulations can change over which we have no sovereignty or control opens up not just the Government but the data that is held on employees and members of the community to considerable risk.[204]

3.68 Unions NSW also identified that in addition to maintaining control, sovereign data storage also boosts the economy through job creation:

> In addition to maximising the control over and commensurate security of the data, this measure will create jobs for local people; something the State undeniably needs in the wake of the economic disruptions caused by the COVID-19 pandemic.[205]

3.69 Picking up on this point, the Australian Information Security Association and the (ISC)^2 expressed the view that the pandemic has highlighted the need to develop strong sovereign capability for the success of the economy. They stated:

> As nation states seek to develop (or in many cases re-develop) sovereign manufacturing capabilities in the aftermath of the COVID-19 pandemic and its economic and national security after-effects, a strong local cyber security and information technology sector is vital for the long-term success of the NSW economy as well as the broader Australian economy, which is heavily reliant on NSW as a driver of economic growth.[206]

3.70 AustCyber advised that by building sovereign capability and investing in enhancing and supporting the cyber security sector in Australia, we can position ourselves as a competitive and attractive player globally:

> The majority of supply of ICT and digital technologies to governments in Australia is largely from offshore markets – it is far from a level playing field. While these markets do have skills and capabilities that are useful here in Australia, fostering local innovation through sovereign procurement arrangements ensures Australia builds its own capabilities for ensuring a trusted Australian digital environment.[207]

3.71 Ms Price also supported sovereign cyber security capability to create jobs and boost the economy. She said:

> Being able to trust the technologies that we deploy to defend against malicious attacks on digital infrastructure and the data that it carries is critical. More than that, we need

[203] Submission 9, Vault Cloud, p 9.

[204] Evidence, Mr Costa, 29 October 2020, p 40.

[205] Submission 25, Unions NSW, p 5.

[206] Submission 20, (ISC)^2, p 9; Submission 24, Australian Information Security Association, p 9.

[207] Submission 3, AustCyber, p 4.

> to be able to have our stake in the sand to be able to sustain the economic growth that we are now relying so heavily on, particularly in pandemic recovery, around the creation of new industries and the jobs and revenue that come from it.[208]

3.72 Business growth, boosting the economy and enhancing innovation were identified by some as drivers for building sovereign cyber security capability. In this regard, Ms Price identified New South Wales as having a real opportunity because over 50 per cent of the sovereign companies that are currently within Australia reside in New South Wales.[209]

3.73 Ms Price told the committee about the work AustCyber has been doing to build this capability within Australia, but she also said that for economic growth in the long term, we need to recognise 'just how central cyber security capability is to the economy now'. She said:

> Being able to foster sustained growth within the cyber security industry that provides those products and services in a globally competitive way is critically important for us to hit our goals as a jurisdiction of New South Wales, but also for the nation, around pandemic recovery and economic growth longer term. [210]

3.74 Mr Vizza from (ISC)^2 supported Ms Price's view and drew the committee's attention to the efforts in this regard by other countries:

> If you look at nations such as Israel and Canada, for instance, they have dedicated a significant percentage of their government mindshare into making sure that they are on top of this. To Ms Price's point, I think that we might have made a slow start.[211]

3.75 The Australian Information Security Association and (ISC)^2 advocated for the NSW Government to 'consider supporting, promoting and using locally made, owned or recognised cyber security and world leading information technology products and services'.[212] These participants provided suggestions as to how the NSW Government could do this, including:

- subsidising certification costs for locally based IT and cyber security products and services and for their staff
- wherever possible, procuring locally based and certified businesses for public sector needs
- actively working with AustCyber to help promote innovative and locally made cyber security products and services to the Asia-Pacific region and the global market.[213]

3.76 Some participants expressed the view that sensitive and critical data should be housed onshore. Ms Price explained that we should think about what data is critical to house onshore and where data is going offshore, we should be clear about where it is and our control over it.[214]

[208] Evidence, Ms Price, 29 October 2020, p 20.

[209] Evidence, Ms Price, 29 October 2020, p 20.

[210] Evidence, Ms Price, 29 October 2020, p 21.

[211] Evidence, Mr Vizza, 29 October 2020, p 21.

[212] Submission 24, Australian Information and Security Association, p 9; Submission 20, (ISC)^2, pp 9-10.

[213] Submission 24, Australian Information and Security Association, p 9; Submission 20, (ISC)^2, p 9.

[214] Evidence, Ms Price, 29 October 2020, p 22.

3.77 Professor Varadharajan stated that not all government services need to be accommodated onshore but where data is sensitive and critical, this should reside within Australian boundaries:

> My view will be to say for certain types of data, which are critical and sensitive, I would suggest the sovereignty data centre. The data should reside within Australian boundaries. That is the over-arching principle.[215]

3.78 Similarly Mr Vizza viewed that some data should be kept onshore, such as medical records.[216] In discussing the European model he advised that under a similar model here, we would retain our critical data onshore and have control over how our data is managed offshore:

> If the State of New South Wales were to adopt that regime that would be very beneficial in that we can benefit from housing certain types of data offshore where we are happy with that but where we keep the crown jewels here in New South Wales where they belong, but we also know that data that has been outsourced is actually being protected adequately.[217]

3.79 Vault Cloud, strong advocates for a sovereign approach, also identified that there is a need to determine sovereign data sets that must remain within Australian jurisdiction, in line with the Federal Government. Vault Cloud recommended a 'target of 25 per cent sovereign requirement in cyber security related procurements as well as the security components of tech procurements'.[218]

3.80 It also viewed that high quality services and products are available onshore:

> Vault is also concerned over the existence of a 'cultural myth' within Government Procurement agencies that hyperscale, high performance and high availability Cloud services are only available from overseas entities at competitive prices, and not from sovereign Cloud service providers.[219]

3.81 Further, according Vault Cloud, the Information Commissioner has stated that from as early as 2017, 93 per cent of Australians did not want to see their data going offshore, yet there has not been any New South Wales legislation that regulates data sovereignty.[220]

3.82 AustCyber argued that Government can enhance and build the quality of sovereign cyber security through its procurement powers:

> Building sovereign cyber security capability through local skills and businesses is vital to ensure Australian digital activity continues to be resilient and secure. Government can encourage and stimulate growth and innovation in local capability by using its purchasing power to ensure its procurement arrangements recognise and encourage sovereign capability.[221]

[215] Evidence, Professor Varadharajan, 29 October 2020, p 7.

[216] Evidence, Mr Vizza, 29 October 2020, p 12.

[217] Evidence, Mr Vizza, 29 October 2020, p 12.

[218] Submission 9, Vault Cloud, p 6.

[219] Submission 9, Vault Cloud, p 6.

[220] Submission 9, Vault Cloud, p 5.

[221] Submission 3, AustCyber, p 3.

3.83 AustCyber provided a number of suggestions to improve approaches to government procurement which included:

- provide incentives and leverage methods to encourage organisations across the NSW economy to buy Australian first where possible
- engage with and preference local companies in writing Government tenders, for example, in cyber security capability and put in place multi-party writing teams where project complexity requires or would also benefit from multinational experience
- develop incentives that encourage investment in nurturing and supporting sovereign capability for export through global value chains
- implement AustCyber's Procurement Sandbox which can assist industry to rapidly upskill in supplying to government, as the majority of early stage companies are inexperienced in selling to Government as a customer.[222]

3.84 Ms Price told the inquiry that the Commonwealth is taking steps to better define what is meant by critical infrastructure and to legislate data sovereignty for certain data and data retention requirements:

> The Minister for Home Affairs is expecting to table draft legislation before the end of this calendar year on new critical infrastructure regulations and legislation around cyber security in critical infrastructure. Part of that is going to be about data sovereignty and data retention requirements. I do not mean retention in the sense of that legislation, I mean retaining data onshore and if it does have to go offshore how do you manage that?.[223]

3.85 The committee did not receive evidence from the NSW Government in respect of work it may or may not be doing in respect of building sovereign cyber security capability including through procurement activities.

