5 DECEMBER 2024

Cyber exposure in the digital world: Preparing for the holiday season and 2025.

Gow-Gates

emergence

cyberSuite

Speakers

Marie D'Have
Team Manager, Executive and Professional Risks | Gow-Gates Insurance Brokers

As Team Manager of Gow-Gates' Executive and Professional Risks team, Marie oversees key Financial Lines for the Corporate and Risk Solutions division, ensuring comprehensive coverage and risk management strategies for clients. Marie brings a strong legal and insurance background, having spent six years as a qualified lawyer in Belgium before transitioning to the Financial Lines team at Marsh in Belgium and subsequently in Australia.

Alexander Kerti
Business Development Underwriter | Emergence Insurance

Alex has experience working in national and global organisations in the digital/tech/software industry.

He is passionate about spreading cyber awareness and helping organisations build cyber resilience.

Alex naturally believes that insurance and cyber security are a necessary partnership for any business operating in 2024.

Cris White
Head of Cyber Advisory | CyberSuite

Chris is a seasoned cyber security expert with two decades of experience, 20 years military planning and operations experience leading crisis management teams and coordinating risk management programs. Chris has experience running military wargaming scenarios and cyber tabletop exercises for boards, organisations, and government entities. Also in managing strategic and organisational risk, with the aim of building cyber resiliency across Australian businesses of varying sizes.

Welcome

> Cyber threat landscape in Australia
> Insights and claims data
> Common threat vectors
> Demystifying insurance
> How to prepare for 2025 and beyond

emergence

Defining cyber & cyber events in Australia.

