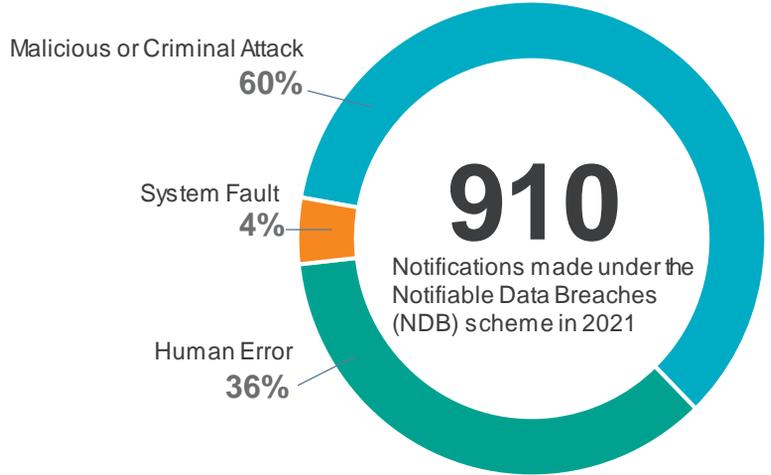# Data Breach

The Cost of a Data Breach

In 2021, the Office of the Australian Information Commissioner (OAIC) received **910** notifications of a data breach that is likely to result in serious harm to an individual whose personal information is involved. Whilst the figure is down from the **1057** notifications received in 2020, a persistent threat remains, particularly in terms of cyber security, with **365** reported breaches a result of cyber security incidents.

Source: OAIC Notifiable Data Breaches Report Jan – Jun 2021, Jul – Dec 2021.

Malicious or Criminal Attack
60%

System Fault
4%

Human Error
36%

910
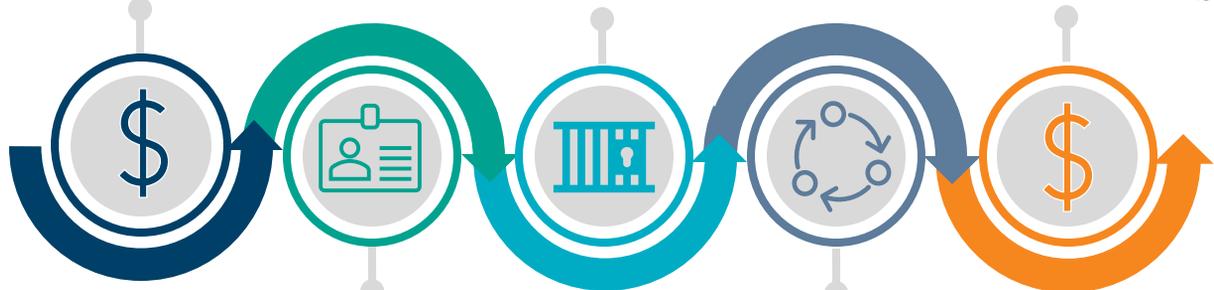Notifications made under the Notifiable Data Breaches (NDB) scheme in 2021

$3.7m
Average total cost of a data breach in Australia in 2021

86
No. of data breaches reported to OAIC in 2021 caused by ransomware

$241
Cost per record of customer personal information lost or stolen (global)

20%
Percentage of breaches caused by compromised credentials (global)

287
Average no. of days to identify and contain a data breach (global)

Source: IBM Cost of a Data Breach Report 2021

Data breach notifications by industry sector, Australia 2021

- Health Service Providers
- Finance incl. Superannuation
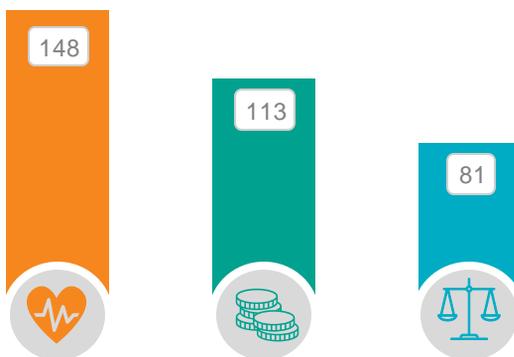- Legal, accounting & management services

	150	148	113	81
	100			
	50			
	0			

Data Breach

Despite the statistics and news headlines, a data breach should not be viewed as an inevitable occurrence for all organisations. There are a number of key activities and strategies available to reduce the likelihood of a data breach occurring, and the impact if a data breach does occur.

How to Prevent a Data Breach

Cyber Security: Invest in your cyber security capabilities and regularly assess the maturity and effectiveness of cyber security controls such as access controls, detection and response processes, resilience capabilities, and data loss prevention tools.

Incident Response Planning: Assemble an Incident Response Team, develop incident response plans, processes and playbooks, and periodically test plans and capabilities to respond to data breaches in optimal times.

Data Governance: Define, develop and mature governance frameworks to manage areas such as data ownership, security, classification, retention, etc.

Third Party Management: Assess security capabilities of key third party providers to identify weaknesses or gain assurance that third parties have adequate capabilities and controls in place to protect your organisation's information.

Privacy Management: Establish a privacy management program to identify, manage and secure personal and sensitive personal information in line with regulatory requirements throughout its lifecycle.

Contact Information

Ewen Ferguson
Managing Director
protiviti®
Global Business Consulting

Direct: +61 478 491 056
ew en.f erguson@protiviti.com.au

Ghislaine Entwisle
Managing Director
protiviti®
Global Business Consulting

Direct: +61 431 285 494
ghislaine.entw isle@protiviti.com.au

Hirun Tantirigama
Director
protiviti®
Global Business Consulting

Direct: +61 423 853 453
hirun.tantirigama@protiviti.com.au

Marc Coleman
Senior Manager
protiviti®
Global Business Consulting

Direct: +61 405 189 472
marc.coleman@protiviti.com.au

protiviti®
Global Business Consulting