3.86 When questioned about what data is held overseas or within New South Wales, Mr Wells, advised that this is a matter for each cluster and it is not the role of his agency to know where every agencies' data is.[224] Mr Wells further advised that the *State Records Act* specifically enables data to be held anywhere, contingent on a risk assessment of how the data is maintained and who can access it.[225]

Committee comment

3.87 The committee was convinced that in addition to the governance and people measures outlined in Chapter 2, the NSW Government has an opportunity to strengthen its cyber security posture by improving the approach to standards; enhancing monitoring and reporting requirements; and establishing a stronger focus on building sovereign cyber security capabilities.

[222] Submission 3, AustCyber, p 3.

[223] Evidence, Ms Price, 29 October 2020, p 23.

[224] Evidence, Mr Greg Wells, NSW Government Chief Information and Digital Officer, Department of Customer Service, 3 February 2021, p 33.

[225] Evidence, Mr Wells, 3 February 2021, p 33.

3.88 The committee notes the NSW Government's improved Cyber Security Policy and the adoption of mandatory requirements, including the Essential 8, however we consider that clarity is required to set a benchmark that all agencies, and their contracted service providers, must meet and not simply report against.

3.89 The committee is concerned that despite the multiple adverse findings by the Auditor-General and warnings from others about the cyber security risks, agencies are slow to adopt the recommendations and strengthen their cyber security measures. As outlined in Chapter 2, the committee considers that part of this problem is that there is no oversight or compliance mechanism in place to require agencies to achieve certain levels of maturity. Secondly, and as highlighted by the evidence in this chapter, there is not a clear set of mandated standards that agencies must demonstrate compliance with.

3.90 The committee also had regard to the evidence regarding the model on which standards should be developed and noted the views regarding ISO and the National Institute of Standards and Technology. Additionally, the committee considered there to be merit in developing baseline security standards for Internet of Things devices, however acknowledges the challenges of this occurring within the confines of New South Wales, when devices can be developed, sold and purchased all over the world. However, it appears to warrant exploration, particularly for Internet of Things devices that the Government adopts or deploys within its agencies and to citizens.

Recommendation 6

That the NSW Government review its Cyber Security Policy to provide clarity around mandatory standards and set a benchmark that all NSW Government agencies must adhere to.

Recommendation 7

That the NSW Government work with industry to determine the most appropriate model for cyber security standards for both NSW Government agencies and cyber security businesses within New South Wales.

Recommendation 8

That the NSW Government investigate avenues for it to improve the security of Internet of Things devices, particularly those adopted or deployed by its agencies.

3.91 The committee notes the evidence regarding monitoring and detection and considers that more attention is required to ensure agencies are adopting the measures most appropriate to their risk level. The committee accepts the evidence from Active Cyber Defence Alliance regarding the need to be more proactive in efforts to detect threats or attacks, however notes that the need for such strategies will vary across agencies. The committee recognises that some agencies, such as the NSW Police Force, may already use more proactive detection methods, however, the committee believes there may be merit in Cyber Security NSW working with agencies to determine where such measures may be warranted and how they are best deployed.

3.92 The committee welcomes the advice that New South Wales is in the process of implementing a mandatory reporting regime, however we are concerned about the slow progress in the development of this scheme and that the reporting threshold appears to be too high. The committee agrees with the evidence regarding the benefits of a mandatory reporting scheme noting that its implementation will support principles of transparency and accountability. It will also facilitate a greater sharing of information regarding attacks, which in turn will build the capability across all agencies. The committee recommends that the scheme to introduce mandatory reporting be prioritised without further delay.

Recommendation 9

That the NSW Government urgently establish a mandatory data breach notification scheme applicable to all NSW Government agencies and its contracted service providers.

3.93 The committee acknowledges the benefits in having a stronger focus on building sovereign cyber security capability. It appears that there is no current a policy regarding the storage of data, including what data should be kept onshore. Cyber Security NSW told the committee that it now has visibility over agencies' 'crown jewels' in terms of sensitive data. The committee is of the view that this list requires reviewing and a risk assessment overseen by Cyber Security NSW conducted, to determine the location of this data and the appropriateness or otherwise of that going forward. It would also be prudent for the NSW Government to develop a policy for the storage of its data to not only ensure a consistent approach, but to give assurances to the public that the approach taken is not ad hoc and up to each individual agency, but rather is coordinated, considered, robust and resilient.

Recommendation 10

That the NSW Government develop a strategy to enhance sovereign cyber security capability which includes building the industry, establishing principles for procuring services onshore and working with agencies to identify what data should be stored offshore.

Chapter 4 Strengthening partnerships

This chapter focuses on the ways in which the NSW Government should work with local government, industry, the public and the Commonwealth to strengthen cyber security.

Local government

4.1 Some participants told the committee about the unique cyber security challenges faced by local councils and the additional support that they require. The NSW Auditor-General identified that threats to local government are potentially harmful to service delivery and may include the theft of information, denial of access to critical technology, or even the hijacking of systems for profit or malicious intent.[226]

4.2 Local Government NSW underscored the local government sectors' vast responsibility for the provision of essential infrastructure and services to local councils throughout the state and the increasing reliance on technology:

> The NSW local government sector is responsible for the provision of a wide range of essential infrastructure and services and manages infrastructure and land assets worth more than $153 billion. The sector is increasingly relying on technology for information management and acknowledges that information technology controls and governance frameworks are essential to ensure that IT systems are protected from inappropriate access and misuse.[227]

4.3 Local Government NSW expressed concern that 'to date there has been a complete lack of NSW Government support to local governments in managing cyber security threats'.[228]

4.4 The need for increased support appears to have been echoed by the Hills Shire Council as it expressed that there was no mention of local government in the NSW Government Cyber Security Strategy and that it was seeking guidelines on minimum cyber security requirements and procedures for responding to a cyber attack.[229]

4.5 Other participants agreed that additional support was required for local government. Palo Alto Networks identified education and funding for local governments as a way to improve their cyber security posture. It said 'that the Government should also work with the private sector to educate … Local Governments on cyber security'. It also suggested that such training be subsidised by the NSW Government and recommended that 'the Government could look to subsidise the cost of purchasing these offerings via a cyber security grants program'.[230]

4.6 Unions NSW, in discussing the need to create and adequately remunerate cyber security jobs, said that this will also assist the NSW Government to become a leader in cyber security and extend support and security models to local government and other organisations:

[226] Submission 6, New South Wales Auditor-General, p 2.

[227] Submission 2, Local Government NSW, p 1.

[228] Submission 2, Local Government NSW, p 1.

[229] Submission 8, The Hills Shire Council, p 1.

[230] Submission 26, Palo Alto Networks, pp 4-5.

> When creating additional cyber security jobs, Unions NSW urges the NSW Government to invest in competitive rates of pay to ensure the most skilled professionals are employed by the Government and our State afforded the best possible protection. This will also assist the NSW Government to become a leader in cyber security and extend support and security models to local government and other organisations.[231]

4.7 In this vein, Local Government NSW outlined that it finds it difficult to attract skilled workers in this field, particularly in rural and regional areas. It noted that, based on its research, '86 per cent of councils in NSW were experiencing a skills shortage and 69 per cent were experiencing skills gaps' when it came to cyber security.[232]

4.8 Mr Tony Vizza, a board member of the Australian Information Security Association spoke about the need to extend support and cyber security requirements to local government. He viewed that mandatory reporting should also apply to local government and expressed dismay that businesses are required to notify under the Federal Scheme, but state and local governments are not:

> … suppliers would have to notify under the Federal scheme because the Federal scheme covers any ABN or any ACN that generates a certain amount of turnover, **so interestingly** they have to notify if they have been breached, but if a state government entity has been breached, or a local government entity, it does not have to.[233]

4.9 The Auditor-General advised that she intends to commence an audit specifically into cyber security in local government in 2021-22.[234] However, in her financial audit report on local government in 2019 she identified a number of cyber security related concerns. The report concluded that 'Councils' cyber security management requires improvement, as most councils are yet to implement the basic elements of governance, such as a cyber security policy or framework'.[235]

4.10 In particular, the Auditor-General identified that:

- 80 per cent of councils do not have formal cyber security policy/framework
- 46 per cent of councils have not included risk of cyber-attack in their risk register
- 67 per cent of councils have not recently performed penetrations testing (cyber-attack simulation)
- 76 per cent of councils have not delivered cyber security training to all of their staff
- 84 per cent of councils do not have separate cyber security budget
- 48 per cent of councils do not have cyber security insurance policy
- 78 per cent of councils do not maintain a centralised register of cyber incident.[236]

[231] Submission 25, Unions NSW, p 5.

