



Navigating the Digital Highway

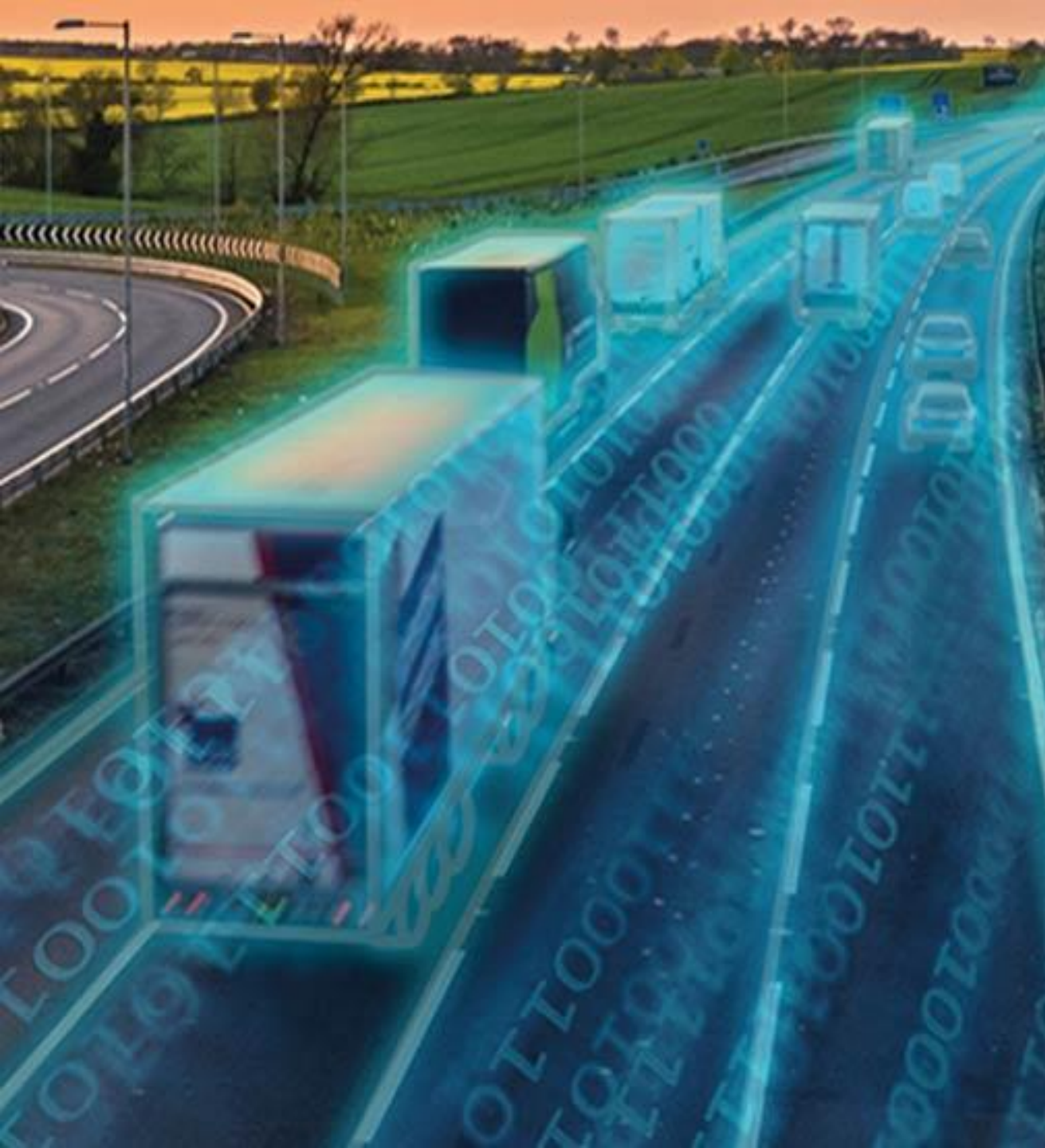
Katrina Hickson

Head of Distribution, Emergence Insurance

emergence



NATROAD



Cyber Risks, Supply Chain Vulnerabilities, and Essential Safeguards for the Transport Industry

