Service Description

Data Breach Response Plan

Scope

The Data Breach Readiness and Response Plan (DBRP) establishes a proactive and structured framework for detecting, containing, assessing, and responding to actual or suspected data breaches across the organisation. It aligns with the OAIC Notifiable Data Breach (NDB) Scheme, the Privacy Act 1988, and best practice guidance drawn from the NIST Cybersecurity and Privacy Frameworks. The service ensures the organisation can contain incidents quickly, assess their impact accurately, notify affected individuals and regulators effectively, and recover securely, minimising both regulatory exposure and reputational harm.

This engagement includes the development and validation of an enterprise-wide breach response framework that defines governance, roles, and escalation procedures. It establishes a dedicated Data Breach Response Team composed of governance, technical, legal, and communications stakeholders to ensure coordinated and accountable action. The plan integrates operational playbooks, checklists, and response templates to support rapid and compliant decision making under the NDB scheme. It also defines clear communication workflows for notifying affected individuals, the OAIC, and key partners. Finally, readiness is verified through tabletop simulations and post incident review exercises, ensuring continuous improvement and organisational resilience in the face of potential data breaches.

Approach

Delivered using six-phase approach, the DBRP service is conducted encompassing the following practical phases:

Discovery & Current State Review

- Review existing breach-management processes, incident workflows, and response documentation.
- Map stakeholder responsibilities (Legal, Security, Risk, Communications, Technology).

Framework & Response Design

- Define governance model and escalation matrix consistent with OAIC NDB guidance.
- Align breach-handling stages with NIST CSF: Identify → Protect → Detect → Respond → Recover.
- Ensure Disaster Recovery and Business Continuity alignment

Playbook Development

- Develop scenarios to support the likes of:
  - Unauthorised access or exfiltration
  - Lost or stolen devices/media
  - Ransomware or encryption events
  - Mis delivery or accidental disclosure
  - Insider or employee-related incidents

Response Templates & Communication Packs

- Develop OAIC-compliant notification templates, internal escalation forms, and external communication scripts.
- Include public statement and media engagement templates (where required).

Testing & Validation

- Support Client led simulation exercises or tabletop tests to validate readiness and timing of responses.
- Measure containment, escalation, and communication effectiveness.

Improvement

- Deliver feedback and maturity roadmap integrating policy, training, and audit recommendations.

Value

- Regulatory Assurance: Ensures compliance with the OAIC NDB Scheme and Privacy Act obligations.
- Incident Readiness: Reduces uncertainty and response time during actual breaches.
- Operational Confidence: Clarifies ownership, escalation paths, and communication channels.
- Reputational Protection: Minimises public, customer, and regulator impact through coordinated action.
- Governance Integration: Strengthens linkage between security operations, privacy management, and executive oversight.

Benefits

These are the key advantages of undertaking this service offering.

- Improves the organisation's ability to detect, contain, and assess data breaches quickly and effectively.
- Ensures compliance with OAIC Notifiable Data Breach obligations within required timeframes.

- Strengthens operational readiness through well-practised and coordinated breach response exercises.
- Reduces the impact of data breaches by enabling faster containment and recovery actions.
- Builds stakeholder trust and enhances organisational resilience through consistent and transparent response practices.

Outputs

These outputs are provided:

- Incident Response Playbooks – step-by-step actions for different breach scenarios.
- OAIC-Compliant Notification Templates – for internal, individual, and regulator communications.
- Breach Assessment & Escalation Matrix – roles, criteria, and authority for activation.
- Simulation & Readiness Report – results of tabletop exercise and response improvement plan.
- Governance Toolkit – includes reporting forms, decision trees, and evidence tracking templates.