[232] Submission 2, Local Government NSW, p 1.

[233] Evidence, Mr Tony Vizza, Board Member, Australian Information Security Association, 29 October 2020, p 14.

[234] Submission 6, New South Wales Auditor-General, p 2.

[235] Submission 6, New South Wales Auditor-General, p 9. See also: https://www.audit.nsw.gov.au/our-work/reports/report-on-local-government-2019.

[236] Submission 6, New South Wales Auditor-General, p 9.

4.11 The Auditor-General recommended that the Office for Local Government develop a cyber security policy by 30 June 2021 to ensure a consistent response to cyber security across councils.[237]

4.12 In its submission to the inquiry, the NSW Government stated that it is working with the Office of Local Government to support councils with cyber security policies and guidance and that it is also engaging with a number of local councils to provide cyber security support with tailored workshops, resources and training sessions. It further advised that 600 staff from 42 different councils have registered for the Cyber Security NSW Essentials Training.[238]

4.13 As noted previously in chapter 2, the NSW Government also outlined that of its recent $240 million investment in cyber security, $60 million of this is to expand the remit of Cyber Security NSW to include support for smaller government agencies as well as councils.[239]

4.14 Local Government NSW noted that while it welcomed this additional support, it was seeking direct financial support to improve cyber security capabilities. It cited the impact of recent events such as COVID-19 and bushfires as a factor:

> The compounding impacts of unprecedented drought, bushfires, floods and the COVID-19 pandemic, coupled with rate pegging and cost shifting, means that council finances are stretched to the limit. Councils need additional financial support from the NSW Government in order to effectively improve their cyber security capabilities.[240]

Businesses and non-government organisations

4.15 Evidence regarding the need to strengthen sovereign cyber security capability through supporting industry and procuring onshore services was set out in chapter 3. In addition to this, participants advised that small to medium enterprises (SMEs) need support to be cyber secure.

4.16 Mr Tony Vizza from (ISC)^2, referred to a statement by the Prime Minister regarding Australian Governments and businesses being at risk of cyber attacks, with New South Wales considered high risk: He noted:

> In July of this year Prime Minister Scott Morrison told the Australian people that Australian governments and businesses were under sustained cyber attack. Federal agencies singled out the State of New South Wales as a specific target for cyber attackers following a number of high-profile breaches that occurred here, most notoriously the breach that occurred at Service NSW in April of this year.[241]

4.17 Professor Vijay Varadharajan, Global Innovation Chair Professor in Cyber Security and the Director of Advanced Cyber Security Engineering Research Centre (ACSRC) at the University of Newcastle expressed concern about the lack of support to SMEs and indicated that they are an important part of the effort to enhance cyber security:

[237] Submission 6, New South Wales Auditor-General, p 9.

[238] Submission 10, NSW Government, p 7.

[239] Submission 10, NSW Government, p 6.

[240] Submission 2, Local Government NSW, p 2.

[241] Evidence, Mr Vizza, Director, (ISC)^2, 29 October 2020, pp 19-20.

> Despite their often-constrained resources, SMEs are essential stakeholders in any effort to enhance cyber security—particularly in light of their role in the supply chain—and their needs must be better addressed.[242]

4.18 Professor Varadharajan explained that SMEs face a number of unique challenges and are 'often time poor, cash flow poor, [have] limited staff expertise and focused on their current products and services'.[243]

4.19 Further, he argued that 'there is an opportunity for the NSW Government to take leadership in enhancing the cyber capability of SMEs especially in the regional areas'. Professor Varadharajan provided the following ideas to enhance the competitiveness of SMEs from a cyber security standpoint:

- strategic advice and thought leadership on security best practice
- targeted and specialised security training
- expertise to their current and future solutions via research and development and innovation
- improved engagement with government agencies.[244]

4.20 Ms Michelle Price of AustCyber identified another area where SMEs required support. In discussing the potential for regulation of data, she identified that support was required to clearly explain cyber security requirements:

> New South Wales is in the box seat to lead here, to provide the kind of translation of that legislation and regulation down into small business. Small business in value chains, as we know, are incredibly exposed to not having the right kind of information and not having the right kind of advice to be able to implement these kinds of practices effectively.[245]

4.21 Similarly, Palo Alto Networks, recommended providing 'cyber security education and funding for SMEs … to improve their cyber security posture'. It went on to suggest that, similar to supporting local government, the NSW Government could look to subsidise the cost of this education via a cyber security grants program.[246]

4.22 The Australian Information Security Association also echoed the importance of education. Mr Vizza told the committee about its vision for everyone, including businesses, to be educated on the risks and ways to protect themselves from these risks:

> AISA's vision is of a world where all people, businesses and governments are educated about the risks and dangers of cyber attack and cyber theft to enable them to take all reasonable precautions to protect themselves.[247]

[242] Submission 15, Professor Vijay Varadharajan, p 4.

[243] Submission 15, Professor Vijay Varadharajan, p 4.

[244] Submission 15, Professor Vijay Varadharajan, p 4.

[245] Evidence, Ms Michelle Price, Chief Executive Officer, AustCyber, 29 October 2020, p 23.

[246] Submission 26, Palo Alto Networks, pp 4-5.

[247] Evidence, Mr Vizza, 29 October 2020, p 10.

4.23 The Australian Information Security Association also stated that a survey conducted in October 2019 of its 6,000 members identified a strong need for additional support for SMEs:

> 76 per cent of respondents believed there should be market incentives to improve cyber security including tax incentives, grants, providing free cyber short-course training to SMEs to ensure that cyber-security features are included and to increase awareness levels.[248]

The public

4.24 There are a range of emerging issues currently impacting the public, which in participants views warrants increased support from Government. The issues that participants identified as causing the need for increased support stem from the:

- prevalence of cyber crime
- increase in online service delivery
- expectation that people's privacy is protected by government
- impact of the COVID-19 pandemic on the way we work and access services online.

4.25 Cyber crime was cited by many participants as a key concern for members of the public, with some citing as many as one in three Australians were the victims of cyber crime in 2018.[249]

4.26 The Australian Cyber Security Centre's Annual Cyber Threat Report stated that 'cybercrime is one of the most pervasive threats facing Australia, and the most significant threat in terms of overall volume and impact to individuals and businesses.'[250]

4.27 The NSW Information and Privacy Commissioners cited data from the Australian Cyber Security Centre, which 'reported in its December 2019 Cyber Crime in Australia that it received 13,672 reports of cybercrime between July and September 2019 and that this equates to an average of 148 reports per day, or one every 10 minutes'.[251]

4.28 The Australian Information Security Association indicated the prevalence of cyber crime is increasing and that as a country we are not doing enough to protect those affected:

> When the 2016 strategy was launched, 1 in 4 Australians was impacted by cyber crime. The situation has deteriorated to the point where 1 in 3 Australians is now impacted by cyber crime, indicating that as a country we are losing the battle to protect businesses, services and the community.[252]

[248] Submission 24, Australian Information Security Association, Attachment A, p 19.

