White Paper

Personal Data Breach Mitigation

4 Step Best Practice Checklist

Huntsman®
Defence-Grade Cyber Security

Personal Data Breach Mitigation

4 Step Best Practice Checklist

The Notifiable Data Breach Scheme under the Privacy Act 1988 (Cth) ('Act') came into effect in Australia on 22 February 2018. The scheme imposes an obligation on entities and agencies subject to the Act to notify individuals whose personal information is subject of a data breach that is likely to result in serious harm to those individuals. Entities must also notify the Australian Information Commissioner of eligible data breaches.

Anticipating, identifying and responding to personal data breaches is an increasingly challenging responsibility for all businesses. Identifying ways to make this more manageable is key to operational and commercial success. We have developed this **4 Step Best Practice Checklist** to offer preventative strategies to minimise the number of data breaches.

The 4 Step Best Practice Checklist Summary

1. How are you protecting against unauthorised and unlawful access, loss or damage
2. How are you ensuring and demonstrating data protection
3. What steps have you taken to protect against external threats of unlawful access, disclosure or loss
4. What steps have you taken to protect against insider data abuse

For each step, to make the process simpler, we will explain:

- **The method to deploy;**
- **The ideal stances you need to have; and**
- **Some example use cases**.

Huntsman®

1 Protect against unauthorised and unlawful access, loss or damage

METHOD:

Monitor the entire enterprise for activity and threat information across platforms, applications, networks, security controls and end points to protect the security of personal data and to alert on breach or misuse.

STANCE:

i **WE KNOW WHAT DATA WE HAVE, ITS SENSITIVITY, WHERE IT IS AND WHO OWNS IT.**

Use Case:
Monitor and alert on access to sensitive data sets, file shares and records.
Monitor all print activity including Doc ID, printer, user, success or fail.

ii **WE HAVE PROTECTED OUR NETWORK AND SYSTEMS FROM MALWARE AND MALICIOUS ATTACKS.**

Use Case:
Continually monitor availability and integrity of firewalls, anti-malware and IPS.
Alert on change and failure.

iii **WE HAVE ESTABLISHED ACCESS CONTROL, THRESHOLDS AND PROCEDURE OVER PERSONAL DATA ASSETS.**

Use Case:
Audit and monitor all OS security groups and policy relevant to databases, apps and file share.
Alert on additions to sensitive groups.

iv **WE MONITOR SUFFICIENTLY TO DETECT AND RESPOND TO CYBER INCIDENTS.**

Use Case:
Alert on email export of personal data to unknown recipients.

2 Ensure and demonstrate data protection

METHOD:

Implement extensive and fully auditable monitoring to allow detailed querying and filtering of data, with drill-down, to enable issues to be rapidly investigated, corroborated and understood.

STANCE:

i **WE EDUCATE AND TEST ALL OUR USERS ON GOOD CYBER SECURITY AWARENESS.**

Use Case:
Alert on activity of new users and those subject to "managed risk".

ii **WE CAN ACCURATELY REPORT ON OUR SECURITY STATUS AT ANY TIME.**

Use Case:
Visualisation of personal data access and use from single user to unit to corporate.
Monitoring establishes How, Where and When access occurs.

iii **WE FREQUENTLY AUDIT AND TEST FOR VULNERABILITIES AND WEAKNESSES.**

Use Case:
Create personal data "honeypots" and alert on internal and external access or change.

iv **WE DESIGN SECURITY AND DATA PROTECTION INTO OUR SYSTEMS AND PROCESSES FROM THE START, AND CAN PROVE IT.**

Use Case:
Monitor application workflows, identifying backlogs and inappropriate processing.

3 Implement security to prevent unlawful access, disclosure or loss

METHOD:

Use security analytics to process data in real-time and identify activity or behaviour indicating misuse or breach of personal data. Use dashboards to enable rapid demonstration of compliance.

