Department of Customer Service

Cyber Security NSW Service Catalogue

January 2024

NSW GOVERNMENT

Acknowledgement of Country

The NSW Department of Customer Service acknowledges the Traditional Custodians of the lands where we work and live. We celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of NSW.

We pay our respects to Elders past and present and acknowledge the Aboriginal and Torres Strait Islander people that contributed to the development of this document.

More information and disclaimer

Contact info@cyber.nsw.gov.au to request Cyber Security NSW services, products or more information. Please note that requests for the offerings outlined in this document are subject to the resource availability of Cyber Security NSW, and are prioritised on a needs basis.

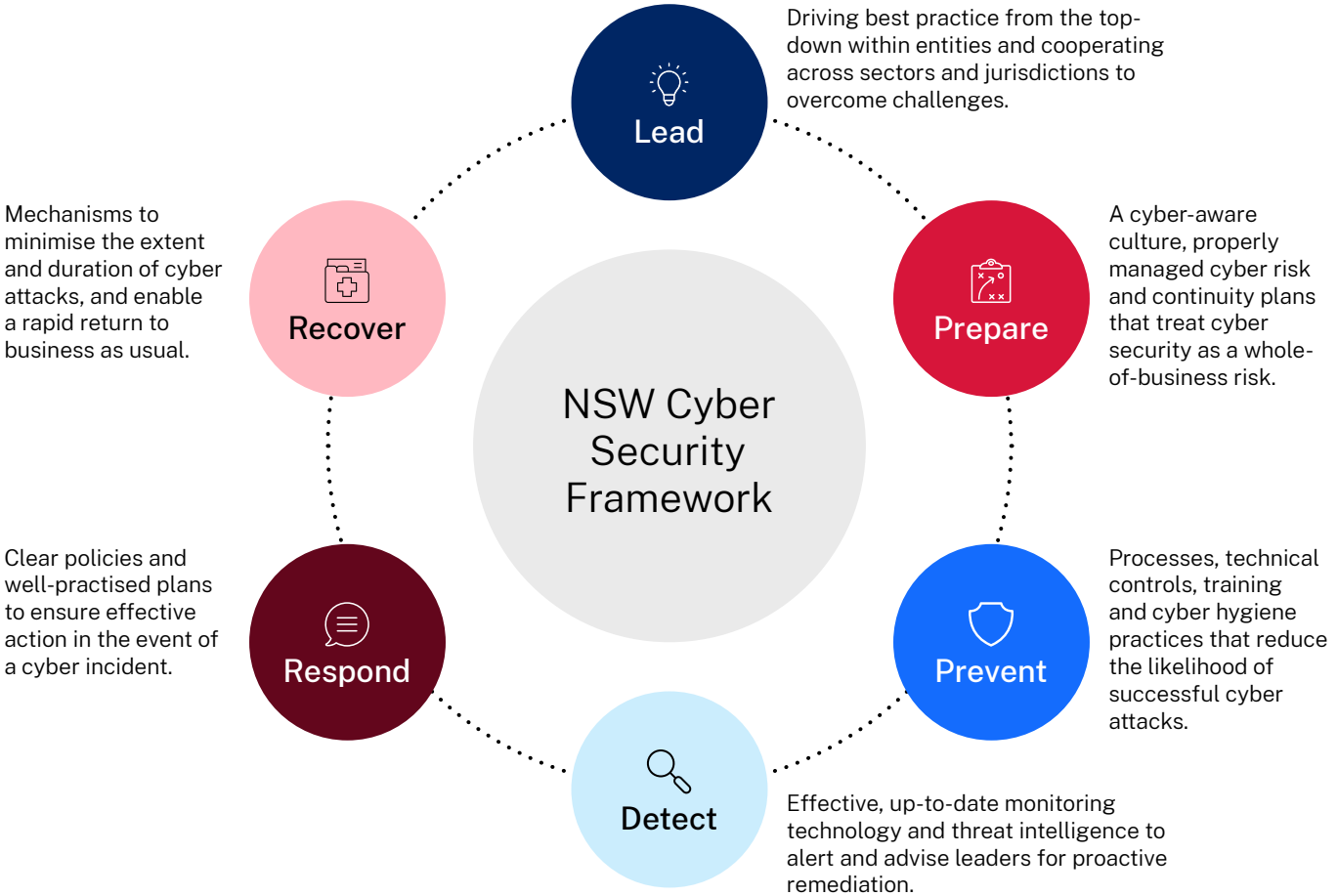
Contents

Overview

Cyber Security NSW provides an all-of-government function to achieve the vision of a cyber-secure NSW Government. Given the broad portfolio of its customers – that is, departments, agencies and local councils – Cyber Security NSW tailors the wide range of products, services and best practice guidance and advice it delivers. This integrated, risk-based approach encompasses technical, people and process-focused initiatives that enhance cyber resilience in line with the NSW Cyber Security Framework.

NSW Cyber Security Framework

Building from the US Government National Institute of Standards and Technology (NIST) Framework, the NSW Cyber Security Framework outlines the end-to-end journey of building cyber resilience. Cyber Security NSW's offerings align to the NSW Cyber Security Framework, working in conjunction to support all NSW Government entities in preparing for, preventing, detecting, responding to and recovering from cyber incidents.



Note: ID Support NSW, established in 2021, provides a nation-leading identity resilience service to NSW customers, which has proven critical in supporting response to, and recovery from, data breaches. Please visit nsw.gov.au/id-support-nsw for more information.

Key products and services

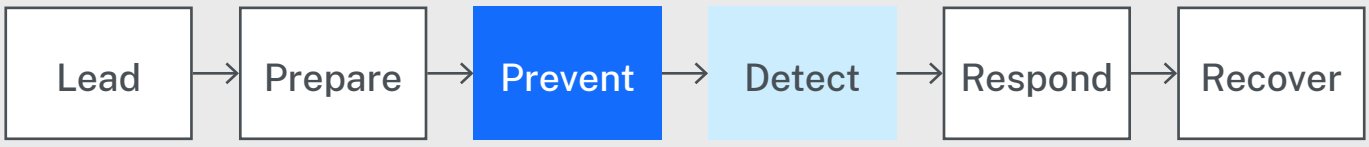
Security assessments	Identify cyber security strengths and areas requiring improvement, and understand how to bolster cyber security protections accordingly.
Awareness and training	Increase cyber security awareness and understanding among staff and contractors, and improve organisational resilience.
Advice and guidance	Obtain expert advice on risk, implementation of the NSW Cyber Security Policy and cyber security matters.
Threat intelligence	Receive proactive and targeted intelligence, as well as recommended mitigations, to enable early warning and action for likely threats in the NSW context.
Incident response	Be supported when cyber incidents occur. Cyber Security NSW can assist with incident response, coordination, initial investigation and digital forensics.

NSW Government entities can contact info@cyber.nsw.gov.au to request, or find out more about, the products and services detailed in this document.

Security assessments

Passive external scanning

Overview	Passive external scanning enables NSW Government entities to understand and remediate their cyber-attack surface.
Service type	Upon request.
Availability	Can be scheduled twice yearly. Typically fulfilled one week from request.
Process	1. Cyber Security NSW analyses the domains and IP addresses identified by the cyber risk platform. 2. Cyber Security NSW identifies vulnerabilities covering common vulnerabilities and exposures (CVEs), missing patches, open ports and misconfigurations. 3. Cyber Security NSW collates this information and recommended actions into a vulnerability report.
Outcome	A comprehensive passive vulnerability report focused on the NSW Government entity as defined within the cyber risk platform. This report provides a list of risks and recommended mitigations.
Benefit to entity	Entity is able to focus on the vulnerabilities most likely to be identified by a threat actor, enabling prioritisation of remediations and control implementation.