[249] See for example: Submission 26, Palo Alto Networks, p 5; Submission 24, Australian Information Security Association, Attachment A, p 2.

[250] Australian Cyber Security Centre, *Annual Cyber Threat Report: July 2019 to June 2020*, p 4, viewed at https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020.

[251] Submission 14, Information and Privacy Commission NSW, p 2.

[252] Submission 24, Australian Information Security Association, Attachment A, p 2.

4.29 At the same time as governments and businesses are undertaking a digital transformation agenda, citizens are also more connected than ever.

4.30 Mr Vizza described this increased connectivity and people's lack of awareness of it, highlighting the range of everyday electronic devices used in homes:

> We are surrounded by technology. The reality of it is that this is a critical issue for all people in Australia and in New South Wales. It is something that we all need to deal with and accept as a problem. We often talk about the fact that most people do not realise how much technology actually exists in their own homes. Our TVs are connected. We all have wi-fi at home and we all have many different bits of technology, all of which connect to the internet.[253]

4.31 Professor Varadharajan expressed concern about the Internet of Things and the vulnerability that this newfound technology creates for users. He said that attackers will always go for low-hanging fruits first – which in his view was the Internet of Things market as these products often do not have a focus on security.[254]

4.32 The increased connectivity of citizens and the growing nature of online government service delivery not only creates risk for citizens to be the target of cyber crime but also concerns about the protection of their privacy. Dr Arnold spoke about cyber crime not just being about the possible theft of a person's identity but also a privacy breach:

> … we often construe data breaches as a matter of identity crime aimed at providing the offender with a wrongful financial benefit. It is important however to recognise that many data breaches are an invasion of privacy, a disregard of the individual's legitimate freedom from arbitrary interference.[255]

4.33 In addition to the increasing need to access government services online, the pandemic was also identified by inquiry participants as creating additional challenges and risks for the public.

4.34 Mr Vizza explained that some of the impacts of the COVID-19 pandemic and the negative effects that it had on people's cyber safety. He said:

> The Australian Cyber Security Centre recorded a huge spike in incidents nationally at approximately the same time, which of course coincided with the advent of COVID-19 and the related lockdowns. That saw people who were understandably preoccupied and anxious with the global pandemic make some poor decisions that saw them succumb to a wave of phishing campaigns, phone-based campaigns and other electronic fraud..[256]

4.35 Similarly, Mr Stephen Knights from the Australian Information Security Association considered that people are more vulnerable to cyber threats when dealing with other challenges. He said 'COVID-19 has sort of taken the tide out and shown the rocks of what is going on in

[253] Evidence, Mr Vizza, 29 October 2020, p 10.

[254] Evidence, Professor Varadharajan, 29 October 2020, p 3.

[255] Submission 16, Dr Bruce Baer Arnold, p 6.

[256] Evidence, Mr Vizza, 29 October 2020, p 10.

society'. He explained that 'unfortunately, when people are vulnerable and their mental states are fragile, they are more likely to fall prey'.[257]

4.36 In addition to the risks to the public, changed working arrangements were also identified by participants as a concern. Representatives from $(ISC)^2$ and Australian Information Security Association spoke about the impact of the pandemic and how the sudden shift to working from home had affected cyber security:

> The rapid and massive shift to working from home has seen workers in both the public and private sectors connect to their workplaces remotely, often using their own computing devices and almost always using home networks where the general level of cyber security is often poor. This has now led to organisations and governments scrambling to implement cloud security, hardening of cyber defences for their datacentres, upscaling of remote network and telework capabilities and providing end user awareness campaigns around cyber security and privacy.[258]

4.37 In response to the risks impacting the public, participants provided a number of suggestions as to how the Government should do more to support the public to assist them to be more cyber secure. This was considered particularly important given several participants identified that many cyber attacks come down to human error.[259]

4.38 Members of the Australian Information Security Association identified a number of ways in which the NSW Government could do more to support citizens in protecting themselves from cyber threats, including:

- increased awareness and education for businesses and the general public
- appoint a dedicated cyber security minister
- anyone who is selling technology or technology services should be held responsible for 'enforcing' security standards in what they sell to business and consumers, with the Government responsible in overseeing the security standards
- industry can better 'bake-in' security at the design phase of systems, applications and digital services, to ensure at the time of production, they are not vulnerable to cyber attack
- as a way to influence general buying decisions and behaviours there could be something similar to a health star rating system for products, digital services and online platforms
- develop resources, guidance including developing quizzes, and video content to allow for easy consumption. [260]

4.39 Similarly, Professor Varadharajan advised of the need to increase awareness of the community so that they understand the impact and consequences of cyber attacks:

[257] Evidence, Mr Stephen Knights, Board Member, Australian Information and Security Association, 29 October 2020, p 11.

[258] Submission 20, $(ISC)^2$, p 6; Submission 24, Australian Information and Security Association, p 6.

[259] See for example: Submission 14, Information and Privacy Commission NSW, pp 2-3.

[260] Submission 24, Australian Information Security Association, Attachment A, pp 6-8.

> … we need to upskill people and we need to increase the awareness and ensure that the impact, the consequences of some of these actions can be understood by the community.[261]

4.40 Mr Tony Vizza, Director Cyber Security Advocacy at (ISC)[2] also expressed support for increased education for the public:

> The first pillar is an understanding that people are the most essential ingredient in any successful cyber security strategy. This involves ensuring that people are aware of the risks, appreciate how those risks can impact their day-to-day lives and take proactive steps to prevent those risks from eventuating[262].

The Commonwealth

4.41 Participants raised concerns about the lack of harmonisation and the opportunities for the NSW Government to work more closely with the Commonwealth.

4.42 Dr Arnold advised that the NSW Government does not have sole responsibility and that 'it needs to work with the Commonwealth, in conjunction with the other jurisdictions and with business'.[263]

4.43 This point was also captured by Mr Rupert Taylor-Price from Vault Cloud, who argued that 'the threats impacting operational technology and other technologies are now across government and across systems'.[264] Vault Cloud outlined concerns that the lack of harmonisation between State and Federal Government reduces security.[265]

4.44 Further, Mr Taylor-Price spoke about the impacts of a lack of harmonisation including that it makes it difficult to operate across agencies and that cyber security is weakened. He said:

> Overall, that disparity between Federal and State Government results in a suboptimal outcome for the country and for all involved. It vulcanises the systems and the data across government, makes it harder to interoperate between different parts of government and is a detriment for all of us. Again, not only is that interoperability a problem but it also results in lower security for the country.[266]

4.45 Mr Milton Baar from ISG Consulting told the inquiry that harmonisation can be achieved but that it requires greater resourcing. He said:

> There was an earlier comment about harmonisation and this is where the harmonisation is important. It can be done and there are frameworks that exist between the Australian National Audit Office or attorneys-general at a State level. There is a capability right now, but there are other issues of implementation and it does not come free.[267]

[261] Evidence, Professor Varadharajan, 29 October 2020, p 2.

[262] Evidence, Mr Vizza, 29 October 2020, p 20.

[263] Submission 16, Dr Bruce Baer Arnold, p 6.

[264] Evidence, Mr Rupert Taylor-Price, Chief Executive Officer, Vault Cloud, 29 October 2020, p 33.

[265] Submission 9, Vault Cloud, p 4.

[266] Evidence, Mr Taylor-Price, 29 October 2020, pp 32-33.

[267] Evidence, Mr Milton Baar, Chief Executive Office, ISG Consulting Pty Ltd, 29 October 2020, p 37.