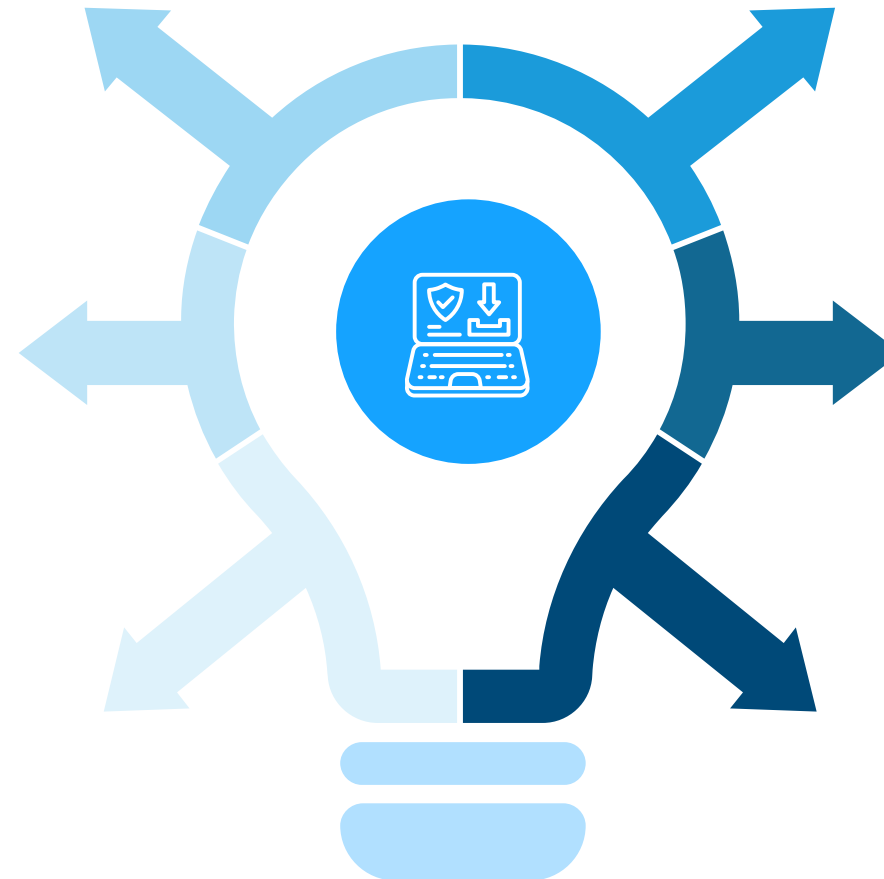
- Digital transformation
- Growing cyber threat landscape
- Supply chain vulnerabilities & ripple effects
- Key Cyber Risks for the Industry
- Cyber Event Claim Example
- Voicemail from a real Cyber Criminal
- Essential safeguards

Digital Transformation of the Transport Industry

Real-time fleet
management systems

Electronic Work Diary
(EWD)

