SMALL BUSINESS DIGITAL CHAMPIONS
AN AUSTRALIAN GOVERNMENT INITIATIVE

(ndp) National Disability Practitioners

NDS National Disability Services

**FACT SHEET** **Session 4** **Cyber Security Part 2**

Let's begin with looking at some advancements in technology across industry sectors:

**Agriculture / Farming**
Chip technology for irrigation, plant management & livestock management , Drones for inspections, Robotics which change the PH and heat the soil, can microscopically remove the weeds and plant/nurture the seedlings,

**Tourism / Hospitality**
**Disney -** Wristband purchasing, room key, GPS and event tickets. Online schedule building and appointment setting - Sharing economy revolution - Handheld device which tests drinks for spiking. iPad ordering for services and meals

**Medical / Nursing**
Immediate collective diagnostics and smart phone testing, 3-D Printing bone and cartilage construction, organ cloning, chip technology for disease tracking

**Mental Health**
Virtual Reality to treat Post Traumatic Stress Disorder, A computer game which examines the triggers for depression, Virtual support groups

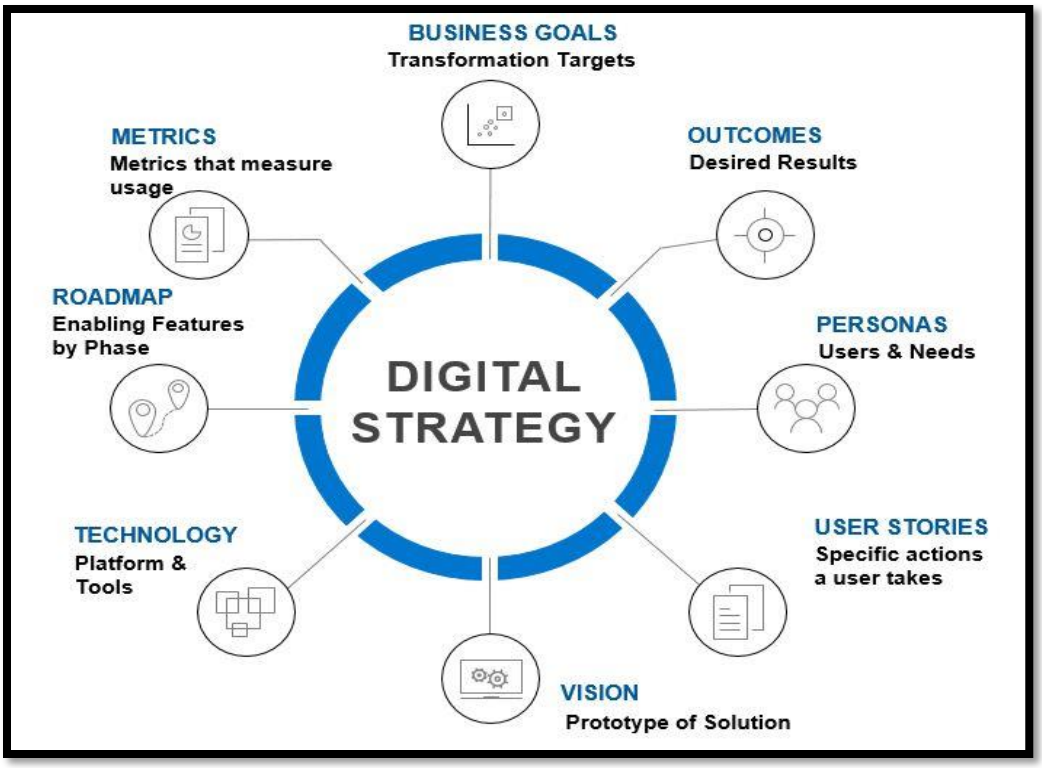
**Aged Care / Disability**
Remote medical treatment, testing for symptoms through mobile technology, addressing isolation issues, allow for greater independence, Braille iPhones, Eye-movement laser motivated keyboards, wheel chairs which can move directly into electric cars and be driven

## The Objectives for Digital Transformation

- Improve Customer Experience
- Increase Efficiency
- Improve Business Decision Making
- Cyber Security
- Improve Innovation
- Transform the business

As we explored in each session of our Webinars, the first step of any organisation to digitally transform is to create a detailed digital strategy.

This takes a commitment from the senior management team who will ultimately drive this strategy. But all staff must be involved. The leading cause for unsuccessful digital strategies is failing to engage staff and failure to collect critical information on the details of all processes and procedures. When a digital strategy is foisted on a workforce it will be criticised and undermined.



**Lack Of Strategy:** **As a refresh: A successful Digital Strategy is split into the following key areas of development.**

Each other of these key areas must be detailed with clear definitions of your goals and a development plan of who is responsible, KPI's for delivery and what resources will be committed. Mapping out what is currently happening throughout the business and new ideas on how to use technology to improve these areas are also important. Don't worry about whether the technology to achieve these goals exists, focus on the ideas, the strategies and the end results required. A digital strategy should be split into the following areas.

- Business Goals – Transformational targets - Big picture, but not a vision statement. But goals which relate to the new goals of your organisation on this digital transformation journey. What do you expect from your executive management, your staff and your technology companies? What are the end goals to map your success back to?

- Outcomes – Specific desired results across each area of the business. This should include estimated percentages of improvement, engagement and profitability. The map to which you quantify success.