4.46 As outlined in Chapter 3, the NSW Government advised that it is in the process of harmonising standards including baseline security standards and additional sector specific standards and guidance.[268]

4.47 Deputy Commissioner David Hudson from the NSW Police Force also referred to work it undertakes with the Commonwealth noting that it works closely with the Commonwealth and has adopted the Commonwealth's Protective Security Policy Framework to support information sharing:

> I think from our organisation, our internal perspective, we were an early adopter of the PSPF, Protective Security Policy Framework, when it was adopted by New South Wales Government from the Commonwealth, and that was because we deal with Commonwealth agencies significantly—the Australian Federal Police, the intelligence agencies—and overseas law enforcement agencies as well. So we had to be assured, and they had to have some assurance with us when sharing information that we were dealing with it appropriately. So we were very early adopters of information classification protocols, which includes technology, and I think we have been engaged with that since 2015.[269]

Committee comment

4.48 The committee acknowledges that cyber security is a shared responsibility with its success dependent on a range of people, technology and processes. The committee's views about improvements to people, technology and processes have been set out in chapters 2 and 3. However, we are also convinced that the Government needs to look beyond its own internal measures and increase the support to other stakeholders in order to improve the State's overall cyber security posture.

4.49 The evidence regarding local councils and the difficulties they face in implementing strong cyber security measures was compelling. The committee is particularly concerned about the risks associated with malicious actors infiltrating the systems underpinning critical infrastructure, such as water, in order to disrupt services to the public. While the committee welcomes the funding already allocated to assist councils, it appears that more support is required. The committee is of the view that the NSW Government should provide further funding to enhance the cyber security capabilities of local councils. In addition the government should engage with Local Government NSW to assist local councils to implement the mandatory requirements it has identified for its own agencies. This should include consulting with local councils as to the applicability of a mandatory reporting scheme at the local government level.

[268] Submission 10, NSW Government, p 7.

[269] Evidence, Deputy Commissioner David Hudson, Investigations and Counter Terrorism, NSW Police Force, 3 February 2021, p 39.

Recommendation 11

That the NSW Government:

- provide further financial support to local councils to enhance their cyber security capabilities
- develop a plan in consultation with Local Government NSW to ensure local councils meet the cyber security standards identified for NSW Government agencies.

4.50 Businesses, including SMEs, are a significant contributor to the New South Wales economy and are increasingly relied upon to provide services and products to the public, including on behalf of government. The committee acknowledge the multiple challenges faced by small business and SMEs and is concerned that this could contribute to a lack of ability to remain up to speed with or implement robust cyber security measures. In this regard the committee agrees with evidence that the Government should continue to provide resources and support to business to assist them to be cyber secure.

4.51 Similarly, we are concerned about the increased risk and impact to the public in respect of cyber crime and data breaches. We know that with an aging population and the ever evolving nature of connectivity and cyber threats, it can be difficult for the public to keep pace with cyber security developments and how they should be protect themselves or act when attacks occur. The increasing nature of online service delivery, the greater connectivity of people, the impacts of COVID as well as the growing cyber related crimes; coupled with evidence that many attacks can be attributed to human error causes the committee significant reason for concern.

4.52 We are of the view that the Government should prioritise this emerging public concern and elevate its existing measures to support the community. Having heard from those directly impacted by cyber attacks, we believe that more should be done to assist and support those impacted.

Recommendation 12

That the NSW Government develop a strategy to improve the cyber safety of citizens that includes:

- education and awareness measures
- consumer protection measures
- advice and support services.

4.53 The committee did not receive significant evidence regarding the work being done across jurisdictions. Despite this, we note the concerns raised by many industry participants regarding the lack of harmonisation, the confusion and duplication and the opportunities to enhance engagement with the Commonwealth and other jurisdictions to improve cyber security measures. The committee recognises the challenges with a federated system in many areas of public policy and service delivery, however we also acknowledge that technology, cyber attacks and systems are not bound by traditional borders or jurisdictions and requires a response that is whole of government, cross jurisdictional and involves industry, business and the wider community.

Appendix 1 Submissions

No.	Author
1	Crown Vetting and Cleard Life Vetting Agency
1a	Crown Vetting and Cleard Life Vetting Agency
2	Local Government NSW
3	AustCyber
4	Name suppressed
4a	Name suppressed
5	Confidential
6	NSW Auditor General
7	Netskope Australia
8	The Hills Shire Council
9	Vault Cloud
10	NSW Government
11	Mosman Council
12	Dr T Madhavan
13	Mercury Information Security Services Pty Ltd
14	Information and Privacy Commission NSW
15	Professor Vijay Varadharajan
16	Dr Bruce Baer Arnold
17	Active Cyber Defence Alliance
18	Office of the Australian Information Commissioner
19	Property Exchange Australia Ltd
20	$(ISC)^2$
21	Dr Bryan Hall
22	Name suppressed
23	ISG Consulting Pty Limited
23a	ISG Consulting Pty Limited
24	Australian Information Security Association (AISA)
25	Unions NSW
26	Palo Alto Networks
27	Name suppressed
28	Ms Claire Falkingham

Appendix 2 Witnesses at hearings

Date	Name	Position and Organisation
Thursday 29 October 2020 Macquarie Room, Parliament House, Sydney	Prof Vijay Varadharajan	Global Innovation Chair Professor in Cybersecurity, University of Newcastle
	Mr Tony Vizza	Director, Australian Information Security Association
	Mr Stephen Knights	Director, Australian Information Security Association
	Ms Michelle Price	Chief Executive Officer, AustCyber
	Ms Judy Anderson	Government Relations and Advocacy Lead, AustCyber
	Mr Tony Vizza	Director of Cyber Security Advocacy – Asia-Pacific, (ISC)^2
	Mr Andrew Cox	Member, Steering Group, Active Cyber Defence Alliance
	Ms Helaine Leggat	Member, Steering Group, Active Cyber Defence Alliance
	Mr Rupert Taylor-Price	Chief Executive Officer, Vault Cloud
	Mr Milton Baar	Director Cyber Security, ISG Consulting Pty Ltd
	Mr John Frisken	Director Professional Services, ISG Consulting Pty Ltd.
	Mr Thomas Costa	Assistant Secretary, Unions NSW
	Ms El Leverington	Legal/Industrial Officer, Unions NSW

Date	Name	Position and Organisation
Wednesday 3 February 2020 **Jubilee Room,** **Parliament House, Sydney**	Witness A	
	Mr Ian Goodwin	Deputy Auditor-General
	Ms Claudia Migotto	Assistant Auditor-General, Performance Audit
	Mr Scott Stanton	Assistant Auditor-General, Financial Audit
	Ms Elizabeth Tydd	Information Commissioner and CEO, Information and Privacy Commission NSW
	Ms Samantha Gavel	Privacy Commissioner, Information and Privacy Commission NSW
	Mr Tony Chapman	NSW Chief Cyber Security Officer and Executive Director, Cyber Security, Department of Customer Service
	Mr Greg Wells	NSW Government Chief Information and Digital Officer, Department of Customer Service
	Mr Damon Rees	Chief Executive Officer, Service NSW, Department of Customer Service
	Deputy Commissioner David Hudson APM	Deputy Commissioner for Investigations and Counter Terrorism, NSW Police Force
	Deputy Commissioner Malcolm Lanyon APM	Deputy Commissioner for Corporate Services, NSW Police Force

Appendix 3 Minutes

Minutes no. 23
Thursday 6 August 2020
Portfolio Committee No. 1 – Premier and Finance
McKell Room, at 2.34 pm

1. **Members present**
   Ms Moriarty, *Chair*
   Mr Borsak, *Deputy Chair*
   Ms Boyd
   Mr Franklin
   Mr Martin
   Mr Searle

2. **Previous minutes**
   Resolved, on the motion of Mr Searle: That draft minutes no 22 be confirmed.