Intrusive external scanning

Overview

Unauthenticated automated tests on external-facing systems to identify vulnerabilities and potential misconfigurations. This scan does not test defensive systems and is therefore not as in depth as a penetration test.

Service type

Upon request.

Availability

Two to four weeks from request.

Process

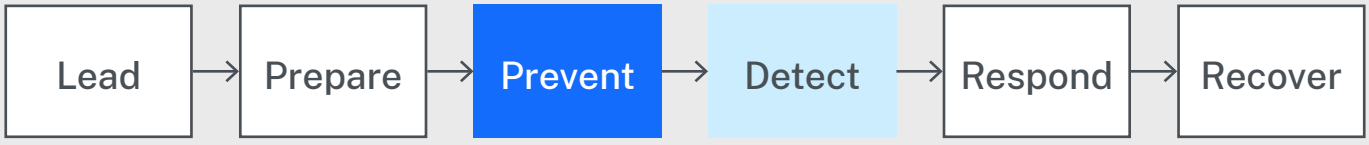
1. Entity provides domains and IP addresses to be assessed in the vulnerability report.
2. Cyber Security NSW conducts analysis to identify vulnerabilities, covering CVEs, missing patches, open ports and misconfigurations.
3. Cyber Security NSW uses this to produce external vulnerability report.

Outcome

A comprehensive external vulnerability report tailored to the requesting entity. This report provides a list of risks and recommended mitigations.

Benefit to entity

Entity is able to focus on the vulnerabilities most likely to be identified by a threat actor targeting a specific NSW Government entity, enabling prioritisation of remediations and control implementation.



Internal vulnerability scanning

Overview

Agent-based scanning on key internal systems to ascertain vulnerabilities and potential misconfigurations. This scan does not test defensive systems and is therefore not as in-depth as a penetration test.

Service type

Upon request.

Availability

Two to four weeks from request.

Process

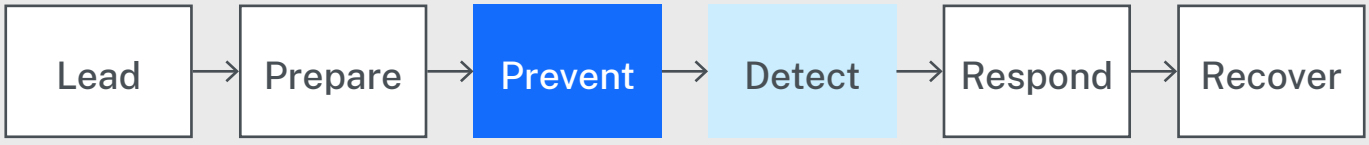
1. Cyber Security NSW installs a cloud-based vulnerability scanning tool with agents in the entity's environment.
2. Scanning tool gathers relevant information.
3. Cyber Security NSW conducts analysis to determine risks and mitigation strategies, and collates this into a vulnerability report.

Outcome

A comprehensive internal vulnerability report tailored to the requesting entity. This report provides a list of risks and recommended mitigation strategies.

Benefit to entity

Ability to focus on the vulnerabilities most likely to be identified by a threat actor who has gained access to the entity's internal infrastructure, enabling prioritisation of remediations and implementation of controls.



Penetration testing

Overview

The penetration testing service covers web applications, web services and network testing. This service only covers systems that are already in production.

Service type

Upon request.

Availability

Typically 10-12 weeks from request, noting there is limited availability for this service.

Process

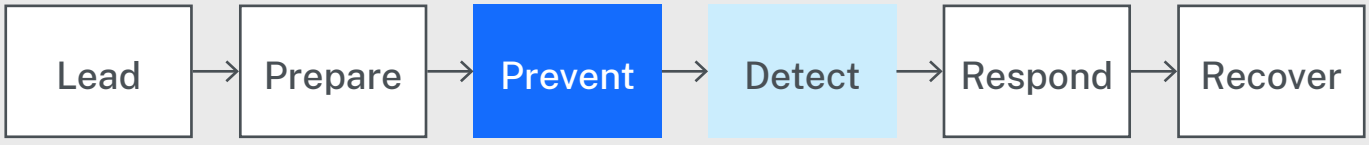
1. The entity proposes the scope of the testing, with this verified by Cyber Security NSW before testing commences.
2. Cyber Security NSW develops a schedule and statement of work. This is provided to the requesting entity for signing prior to the commencement of testing.
3. The entity and Cyber Security NSW undertake preparation work, including: user account and IP address whitelisting; creating backups; and establishing available contacts.
4. Cyber Security NSW notifies the entity that testing will commence.
5. Cyber Security NSW provides any critical and high severity findings to the entity immediately.
6. Cyber Security NSW creates a detailed report for the entity.

Outcome

A detailed matrix of findings for technical team members, along with a comprehensive report of the systems within scope using multiple techniques, including those used by threat actors. A meeting can be arranged to discuss findings and demonstrate the consequences of the risks identified. One retest is included within three months to verify that remediations have been properly implemented.

Benefit to entity

The entity is provided with a broad view of their cyber security risk footprint for the systems within scope.



Health Check

Overview

The Health Check is focused on the mandatory controls identified in the Australian Cyber Security Centre (ACSC) Essential Eight baseline mitigation strategies for cyber incidents. The Health Check reviews people, processes and technology through a technical lens to assess the maturity level against the ACSC Essential Eight.

Service type

Upon request.

Availability

Six to eight weeks from request, noting there is limited availability for this service.

Process

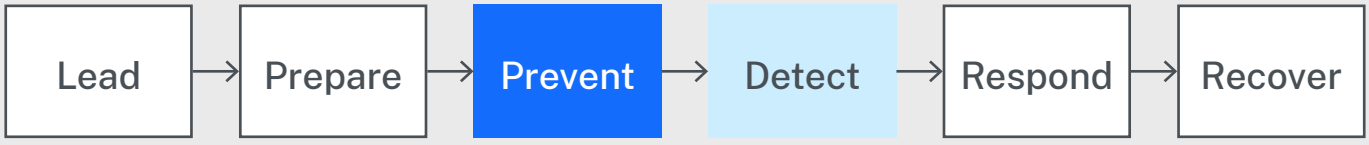
1. The entity provides relevant documentation for the Health Check, as directed by Cyber Security NSW.
2. Cyber Security NSW conducts interviews with select staff.
3. Cyber Security NSW conducts technical assessments.
4. Cyber Security NSW uses this information to produce a cyber security maturity report for the entity.

Outcome

The entity receives a point-in-time cyber security maturity assessment report that includes actionable plans to improve cyber security maturity. Where appropriate, Cyber Security NSW may provide assistance to action those plans.

Benefit to entity

The entity has a comprehensive view of its cyber security risk footprint for the assessed areas, which it can use to inform its approach to reducing cyber risk and increasing resilience.



Password Hygiene Tool

Overview

The Password Hygiene Tool scans Windows Active Directory (AD) accounts for issues such as: compromised passwords; duplicate passwords; passwords with no expiry; and accounts with no set password. This service provides a technical solution to alert entities of security concerns that were previously unable to be monitored.

Service type

Upon request.

Availability

Four to six weeks from request.

Process

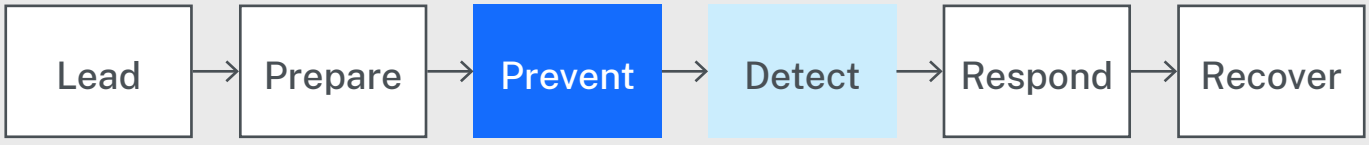
1. Cyber Security NSW runs the Password Hygiene Tool for the entity.
2. The Password Hygiene Tool compares each user's credentials in the AD environment to a list of hashes sourced from the "Have I Been Pwned" (HIPB) database of compromised passwords.
3. Cyber Security NSW provides a report of the results to the entity.

