Navigating Cyber Security – **Advice for Secretaries & CEOs**

LEADERSHIP

Know:

- Who is your **most senior accountable officer**? Do they genuinely *own* the risk? Will they mobilise the whole of organisation response?
- Do you understand your organisation's **cyber risk appetite**?
- Ask the Government Chief Information Security Officer (GCISO) for advice and support

Do:

- Treat cyber security as a whole-of-business **risk management** issue
- Put cyber security as a **standing agenda item for governance** committees (senior executive leadership; Audit & Risk Committee)
- Build a cyber security **awareness culture** that reports issues and asks questions

PREPARE

Know:

- Do you have your CISO's **contact details** on your phone? And the GCISO's[1]?
- How prepared is your organisation for a significant cyber incident?
- Who is protecting your information and systems? How well are they doing it?

Do:

- A whole-of-organisation **cyber incident response plan**
- Integrate cyber security in business continuity plans
- Involve your **media and communications** team

PREVENT

Know:

- What is the full range of information you hold?
- Who has access to your information? Do they need it?
- Who may want to access it or corrupt it?
- What services do you provide and to whom?
- Do you have appropriate cyber insurance in place?

Do:

- Adhere to the **Cyber Security Policy** & minimum standards
- Understand where your information stored and who manages it
- Include **cyber security requirements in contracts**

DETECT

Know:

- Eliminating *all* incidents is near impossible because
  - new vulnerabilities are discovered all the time
  - you are highly dependent on many other players
- Enterprise IT may differ from Operational Technology (buildings, MRIs, Trains) but they are all interconnected

Do:

- **Report incidents to the GCISO[1]**; to the ACSC[3] if it serious and after hours; to NSW Police if suspicious
- Consider advice from the GCISO and inform the GCISO of actions taken

RESPOND

Know:

- Everyone needs to know what to do when cyber-attacks occur through effective policies and regular practice
  - Who you will call for help?
  - What you will say to the media?
  - Who will be the public face?

Do:

- Have providers on standby to help address incidents (and not just the technology)
- Your CIO should quickly **contain** and **eradicate**
- Work with the GCISO on WoG response and escalation

RECOVER

Know:

- **Understand the impacts**
  - to others if information leaks or is lost?
  - to others if your services stop?
- Understand the **competing priorities** of safety and harm prevention vs service restoration

Do:

- Ensure victims of cyber security incidents are directed to psychological support[2]
- Back up – it is the best way to address ransomware

REVIEW

Do:

- Undertake **lessons learnt exercises** after any cyber incident in order to apply improvements across all aspects of the cyber security framework
- Undertake **formal testing exercises** at least every 12 months to assess readiness, resilience and capability gaps
- Extend invitations to agencies in your cluster to learn how to work together to resolve incidents including skill sharing when needed

1. cybersecurity@finance.nsw.gov.au
2. idcare.org/contact/get-help-now, 1300 432 273
3. cyber.gov.au, 1300 CYBER1 (1300 292 371)