Department of Customer Service

Cyber Security NSW Strategic Plan

FY2023-2024

November 2023 | Version 2.0

Cyber Security NSW

Cyber Security NSW is a whole-of-government function within the Digital.NSW division of the NSW Department of Customer Service, led by the NSW Chief Cyber Security Officer.

Our purpose

Supporting NSW Government departments, agencies and local councils in continually improving their cyber resilience, and providing strategic cyber security leadership.

Our mission

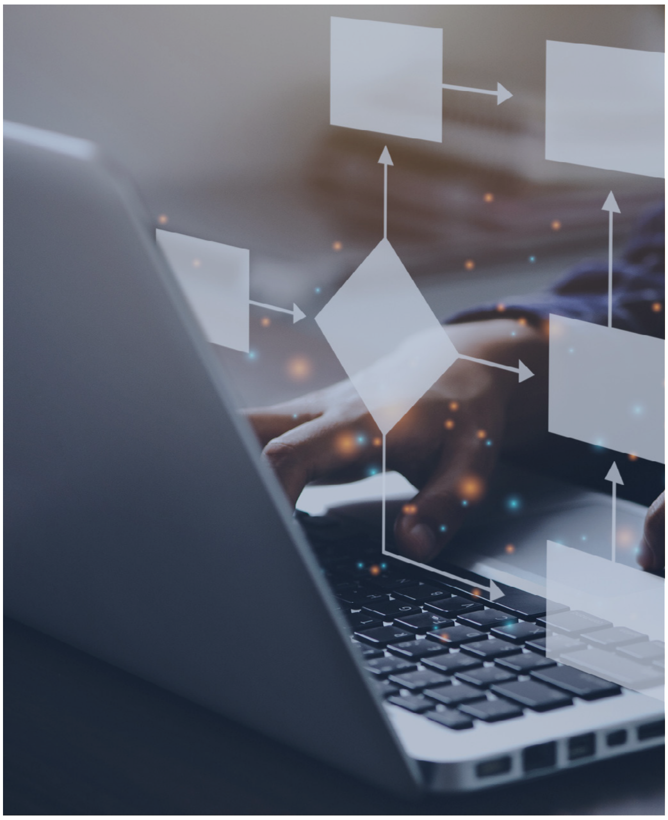
To achieve a cyber-secure NSW Government that has robust risk management and rigorous protections to safeguard the confidentiality, integrity and availability of public systems, services and data for NSW communities.

Our role

Cyber Security NSW provides a wide range of tailored products, services and best practice advice and guidance to NSW Government departments, agencies and local councils. We also lead and coordinate whole-of-government cyber security strategies and the NSW Government response to significant cyber security incidents and crises.

Our integrated, risk-based approach encompasses technical, people and process-focused initiatives that work together to improve cyber risk management and cyber security holistically.

We collaborate and coordinate with departments, agencies, local councils, law enforcement, ID Support NSW and other cyber security agencies within NSW and nationally.



Strategic direction

Pillars

Minimising exposure to cyber risks and the impact of cyber security incidents

1 Lead

Driving best practice from the top-down within entities and cooperating and influencing across sectors and jurisdictions to overcome cyber challenges.

2 Prepare

A cyber-aware culture, properly managed cyber risk and continuity plans that treat cyber security as a whole-of-business risk.

3 Prevent

Processes, policies, technical controls, training and cyber hygiene practices that reduce the likelihood of successful cyber attacks.

4 Detect

Effective, up-to-date monitoring technology, threat intelligence and assistance to alert and advise leaders for proactive remediation.

5 Respond

Clear policies and well-practised plans to ensure effective action in the event of a cyber incident.

6 Recover

Mechanisms to minimise the extent and duration of cyber attacks, and enable a rapid return to business as usual.

Strategic objectives

- Foster partnerships and strengthen collaboration with the public and private sectors to manage cyber risks and threats.
- Provide best practice cyber security advice and guidance.
- Shape and influence public cyber security policies in NSW and nationally.
- Elevate cyber security awareness, best practice and a cyber-safe culture.
- Guide strategic cyber security decision-making across NSW Government.