Predictive maintenance



Route optimisation –
sustainable practices

Data-driven decision
making

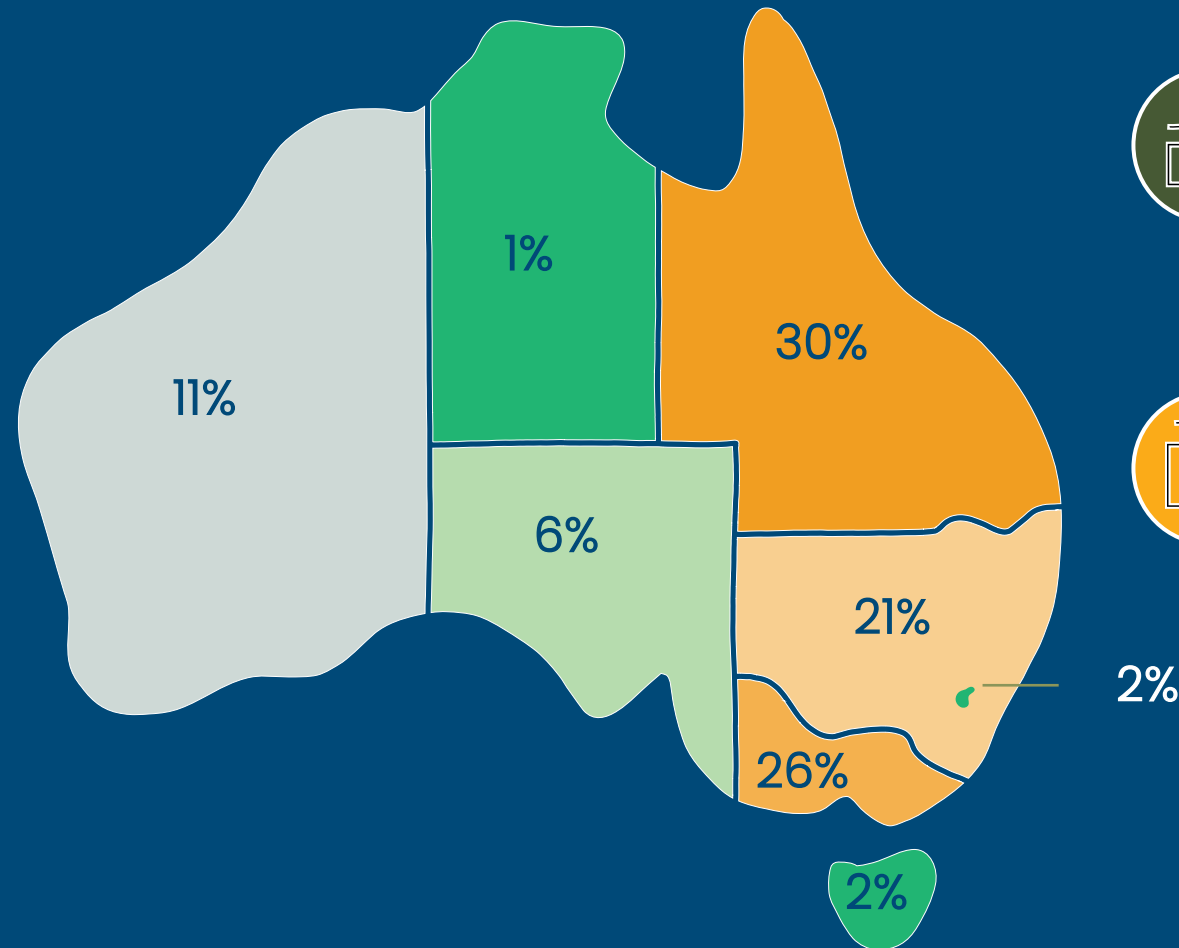
Warehouse automation

Growing cyber threat landscape



FY23 Australian Statistics

- 94,000 cybercrime reports
- Up 23% on prior year
- Average a report every 6 minutes
- Transport accounted for 21% of 'critical infrastructure' reporting entities
- Email Compromise and Business Email Compromise highest reported events
- 10% included Ransomware