Outcome

A visual report of multiple metrics, plus comprehensive user account data categorised into areas of risk.

Benefit to entity

A comprehensive view of the state of the requesting entity's password landscape, and insights into their account management practices.



Key website monitoring

Overview

Monitoring of all NSW Government externally accessible websites at the top layer (*.nsw.gov.au) using a bespoke tool developed by Cyber Security NSW. Further domains can be monitored if required.

Service type

Ongoing.

Availability

Notifications within business hours. Additional domains can be added by request.

Process

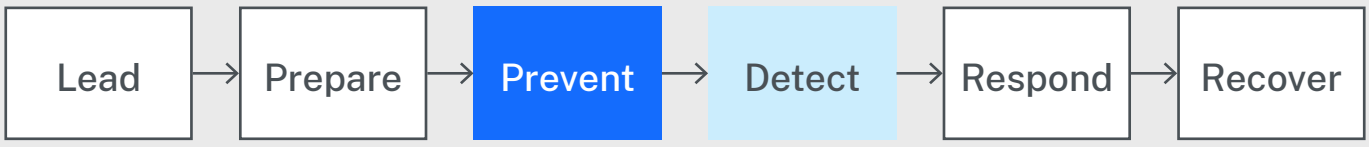
1. Cyber Security NSW verifies additional domains for ownership.
2. If the tool detects a change against the known good snapshot of the website, a Cyber Security NSW analyst reviews the site to check for malicious changes.
3. If a negative change is detected, Cyber Security NSW notifies the entity of the issue.

Outcome

Entities are notified of maliciously compromised sites.

Benefit to entity

The ability to quickly remediate impacted websites, limiting: risks to the reputation of the entity and the NSW Government; and potential impacts to NSW communities.



Open-source intelligence (OSINT)

Overview

An overview of information about the requesting entity that is exposed to the public and may be used by adversaries in order to target the entity and/or staff.

Service type

Upon request.

Availability

Within two weeks from request.

Process

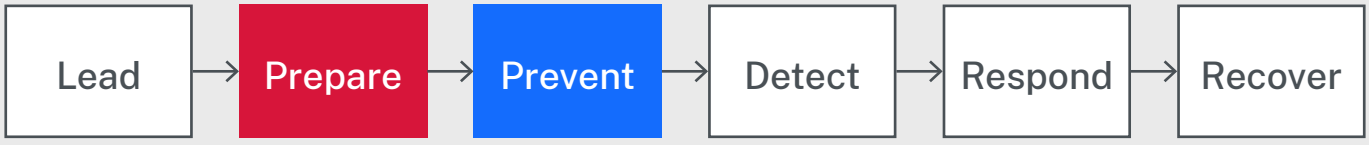
1. The entity and Cyber Security NSW define the scope of the investigation.
2. Cyber Security NSW uses a suite of open-source tools, information sources and strategies to uncover information relevant to the scope.
3. Cyber Security NSW identifies sensitive and personal information, and analyses the associated risks.
4. This is collated into a report for the entity.

Outcome

A report outlining relevant information present in the public domain, with recommendations on potential mitigation strategies.

Benefit to entity

The entity gains an understanding of the risk presented by the information that is on the public domain. This allows the entity to plan mitigation activities based on those risks.



Vulnerability risk management platform

Overview

Access to a vulnerability monitoring service that includes third-party vendor monitoring. This helps prevent and mitigate cyber security risks by monitoring the entity's, and their vendors', domains in a simple, easy-to-understand system. The platform can provide cyber security ratings and automatically detect leaked credentials and data exposures.

Service type

Upon request.

Availability

One week from request, pending licence availability.

Process

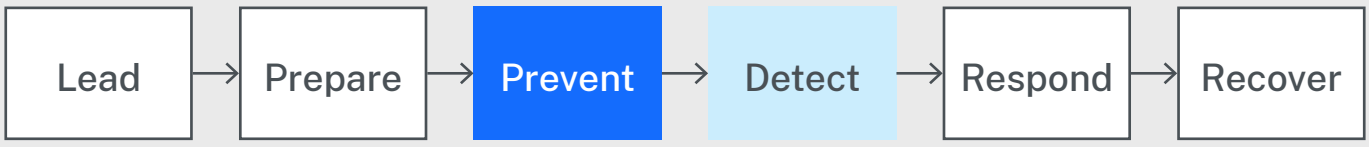
1. Entity submits request.
2. Cyber Security NSW assesses request to determine whether there are available licences. If there are, Cyber Security NSW will proceed with onboarding the entity to the platform.
3. Cyber Security NSW conducts training in partnership with the vendor.

Outcome

An improved view of the entity's attack surface, which gives the entity access to useful information for planning cyber risk mitigation activities.

Benefit to entity

Reduced cyber risk profile and improved resilience against attacks.



Vendor security risk

Overview

Assessment on current or potential third parties in relation to risks centred around their websites, network, email, phishing and malware, brand and reputation.

Service type

Upon request.

Availability

One week from request. Only available to entities that have not been onboarded to the vulnerability risk management tool.

Process

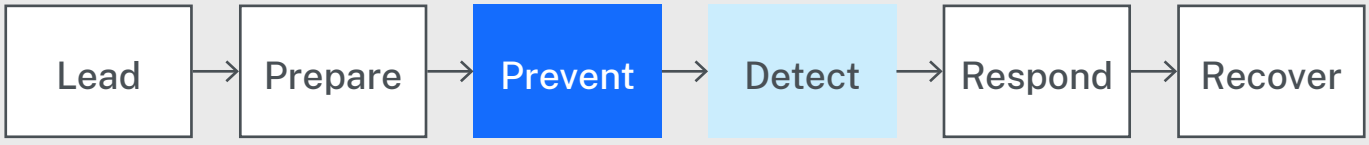
1. Vendor is added to the vulnerability risk management tool. The tool takes at least 24 hours to collect required data.
2. The tool analyses data and collates a report.
3. Cyber Security NSW provides the entity with relevant cyber risks and suggested mitigations.

Outcome

A comprehensive risk assessment of a specific third-party vendor.

Benefit to entity

An improved understanding of third-party cyber risk, which allows the entity to make informed decisions when selecting and managing vendors.



ACSC vulnerability data

Overview

Information on vulnerabilities from the ACSC and the scope and likelihood of remediation. These notifications include, but are not limited to, quarterly Cyber Hygiene Improvement Programs (CHIPs) and ad-hoc High-Priority Operational Tasking CHIPs (HOTCHIPs).

Service type

Ongoing.

Availability

Two business days from provision by the ACSC.

Process

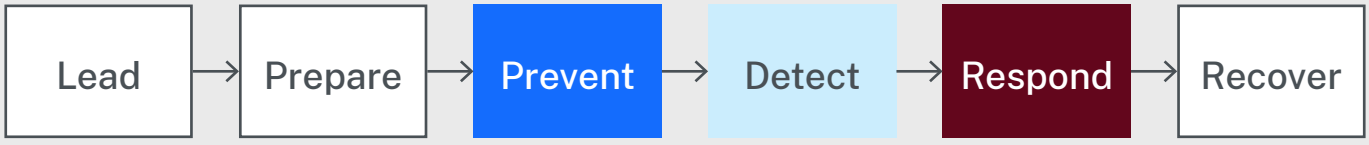
1. Cyber Security NSW analyses and assesses data received from the ACSC to determine if further action is required.
2. Cyber Security NSW communicates with NSW Government entities as required.
3. Cyber Security NSW follows up with impacted entities for one month on impacted systems, patching progress and so forth.