Overview

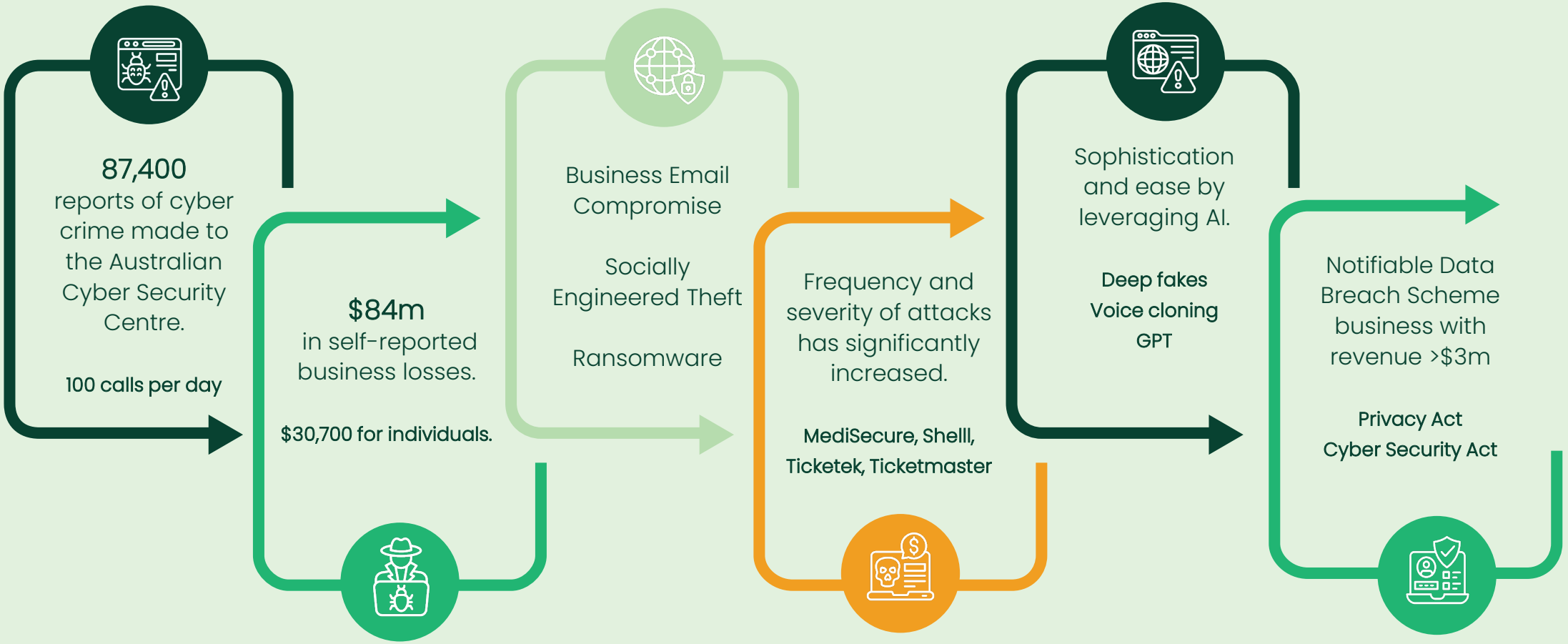
Defining Cyber

- A cyber event is defined a malicious attack, unintended disclosure of, or unauthorised access to your digital systems, data or technology.
- Successful attacks or breaches lead to devasting business interruption, loss of data, financial damage and reputational harm.
- Events are drastically increasing in Australia, both in frequency and in severity.
- Cyber events are currently dominating Australian headlines as we're viewed to be low hanging fruit.

- **Canva** – 139 million customers had PII stolen.
- **Latitude** –$76m in losses and 14 million customers affected.
- **Optus** –$140m in losses and 9.8 million customers affected.
- **MediBank** - $125m in losses and 9.7 million customers affected.