3. **Correspondence**
   The committee noted the following items of correspondence:

   Received:
   - 4 August 2020 – Correspondence from Ms Abigail Boyd, requesting a meeting of Portfolio Committee No. 1 to consider a proposed self-reference into cyber security.
   - 28 July 2020 – Correspondence from the Hon Tara Moriarty MLC and Hon Adam Searle MLC, requesting a meeting of Portfolio Committee No. 1 to consider a proposed self-reference into cyber security.
   - 9 June 2020 – Email from Mr Greg Cameron to committee, concerning Budget Estimates evidence.

4. **Consideration of terms of reference**
   The committee considered the following proposed terms of reference:

   That Portfolio Committee 1 – Premier and Finance inquire into and report on cyber security and digital information management in New South Wales, and in particular:
   a) The number of cyber security incidents and data breaches involving NSW Government agencies;
   b) The monitoring and response to cyber security incidents and data breaches across the NSW Government;
   c) The policies and procedures underpinning the management of digital information by the NSW Government;
   d) Systems management within NSW Government agencies including outages, backups and cyber security;
   e) The financial costs and other impacts of cyber security incidents, data breaches and outages involving NSW Government agencies;
   f) Expenditure on cyber security, digital services and digital infrastructure across the NSW Government;
   g) The management of public access to digital information under GIPA and similar processes including coverage of mobile based and online platforms;

h) Contractual arrangements between the NSW Government and providers of digital services and infrastructure, including:
   (i) Provisions relating to cyber security generally; and
   (ii) Reporting obligations and the monitoring of cyber security incidents;

i) The extent and impact of outsourcing of government information systems, including:
   (i) Outsourcing to entities which are owned overseas;
   (ii) The risks involved with outsourcing government information systems.

j) The support provided by the NSW Government to local councils and other organisations in relation to cyber security;

k) The NSW Government's response to cybercrime in the community generally; and

l) Any other related matter.

Resolved, on the motion of Mr Searle: That the committee adopt the proposed terms of reference for an inquiry into cyber security.

5. Inquiry into Cyber security

5.1 Inquiry timeline

Resolved on the motion of Mr Searle: That the inquiry timeline be as follows:

- Submissions – closing date of 20 September 2020
- 1-2 hearings in October/November.

5.2 Stakeholder list

Resolved on the motion of Mr Searle: That the secretariat circulate to members the Chairs' proposed list of stakeholders to provide them with the opportunity to amend the list or nominate additional stakeholders, and that the committee agree to the stakeholder list by email, unless a meeting of the committee is required to resolve any disagreement.

5.3 Advertising

The committee noted that all inquiries are advertised via Twitter, Facebook, stakeholder letters and a media release distributed to all media outlets in New South Wales.

6. Adjournment

The committee adjourned at 2.40 pm, *sine die.*

Tina Higgins
Clerk to the Committee

Minutes no. 24
Thursday 29 October 2020
Portfolio Committee No. 1 – Premier and Finance
Macquarie Room, Parliament House at 9.45 am

1. Members present

Ms Moriarty, *Chair*
Mr Amato (substituting for Mrs Ward) (via teleconference)
Mr Khan (substituting for Mr Franklin)
Mr Martin

Mr Searle
Mr Shoebridge (substituting for Ms Boyd for the duration of the inquiry into cyber security)

2. Apologies
Mr Borsak

3. Previous minutes
Resolved, on the motion of Mr Searle: That draft minutes no. 23 be confirmed.

4. Correspondence
The committee noted the following items of correspondence:

Received:

- 2 July 2020 – Emails from a member of the public in relation to allegations about the conduct of the Attorney General.
- 6 August 2020 – Email from Ms Abigail Boyd MLC to the secretariat advising that Mr David Shoebridge MLC will be substituting for her for the duration of the inquiry into cyber security.
- 20 August 2020 – Email from Australian Security Intelligence Organisation to the Chair, declining the invitation to make a submission to the inquiry into cyber security.
- 9 September 2020 – Email from Mr Jake Farquharson, Parliamentary Support, Australian Electoral Commission, declining the invitation to make a submission to the inquiry into cyber security.
- 21 September 2020 – Email from Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division, National Resilience and cyber Security Group, Department of Home Affairs declining the invitation to make a submission to the inquiry into cyber security.
- 17 October 2020 – Email from Mr Danny O'Hara to the committee, regarding a 2014 Portfolio Committee No. 3 report into Tourism in Local Communities.

Resolved, on the motion of Mr Shoebridge: That unless a new issue arises, all correspondence received from the member of the public known to the Committee in relation to allegations about the conduct of the Attorney General remain confidential with no action taken.

5. Inquiry into Cyber security

5.1 Election of Deputy Chair
Resolved, on the motion of Mr Shoebridge: That for the purposes of today's hearing Mr Searle act as the Deputy Chair.

5.2 Public submissions
The committee noted that submissions nos 1, 1a, 2, 3, and 6 to 26 were published by the committee clerk under the authorisation of the resolution appointing the committee.

5.3 Partially confidential submissions
Resolved, on the motion of Mr Shoebridge: That the committee keep the following information confidential, as per the request of the author: identifying information in submission no. 22.

Resolved, on the motion of Mr Shoebridge: That the committee authorise the publication of submission nos 4, 4a, with the exception of identifying and/or sensitive information which are to remain confidential, as per the recommendation of the secretariat.

5.4 Confidential submissions

Resolved, on the motion of Mr Shoebridge: That the committee keep submission no. 5 confidential, as per the request of the author.

5.5 Hearing on 20 November 2020

Resolved, on the motion of Mr Shoebridge: That, due to the reserve sitting day scheduled for 20 November 2020, the committee cancel its public hearing scheduled for that date, with the secretariat to canvass availability via email for an alternative date.

5.6 Public hearing

Witnesses, the public and the media were admitted.

The Chair made an opening statement regarding the broadcasting of proceedings, adverse mention and other matters.

The following witness was sworn and examined:

- Prof Vijay Varadharajan, Global Innovation Chair Professor in Cyber security, University of Newcastle.

The evidence concluded and the witness withdrew.

The following witnesses were sworn and examined:

- Mr Tony Vizza, Director, Australian Information Security Association
- Mr Stephen Knights, Director, Australian Information Security Association.

The evidence concluded and the witnesses withdrew.

The following witnesses were sworn and examined:

- Ms Michelle Price, Chief Executive Officer, AustCyber
- Ms Judy Anderson, Government Relations and Advocacy Lead, AustCyber

Mr Tony Vizza, Director of Cyber Security Advocacy – Asia-Pacific, (ISC)^2 was also examined and had been sworn in earlier this day.

The evidence concluded and the witnesses withdrew.

The following witnesses were sworn and examined:

- Mr Andrew Cox, Member, Steering Group, Active Cyber Defence Alliance
- Ms Helaine Leggat, Member, Steering Group, Active Cyber Defence Alliance.

The evidence concluded and the witnesses withdrew.

The following witnesses were sworn and examined:

- Mr Rupert Taylor-Price, Chief Executive Officer, Vault Cloud
- Mr Milton Baar, Director Cyber Security, ISG Consulting Pty Ltd
- Mr John Frisken, Director Professional Services, ISG Consulting Pty Ltd.

The evidence concluded and the witnesses withdrew.

The following witnesses were sworn and examined:

- Mr Thomas Costa, Assistant Secretary, Unions NSW
- Ms El Leverington, Legal/Industrial Officer, Unions NSW.

The evidence concluded and the witnesses withdrew.

Witnesses, the media and the public withdrew.

5.7 Correspondence
The Committee noted the following items of correspondence:

Received:

- 28 October 2020 – Email from Randall Stewart, Senior Policy and Project Officer, NW Police Force to the secretariat advising that NSW Police Force is declining the committee's invitation to give evidence to the cyber security inquiry as the inquiry's terms of reference is more relevant to other departments and agencies.

Resolved, on the motion of Mr Shoebridge: That the chair write to the Commissioner, NSW Police Force asking to reconsider the position of not sending representatives to give evidence to the cyber security inquiry and noting the importance of the NSW Police Force in enforcing cyber security laws.