Outcome

Entities are notified of potential vulnerabilities, the scope and likelihood of potential issues and mitigations.

Benefit to entity

Entities have the opportunity to reduce cyber risk and improve resilience to a cyber attack.



Awareness and training

Live cyber security awareness training

Overview

Cyber Security NSW's Essentials cyber security awareness training is available to all NSW Government staff and contractors. The training is delivered via live, interactive, online sessions and is tailored, with: Essentials Standard for all users; Essentials Plus for a privileged user audience; Essentials Premium for executive staff; and Essentials for Councillors for local government councillors and senior officers.

Service type

Ongoing.

Availability

Entities are notified of the training schedule quarterly. Each quarter, Cyber Security NSW holds: four Essentials Standard sessions; two Essentials Plus sessions; four Essentials Premium sessions; and one Essentials for Councillors session (or more as required).

Process

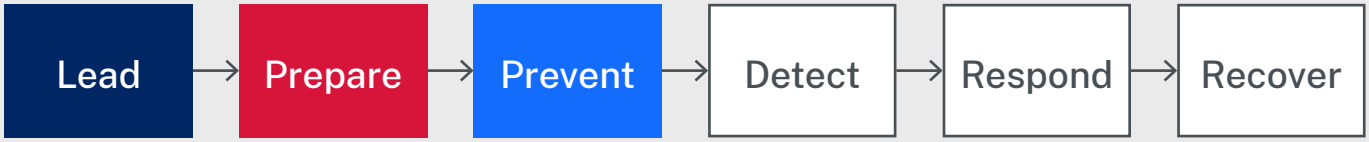
1. Entity training coordinator contacts Cyber Security NSW to register staff for an Essentials live training session.
2. Cyber Security NSW works with training coordinator to determine registration and reporting requirements.
3. Training coordinators are provided with registration links (including pre-training information and quiz) for distribution to participating staff and contractors.
4. Entity participants attend the live training session they registered for. This includes participation in interactive cyber security awareness polls and quizzes.
5. Cyber Security NSW provides attendees with a post-session pack, which includes cyber hygiene checklists, tips to detect phishing, information on reporting threats and incidents, and further resources.

Outcome

Staff and contractors receive baseline cyber security awareness training, in line with materials developed by Cyber Security NSW. Training coordinators receive quarterly reporting on live training attendance, including attendance records, insights from polls, and comparisons of pre-and post-training quiz results.

Benefit to entity

Staff and contractors develop increased cyber security awareness and entities receive training insights.



Cyber security learning e-modules

Overview

These tailorable e-modules can be input into entities' learning management systems (LMSs) to deliver on-demand cyber security awareness training. E-modules are available in: Essentials Standard for all users; Essentials Plus for a privileged user audience; Essentials Premium for executive staff; and an Essentials refresher for those who have previously completed training.

Service type

Upon request.

Availability

Two to four weeks from request.

Process

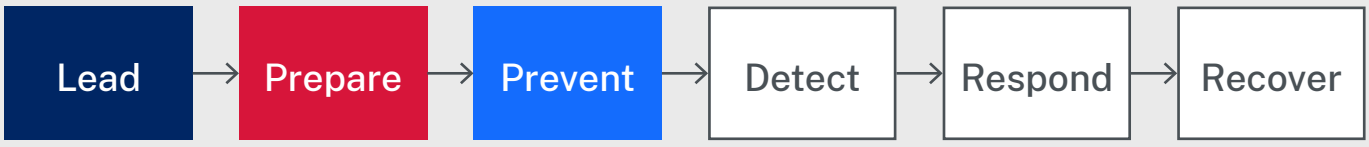
1. Entity training coordinator contacts Cyber Security NSW to request the e-module information pack.
2. Cyber Security NSW works with the entity to determine the scope of changes and reporting outcomes based on the entity's systems and needs.
3. Cyber Security NSW develops tailored e-modules and provides them to the entity as SCORM files to be uploaded to the entity's LMS.
4. Cyber Security NSW notifies entity of updates to course content periodically. The entity provides feedback on the content and design as needed.
5. Entity provides Cyber Security NSW with quarterly reports on: staff headcount; assigned staff numbers when mandatory training has been assigned; and attempt and completion statistics.

Outcome

Staff and contractors have access to on-demand cyber security awareness training. E-modules can be assigned as mandatory training to help entities meet NSW Cyber Security Policy obligations and increase cyber security maturity.

Benefit to entity

Increased access to cyber security awareness training that has been tailored to entity needs.



Awareness materials

Overview

Cyber Security NSW offers a suite of awareness materials that can be adapted by, or co-branded with, the requesting entity.

Service type

Upon request.

Availability

Within three business days from request for standard materials.

Process

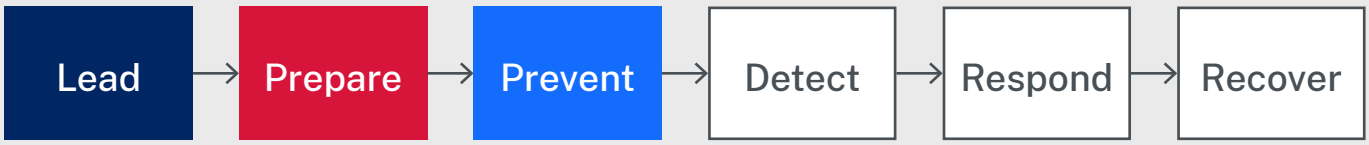
1. Entity accesses and uses Cyber Security NSW's suite of cyber security awareness materials that are available online.
2. The entity can request these materials in an editable format, so that the entity can adapt or co-brand them.

Outcome

Entity can use awareness materials developed by Cyber Security NSW to amplify consistent cyber security messaging to staff, with this messaging able to be tailored as needed.

Benefit to entity

Increased cyber security awareness among staff.



Awareness campaigns

Overview

Communications guidance and accompanying toolkits to assist in streamlining internal communications and ensure consistency in awareness messaging across government.

Service type

Ongoing.

Availability

Quarterly with additional resources released as needed to support featured awareness events or new resources.

Process

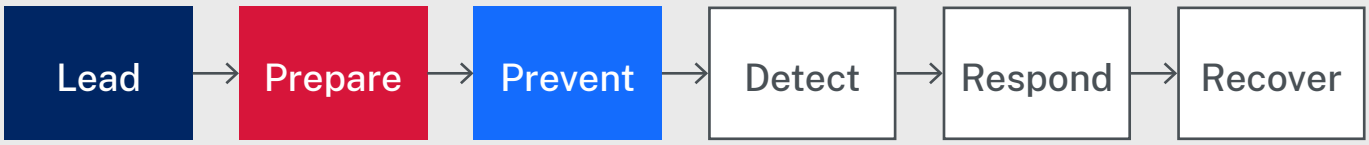
1. Cyber Security NSW coordinates with government and non-government partners to coordinate and amplify relevant cyber security awareness campaigns.
2. Tailored communications and materials are packaged and distributed to entities to standardise internal communications.

Outcome

Entity is provided with communications, materials and digital assets to assist in the amplification of cyber security awareness campaigns.

Benefit to entity

Streamlined internal communications and consistent messaging to support cyber security awareness campaigns created by the NSW Government and its partners, with minimised effort by the entity.



Community of Practice and other cyber security forums

Overview

Cyber Security NSW hosts a range of forums that support information sharing across entities:

- Cyber Security Community of Practice brings together cyber professionals, leaders and those interested in cyber security from across the NSW Government to provide regular updates and foster knowledge sharing
- Cyber Security Councils Forum is specific to local councils and creates a community to exchange information relating to issues, trends and threats encountered in the local government sector
- Cyber Security Awareness Working Group provides a forum for cyber security awareness teams working across the NSW Government.