Australian Signals Directorate FY24

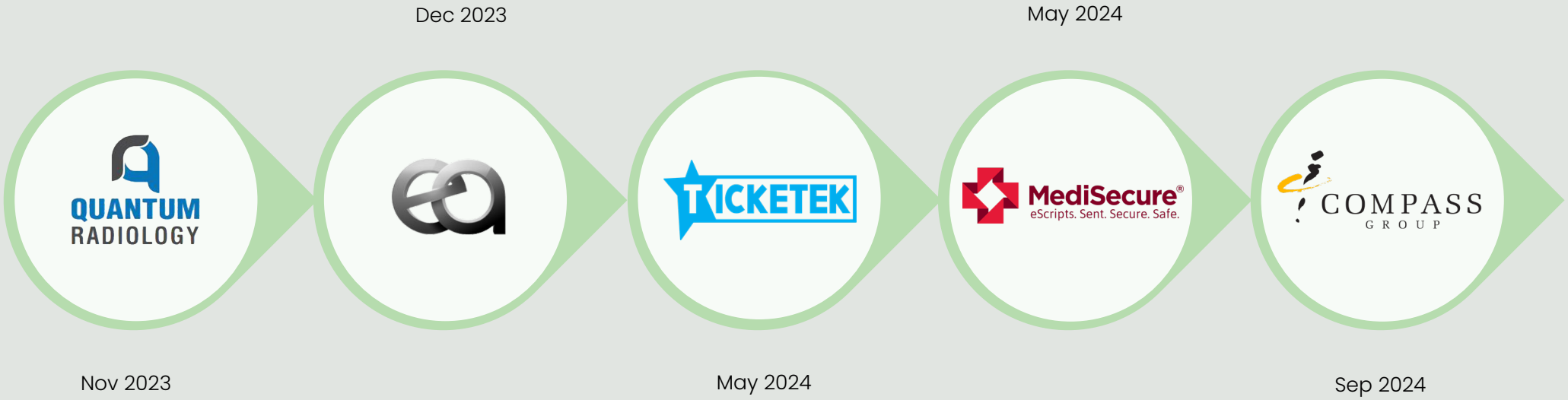
Cyber Events in Australia



emergence

2023 → 2024

Recent events in Australia



emergence

Emergence Data

Claim Trends

Claim Count

Dec 22 - 23

125%

Business Interruption

Ransomware

77%

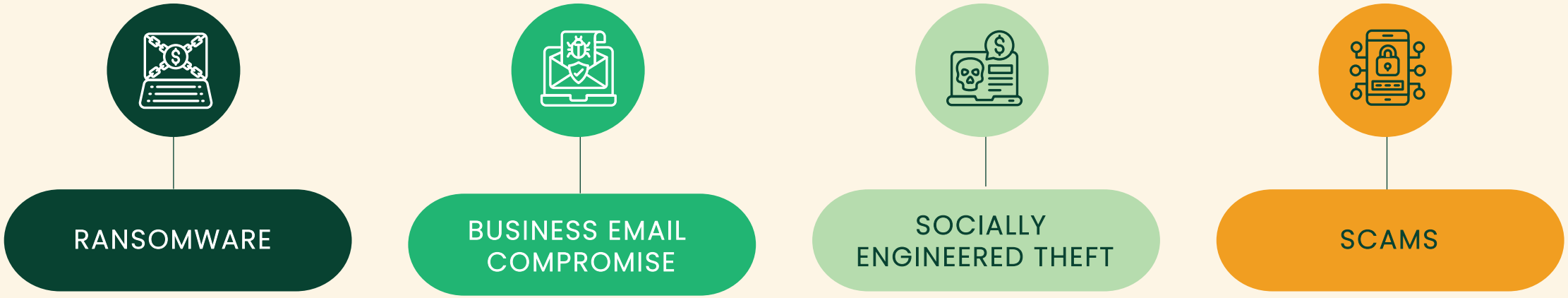
Policy Coverage

Response costs &
Business Interruption

85%

emergence

Threat Landscape



emergence

ANY AGE, ANY LOCATION, ANY TIME

who's responsible for these attacks?

ORGANISED CRIME
Solely focused on maximizing profit, this is the largest growing problem faced globally

NATION STATES
Hack for the global advantage they can give their country

SCRIPT KIDS
Hack for fun or fame with the skills to inflict harm

HACKTIVISTS
Hack for political elections and social reasons

INSIDERS
Internal employees who steal and sell information

emergence

How I would hack you...

Business Email Compromise

- Gain access to your email
- Scam your suppliers or clients

Socially Engineered Theft

- Phishing, vishing, other social engineering techniques
- Convince you or your staff to pay money

How to prevent cyber incidents

- Multi-factor Authentication
- Cyber Awareness Training
- Password Hygiene
- Update your software and devices
- Backup your critical data
- Have an Incident Response Plan

emergence

Demystifying cyber insurance, and how cover responds.

Cyber insurance

Section A - First Party Losses

Losses that directly affect the insured's business:

- Business interruption
  - Reduction of revenue or increased costs of working
- Ransom / extortion
  - Payments to fulfill a ransom or extortion demand

Section B - Third Party Losses

Claims made against the insured's business due to a cyber event:

- Legal expenses including defence costs, settlements, awards and damages.
- Multimedia injury or PCI liability
- Civil fines and penalties
- Regulatory fines and penalties

Section C - Response Costs

Costs associated with the management and remediation from a cyber event:

- Crisis management
- PR, legal, communications
- Data securing and restoration
- Virus extraction
- Notification to affected individuals and businesses

emergence

Additional covers

Criminal Financial Loss

- Socially engineered theft
- Push payment theft
- Financial theft

Tangible Property

- Replacement of tangible property that has been impacted or damaged due to a cyber event.

Non-IT Contingent Business Interruption

Impact on business costs

1. A supplier outage; or
2. A supplier system failure

Directors & Officers

- Covers the director's personal liability arising out of a cyber wrongful act in your business.

emergence

Notification Requirements

NDBS

- Unauthorised access to, or unauthorised disclosure of personal information about one or more individuals
- >$3m must notify OAIC within 30 days of breach
- Must conduct full assessment of impact
- Must inform each individual impacted or compromised

Fines & penalties

- Minimum $50m
  or
- 30% of annual revenue
  or
- $420k per individual affected
- Invasion of privacy - max remedy of $478k
- Civil penalties - $3.3m per contravention
- Infringement notices – up to $66k

Business impact

- Immediate decline and halt of revenue
- Reputational harm
- Counter legal pursuits
- Post incident restoration
- Legal and notification costs
- Ongoing revenue impacts

Ransom payment

- Must conduct sanction check on threat actor group
- Negotiate ransom payment
- Facilitate bitcoin transaction
- Receive decryption key and commence restoration
- Post incident remediation and planning
- Media statements / rep harm

emergence

Claims &
Incident response

Ransomware

$16m revenue

Incident Details

Staff member couldn't log in and noticed ransom note on the computer.

IT confirmed ransomware attack had been deployed and entire IT network inaccessible.

Insured immediately called the Emergence hotline.

Triaged with the CEO, CFO and MSP immediately.

Forensic retained and brought into the triage call.

Identified to be a Zero Day Citrix Netscaler Vulnerability.

Negotiations

Demanded $400K USD ransom.

Professional negotiator engaged.