- Personas – Users and Needs – Who are the engagement key stakeholders? What level of security can they access your systems? Develop the levels of access and who can access the system. Through their phones, home computers, work stations only, any other devices?

- User Stories – Specific actions a user takes – how do people use your current systems? How would you like them to use the systems in the future? The beginning of mapping which leads into Vision.

- Vision – Prototype of solution – The actual mapping of the system you are looking to develop. Detailed wireframes of the processes, step by step in the system.

- Technology – Platform and tools – What are your legacy systems and what type of systems do you want into the future? (not by name, but by function)

- Roadmap – Enabling features by phase. The strategy for mapping the timing and KPI's of the successful strategy.

- Metrics – Metrics that measure usage, data, analytics, feedback and communication.

**Data Breach Legislation - NDB Scheme**

Data breaches are commonplace in an increasingly digital world.

New laws are now in effect that will require thousands of Australian companies to notify individuals and the Government if they believe a data breach has occurred within their IT systems causing personal information to be compromised.

**What is it?**

Australia's new mandatory data breach reporting laws came into effect on **22nd of February 2018**.

Known as the Notifiable Data Breaches (NDB) scheme, this new legislation will be contained within Part IIIC of the *Privacy Act 1988* and largely mirror similar laws introduced in other countries including the USA.

**Who does it apply to?**

Any agency or organisation already subject to the *Privacy Act* (known as an APP entity). This includes Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of at least $3 million, health service providers and more.
Generally small business operators (including sole traders and unincorporated associations) with an annual turnover under $3 million will not be subject to the NDB scheme's obligations

**Why Legislate?**

Recent high profile data breaches include Facebook, My Fitness Pal and in 2016 there was an admission by the Red Cross that the personal data of over half a million Australian blood donors may have been compromised.
These new laws are overdue and much needed to equip individuals with greater certainty in relation to the security of their personal information.

Then there was the Uber debacle (where 1 in 10 Australians were most likely affected).
The personal information of reportedly 57 million Uber customers and drivers were stolen (including names, email addresses and mobile phone numbers).

Plus Uber's failure to disclose this massive breach for over a year to the Commissioner and the company paid US$100,000 to the perpetrators to delete the stolen data.
There was a distinct failure to notify affected individuals and regulators.
Had Australia's new mandatory data breach reporting laws been in effect, Uber would have been penalised for their failure to contact victims and report the breach to the Australian Information Commissioner

**How often do data breaches occur?**

Major data breaches occur in Australia every day and are often covered up with those most effected having little to no knowledge that their personal information has been compromised.

In 2019 an average 19,800 records were compromised in each *Australian data breach* in the past year.

Number of data breaches reported under the NDB scheme by quarter — All sectors

NDB Quarterly Total number of notifications:

| | |
|---|---|
| July to September 2018: | 245 |
| October to December 2018: | 262 |
| January to March 2019: | 215 |
| April to June 2019: | 245 |

**What are the new obligations?**

If the organisation incurs an "eligible data breach", within 30 days it must notify individuals whose personal information is likely to result in serious harm due to the breach.

The notification must include recommendations about the steps individuals should take in response to the breach.

The organisation must also alert the Australian Information Commissioner of an eligible data breach.

This can be done through an online form, the Notifiable Data Breach statement, and here you will find what to include in the statement.

An **eligible data breach** is one in which there is unauthorised access, disclosure or loss of personal information held by an entity and that access, disclosure or loss is "likely to result in serious harm to any of the individuals to whom the information relates".

Examples may include the hacking of a database containing personal information or personal information that is mistakenly provided to the wrong person.

The scheme is **not retrospective** so if the breach occurred prior to 22 February 2018, even if it is discovered after this date, then it is not considered an eligible data breach for the purposes of this scheme.
The legislation distinguishes between notifiable and non-notifiable breaches. If an organisation can show that it has taken appropriate steps to mitigate the breach, then notification is not required

**What if I fail to report?**

The consequences are potentially significant with a business that fails to report an eligible breach
Penalties of up to $360,000 for individuals and $1.8 million for organisations.

For those affected, the release of personal names, email addresses and phone numbers may leave them susceptible to phishing attacks. Information such as driver's licence numbers and bank account details could lead to fraud, identity theft and money laundering.

**How can I prepare?**

Firstly, determine whether your agency or organisation is subject to the NDB scheme.

Check out the Information Commissioner's *Guide to securing personal information*.

Be aware of how personal information is stored and managed.

Have in place a data breach response plan. The Information Commissioner has an excellent guide to help prepare such a plan.

Seek legal advice at any step along the way to ensure that you are fully aware of your obligations, ensuring the safety of staff and customers, and have in place procedures and protocols should a data breach occur.

## Useful Links

Legislation: Privacy Amendment (Notifiable Data Breaches) Act 2017

Australian Information Commissioner's website about the Notifiable Data Breaches Scheme

Uber CEO Dara Khosrowshahi's blog post 21 November 2017

Red Cross Blood Service admits to personal data breach affecting half a million donors – ABC News 28 October 2016

*The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances*

**Resources:**

Small Business Digital Champions online hub

www.ndp.org.au/learning-hub/small-business-digital-champions-project.

The hub will house all information related to the project, including fact sheets, webinars, online courses and more. Individuals can register to receive a monthly e-newsletter to keep undated on new resources.