Service type

Ongoing.

Availability

Membership is required. Forum meetings are held quarterly though groups have access to a dedicated Microsoft Teams channel for ongoing information sharing.

Process

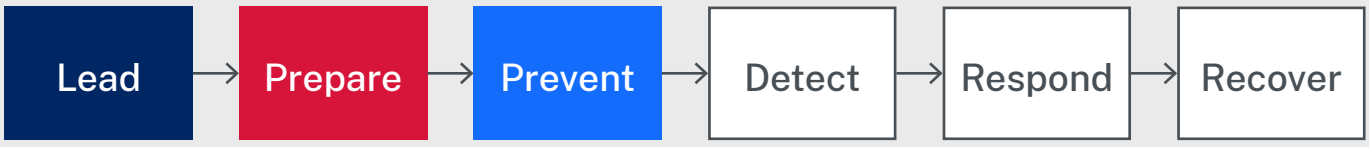
1. NSW Government staff contacts Cyber Security NSW to request membership to a particular forum.
2. NSW Government staff attend quarterly forum meetings and participate in ongoing discussions.

Outcome

NSW Government staff have access to member-only materials and discussions.

Benefit to entity

Access to a community of practitioners sharing regular cyber security updates and relevant materials.



Exercise-as-a-Service (EaaS) offering

Overview

Cyber Security NSW designs and facilitates bespoke discussion-based cyber incident response exercises to assist NSW Government entities in testing and refining their incident response plans and procedures.

Service type

Upon request.

Availability

Five to seven weeks from request.

Process

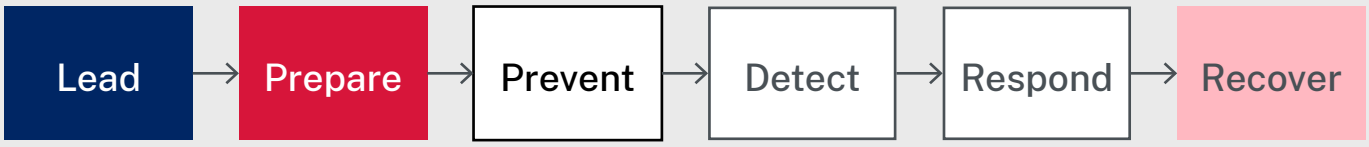
1. Entity contacts Cyber Security NSW to request exercise. Cyber Security NSW provides initial information pack.
2. Cyber Security NSW evaluates the request and meets with the entity for an initial discussion. Following the meeting, Cyber Security NSW requests required documentation for review.
3. Cyber Security NSW develops a concept document and scenario narrative in collaboration with the entity.
4. Once endorsed, Cyber Security NSW prepares all exercise materials.
5. Cyber Security NSW facilitates and observes the cyber incident response exercise for the entity.
6. Following the exercise, Cyber Security NSW provides an After-Action Report to the entity that outlines key observations, insights and recommendations related to the exercise objectives.
7. Cyber Security NSW follows up with the entity regarding actions from the report.

Outcome

Entity tests their cyber incident response plans and procedures, per the Mandatory Requirement under the NSW Cyber Security Policy.

Benefit to entity

Entity receives insights into their cyber incident response plans, helping inform future changes to improve cyber resilience.



Build-an-Exercise offering

Overview

Cyber Security NSW provides resources to empower NSW Government entities to independently conduct cyber incident response exercises, guiding a small group of key cyber incident response staff through a series of structured injects and questions related to a specific area of cyber security.

Service type

Upon request.

Availability

One to seven business days from request.

Process

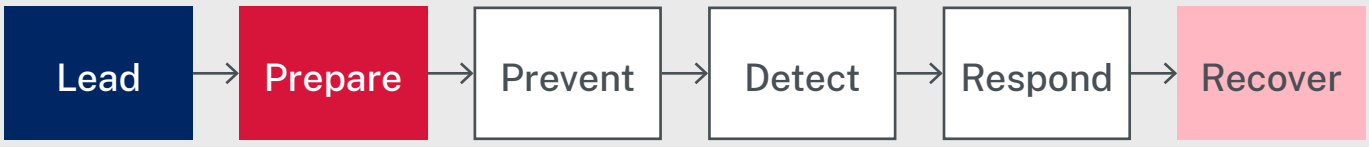
1. Entity contacts Cyber Security NSW to request information pack and expression of interest form.
2. Entity completes and returns expression of interest form.
3. Cyber Security NSW evaluates the request and provides the entity with relevant resource packs that include cyber incident response exercise scenarios, guidelines and reporting templates.
4. Entity organises and conducts their own cyber incident response exercise.
5. Following the exercise, the entity completes an After-Action Report that outlines key observations, insights and recommendations related to exercise objectives.

Outcome

Entity tests their cyber incident response plans and procedures, validates capabilities, and identifies aspects of their cyber arrangements and processes that could be improved.

Benefit to entity

Entity has the opportunity to practise their cyber incident response plans, meeting a Mandatory Requirement of the NSW Cyber Security Policy. In addition, the entity has a better understanding of the cyber risks the organisation is exposed to and what changes should be made to improve cyber resilience.



Access to external learning platform

Overview

Cyber Security NSW administers access to an external learning platform for users across the NSW Government. The platform offers over 600 accredited short courses and pathways to microcredentials.

Service type

Upon request.

Availability

Limited by the number of available licences. Additional users will be placed onto a waiting list and assigned a licence once it becomes available.

Process

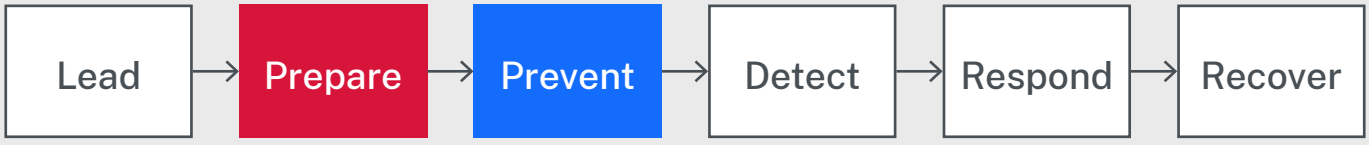
1. NSW Government staff member contacts Cyber Security NSW to request access to the platform.
2. NSW Government staff member completes courses of their choosing. Exam costs and certifications are not funded by Cyber Security NSW, but can be undertaken by learners or sponsored by their entity.
3. Cyber Security NSW provides ongoing support to learners, including communications on course availability, annual training competitions, and goal setting and course recommendations.

Outcome

Access to recognised training providers and specialist vendors to increase the cyber security knowledge and skills of NSW Government staff.

Benefit to entity

Training to advance the cyber security skills of the entity's workforce, at no cost to the entity.



Advice and guidance

Templates and resources

Overview

Cyber Security NSW has developed templates and resources to help entities create incident response plans, access control policies, information security policies, acceptable use policies and other plans and policies. Support resources include the Uplift Toolkit and Risk Toolkit.

Service type

Upon request.

Availability

Within two business days from request.

Process

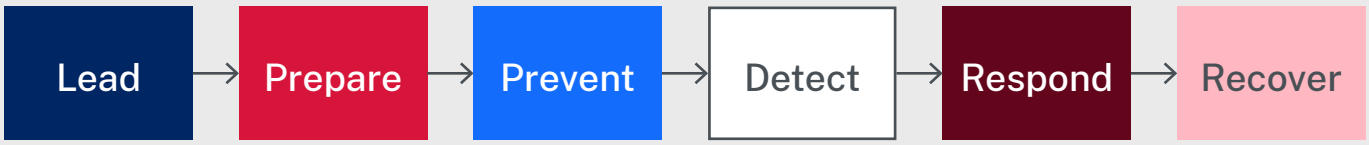
1. Entities can access a number of these templates and resources via relevant forum Teams channels, such as the Cyber Security CoP channel.
2. Alternatively, the entity can contact info@cyber.nsw.gov.au to request templates and resources.

