

# Association of Corporate Counsel

## Cyber Risk: The in-house lawyer's role

Sally McRae – Legal Counsel, National Australia Bank Limited  
Blare Sutton – Partner (Technology), McGrathNicol



McGrathNicol



---

## Discussion objectives



Defining "Cyber Risk" and what it really means



Understand the full scope of "cyber" and how it might affect you



An example of how easily cyber breaches can occur



Practical examples of success stories and challenges



Some actionable takeaways

---

# What do we mean by “Cyber Risk”?

- ‘Cyber risk’ means any risk of financial loss, disruption or damage to the reputation of an organisation from ***some sort of failure*** of its information technology systems (Institute of Risk Management – emphasis added).
- Deliberate or unauthorized breaches of IT systems for
  - Espionage
  - Extortion
  - Reputational Damage
- Unintentional / accidental breaches
  - Human error
  - “Out of scope”
- System failure
  - Internally managed
  - Externally controlled

---

# Technology - the enabler

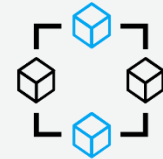
Many new and emerging technologies are now enabling and causing disruption including:



Internet of things (IoT)



Robotics (automation)



Blockchain technologies



Advancements in analytics



Artificial Intelligence  
and machine learning (AI)

---

## How invasive is technology in your organization?

- Consider the breadth of technology use across your organization
  - Inventory & Asset Management
  - Production (plant equipment, machinery, vehicles)
  - Financial
  - Communications

## What about the “Internet of Things”?

- From security cameras, coffee machines and refrigerators to cranes and trucks

## What are your crown jewels?

- Information classification
- Critical systems & failure stance (open/closed)
- Monetary transfers

---

# Cyber in the cloud – does it change the risk?

- Amazon Sydney Datacentre failure
- Navitaire system failure & Virgin Airlines
- Royal Bank of Scotland upgrade failure
- Carrilion collapse
- Dropbox security failure
- Equinix power outage drops AWS DirectConnect
- Microsoft Azure datacenter struck by lightning
- Human error at AWS

---

## Modern Cyber Attack – An example

- Attacks are more sophisticated
- Social engineering is real – settlement fraud
- Email and text messages from trusted contact
- Separate authorization
- Link to system

---

## Some insights and initiatives

- New fast payments in Australia (NPP)
- The UK experience: Friday Afternoon Fraud
- Scamming: whose risk, who pays?
- NAB's security work aimed at reducing SME Cyber risk
- Risks associated with cloud contracting



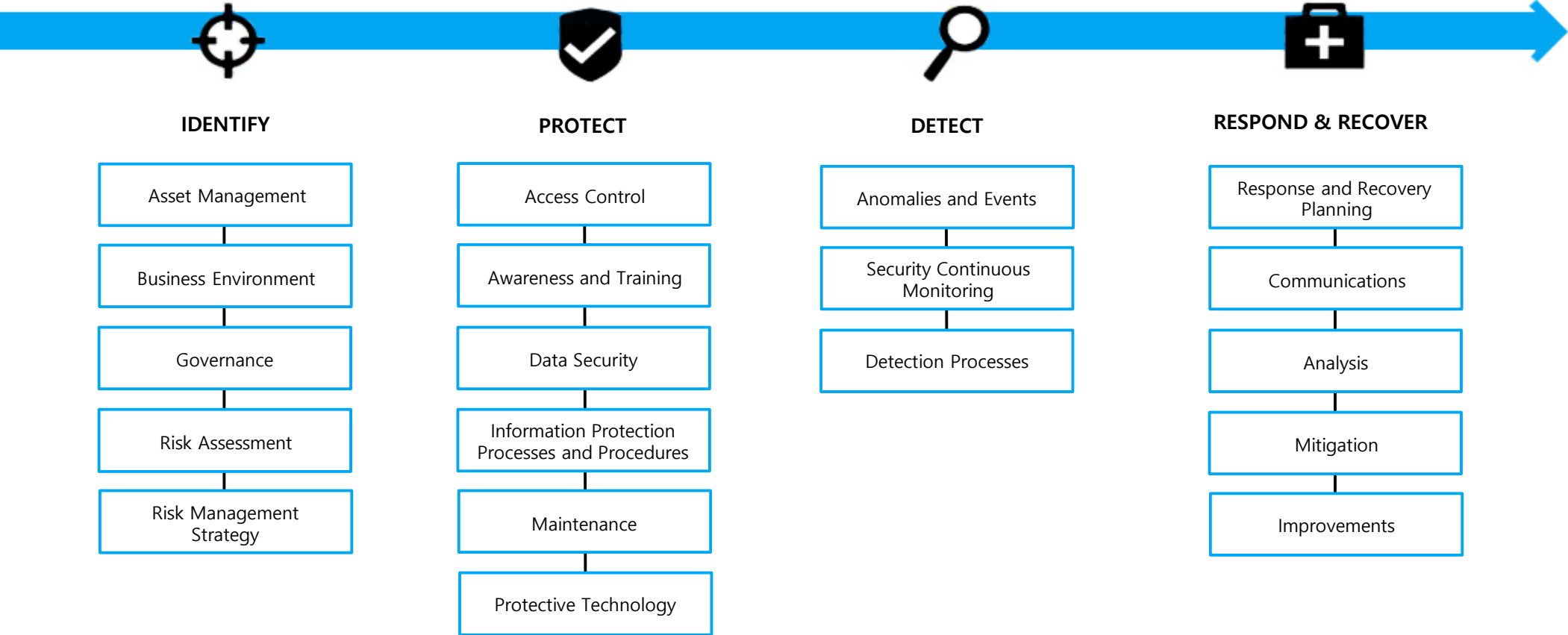
---

# Iceberg impact of a cyber incident

- Forensic investigation
- Breach notification & call centre
- Credit & Identity Monitoring
- PR firm
- Legal defense & indemnity costs
  
- Reputational damage
- Loss of customers
- Stock devaluation
- Corrective measures
- IT upgrade costs
- Devaluation of intellectual property
- Lost opportunity cost



# Cyber resilience





## Resilience tier scale




---


## Governance

 Are cyber risks fully integrated in the enterprise risk management process?

 Who on the board is responsible for cyber risk?

 What is our appetite for cyber risks, and have we communicated it?

 What is our regulatory and legal exposure?

 Which privacy / data security laws and regulations do we have to comply with?

 Are we getting enough assurance around cyber risk from our internal audit programme?

# Top 5 initiatives for resilience

Initiative	Action Items
<b>Get a baseline</b>	<ul style="list-style-type: none"><li>▪ Conduct a current state cyber resilience assessment (risk assessment)</li><li>▪ Survey your Board and Executive teams</li><li>▪ Consider conducting some internal, controlled technical testing</li></ul>
<b>Tackle the governance &amp; strategy layer</b>	<ul style="list-style-type: none"><li>▪ Assign a senior sponsor with influence</li><li>▪ Define the risk appetite statement for cybersecurity, privacy or information risk</li><li>▪ Define the strategy that will improve the current state and manage on-going resilience</li><li>▪ Assign operational responsibility to a single person to build and drive</li></ul>
<b>A plan to respond &amp; recover</b>	<ul style="list-style-type: none"><li>▪ Accept that incidents and events will occur</li><li>▪ Produce an action plan that brings all divisional stakeholders together to manage a crisis, not just IT</li><li>▪ Establish on-demand, external support for specialist services i.e. digital forensics and IR</li></ul>
<b>Safety &amp; awareness</b>	<ul style="list-style-type: none"><li>▪ Establish a regular safety and awareness engagement program (e.g. newsletters, eLearn, new starter briefings, a portal or repository of on-demand materials)</li><li>▪ Conduct a roadshow of briefing sessions</li><li>▪ Conduct controlled exercises that practically demonstrate what this is all about (e.g. phishing)</li></ul>
<b>Get operational</b>	<ul style="list-style-type: none"><li>▪ Create the partnership between Risk, Compliance and IT</li><li>▪ Start with the "essential eight"</li><li>▪ Transition to initiatives that mitigate current state risks, and aim to shorten the gap between something happening, you knowing something has happened and you doing something about it</li></ul>

---

# Practical examples – what has worked



## Resilience, Health & Risk Assessments

Getting an accurate view of current state against a reputable framework



## Privacy, Cyber & Information Risk Governance

Taking a top down approach and making someone accountable



## Post Incident Improvements

Looking critically at incidents and events and making lasting changes



## Managed Services

Going to market with a clear plan for on-going capability support



## Proactive Reporting

Taking a proactive approach on reporting to the Board even though the message in the beginning might be difficult



## Co-sourcing

A dedicated “burst period” of external support that establishes the foundation and hands over momentum

---

# Practical examples – what hasn't worked



## Awareness & Training

Unimaginative awareness and training initiatives that default to annual attestations



## IT-only Response Plans

Response plans that are only focused on IT and do not extend into Risk, Comms, Legal, HR and others



## Response without detection

A reliance on seemingly robust response plans with no thought given to enhancing detection capabilities



## Detection that isn't tuned

Turning on all the "noise" but not setting the rules by which things will be flagged



## Getting "To Do List" focussed

Getting tactical on changing red to amber without keeping an eye on the bigger picture

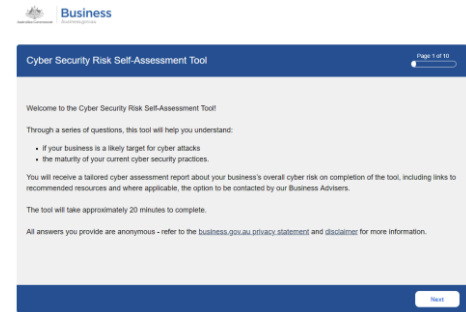


## Bottom Up

Burying the responsibility to far down the org chart that there are too many hurdles to jump for budget, air time and influence

# Resources for SME

- Cyber Security Risk Self-Assessment Tool  
<https://cybertool.business.gov.au/form/SelfAssessment>



- The Essential Eight  
<https://acsc.gov.au/publications/protect/essential-eight-explained.htm>



- ACSC's Strategies to Mitigate Cyber Security Incidents  
<https://www.acsc.gov.au/infosec/mitigationstrategies.htm>



- ACORN  
<https://www.acorn.gov.au/>





# Navigating Cyber Security



## 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<sup>1</sup>?
- 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<sup>1</sup>**; to the ACSC<sup>3</sup> 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<sup>2</sup>
- 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](mailto:cybersecurity@finance.nsw.gov.au)
2. [idcare.org/contact/get-help-now](https://idcare.org/contact/get-help-now), 1300 432 273
3. [cyber.gov.au](https://cyber.gov.au), 1300 CYBER1 (1300 292 371)



---

Q & A