STANCE:

i **WE CONTROL USE OF REMOVABLE MEDIA ACROSS ALL DEPARTMENTS.**

Use Case:
Monitor and alert on Windows PnP events indicating connection of removable media & devices.

ii **WE HAVE CONTINUOUS VISIBILITY OF PERSONAL AND SENSITIVE DATA CONFIDENTIALITY, INTEGRITY AND AVAILABILITY.**

Use Case:
Real time dashboards showing Confidentiality, Integrity and Availability status of all sensitive data assets.

iii **WE HAVE MULTIPLE CONTROLS ACROSS THE BUSINESS AND HANDLE ALL THE ALERTS THEY GENERATE.**

Use Case:
Correlate privilege user network authentication with critical business service change likely to lead to failure. Automatically analyse, alert and remediate.

iv **WE HAVE ACTIVE POLICIES FOR HOME WORKING, REMOTE ACCESS AND MOBILE DEVICES.**

Use Case:
Monitor corporate mobile devices and alert on attempted connection to data services when “out of country”.

4 Take steps to protect against insider data abuse

METHOD:

Monitor use of applications and access to data across the enterprise, but also monitor users, privileges and behaviours in order to spot unauthorised use by insiders or compromised users.

STANCE:

i **WE KNOW AND CONTROL WHO HAS ACCESS TO PERSONAL DATA WITHIN OUR ORGANISATION ON PREMISE AND IN THE CLOUD.**

Use Case:

Monitor and alert on Windows PnP events indicating connection of removable media & devices.

ii **WE KNOW AND MONITOR THE USERS WHO HAVE THE PRIVILEGE TO EXPORT PERSONAL DATA.**

Use Case:

Monitor the connection of USB device to the network, correlated with current user, terminal and data. Alert on non-compliance with policy.

iii **WE DETECT WHEN ROGUE USERS AND COMPROMISED ACCOUNTS ARE ACTIVE.**

Use Case:

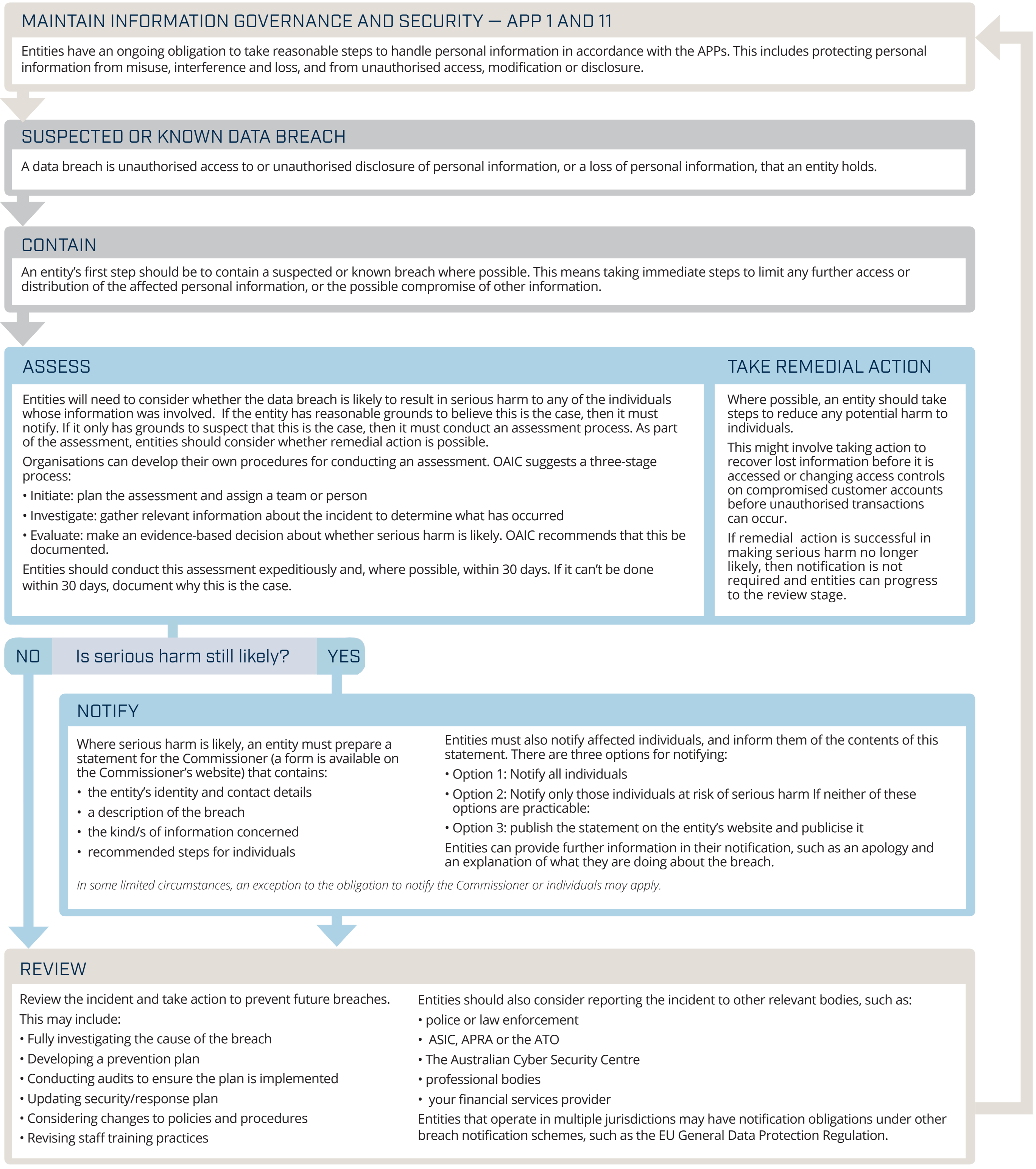
Monitor and correlate network terminals, devices and users to identify and alert on unusual access e.g. CEO account authenticates from external IP at 3am.

