information and privacy commission new south wales

Glossary **August 2024**

Defining the causes of a data breach

Who is this information for?	NSW public sector agencies who are making a notification of an eligible data breach to the NSW Privacy Commissioner
Why is this information important to them?	This glossary will assist agencies to identity and define the cause of a data breach

Agencies are required to provide information on the cause of a data breach when notifying the Privacy Commissioner of an eligible data breach under the NSW Mandatory Notification of Data Breach Scheme (MNDB Scheme). This information is collated and reported on by the Privacy Commissioner under three categories:

- human error
- malicious or criminal attack, and
- system fault.

Determining the cause of a data breach is an important part of the data breach response process. Accurately identifying how a breach occurred will assist the agency to take the appropriate steps to contain the breach, mitigate potential harm to affected individuals and identify measures to prevent further breaches occurring in the future.

Agencies should consult this glossary to identify the cause of the breach when making a notification of an eligible data breach.

Term	Definition
Human Error	**An unintended action by an individual directly resulting in a data breach**
Failure to use BCC when sending email	Sending an email to a group by including all recipient emails addresses in the 'To' field, thereby disclosing all recipient email address to all recipients
Failure to redact personal information	Failure to effectively remove or de-identify personal information from a record before it is disclosed
Incorrect personal information attached to a client file	Personal information is attached to an incorrect client file which is subsequently accessed
Insecure disposal	Disposing of personal information in a manner that could lead to its unauthorised disclosure, for example, using a public rubbish bin to dispose of customer records instead of a secure document disposal bin
Loss of paperwork or data storage device	Loss of a physical asset containing personal information, for example, leaving a folder or a laptop on a bus
Personal information sent to the wrong recipient	Personal information sent to the wrong recipient via email, fax, mail or other method
Unauthorised access	Accessing personal information without authority or for a purpose not related to their duties or functions

Term	Definition
Unauthorised verbal disclosure	Disclosing personal information verbally without authorisation, for example, calling it out in a waiting room or providing via a conversation
Unauthorised disclosure by unintended release or publication	Unauthorised disclosure of personal information in a written format, including via paper documents or online
Malicious or Criminal Attack	**A malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain**
Theft of paperwork or data storage device	Theft of a physical asset containing personal information
Social engineering/impersonation	An attack that relies heavily on human interaction to manipulate people into breaking normal security procedures and best practices to gain access to systems, networks or physical locations
Rogue employee/insider threat	An attack by an employee or insider acting against the interests of their employer or other entity
Cyber incident	A cyber incident targets computer information systems, infrastructures, computer networks or personal computer devices
Malware	Short for 'malicious software'. Software used to gain unauthorised access to computers, steal information and disrupt or disable networks. Types of malware include trojans, viruses and worms
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment
Phishing (compromised credentials)	Untargeted, mass messages sent to many people asking for information, encouraging them to open a malicious attachment, or visit a fake website that will ask the user to provide information or download malicious content
Brute force attack	A process to determine a cryptographic key or password that proceeds by systematically trying all alternatives until it discovers the correct one
Compromised or stolen credentials (method unknown)	Credentials are compromised or stolen by methods unknown
Hacking	Unauthorised access to a system or network (other than by way of phishing, brute-force attack or malware), often to exploit a system's data or manipulate its normal behaviour
Business email compromise	A form of cybercrime that uses email fraud to attack an organisation to achieve a specific outcome that negatively impacts the target organisation
System Fault	**A business or technology process error not caused by direct human error**

Term	Definition
Mail merge failure	A system failure which results in personal information being misdirected to the incorrect individual
Unintended release or publication	A system failure which results in the release or publication of personal information

Other useful resources

Other resources that may be useful on this topic include:

- Guide to managing data breaches in accordance with the Privacy and Personal Information Protection Act 1998 (NSW)
- Guidelines on the assessment of data breaches under Part 6A of the PPIP Act

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this glossary is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.