First print

Cybersecurity (Protections and Preventions) Bill 2023

Lead Sponsor:	The Hon Lucy Allen, Youth Member for Bega *Youth Shadow Minister for Business and Employment*
Sponsors:	The Hon Laura Strawbridge, Youth Member for Wahroonga The Hon Vanessa Lin, Youth Member for Heffron The Hon Brayden Whitford, Youth Member for Londonderry The Hon Yuki Wang, Youth Member for Ryde The Hon Krish Nair, Youth Member for Castle Hill
Lead Refuter:	The Hon Hamish Longstaff, Youth Member for North Shore *Youth Minister for Business and Employment*
Refuters:	The Hon Eamonn Ryan, Youth Member for Cronulla The Hon Braydon Monahan, Youth Member for Tweed The Hon Antony Di Mattia, Youth Member for Balmain

Contents

Cybersecurity (Protections and Preventions) Bill 2023

Act no. , 2023

A Bill for

An Act to strengthen cybersecurity within New South Wales businesses and society by establishing a central agency which ensures protections, preventions and responses in the event of a cyber-attack; and for other purposes.

Explanatory notes

In the midst of a rapidly changing globe experiencing rapid technological development, across the world, consumers have been subject to data breaches. High profile hacks targeting businesses such as Optus and Medibank have stolen personal information and left individuals in fear. The Australian Cyber Security Centre recorded an astounding 76,000 cybercrime reports, a 13% increase from the previous financial year. With these alarming figures, it is clear this is a significant problem that will only worsen as society becomes more integrated with technology.

In the aftermath of Australian telecommunications company Optus's cyber-attack in September 2022, Ben Zocco of Slater and Gordon Lawyers described this attack as "Potentially the most serious privacy breach in Australian history, both in terms of the number of affected people and the nature of the information disclosed." This exemplifies the disturbing extent that recent breaches have had on consumers.

Across the state, thousands of businesses run day and night, boosting our state's economy, however some run unprotected from cyber-attacks. This for most business owners is simply not a choice. With our state still recovering from a global pandemic and increasing amounts of taxes it has become a miracle for some businesses to break even on profits yet alone purchase cyber protection.

In order to protect consumers and businesses from potential future cyber-attacks, the initial objective of this bill is to establish The NSW Cyber Security Commission, an independent statutory authority to replace Cyber Security NSW to administer and enforce the means of the Act. This meets Recommendation 1 of a report titled Cyber Security by Portfolio Committee No.1- Premier and Finance for tabling in the Legislative Council which calls for "The NSW Government to review the functions of Cyber Security NSW and provide it with a clearer mandate to oversee agencies' cybersecurity progress and ensure their compliance with the NSW Cyber Security Policy." A centralised commission with the powers outlined in the objectives below will be beneficial to consumers and businesses in New South Wales by ensuring data is protected, establishing a mandatory reporting scheme, creating educational initiatives, enhancing cyber skills within the workplace and banning the payment of ransoms.

The most concerning part of the Optus 2022 cyber-attack was how easily it was conducted. Hackers were able to extract critical customer data from an unprotected application programming interface, one which didn't even require a username or password. This was a complete failure on the part of Optus to protect the customer data they collected. One of the objectives of this bill is to ensure a responsibility on the part of businesses to protect customer data by mandating large businesses that collect valuable data by implementing 8 essential strategies to minimise the risk of data breaches for businesses listed by the Australian Cyber Security Centre. These include application control, MS Office macro settings, user application hardening, restricting administrative privileges, patch applications, multi-factor authentication, patching operating systems, and regular backups. Thus, reforming the law to ensure businesses that collect valuable personal data have protections for that data, significantly reducing the frequency of large data breaches and making them much harder to perform.

Businesses should have an obligation to report all cyber security breaches that occur within their business to both the consumer and the Office of the Australian Information Commissioner. This idea will then align with NSW Cyber Security's recommendation of establishing a mandatory data breach notification scheme. Which is to notify the OAIC and individuals when a serious data breach has occurred. Customers should have the right to know if their data has been stolen and how to protect themselves from further data breaches. With technology rapidly developing, a mandatory reporting scheme for all businesses across NSW needs to be established to help businesses protect their data as well as the consumers from data breaches.