Outcome

Entities have resources and templates that can help them create their own tailored cyber security documents.

Benefit to entity

These resources remove or reduce the need for entities to outsource the creation of documents, processes and guidance, generating cost savings for entities, while also building internal skills and competencies.



Policy advice

Overview

Cyber Security NSW provides cyber security policy advice, addresses general policy queries and directs entities to the appropriate stakeholders if required.

Service type

Upon request.

Availability

Within two business days from request.

Process

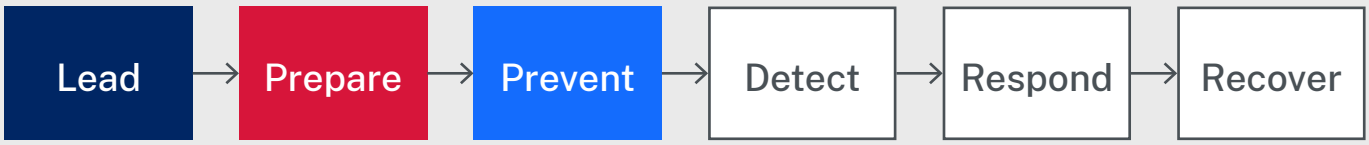
1. Entity requests advice from Cyber Security NSW.
2. Cyber Security NSW determines the scope of the request, clarifying with the entity if required.
3. Cyber Security NSW consults with the wider branch, or outside the agency as required, to develop a response. This response is reviewed by senior team members.
4. The response is provided to the entity.

Outcome

Entity receives timely and approved advice on their cyber security policy query.

Benefit to entity

This service saves the entity time and resources, and ensures their alignment with NSW Government best practice.



NSW Cyber Security Policy guidance

Overview

Cyber Security NSW is responsible for maintaining the NSW Cyber Security Policy. Entities can receive advice on implementation of the policy, including resources and templates to assist with its implementation, and extensive guidance documents on its mandatory requirements.

Service type

Upon request.

Availability

One to seven business days from request.

Process

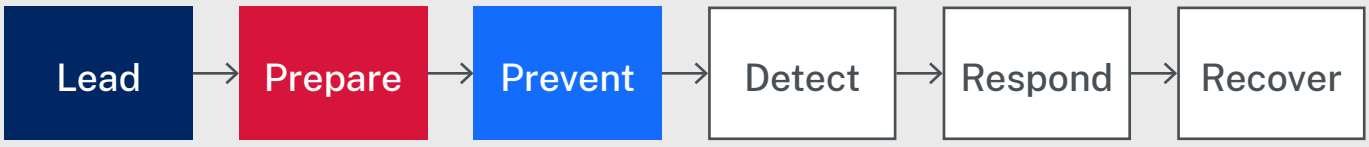
1. Entity requests advice from Cyber Security NSW.
2. Cyber Security NSW determines the scope of the request.
3. Cyber Security NSW develops a response.
4. This guidance is provided to the entity.

Outcome

The entity receives clear advice on implementation of the NSW Cyber Security Policy.

Benefit to entity

The entity has a better understanding of how to implement the NSW Cyber Security Policy, supporting cyber security maturity uplift and reducing reliance on, and the cost of, services provided by consultants and managed services. As the NSW Cyber Security Policy is updated annually, this guidance helps ensure the entity understands any updated Mandatory Requirements.



Local government guidelines

Overview

The Cyber Security Guidelines – Local Government allow local councils to assess their cyber security maturity and plan their uplift. The guidelines outline cyber security standards and controls recommended by Cyber Security NSW for NSW local government entities.

Service type

Ongoing.

Availability

Available online.

Process

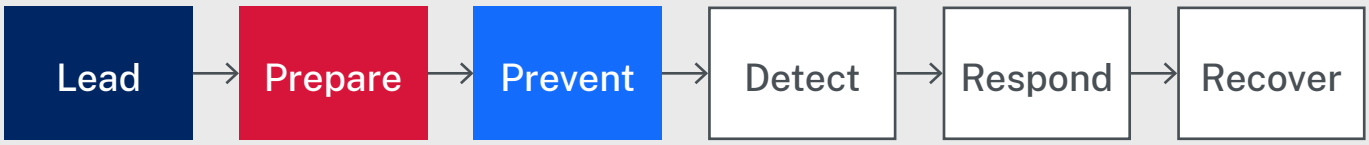
Entities can access the Cyber Security Guidelines – Local Government online: https://www.olg.nsw.gov.au/wp-content/uploads/2022/12/2022-Cyber-Security-Guideline-Local-Government.pdf

Outcome

The local council has guidance to self-assess and uplift their cyber security maturity.

Benefit to entity

Following these guidelines helps reduce the likelihood, impact and cost of cyber attacks. In addition, they generate savings, as local councils do not have to outsource this work.



Cyber security maturity uplift assistance

Overview

Cyber Security NSW provides feedback on NSW Cyber Security Policy maturity reports and advice on how to meet uplift requirements.

Service type

Upon request.

Availability

One to seven business days from request.

Process

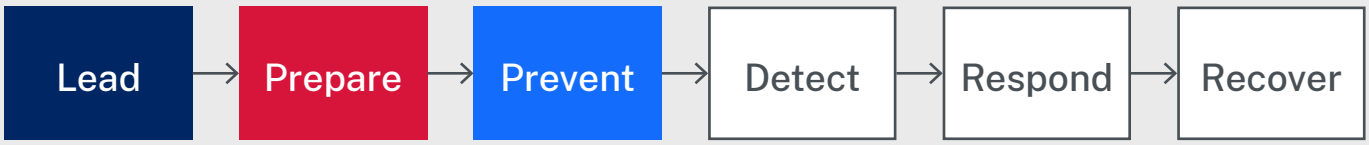
1. Entity requests advice from Cyber Security NSW.
2. Cyber Security NSW determines the scope of assistance required, and consults the entity as needed.
3. Cyber Security NSW completes necessary assessments and holds further discussions with the entity as required.
4. Cyber Security NSW provides collated feedback to the entity.

Outcome

Entity receives clear, timely and approved advice on how to best target resources for cyber security maturity uplift activities.

Benefit to entity

Cyber Security NSW's advice helps entities comply with the NSW Cyber Security Policy and improve their cyber security maturity. This leads to quantifiably enhanced cyber security maturity that reduces the likelihood, impact and cost of cyber attacks. In addition, having advice on how to best target cyber security initiatives can generate cost savings for the entity.



All-of-government cyber security advice

Overview

Cyber Security NSW can provide advice on all-of-government submissions, papers for consultation and other major cyber security decisions, as required by senior executives.

Service type

Upon request.

Availability

One to six weeks from request.

Process

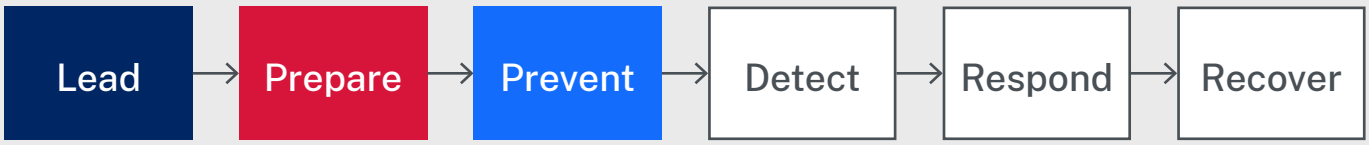
1. Senior executive from NSW Government requests advice from Cyber Security NSW.
2. Cyber Security NSW may consult with requesting entity before developing a response.
3. Cyber Security NSW develops advice, consulting with internal and external parties as required.
4. Cyber Security NSW provides the consolidated response to the entity.