- Deliver or facilitate services to support under-resourced agencies and local councils.
- Increase the capabilities of all NSW Government staff to enhance cyber resilience.
- Proactively identify and analyse current and emerging threats.
- Provide advice and end-to-end solution recommendations on emerging threats to NSW Government.

- Prevent cyber security incidents and reduce their impact and spread by promoting best practice, and advising on and assisting with technical solutions.
- Building cyber readiness and resilience through the development and exercising of cyber security incident response plans and business continuity plans.
- Support Digital Restart Fund submissions for cyber security initiatives.

- Detect at-risk assets and vulnerabilities and lead remediation.
- Provide effective and timely intelligence and advice to relevant stakeholders.
- Conduct continuous scanning, penetration testing and dark web monitoring.

- Triage requests and provide coordination, assistance, advice and team augmentation for reported incidents.
- Lead the whole-of-government response to significant cyber security incidents and crises.

- Analyse reported cyber incidents to develop lessons learned and inform future strategies.
- Assist NSW Government entities in developing and implementing business continuity plans.
- Design and facilitate bespoke cyber incident response exercises.

Guiding principles

Risk culture

Customer-centric

Coordination

Enabling digital transformation

Values

Trust

Collaboration

Leadership

Innovation

Responsiveness

Our environment

Key figures from 2022 NSW Government Cyber Threat Report

1/2

of confirmed cyber security incidents reported by NSW Government entities involved social engineering tactics

1/3

of successfully prevented cyber attacks targeting NSW Government entities were attributed to multiple factors, including good cyber hygiene and security controls

1/2

of reported incidents were discovered by a source that was external to the entity

1/3

of confirmed incidents involved malware

Top challenges facing the NSW Government

Operational fatigue and resourcing issues are common across the industry, which is facing high demand for cyber security specialists.

Insufficient funds for cyber security initiatives, e.g. many entities cannot afford to implement the Essential Eight controls.

Globally, critical infrastructure is increasingly being targeted by threat actors engaged in cybercrime and state-sponsored espionage.

External attack surface challenges –including legacy systems, shadow IT, staff changes and a lack of documentation – increase risk for entities.