Implementing cybersecurity education initiatives in schools and workplaces accentuates the importance of providing staff and students with the skills and knowledge to prevent and respond to cybersecurity threats, specifically after the large Medibank and Optus breaches. Within the education scope, it is well understood that students are acquiring technological skills earlier in their development. Workplace initiatives would be provided to companies that demonstrate a need for enhanced cybersecurity measures, particularly those handling sensitive customer data. These initiatives aim to develop a culture of cybersecurity awareness, encouraging individuals to protect their personal and digital assets and to contribute to the resilience of NSW's digital infrastructure. Following the implementation of these programs, its impact will be measured through voluntary surveys and feedback from participants or leaders of schools and/or workplaces, allowing for data-driven refinements to be made over time. Examples of educational programs and training materials to be provided may include interactive workshops, online courses and simulations that address topics such as password management, phishing awareness, and secure data handling, tailored to the specific needs and skill levels of the target audience.

Once an organisation is hacked, hackers may request a ransom from a hacked business to free data or prevent the data from being leaked. One of the objectives of this bill is to ban the payment of ransoms to hackers. Payment of ransoms is not a guarantee that the data will be returned or not leaked, therefore the payment of ransoms may only encourage hackers. Paying ransoms also legitimises criminal activity and undermines the rule of law. It sends a message that criminal activity is an acceptable way to profit and will only encourage hackers to continue. Banning ransom payments will reduce the financial incentives for cybercriminals and discourage them from targeting NSW businesses and individuals. Banning ransom payments is a necessary step to deter cybercriminals and protect the security and privacy of individuals and businesses in New South Wales.

As technology evolves drastically, hacks are ultimately bound to happen. Whilst prevention methods may be a great concept of deterrence and lower rate of casualties, in the end hacks may still occur. We can't guarantee that the government has the quality protection to prevent hacks. Hence, the refuters believe it is pivotal that we prosper a body that will work with businesses that are hacked in order to limit or reduce the rate of damage. Parliamentarians should care about creating a body that will seek to help businesses during a time of breach. Whilst a hack can damage or be a risk itself, the next procedure is to see how much of the damage has been done. Providing a body will reduce the additional data breach. Businesses may go to private companies that specialise in white hat hacking, however businesses may not have the funding, and so may not be able to access them. Providing a free or low-cost body will allow businesses to access the government initiative within a short time of the hacks occurring.

There is currently no NSW Government body that specialises in the investigation and providing incentives to limit the effects of attacks. The main reason for this is due to the recent evolving

technological change in which law hasn’t kept up with. Only recently have politicians and media been aware of such occurrences due to recent cases of data breaches.

It is vital to work with businesses, not against them. This bill is about helping business-consumers relationships thrive and this should not be at cost to the business. If governments mandate expensive security measures, we cannot expect businesses that are struggling to stay afloat to cover the expenses of such measures. The cost of cyber security is dire. Businesses struggling to break even don't need such pressure on their firms. Government grants for businesses to develop cyber protections are an important step to not only help business-consumer relations but also further government-business relations. In order to ensure that this statute won't just be more red tape, we implore that such measures need to be taken to make sure that businesses are at cost. Such incentives including government grants will attract businesses to take these funds and install security. Not only does this benefit the company but will attract customers if it is made accessible to the consumers. If implemented, this approach would be one of the first steps of prevention of cyber-attacks. Customers or companies can't afford attacks like what we have seen recently, so we can expect them to pay out of pocket to stop these vicious attacks.

The Youth Legislature of New South Wales enacts—

Part 1 Preliminary

1 Name of Act

This Act is the *Cybersecurity (Protections and Preventions) Act 2023*.

2 Commencement

The Act commences on the day that is 1 year after the date of assent to this act.

3 Relationship with other Acts and laws

This Act prevails to the extent of an inconsistency with another Act or law.

4 Objects

The objects of this Act are to—

(1) address the persisting issue of cybersecurity within NSW, in order to protect consumers and businesses,

(2) establish a central government agency, the NSW Cybersecurity Commission to enforce and administer the clauses of this Act,

(3) implement cybersecurity education initiatives.

5 Definitions

In this Act—

cyber attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. Cyber attacks can disable computers, steal personal information and data, or use a breached computer as a launch point for other attacks.

cyber relates to Information Technology (IT), and anything related to modern computing, such as the internet, technology and virtual reality.

cyber safe refers to the practice of being safe and secure online, in preventing personal attacks or criminal activities.

cyber security refers to every aspect of protecting an organisation / business / company and its employees and assets against modern computing and Information Technology threats.

Cybersecurity Commission is the body within this Act which will oversee cybersecurity standards within New South Wales

data breach means an incident involving the unauthorised release of confidential information

mandatory reporting means a system obligating organisations to disclose if a certain event has occurred.

hacking is usually a form of digital attack performed from a remote location which can be utilised to release data or otherwise harm any person or organisation which is targeted.

ransom means a sum of money or other service demanded as a result of leverage over a person, company or other structure.

Note— The *Interpretation Act 1987* also contains definitions and other provisions that affect the interpretation of this Bill.

Part 2 Establishment of the NSW Cyber Security Commission

6 Establishment of the NSW Cyber Security Commission

The NSW Cyber Security Commission shall be established as a centralised, independent statutory authority.

7 Minister to have jurisdiction

The Minister administering the *Government Information (Information Commissioner) Act 2009 No 53* shall have jurisdiction over this authority.

8 Function of the Commission

The Commission has the function to—

(a) enforce and administer the means and clauses of this bill;

(b) override existing government bodies with relation to cybersecurity, including Cyber Security NSW;

(c) meet recommendation 1 of the Legislative Councils 2021 "Cybersecurity" Report by Portfolio Committee No.1;

(d) oversee agencies' cybersecurity progress and ensure compliance with policy; and

(e) monitor and respond to cybersecurity incidents and data breaches across the NSW Government.

Part 3 Provisions to Reduce Cyber Risk and Prevent Cyber Loss

9 Implementation of Essential Eight Cybersecurity Strategies

NSW Businesses that hold large volumes of data must implement the eight strategies to minimise the risk of cyber attacks and data breaches which are—

(1) Centralisation of application control in business computer networks,

(2) Installation of patches and updates within 48 hours of release,

(3) Configuring Microsoft Office Macro settings,

(4) User application hardening and feature blocking,

(5) Restricting administrative privileges,

(6) Patching operating systems within two weeks of release,

(7) Implementing multi-factor authentication, and

(8) Regular software backups.

10 Banning Payment of Ransoms

(1) Businesses who have been subject to a data breach and are asked to pay a ransom for the protection of data are—

(a) forbidden to pay the ransom;

(b) must report the request of ransom to the New South Wales Cyber Security Commission; and

(c) if payment is made, penalties at the discretion of the Commission shall apply.

Part 4 Strengthening Cybersecurity Education

Division 1 Education Initiatives to Support Cyber-Security Literacy and Awareness

11 Education initiatives

(1) There shall be education initiatives to achieve cyber safety and strengthen cybersecurity in the workforce and education sectors.

(2) This will be facilitated by the NSW Cyber Security Commission.

12 Training in the workforce

(1) Mandatory comprehensive training programs within the NSW workforce will—

(a) address the need for continuous cybersecurity education within the digital workforce; and

(b) prepare employees with skills necessary to identify cybersecurity threats.

(2) These programs will be mandatory to ensure employees and businesses are equipped with the skills and knowledge to be safe from cyber attacks.

13 Universal Cyber Security Course

The NSW Cyber Security Commission shall create a universal cyber security course.

14 Curriculum Development

(1) There shall be a standardised cybersecurity curriculum within primary education institutions to cultivate a bring awareness to cybersecurity and tools to identify cybersecurity threats.

(2) This will be in consultation between the Minister administering the *Education Act 1990 No 8* and the Minister administering the *Government Information (Information Commissioner) Act 2009 No 53*.

Division 2 Funding for Businesses

15 Businesses to receive funding

Businesses will be able to qualify for funding of up to 80% of the cost of the required security as prescribed in clause 9.

16 Qualification of Businesses

(3) Businesses are required to have the following in order to qualify for the funding as prescribed in clause 15—

(a) revenue of less than $1.5 million per annum; or

(b) an employee number of no more than 200; or

(c) unincorporated of any size businesses withholding sensitive information of direct clients; or

(d) businesses in regional or rural areas.

(4) Without limiting clause 16(1)(a), clause does not have to be met for businesses of agricultural or industrial classification.

Part 5 Responses in the event of a cyber attack

Division 1 Mandatory reporting of cyber attacks

17 Disclosure in the event of a cyber attack

(5) Any business that has a cyber attack or the unintended disclosure of confidential information must:

(a) report the event to the NSW Cyber Commission, and

(b) stakeholders of the business.

18 Timeframe for mandatory reporting

The disclosure as prescribed in clause 17 must be completed within 24 hours of the attack.

Division 2 Government incentives

19 Authorisation of Government incentives

(6) The NSW Government may support and provide incentives to victims, specifically the businesses, employers, employees and clients who may be victims of any attack.

(7) The incentives will be provided by the "Business Support Branch of Service NSW".

20 Application of incentives

(8) Government Agency can—

(a) actively cooperate with the NSW Cyber Security Commission and seek advice on providing initiatives to businesses and victims;

(b) allow Service NSW to support businesses and victims with Government revenue to limit the effects of the cyber attack breach;

(c) encourage greater recommendations and direction to those who are victims to cyber attack;

(d) provide high-skilled labour for businesses in order to restore data and/or limit data breach effect; and

(e) provide cyber security educational training for new businesses.

Produced for The Y NSW Youth Parliament 2023