Outcome

Requestor receives clear advice on improving the NSW Government's cyber resilience.

Benefit to entity

Cyber Security NSW's all-of-government advice is strategic and shapes NSW policies in ways that align with the NSW Cyber Security Policy and other strategic goals. All-of-government advice provides situational awareness to identify current and future opportunities to strengthen the cyber security maturity of the NSW Government.



Digital Restart Fund (DRF) advice

Overview

The DRF is administered by the Department of Customer Service and is designed to support digital and information and communication technology initiatives. Cyber Security NSW provides high-level strategic advice to entities submitting a DRF business case under $5 million.

Service type

Upon request.

Availability

One to five business days from request.

Process

1. Entity submits business case to Cyber Security NSW. Entities may also reach out to Cyber Security NSW for business case advice prior to draft submissions.
2. Cyber Security NSW conducts a strategic review of strategic cyber security concerns.
3. Cyber Security NSW provides entity with final recommendation report.

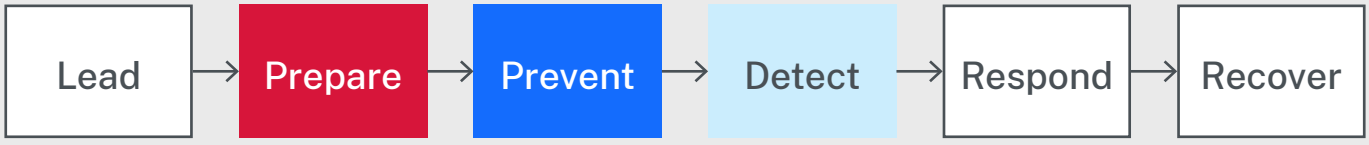
Outcome

The entity receives a final recommendation report that addresses the following areas of concern, as relevant:

- scope – e.g. whether: funding exceeds $5 million; items are out of scope for cyber uplift; ongoing and existing business-as-usual costs have been included or funding requests outside of the funding window overlap with current Cyber Security NSW initiatives.
- feasibility – e.g. overly ambitious scope for planned time and budget, no consideration for handover activities, no consideration for ongoing funding after uplift or high-rated residual risks that might jeopardise success of the project.
- general clarification – e.g. the DRF template or additional Appendix E is incomplete or not provided.
- other additional information that should be provided.

Benefit to entity

The entity receives clear and tailored advice that addresses the scope and feasibility of the DRF application, and outlines any missing or incomplete information. This allows the entity to make required amendments to their DRF submission.



DMARC support

Overview

Ongoing support to agencies and local councils that have implemented domain-based messaging authentication, reporting and conformance (DMARC) controls on their domains. This may include implementation and configuration guidance or support in diagnosing issues and incidents.

Service type

Ongoing.

Availability

Within two business days from request.

Process

For incidents:

1. Entity submits incident support request to Cyber Security NSW.
2. Cyber Security NSW triages request, prioritising and investigating verified DMARC incidents that impact email delivery.
3. Cyber Security NSW uses the DMARC reporting platform and external tools to diagnose DMARC issues. Where required, Cyber Security NSW engages the external DMARC vendor to escalate issues and provide expert guidance.

For general support:

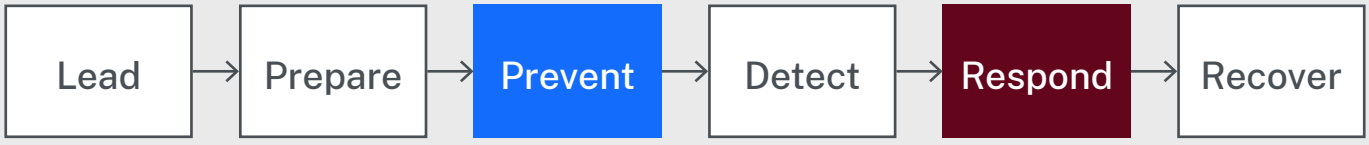
1. Entity submits general support request to Cyber Security NSW.
2. Cyber Security NSW provides entity with DMARC reporting platform onboarding, training and other support, as required.

Outcome

Entities can obtain advisory support for implementation, maintenance and analysis of issues and incidents.

Benefit to entity

Minimised email sending outages related to DMARC issues, and decreased risk of email spoofing and phishing attacks using a NSW Government domain.



Assurance for cyber security funding submissions

Overview

Cyber Security NSW provides assurance advice on funding submissions referred by NSW Treasury, assessing their alignment to NSW Government priorities and policies, as well as other cyber security frameworks.

Service type

Upon request.

Availability

Two to eight weeks from request by NSW Treasury.

Process

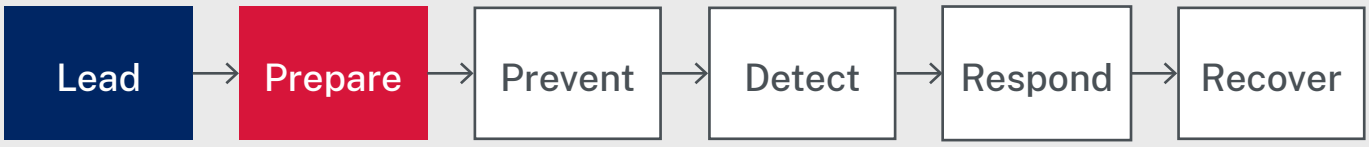
1. NSW Treasury requests Cyber Security NSW to provide assurance advice on a NSW Government entity's cyber security funding request.
2. Where appropriate, Cyber Security NSW may hold a planning meeting with the entity to find out more about the funding submission.
3. Cyber Security NSW reviews the funding request, assessing how the submission aligns to NSW Government: priorities; ICT and digital strategy and policy; and cyber security strategy and policy. In its assessment, Cyber Security NSW also considers: the criticality of the service need/problem; how the project reduces organisational risk; and alignment to additional frameworks, such as zero-trust principles, ISO 270001 and so forth.
4. Cyber Security NSW completes its assessment and provides it to NSW Treasury.

Outcome

NSW Treasury receives an assurance assessment on cyber security budget bids submitted by NSW Government departments, agencies and local councils.

Benefit to entity

NSW Treasury has advice to help prioritise cyber security funding across the NSW Government.



Best practice cyber security advice

Overview

Best practice information on various cyber security matters that are of strategic importance to the NSW Government.

Service type

Upon request.

Availability

Two to eight weeks from request.

Process

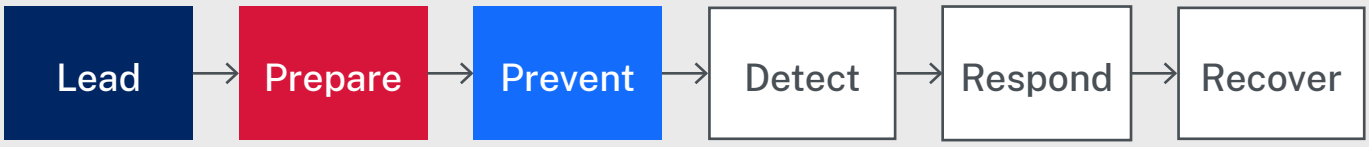
1. Entity requests support from Cyber Security NSW.
2. Cyber Security NSW assesses whether request is strategically beneficial, and then defines the scope of the investigation.
3. Cyber Security NSW gathers information on the subject and analyses it for relevancy.
4. Cyber Security NSW develops advice in line with the objectives of the requesting entity.
5. Cyber Security NSW provides advice directly to the entity.

Outcome

Entity receives guidance on systems, services or other aspects of best practice to guide the entity in minimising cyber risk.

Benefit to entity

Improved configuration and use of systems, services and so forth with recognised cyber risk.