Requested proof of files while assessing the file-tree.

Unable to recover from back-ups – entire environment ceased and extracted.

Sanction check on Qantam and recipient wallet.

Ransom amount agreed and payment facilitated.

Decryption key provided, restoration process commenced and systems rebuilt.

Final Claim

IT Forensics = $50,750

Legal Counsel = $50,000

Public Relations = $15,700

Ransom + Negotiator = $405,000

Total Claim = $520,000

Data restoration policy

Data protection policy

Incident Response Plan

Business Email Compromise

$30m revenue

Incident Details

Internal staff member received an email which appeared to be from a director. The email had a file attached - clicked on the file but nothing downloaded.

This was a malicious file which allowed the threat actor to gain access to their mailbox.

Threat actor moved through the business' mailbox and harvested all key client details.

Impersonating the staff member, they sent updated bank details attached with invoices to all clients.

Accrued $290k in payments in one week. Submitted second invoices which were being paid, until one person called the business to confirm works prior to paying.

Steps Taken

Insured immediately called Emergence hotline. Triage with CEO and IT contractor.

All sites were shutdown until investigation was completed.

Forensics entered their network and identified the staff member had been compromised weeks prior.

Emergence had to rebuild their entire network and secure their mailbox environment.

Legal counsel retained to provide extensive privacy advice, notify government bodies and contractors.

Notification advice provided to all subcontractors and businesses compromised.

Final Claim

Forensics - $15,000

Legal Counsel – $20,000

Public Relations – $8,000

Reimbursement - $250,000

Total Claim = $293,000

Section C & D

Cyber event response costs

Criminal financial loss

emergence

Be prepared for holiday season and throughout 2025.

Tips for holiday season

Attacks

- Stay vigilant against targeted scams and invoice fraud
- Be wary of urgent or unusual requests

Staff Changes

- Reduced staff availability
- Staff with new and additional responsibility

Preparation

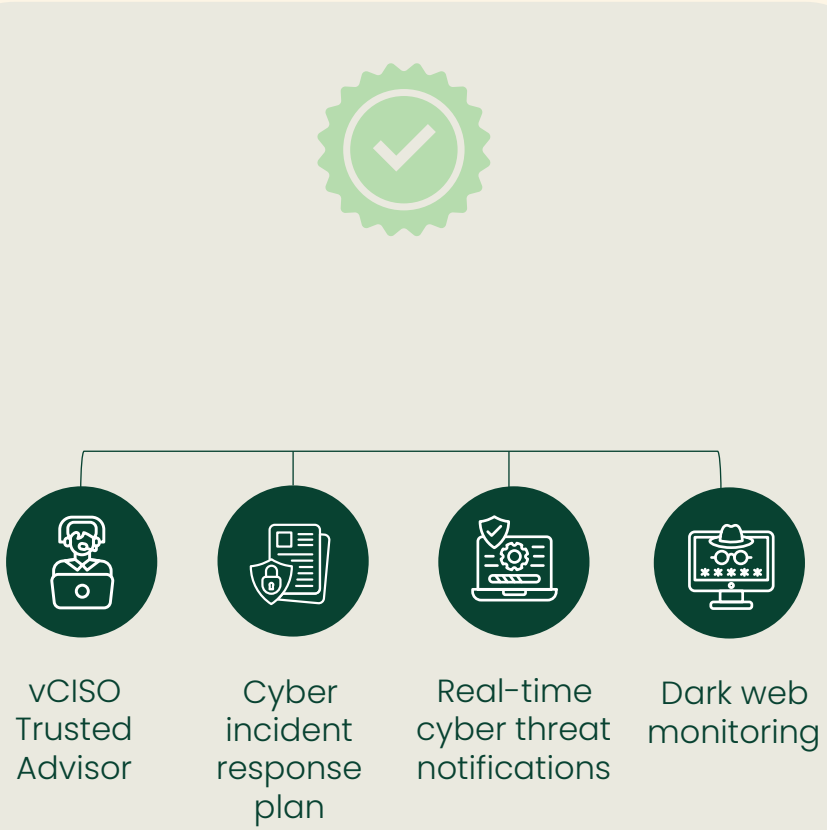
- Review Incident Response Plans
- Remind staff of what to look for and how to respond

