DATA BREACH RESPONSE PROCESS

REGULAR SECURITY POSTURE

Protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

To comply with your obligations under the Australian Privacy Principles, your organisation should consider:

- the sensitivity of the personal information
- the harm likely to flow from a security breach
- developing a compliance and monitoring plan, and
- regularly reviewing your information security measures

DATA BREACH OCCURS

Personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse or interference.

KEY STEPS IN RESPONDING TO A DATA BREACH

STEP 1 — **Contain the breach and make a preliminary assessment**

- Call Computer One
- Take immediate steps to contain breach
- Designate person/team to coordinate response

STEP 2 — **Evaluate the risks for individuals associated with the breach**

- Consider what personal information is involved
- Determine whether the context of the information is important
- Establish the cause and extent of the breach
- Identify what is the risk of harm

STEP 3 — **Consider breach notification**

- Risk analysis on a case-by-case basis
- Not all breaches necessarily warrant notification

SHOULD AFFECTED INDIVIDUALS BE NOTIFIED?

Yes, where there **is a real risk of serious harm**, notification may enable individuals to take steps to avoid or mitigate harm. Consider:

- Legal/contractual obligations to notify
- Risk of harm to individuals (identity crime, physical harm, humiliation, damage to reputation, loss of business or employment opportunities)

PROCESS OF NOTIFICATION

- **When?** - as soon as possible
- **How?** - direct contact preferred (mail/phone)
- **Who?** - the entity with the most direct relationship with the affected individual(s)
- **What?** - description of breach, type of personal information involved, steps to help mitigate risks and contact details for information and assistance

SHOULD OTHERS BE NOTIFIED?

- **Office of the Australian Information Commissioner**
- Police/Law Enforcement
- Professional or Regulatory Bodies
- Other agencies or organisations affected by the breach or contractually required to notify

STEP 4 — **Review the incident and take action to prevent future breaches**

- Work with Computer One to fully investigate the cause of the breach
- Develop a Prevention Plan
- Audit to ensure plan is implemented
- Update security/ response plan
- Make appropriate changes to policies and procedures
- Revise staff training practices

COMPUTERONE
www.computerone.com.au
1300 667 871