Strategic cyber security contract advice

Overview

Provide support for contract development and negotiation, where there is a strategic importance to the NSW Government, to ensure cyber security is appropriately addressed.

Service type

Upon request.

Availability

Two to eight weeks from request.

Process

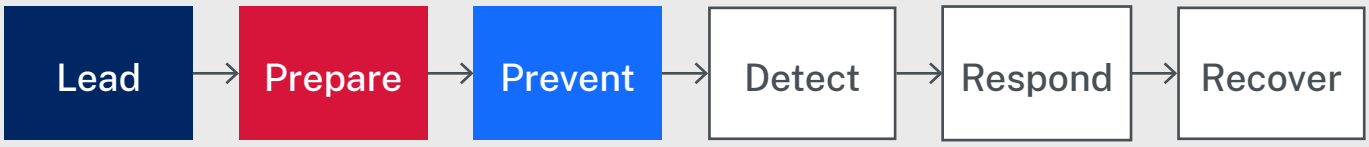
1. Entity requests support from Cyber Security NSW. Cyber Security NSW assesses whether there is a strategic need for this service.
2. Cyber Security NSW gains an understanding of the intended contract outcome and the data involved in the contract or service.
3. Cyber Security NSW identifies areas where cyber security should be addressed and suggests language adjustments or new inclusions. The intent of any cyber clauses and the impact on cyber risk and resilience for the subject of the contract is communicated.
4. Entity undertakes negotiations to obtain the highest possible cyber security protection for the individual circumstances.

Outcome

Cyber security is treated appropriately in the entity's contract with a service provider.

Benefit to entity

Entity gains an understanding of changes, inclusions and the risks of areas that could not be resolved satisfactorily. This reduces cyber risk in contracts and improves the cyber resilience of the entity.



Threat intelligence

Threat assessments

Overview

Cyber Security NSW gathers and analyses information to develop threat assessments that report on specific threats and issues, as defined by the requesting entity.

Service type

Upon request.

Availability

One to two weeks from request.

Process

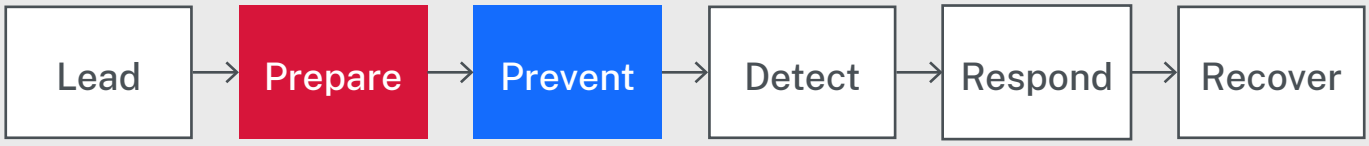
1. Entity requests threat assessment from Cyber Security NSW, outlining threat/issue they are looking to find out more about.
2. Cyber Security NSW undertakes NSW-specific analysis using a wide variety of open and closed sources.
3. Cyber Security NSW produces a threat assessment tailored to a specific context, such as an individual entity, sector or capability.

Outcome

Entity receives intelligence brief, report or threat briefing on their identified topic.

Benefit to entity

Entity has a deeper understanding of the cyber threat and how it is most likely to impact the entity, enabling consideration of appropriate controls and responses.



Intelligence products

Overview

Cyber Security NSW proactively identifies and reports on cyber threats that may impact the NSW Government environment.

Service type

Ongoing.

Availability

Subscription based.

Process

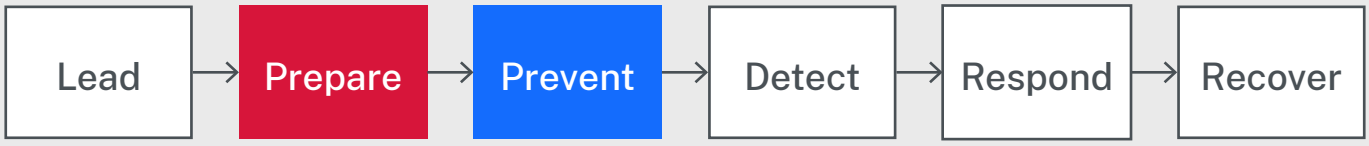
1. Cyber Security NSW uses a wide variety of open and closed sources to produce analysis specific to the NSW Government environment.
2. Cyber Security NSW disseminates intelligence to inform NSW Government entities of threats and security issues of concern.

Outcome

Entities receive alerts, advisories, briefs and reports that inform them of cyber threats and emerging issues relevant to the NSW Government context.

Benefit to entity

Entities are informed of threats and issues likely to affect their cyber environment, enabling proactive mitigation and decisive action.



Dark web monitoring

Overview

Cyber Security NSW proactively identifies and reports on cyber threats that may impact the NSW Government environment.

Service type

Upon request.

Availability

Within one to seven business days, depending on urgency of request.

Process

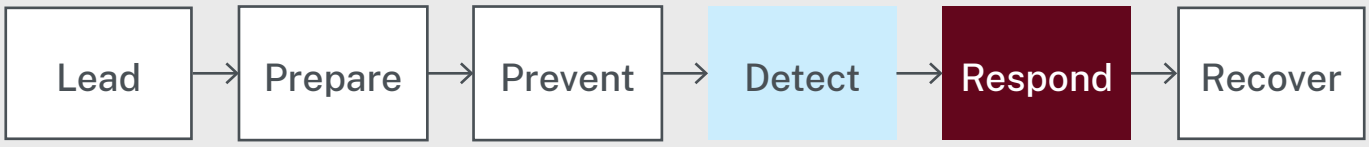
1. Entity requests dark web monitoring for a particular issue or incident.
2. Cyber Security NSW undertakes automated and ad-hoc searching of dark web repositories based on the agreed requirements for information.
3. Cyber Security NSW provides updates on findings to the entity.

Outcome

Information regarding threats, credentials for sale, leaks and groups targeting the entity, the NSW Government or NSW members of the public is surfaced.

Benefit to entity

Entities are alerted to potential and emerging threats and trends that are not yet widely known. This information can help enable a considered and measured response.



Incident response

Incident triage and containment

Overview

Cyber Security NSW proactively identifies and reports on cyber threats that may impact the NSW Government environment.

Service type

Upon request.

Availability

24/7 response for urgent incidents.

Process

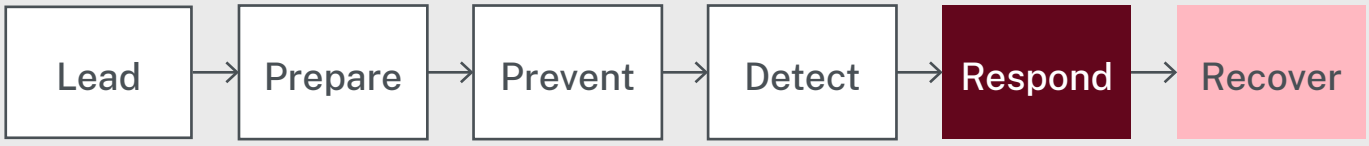
1. Entity reports cyber incident to Cyber Security NSW via email, the Cyber Security NSW Cyber Portal or, for time-critical cyber security matters that require urgent support, the 24/7 reporting hotline (these details are disseminated directly to NSW Government entities).
2. Cyber Security NSW triages incoming incident notifications and determines what level of assistance is required.
3. Cyber Security NSW provides incident coordination and assistance, which may involve technical and forensic analysis and advice, intelligence support and monitoring, and coordination across government, law enforcement and regulatory bodies, as required.

Outcome

Victim entities receive guidance and practical assistance to achieve the best possible business outcome in a timely manner.

Benefit to entity

The victim entity is supported in responding to and recovering from cyber incidents through added capability, capacity and experience.



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