Our environment

Key targets

Critical infrastructure

- Utilities
- Transport
- Government

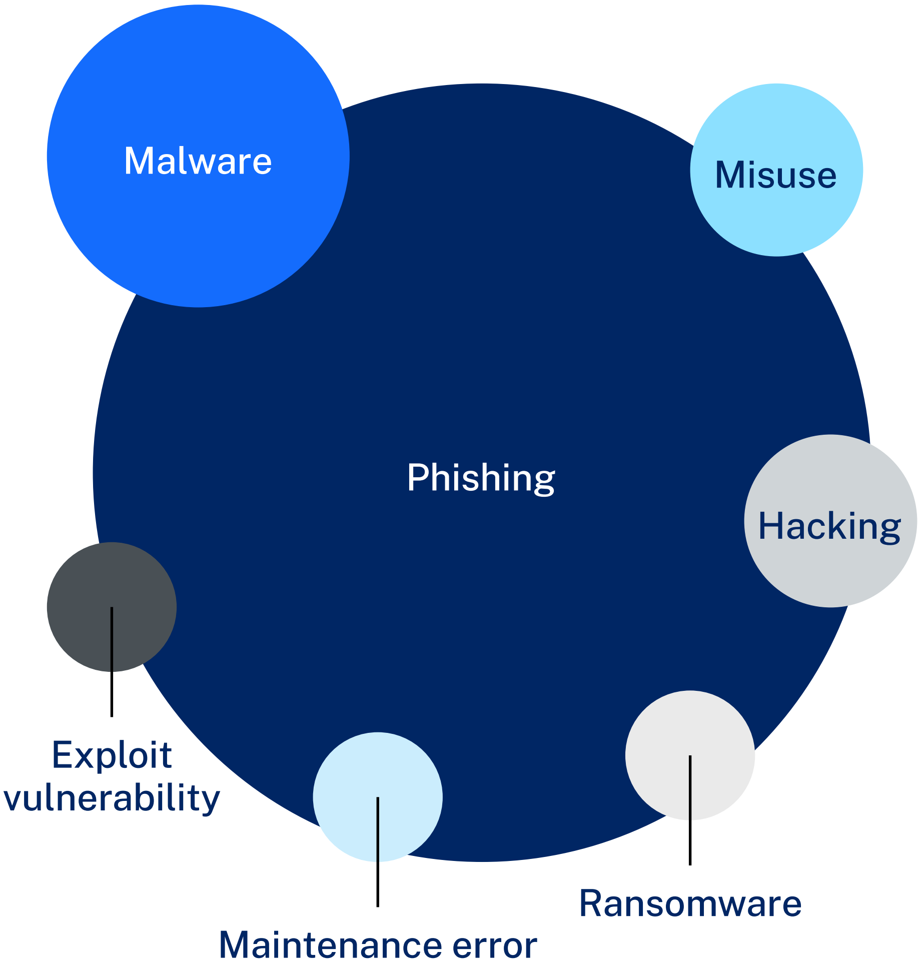
Human

- Identity theft
- Fraud
- Burnout
- Trust

Data

- Intellectual property
- Personal information
- Health information
- Sensitive government data
- Financial data

Common threat types and prevalence



Persistent initial vector methods

1/3 of incidents involved phishing techniques for initial access, which made it the top pathway to compromise in FY2021-2022.

In FY2021-2022, NSW accounted for 22% of the 76,000 cybercrime reports submitted to the Australian Cyber Security Centre (ACSC).

In FY2021-2022, the self-reported financial losses due to business email compromise incidents averaged $69,900 in NSW, according to the ACSC.

Key performance indicators

Key priorities

Measures

Culture

- Increases in completion of cyber security awareness training across the whole of NSW Government, including local councils.
- Awareness training completed (by type, method and agency/council).
- Live training awareness registrations vs attendance.
- Cyber awareness quiz results pre-training vs post training.
- Portion of staff completing cyber awareness training who are unsure how to report phishing incidents prior to training.
- Lowest and highest scoring quiz questions from quiz results.
- Live training feedback quiz results.
- E-module course ratings.
- Number of Community of Practice attendees.
- Community of Practice registration vs attendance over financial year.
- Number of events and presentations.
- Number of cyber security awareness materials produced.
- Active users/usage of external learning platform.
- Number of exercises provided by Cyber Security NSW.
- Number of recommendations provided by Cyber Security NSW in post-exercise reports vs adoption of the recommendations by recipient agency.
- Delivery of build-your-own exercise resource.

Intelligence sharing

- Cyber Security NSW represented at all National Cyber Security Committee meetings.
- Number of new requests and taskings to Cyber Security NSW's Intelligence & Response team.
- Number of intelligence disseminations.
- Number of threats and issues monitored.

Vulnerability management and incident response

- Proportion of incidents that are reported to Cyber Security NSW within 24 hours of discovery.
- Number of incidents under active management.
- Number of operational on-call contacts and engagements.
- Number of health checks completed.
- Number of ACSC Cyber Maturity Measurement Program engagements performed.
- Provide 2 reports from Cyber Security NSW's vulnerability risk management platform per year to all agencies and local councils that do not have access to the platform.
- Number of vulnerability scans.
- Number of penetration tests.
- Number of managed vulnerability monitoring agents.
- Completed weekly emails and alerts.
- Number of websites monitored.
- Number of supplementary reports.

Reporting

- Progression towards agency target maturities against the NSW Cyber Security Policy reporting for FY2022-2023, in comparison with the previous financial year.

Advisory

- Number of ICT Assurance Framework (IAF) reviews performed.
- Number of IAF Project Registrations performed.
- Number of views on policy-related published resources.
- Provide policy-related templates and resources within 2 business days upon request.
- Provide policy and local government guidance advice within 2 business days.
- Provide NSW Cyber Security Policy guidance within 1-7 business days.
- Provide whole-of-government cyber security policy advice within 7-30 days, dependent on complexity of request and resource availability.

Note: All items will be reported against quarterly except "Progressions towards agency target maturities" and "Delivery of build-your-own exercise resource", which will be reported against once during the financial year.

Alignment with NSW Government strategies and plans

Customer Service State Outcomes 2022-2023

The Department of Customer Service has the authority to plan, prioritise, fund and drive digital transformation and customer service across every department of the NSW Government.

Cyber Security NSW directly contributes to the department outcome of 'digital leadership and innovation in government services', because it requires strong cyber security posture to ensure that systems and services are connected, protected and trusted, including the ability to prevent and mitigate cyber security threats.

'Beyond Digital' Strategy 2019 (minor release May 2022)

The 2019 NSW Digital Government Strategy 'Beyond Digital' reframes the trend of digitising Government as a means to achieve greater productivity and customer experience. As part of the strategy, there is an acknowledgement that digital transformation must be underpinned by 'strong security and privacy foundations'. A key commitment of Beyond Digital was the development of the Cyber Security Strategy in 2020.

The last major update release occurred in November 2021 and the last minor update occurred in May 2022 – there were no direct changes regarding the cyber security strategy.

NSW State Infrastructure Strategy 2022-2042: Building Momentum

The State Infrastructure Strategy is a 20-year infrastructure investment plan for the NSW Government. Strong cyber security is essential in high risk and critical infrastructure. Cyber Security NSW builds whole-of-government cyber resilience by combining incident response, strong governance, transparent reporting mechanisms and intelligence sharing. Cyber Security NSW also engages with the broader cyber security community, across all levels of government and industry.

Compliance with the NSW Cyber Security Policy October 2021

The Compliance with the NSW Cyber Security Policy report assessed the 10 agencies' compliance with the NSW Cyber Security Policy in 2020.

The report found that the policy was not achieving the objectives of improved cyber security culture, governance and controls. The report highlighted the very low levels of maturity across the Essential Eight and strongly recommended Cyber Security NSW to work with agencies to improve cyber resilience as a matter of urgency.

Alignment with NSW Government strategies and plans

2021 NSW Cyber Security Strategy

This strategic plan built on the previous strategies to enable NSW to become a world leader in cyber security. To achieve this vision, the strategy details a number of principles and is underpinned by Cyber Security NSW's work in uplifting cyber resilience and maturity across the whole of NSW Government.

NSW Customer Strategy May 2021

The heart of the **NSW Customer Strategy** is for the NSW Government to become the most customer-centric government by 2030. It is essential to this strategy that the customers of NSW feel protected through the provision of services. In order to maintain these services, robust cyber security is crucial. Cyber security breaches and incidents can erode customer trust, which is vital to meeting this goal.

Cyber Security NSW is in a unique position to support whole-of-government cyber resilience and maturity uplift to protect customer data and maintain community trust.

NSW Government Cyber Security Incident Emergency Sub Plan December 2018

The NSW Government Cyber Security Incident Emergency Sub Plan is part of the State Emergency Management Plan, which is the whole-of-government plan for significant cyber security incidents or crises affecting NSW Government entities.

This plan aims to protect the NSW community from the consequences of a significant cyber security incident to reduce the impact to NSW Government services, assets and infrastructure, as well as coordinate the information flow between agencies, business continuity personnel, emergency management, cyber security industry and the public.

NSW Government Connectivity Strategy

The NSW Telco Authority has developed the **NSW Connectivity Strategy** to ensure customers, businesses and emergency services stay better connected through a coordinated and collaborative NSW Government approach to digital connectivity initiates.

This strategy aims to accelerate the access to digital services, align with global best practices and close the digital divide between metropolitan, rural and regional areas. Cyber security must underpin all digital services. NSW customers rely on connectivity to utilise digital government services, and therefore to maintain connectivity and customer trust, a strong cyber security strategy is essential.

Our budget

Cyber Security NSW was established in 2019 and allocated $60 million from the Digital Restart Fund in 2020 for 3 financial years of operation. In this time, the agency has grown rapidly to establish 8 specialist teams that bolster the NSW Government's capability to prepare, prevent, respond to and recover from cyber security incidents.

As the budget for FY2023-2024 would unlikely be settled by June 2023 (due to the timing of the state election), in January 2023 the Expenditure Review Committee approved operational funding of $27.6 million for Cyber Security NSW for FY2023-2024.

Department of Customer Service

2/24 Rawson Place
Haymarket NSW 2000

Office hours:
Monday to Friday
9am - 5pm

E: info@cyber.nsw.gov.au
W: digital.nsw.gov.au/policy/cyber-security

NSW GOVERNMENT