6. Adjournment
The committee adjourned at 3.11 pm, *sine die.*

Sam Griffith
Clerk to the Committee

Minutes no. 25
Wednesday 3 February 2021
Portfolio Committee No. 1 – Premier and Finance
Jubilee Room, Parliament House, Sydney at 10.19 am

1. Members present
Ms Moriarty, *Chair*
Ms Boyd (*for Budget Estimates*) (from 10.19 am to 10.30 am)
Mr Franklin (from 11.00 am)
Mr Martin
Mr Searle
Mr Shoebridge (from 11.00 am)
Mrs Ward

2. Apologies
Mr Borsak
Mr Franklin (for consideration of Budget Estimates 2020-2021 resolutions)

3. Previous minutes
Resolved, on the motion of Mr Searle: That draft minutes no. 24 be confirmed.

4. Correspondence
The Committee noted the following items of correspondence:

Received:

- 18 November 2020 – Email from Sarah Croxall, Office of the Australian Information Commissioner, to the secretariat, declining the committee's invitation to appear at the cyber security inquiry hearing on 3 February 2021, but noting the office would be pleased to answer any specific questions in relation to the Notifiable Data Breach scheme.

- 19 November 2020 - Email from the Office of the Hon Robert Borsak MLC, to the secretariat, advising Mr Borsak is an apology for cyber security inquiry activity in February and March 2021.
- 1 December 2020 – Email from Kelly Kwan, Executive Officer, Local Government NSW, to the secretariat, declining the committee's invitation to appear at the cyber security inquiry hearing on 3 February 2021 and noting they can respond in writing to any questions related to their submission.
- 2 December 2020 – Email from Dan, Operations, Australian cyber Security Centre, to the secretariat, declining the committee's invitation to appear at the cyber security inquiry hearing on 3 February 2021.

Sent:

- 17 November 2020 – Letter from chair to Commissioner Mick Fuller APM, NSW Police Force, re-inviting NSW Police Force to attend a hearing for the cyber security inquiry on 3 February 2021.

5. Inquiry into Budget Estimates 2020-2021 – procedural resolutions

The committee noted the Budget Estimates timetable for 2020-2021 agreed to by the House, with hearings commencing at 9.30 am and concluding by 8.30 pm, for Portfolio Committee No. 1:

Date	Portfolio
Thursday 25 February 2021	Special Minister of State, Public Service and Employee Relations, Aboriginal Affairs and the Arts (Harwin)
Monday 1 March 2021	The Legislature (Ajaka)
Thursday 4 March 2021	Premier (Berejiklian)
Monday 8 March 2021	Treasury (Perrottet)
Wednesday 10 March 2021	Jobs, Investment, Tourism and Western Sydney (Ayres)
Friday 12 March 2021	Finance and Small Business (Tudehope)

5.1 Allocation to question time and total hearing time

Resolved, on the motion of Mr Searle: That, with no government questions being asked:

- the Special Minister of State, Public Service and Employee Relations, Aboriginal Affairs and the Arts portfolios be examined from 9.30 am to 12.30 pm and from 2.00 pm to 5.00 pm, with an additional 15 minutes reserved for government questions.
- the Legislature portfolio be examined from 9.30 am to 11.30 am, with an additional 15 minutes reserved for government questions.
- the Premier portfolio be examined from 9.30 am to 12.30 pm and from 2.00 pm to 5.00 pm, with an additional 15 minutes reserved for government questions.
- the Treasury portfolio be examined from 9.30 am to 12.30 pm and from 2.00 pm to 5.00 pm, with an additional 15 minutes reserved for government questions.

- the Jobs, Investment, Tourism and Western Sydney portfolios be examined from 9.30 am to 12.30 pm and from 2.00 pm to 5.00 pm, with an additional 15 minutes reserved for government questions.
- the Finance and Small Business portfolios be examined from 9.30 am to 12.30 pm and from 2.00 pm to 5.00 pm, with an additional 15 minutes reserved for government questions.

Resolved, on the motion of Mr Searle: That:

- the Minister and Parliamentary Secretary appear from 9.30 am until 12.30 pm
- departmental staff appear from 9.30 am until 5.15 pm.

Resolved, on the motion of Mr Searle: That for the portfolio of the Legislature the President and departmental staff appear from 9.30 am until 11.45 am.

5.2 Witness requests

Resolved, on the motion of Mr Searle: That:

- the list of witnesses suggested by the Opposition be circulated to the committee for comment
- the committee provide witness requests to the secretariat by 12 pm, Thursday 4 February 2021.

Resolved, on the motion of Mr Searle: That the committee invite the following parliamentary secretaries to appear as a witness at the hearings:

- Hon Scott Farlow MLC, Parliamentary Secretary to the Treasurer
- Hon Ben Franklin MLC, Parliamentary Secretary for the Arts
- Mr Geoff Provest MP, Parliamentary Secretary for Tourism and Major Events
- Hon Gabrielle Upton MP, Parliamentary Secretary to the Premier
- Mr Ray Williams MP, Parliamentary Secretary to the Premier and Western Sydney.

6. Inquiry into Cyber security

6.1 Deputy Chair

Resolved, on the motion of Mrs Ward: That, in the absence of the Deputy Chair, Mr Searle act as Deputy Chair for the purposes of this meeting.

6.2 Public Submissions

The following submissions were published by the committee clerk under the authorisation of the resolution appointing the committee: submission nos. 23a and 28.

6.3 Partially confidential submission

Resolved, on the motion of Mrs Ward: That the committee keep the following information confidential, as per the request of the author: identifying information in submission no. 27.

6.4 Confidential submission

Resolved, on the motion of Mrs Ward: That submission no. 22 (previously name suppressed) be made confidential at the request of the author.

6.5 Answers to questions on notice

The following answers to questions on notice and supplementary questions were published by the committee clerk under the authorisation of the resolution appointing the committee:

- Active Cyber Defence Alliance, received 18 November 2020
- Australian Information Security Association, received 25 November 2020.

6.6 In camera witness

The committee noted that it had agreed via email in December 2020 for Witness A to give in camera evidence at the hearing on 3 February 2021.

6.7 Report deliberative

The committee noted that the report deliberative for the inquiry into cyber security will take place at 2.30 pm on 19 March 2021 in the McKell Room.

6.8 In camera hearing

The committee proceeded to take evidence *in camera*.

Persons present other than the committee: Mr Sam Griffith, Ms Kate Bogatova, Mr Andrew Ratchford and Hansard reporters.

The Chair made an opening statement regarding a range of matters.

The following witness was sworn and examined:

- Witness A.

Witness A tendered the following documents:

- Evidence, General Purpose Standing Committee No. 1, Inquiry into Budget Estimates, Finance, Services and Property, 2 September 2015
- Evidence, Portfolio Committee No. 1 – Premier and Finance, Inquiry into Budget Estimates, Finance, Services and Property, 4 September 2017.

The evidence concluded and the witness withdrew.

The *in camera hearing* concluded at 11.00 am.

Resolved, on the motion of Mr Searle: That the committee accept and not publish the following documents tendered by Witness A during the *in camera* hearing:

- Evidence, General Purpose Standing Committee No. 1, Inquiry into Budget Estimates, Finance, Services and Property, 2 September 2015
- Evidence, Portfolio Committee No. 1 – Premier and Finance, Inquiry into Budget Estimates, Finance, Services and Property, 4 September 2017.

6.9 Public hearing

The committee proceeded to take evidence in public.

Witnesses, the public and media were admitted.

The Chair made an opening statement regarding the broadcasting of proceedings and other matters.

The following witnesses were admitted, sworn and examined:

- Mr Ian Goodwin, Deputy Auditor-General
- Ms Claudia Migotto, Assistant Auditor-General, Performance Audit
- Mr Scott Stanton, Assistant Auditor-General, Financial Audit.