iv **WE UNDERSTAND HOW PERSONAL DATA IS USED THROUGH OUR BUSINESS.**

Use Case:

Monitor database workflow to identify irregular patterns of activity indicating potential user negligence or mistake.

This paper outlines a best practice checklist to assist in mitigating against a personal data breach. Importantly the achievement of these initiatives requires the successful management of competent technology, personnel and process. To assist organisations in meeting their new personal data Protection obligations the Office of the Australian Information Commissioner (OAIC) recently added a Data Breach Response Summary to its website to provide an overview of the process of a typical data breach response, including the Notifiable Data Breach Scheme requirements. The summary sets out the steps the OAIC considers that an organisation or agency should take when faced with a suspected personal data breach. The summary along with the more detailed resources made available by the OAIC can be found at: **www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme**



MAINTAIN INFORMATION GOVERNANCE AND SECURITY — APP 1 AND 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

SUSPECTED OR KNOWN DATA BREACH

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

CONTAIN

An entity's first step should be to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

ASSESS

Entities will need to consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an assessment process. As part of the assessment, entities should consider whether remedial action is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- Initiate: plan the assessment and assign a team or person
- Investigate: gather relevant information about the incident to determine what has occurred
- Evaluate: make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

TAKE REMEDIAL ACTION

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO | Is serious harm still likely? | YES

NOTIFY

Where serious harm is likely, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- Option 1: Notify all individuals
- Option 2: Notify only those individuals at risk of serious harm If neither of these options are practicable:
- Option 3: publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

REVIEW

Review the incident and take action to prevent future breaches.

This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Achieving confidence with Huntsman Security

To improve your security approach and monitor all cyber security dimensions of your enterprise contact Huntsman Security for information on best practice, our expert views or to discuss our work in this area.

Contact Huntsman Security for more information on solutions proven to deliver detection to resolution of user misuse, breaches and external attacks in both large and small deployments.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street, Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

AMERICAS

toll free: **1-415-655-6807**

e: **usinfo@huntsmansecurity.com**

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman