HIGH FUNCTIONING BOARD

Govern With®

Eight Best Practice Strategies to Prevent Cyber Attacks

WEBINAR

MAY 25TH, 2023

Today's Presenters

Webinar Host

Wes Ward
(Intensely Curious)

Govern With®

Governance Expert

Fi Mercer

Govern With®

Cyber Expert

David Rudduck

solis

PRESENTER BIOGRAPHY

Cyber Expert

David Rudduck

solis

Current:

- CEO - CFC Security Australia Aon Risk
  - Solis Security: Advisory, Security & Response
  - CFC Response: Forensics and Response to CFC insurance policy holders

Background

- Founded ‘Insane Technologies’ - Jan 2000
- Acquired CFC - April 2021
- Merged with Solis Global - Oct 2022

Education

- CISSP, GCFE, GCFA, GCFE

Passionate about empowering Boards & Executives with the knowledge to make informed decisions

PRESENTER BIOGRAPHY

Governance Expert

Fi Mercer

Govern With®

- CEO & Founder GovernWith
- **GovernWith**: Next Generation Governance Review, Director Capability Development and Board Succession service
- **Specialist Skills**: Highly regulated, government funded, not for profit industry sectors
- **Education**: Entrepreneurship, innovation and venture capital studies, Haas Business School, Berkeley (Silicon Valley)

Biggest Director Capability Gaps

Director Capability Gaps

Capability	Director Result	Skills Category	Impact Level
ICT Strategy & Governance	**27.52%**	**Contemporary**	**High**
Data Analysis	27.59%	Contemporary	Medium
Safety	34.59%	Contemporary	High
Culture	37.00%	Contemporary	High
ESG Skills	**39.71%**	**Contemporary**	**High**

"What Capability has the potential to disproportionately negatively impact your organisation the most?

AGENDA

1. **Communicating Cyber Risk to the Board**
    a. The Problem
    b. Quantifying Cyber Risk
    c. Cyber Security Frameworks (**Essential Eight & ANOTHER**)
    d. The Role of the Board
2. **Challenges**
3. **Case Studies**

BOARD GOVERNANCE

Cyber Security is a Board Responsibility

PART ONE: THE PROBLEM (THE LANGUAGE)

Communicating Cyber Security Risk to the Board

I.T. DEPT

We Need More Resources

THE BOARD

Why More? Risk Level?

BUDGET

PART ONE: THE PROBLEM

Latitude

1. **Stolen credentials** used to access personal data from two service providers.
2. **Overcollection and retention of data** and associated privacy issues (retained data went back to 1995).
3. **Legal and regulatory implications** – OAIC, AFP investigating + class-action underway
4. **Nature and type of data stolen** – personal information and sensitive identification documents for up to 14m individuals.
5. **Sensitivity of data and impact on customers** – high risk of fraud.

Medibank

1. **Data stolen** – personal information, highly sensitive health, medical records, claims information that can't be replaced.
2. **Destructive extortion actions** undertaken by ransomware group (REvil).
3. **Financial impact** – no cyber insurance, set aside $35M, class-action payouts, penalties, ASX trading halt, impact on share price/market cap.
4. **Legal and regulatory implications** – Multiple class actions underway. Changes to Privacy Act (1998). APRA investigation. Directors' liability concerns.
5. **Reputational damage and PR/Comms** failures.

Optus

1. **Potential IT risk assessment and** project governance failures and criticism of Optus' data security practices
2. **Overcollection and retention** of data and associated privacy issues.
3. **Reputational** damage and **financial impact** – CEO expects $140M of losses, customer churn, future revenue loss, and liabilities.
4. **OAIC investigation underway** and incident sited as reason why *Privacy Act* penalties amendments were urgently needed.
5. **Legal implications** – multiple class-actions underway. Triggered fast-tracked legislative changes.

PART ONE: QUANTIFYING THE RISK

Revenue Impacts

'10 percent of Optus customers leave' following the Optus cyber attack which impacted 9.8 million customers.

The Australian

56 percent of customers consider **"changing telcos** as a direct result of the Optus cyber attack"

EFTM Mobile Phone Survey

Identity Document Costs

$193 cost to replace a passport for the time remaining on an existing passport.

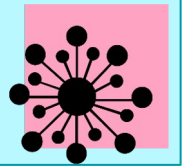
$308 cost to obtain a 10-year replacement passport.

The cost to replace an Australian drivers licenses typically ranges from **$22** to **$42.60** per license.

Regulatory and Civil Liability

Maurice Blackburn, Bannister Law and Centennial Lawyers have united to run a complaint against **Medibank.**

Compensation could range between $500 and $20,000.



Government Fines

Proposed fines of $50 million, 3x the value of the misuse of the information, or 30% of company's adjusted turnover. Whichever is the greater.

‘NON I.T.’ CYBER RISKS RECAP

1. Reputation
2. Balance Sheet
3. Core Business Disruption

BOARD GOVERNANCE

Cyber Security Risk Mitigation Frameworks

Govern With®

BOARDROOM PLUS

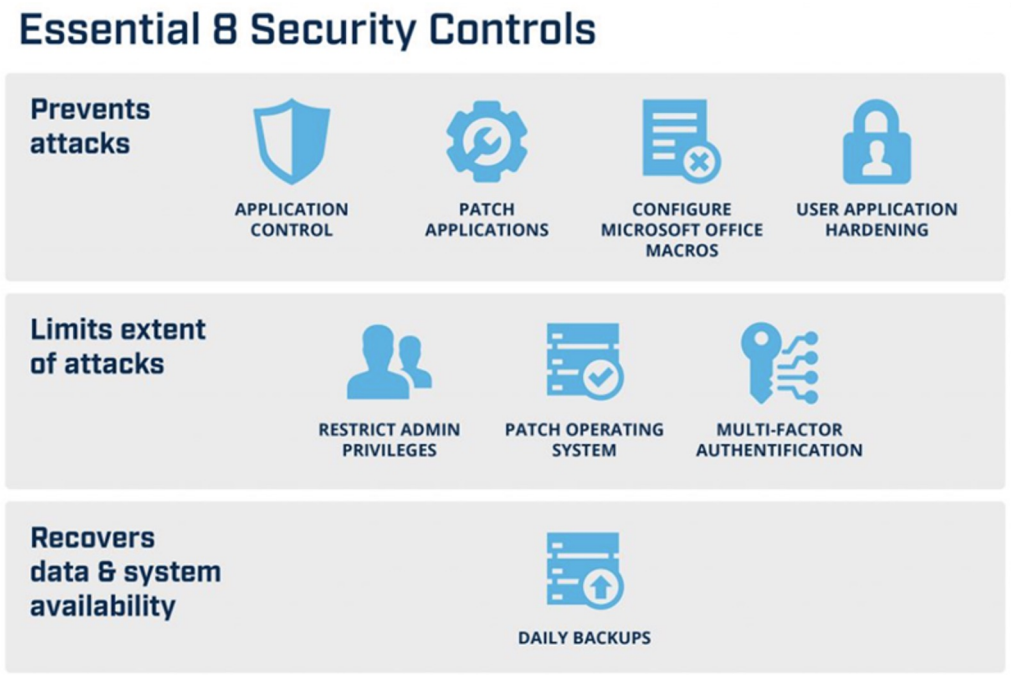
THE ESSENTIAL EIGHT FRAMEWORK

The ESSENTIAL EIGHT

The Essential 8 consists of eight essential mitigation strategies, or technical controls, designed to help organizations mitigate or prevent cybersecurity incidents.

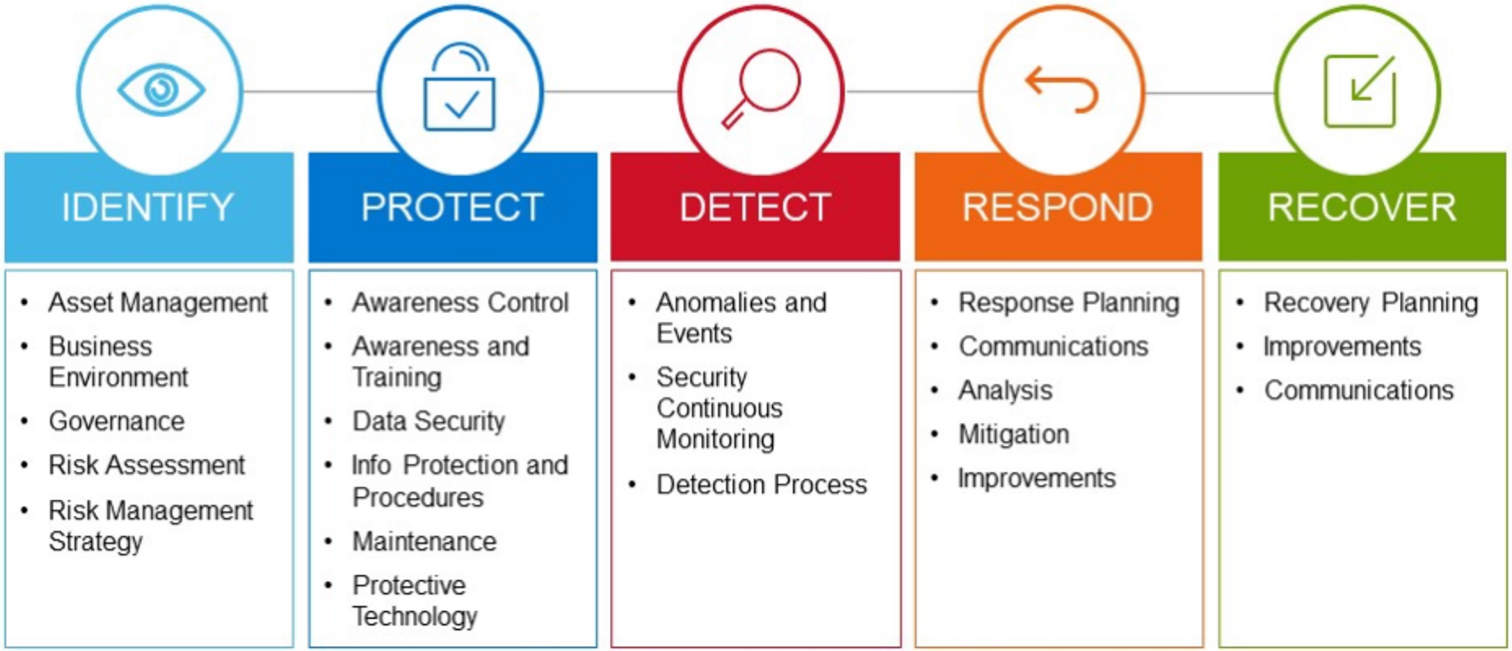
These strategies cover three key areas – **prevention, limitation, and recovery** – ranked by a maturity score from Level 0 – Level 3.

Very popular in defence and government, difficult to implement in most commercial enterprises.



NIST CYBER SECURITY FRAMEWORK

National Institute of Standards & Technology



NIST CYBER SECURITY FRAMEWORK

National Institute of Standards & Technology (NIST)

1. US Framework
2. Based on existing standards, guidelines and practices
3. Clear Categories and Functions
4. Vendors are using it to help buyers

BOARD GOVERNANCE

1. No Board Capability
2. No knowledge of the Basics
3. No Cyber Model

WHY BOARDS ARE FAILING TO MANAGE CYBER RISKS

CHALLENGES: FAILING ORGANISATIONS

- Do Nothing: Business as usual. *“She’ll be Right”*
- Skipping the Basics…. *No MFA, Password Phrases*
- Information Governance… *?*
- Don’t Practice:
  - Do you have an **Incident Response Plan (IRP)**?
  - When did you last test it with a **cyber incident simulation** (tabletop exercise)?

CHALLENGES: BRING YOUR OWN DEVICE (BYOD)

CHALLENGES: SUPPLY CHAIN

SUPPLIER HACKED

14 million users
$50MM Class Action

Latitude Financial Services

CLIENTS HURT

JB HI-FI
Amart
UltraTune
Harvey Norman

GO ANYWHERE®
File Transfer Software

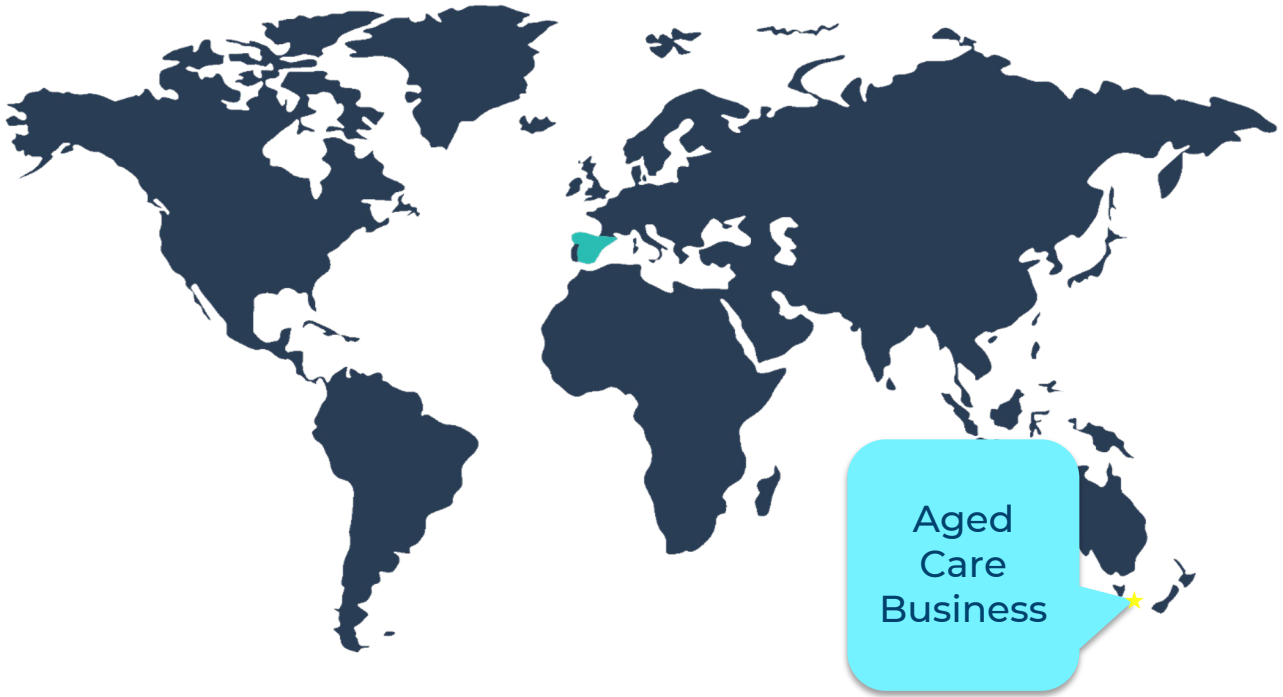
RioTinto

CYBER GOVERNANCE MODELS

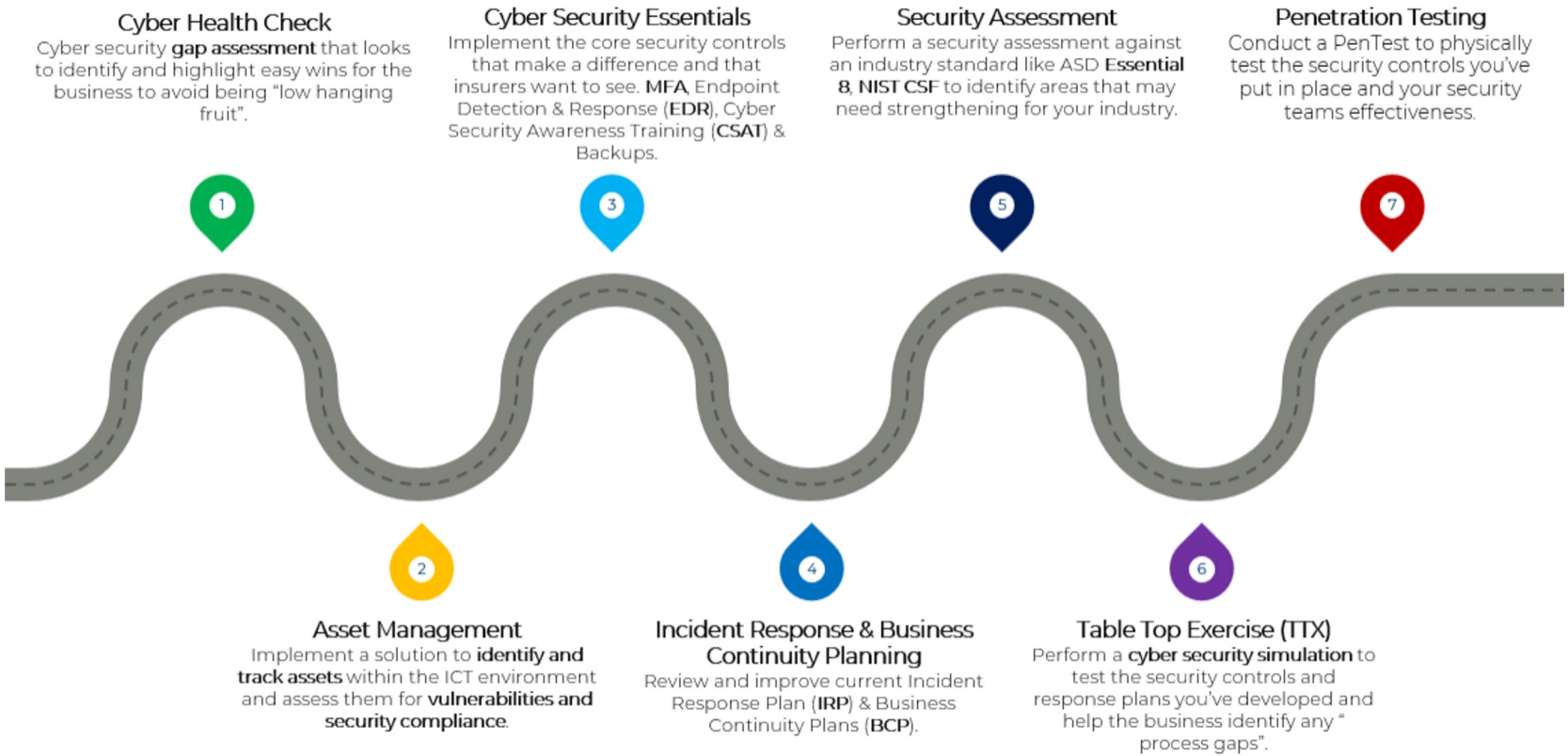
LARGE AND SMALL ORGANISATIONS

1. Add ‘Cyber’ to Risk Committee
2. Standing Board Agenda Item
3. Dedicated Cyber Sub Committee
4. Shared Cyber Committees

CASE STUDIES: AGED CARE



SOLIS: The Cyber Security Roadmap



CYBER GOVERNANCE TIPS

1. Cyber Security sits with the Board
2. All Board and Executive should up skill in Cyber security to know and check in that these 8 things are being done
3. Recruit directors with cyber skills
4. Cyber Security needs to be a strategic pillar
5. Do scenario planning about cyber-attacks and the consequences
6. Have a Cyber Board Sub Committees to lead on the expertise and advise
7. Cyber needs to become a standing item on the Board agenda
8. Start each Board Meeting with a Cyber Security Story from representatives from around the organisation and how it effects safety and quality of care

GOVERNANCE

insights sessions

data driven
informal q&a
conversational

EXPAND THE CONVERSATION

Governance Fireside Chat

GovernWith.com/insights-session

HOW TO RESPOND TO AN ATTACK

Thursday, June 29th, 11am