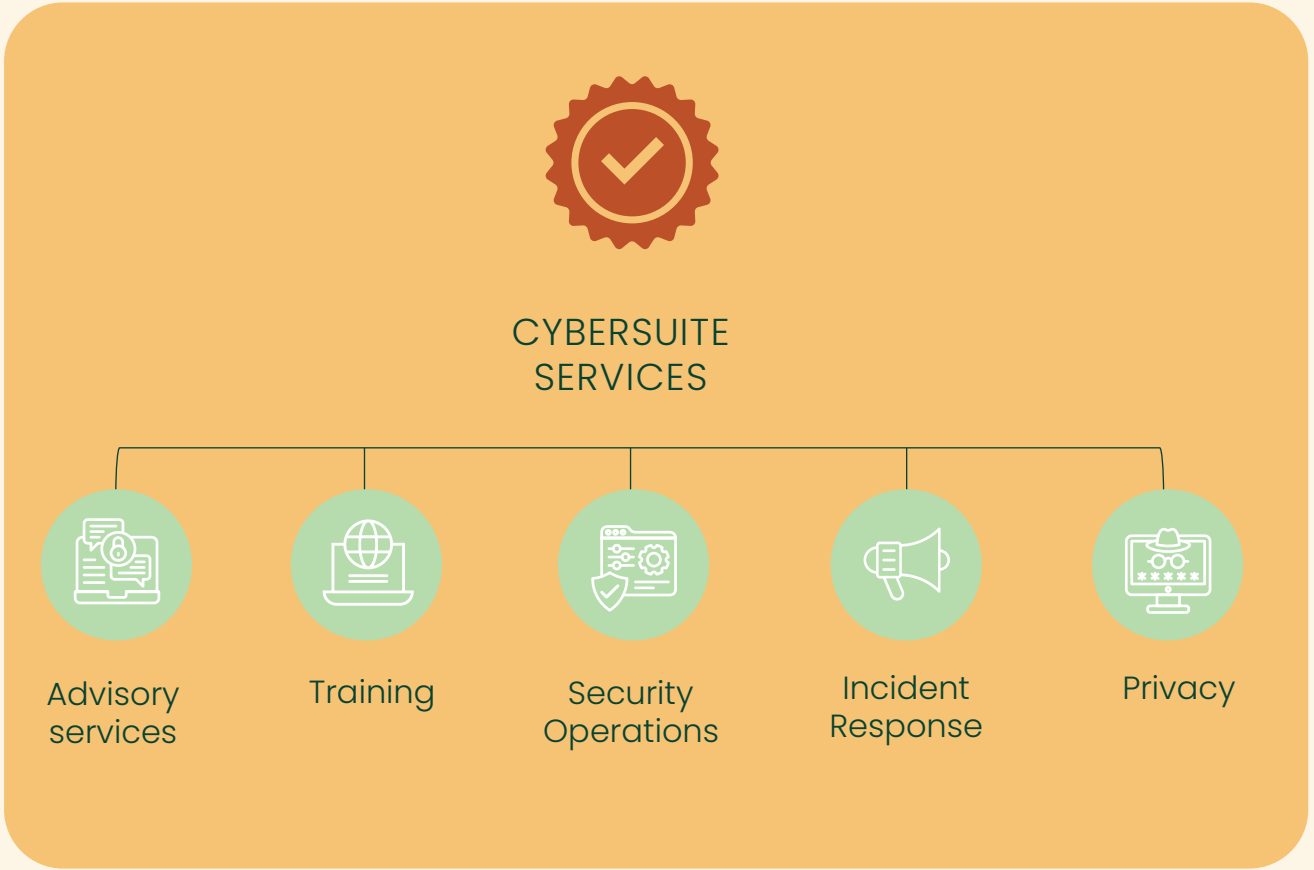
Plan ahead

Be cyber secure in 2025

- Regulatory changes: Cyber Security and Privacy Acts
- Understand the what data is your responsibility
- Run a digital fire drill – tabletop exercise
- Put key controls in place:
  - MFA
  - Patching (Updates)
  - Strong passwords
  - Offline backups
  - Incident Response Plan

cyberSuite





emergence

Thank you

Cris White

Head of Cyber Advisory

Marie D'Have

mdhave@gowgates.com.au

+61 400 992 911

Alexander Kerti

Business Development Underwriter

Questions