Cyber Security Guidance

National Cyber Security Centre

*The Traffic Light Protocol (TLP) marking is used to ensure that sensitive information is shared with the correct audience. Recipients can spread **TLP: CLEAR** information to the world, there is no limit on disclosure. Information sources may use **TLP: CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP: CLEAR** information may be shared without restriction.*

Responding to Third-Party Data Breaches

New Zealand organisations should consider the risk of third-party data breaches to their own cyber security. Where a data breach includes account information or user credentials, malicious cyber actors can leverage this information to conduct password attacks and targeted social engineering. If you suspect your organisation is affected by a third-party data breach, the NCSC recommends you consider the following mitigations to address the risks.

Training and Awareness

Governance

Review the Acceptable Use policy and ensure adequate policies exist that restrict staff from using official IDs and login passwords as credentials for external websites. Refer to the NZ Information Security Manual NZISM 14.3.13 for further guidance.

Security awareness training and culture

Contact affected staff and warn about the risk from re-using official ID and passwords for personal use on external websites, especially if the websites do not have a clear work purpose.

Ensure all staff receive regular cyber awareness training and understand their responsibility to help maintain the organisation's security. Security awareness is part of meeting the Protective Security Requirements (PSR) and helps to protect people, information and assets. This could include mandatory eLearnings and participation in the CERT NZ Cyber Smart week campaign. Refer to the NZISM 9.1 and PSR for guidance about information security awareness and culture. Security culture is set from the top, and it is imperative the senior leadership team endorse security awareness initiatives.

User Access Management

The discovery or public announcement of data breaches may occur months or years after they happen. It underscores the importance of effective user access management both before and after your organisation becomes aware of third party data breaches.

User account management and off boarding

Ensure there are processes in place for the entry, exit, and internal movement of employees. Immediately remove access to data and systems from accounts of departing employees. Ensure the off boarding process considers cloud assets and physical devices. Deactivate any service accounts, and activate them only when maintenance is performed.

Account clean-ups

Periodically review the Active Directory (AD) user list against the HR movement lists to identify any undeleted AD accounts belonging to terminated employees. Such accounts should be disabled immediately and logs reviewed for suspicious sign-in activity.

Shared accounts

Generic, shared accounts are usually linked to critical applications, servers, platforms and databases. The use of generic accounts should be actively monitored and logged. Passwords must be immediately changed when someone who used the account no longer needs access.

Audit log review

At a minimum, consider reviewing the activity logs of the impacted privileged accounts (if any) to identify suspicious sign-in activity.

The PSR outlines the Government's expectations for managing personnel, physical and information security. Specifically, the core policy PERSEC 3 addresses the management of departing staff and their access.

Authentication

Password change

Contact the affected users linked to the breaches to ensure their passwords are changed.

Password policy

Review and update the password policy to ensure it aligns with industry best practices. Please refer to the NZISM 16.1.40 for password policy guidance. In addition, CERT NZ has also released password guidance. We are aware of conflicting recommendations regarding password changes. Please refer to the NZISM FAQ for information on addressing differing recommendations and approaching password policies if required.

Multi-factor authentication (MFA):

MFA can help prevent account takeovers. MFA is a critical tool in mitigating malicious cyber activity. Do not exclude any user, particularly administrators, from an MFA requirement.

Third Party Risk Management

Supply chain risk

Assess the management of third party risk and ensure vendors with system access understand and agree to comply with the Acceptable Use Policy. Where possible, consider building minimum security requirements into the supplier contracting process. The NCSC issued a Joint Cyber Security Advisory about threats to managed service providers and provides recommendations to help manage supply chain risk.

Third party assurance

Implement a robust third party security framework to help manage the risk related to external service providers. Refer to the NCSC Supply Chain Cyber Security Guidance.

The NCSC can be contacted by email at: **info@ncsc.govt.nz**
We encourage you to contact us at any time if you require any further assistance or advice.