The evidence concluded and the witnesses withdrew.

The following witnesses were admitted, sworn and examined:

- Ms Elizabeth Tydd, Information Commissioner and CEO, Information and Privacy Commission NSW
- Ms Samantha Gavel, Privacy Commissioner, Information and Privacy Commission NSW.

The evidence concluded and the witnesses withdrew.

The following witnesses were admitted, sworn and examined:

- Mr Tony Chapman, NSW Chief Cyber Security Officer and Executive Director, Cyber Security, Department of Customer Service
- Mr Greg Wells, NSW Government Chief Information and Digital Officer, Department of Customer Service
- Mr Damon Rees, Chief Executive Officer, Service NSW, Department of Customer Service.

The evidence concluded and the witnesses withdrew.

The following witnesses were admitted, sworn and examined:

- Deputy Commissioner David Hudson APM, Deputy Commissioner for Investigations and Counter Terrorism, NSW Police Force
- Deputy Commissioner Malcolm Lanyon APM, Deputy Commissioner for Corporate Services, NSW Police Force.

The evidence concluded and the witnesses withdrew.

The public hearing concluded at 3.58 pm.

7. Adjournment
The committee adjourned at 3.59 pm, until *sine die.*

Sam Griffith
Clerk to the Committee

Draft Minutes no. 32
Friday 19 March 2021
Portfolio Committee No. 1 – Premier and Finance
Room 1043, Parliament House, Sydney at 2.31 pm

1. Members present
Ms Moriarty, *Chair*
Mr Franklin
Mr Martin
Mr Searle
Mr Shoebridge
Mrs Ward

2. Apologies
Mr Borsak

3. Correspondence
The committee noted the following items of correspondence:

Received:

- 2 March 2021 – Correspondence from the Office of Minister Dominello, to the secretariat providing Department of Customer Service answers to questions on notice and supplementary questions
- 4 March 2021 – Correspondence from Mr Randall Stewart, Senior Policy and Project Officer, NSW Police Force to the secretariat providing answers to questions and supplementary questions and transcript corrections.

4. Inquiry into Cybersecurity

4.1 Public submission attachment

Resolved, on the motion of Mr Franklin: That the committee publish Attachment A to submission no. 24 by the Australian Information Security Association as the attachment contain information referred to in the Chair's draft report.

Mr Shoebridge and Mrs Ward joined the meeting at 2.32 pm.

4.2 Answers to questions on notice

The committee noted the following answers to questions on notice and supplementary questions published by the committee clerk under the authorisation of the resolution appointing the committee:

- Department of Customer Service, received 2 March 2021
- NSW Police Force, received 4 March 2021.

4.3 In camera transcript

Resolved, on the motion of Mr Searle: That, following consultation with Witness A, the transcript of their evidence from 3 February 2021 be published with their name suppressed.

4.4 Consideration of Chair's draft report

The Chair submitted her draft report entitled *Cyber security*, which, having been previously circulated, was taken as being read.

Resolved, on the motion of Mr Martin: That paragraph 2.1 be amended by inserting at the end 'The number of affected people has subsequently been reduced to 104,000 following further investigations. [FOOTNOTE: https://www.service.nsw.gov.au/cyber-incident]'.

Resolved, on the motion of Mr Martin: That the following paragraph be inserted after paragraph 2.18: 'Service NSW has partnered with Independent cyber support community service IDCARE to provide an additional level of expert support. [FOOTNOTE: https://www.service.nsw.gov.au/news/service-nsw-notifies-customers-relation-cyber-incident]'.

Resolved, on the motion of Mr Martin: That the following paragraph be inserted after paragraph 2.29:

> Mr Rees also outlined that Service NSW was undertaking work to reduce the manual handling of information:
>
> > That requires, in many cases, the fundamental digitisation of those processes end-to-end so that the information does not have to be manually handled. It is an important piece of work. It is not a quick or easy or fast piece of work, but that is the work that we are mobilising now with our partner agencies. [FOOTNOTE: Evidence, Mr Rees, 3 February 2021, p 29].

Resolved, on the motion of Mr Martin: That Finding 3 be amended by omitting 'That Service NSW' and inserting instead 'That, while Service NSW has taken steps to reduce its dependency on email, it'.

Mr Searle moved: That the following paragraphs, new finding and new recommendation be inserted after 2.86:

> The committee notes the report of Standing Committee on Law and Justice of this House on 3 March 2016 on remedies for the serious invasion of privacy in New South Wales. That inquiry heard evidence from individuals, academics, legal experts, media and arts representatives, as well as from privacy experts including the NSW Privacy Commissioner, with the vast majority of stakeholders arguing strongly for the introduction of a statutory cause of action on the basis that existing legal remedies were inadequate. The bulk of evidence was that the available civil remedies, in particular the equitable action for breach of confidence, was inaccessible, offered a 'poor fit', and failed to offer appropriate remedy to people who suffered a serious invasion of privacy. Stakeholders expressed frustration at the lack of decisive action on this issue, despite several eminent reports recommending a similar course.
>
> Privacy is an asset. Once it is lost, it cannot be recovered. The impacts of that loss can be devastating. The committee agreed that there is a clear need to ensure better protection of privacy, and to provide adequate remedies to people who experience a serious invasion of privacy. To that end, the committee recommended that the NSW Government introduce a statutory cause of action for serious invasions of privacy, based on the model proposed by the Australian Law Reform Commission in its 2014 report *Serious Invasions of Privacy in the Digital Era* (see recommendations 3 and 4 of that inquiry).
>
> The committee notes the NSW Parliament has enacted criminal laws to deal with so-called *'revenge porn'* but considers that further action is needed in this area and supports the implementation of the recommendations of the Law and Justice Committee report on remedies for the serious invasion of privacy in New South Wales. The implementation of those recommendations would create a legal framework that would significantly assist those persons who have been the victim of cyber attacks, such as in the cyber enabled attack on Service NSW and the subsequent data breach of thousands of citizens' personal data.
>
> **Finding X**
>
> That the NSW Government lacks any real framework or clear processes within government to properly and expeditiously deal with requests by people in the community for assistance in the event of a breach of their data. People who suffer data breaches are left to their own resources and the existing, unsatisfactory state of the law where very few persons are eligible for relief, assuming they have the financial resources to seek it.
>
> **Recommendation X**
>
> That the NSW Government urgently address the matters identified in Finding X and implement a framework or clear process within government to properly and expeditiously deal with requests by people in the community for assistance in the event of a breach of their data.

Question put.

The committee divided.

Ayes: Ms Moriarty, Mr Searle, Mr Shoebridge

Noes: Mr Franklin, Mr Martin, Mrs Ward

Question resolved in the affirmative on the casting vote of the Chair.

Resolved, on the motion of Mr Shoebridge: That:

- The draft report, as amended, be the report of the committee and that the committee present the report to the House;
- The transcripts of evidence, submissions, tabled documents, answers to questions on notice and supplementary questions, and correspondence relating to the inquiry be tabled in the House with the report;
- Upon tabling, all unpublished attachments to submissions be kept confidential by the committee;
- Upon tabling, all unpublished transcripts of evidence, submissions, tabled documents, answers to questions on notice and supplementary questions, and correspondence relating to the inquiry, be published by the committee, except for those documents kept confidential by resolution of the committee;
- The committee secretariat correct any typographical, grammatical and formatting errors prior to tabling;
- The committee secretariat be authorised to update any committee comments where necessary to reflect changes to recommendations or new recommendations resolved by the committee;
- Dissenting statements be provided to the secretariat within 24 hours after receipt of the draft minutes of the meeting;
- The report be tabled in the House on Thursday 25 March 2021; and
- The Chair to advise the secretariat and members if they intend to hold a press conference, and if so, the date and time.

5. Adjournment

The committee adjourned at 2.51 pm, *sine die.*

Sam Griffith
Clerk to the Committee