Queensland and Victoria report disproportionately higher rates of reporting



New South Wales reported highest average losses

Cybercrime is a multibillion-dollar industry



\$8 TRILLION USD
Est. Globally

Loss of revenue

Increased costs of working

Reputation damage

Cyber event response costs

Notification costs and monitoring



\$3.5 BILLION AUD
Est. Australia

True figure could much higher due to underreporting

Business email compromise, Ransomware and fraud all contribute



TYPES OF CYBER CRIMINALS

Nation State
- Hack for their country

Organised Crime
- Hack for profit

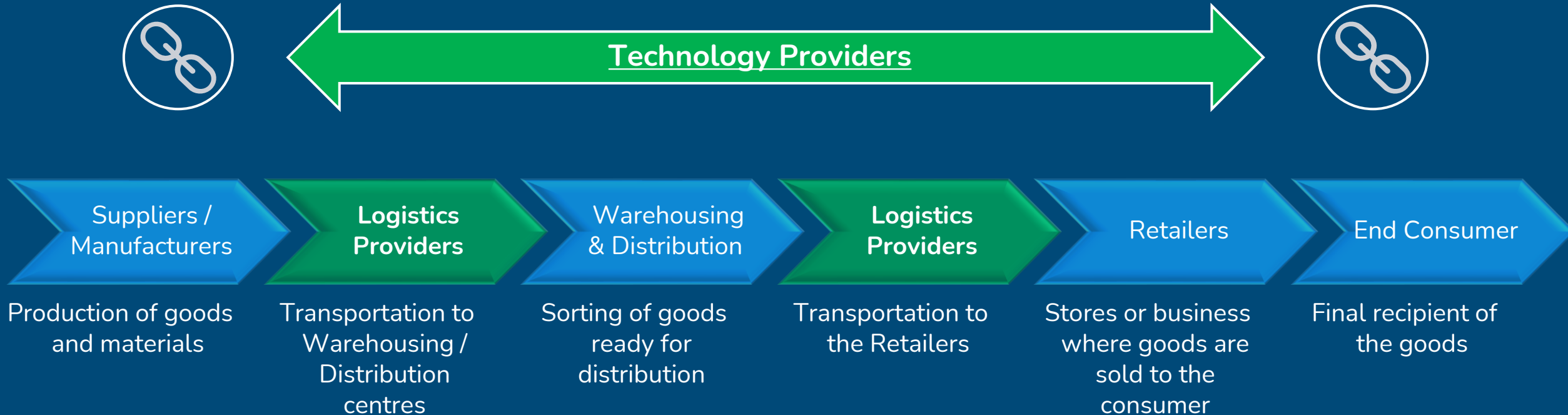
Script Kids
- Hack for fun/fame

Insiders
- Internal employees

References:

CyberSecurity Ventures, leading research firm in cybersecurity industry,
Australian Cyber Security Centre, The Office of the Australian Information Commissioner,
Australian Institute of Criminology

Supply Chain Vulnerability in the Transport Industry



Ripple effects - upstream and downstream cyber event



Key risks for the Transport Industry



RANSOMWARE
ATTACKS



SUPPLY CHAIN
VULNERABILITY



DATA
BREACHES



CYBER
EXTORTION



SOCIALLY
ENGINEERED THEFT



IoT CONNECTED
VEHICLES



HACKING/
CRIMEWARE



INSIDER AND
PRIVILEGE MISUSE



DENIAL OF
SERVICE (DOS)

Cyber Event Claim Example



Background

- Turnover: \$7.1m p/a
- Policy limit: \$1m
- Excess: \$2,500
- Indemnity Period: 30 Days

Who was it?

- Industry – Transport & Warehousing
- Head office – Queensland

What happened?

- Insured logged into system and was greeted with a ransom note
- Access to their systems were denied
- The Ransom note informed them that their files were locked and they would need to pay a ransom to retrieve their data
- A Chatbox was downloaded by the Cyber Criminal to negotiate the ransom

How was it fixed?

- Data recovery costs
- With difficulty...
 - Data eventually accessed, decrypted and restored some data
 - Large amount of historical data had to be manually reconstruction requiring 3 temps for 28 days
- No exfiltration of data
- Included recommendations for the insured to implement more robust cyber security

How was it covered?

- Cyber Event Response Costs
- Loss of revenue
- Extra operating expense

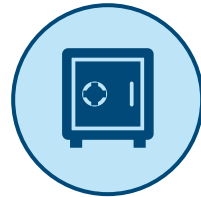
Final outcome

- Claim total bill **\$215,000**
- Predominantly loss of revenue
- Substantial Response Costs
 - IT vendors, system replication
 - Data recovery
- Legal Expense

Essential Safeguards – Low Cost Big Impact



Speak to your IT
Provider about
Cyber Security



Offline Backups



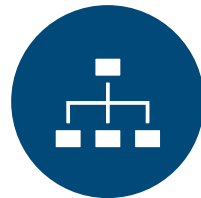
Regularly test back
ups



Implement Multi
Factor
Authentication



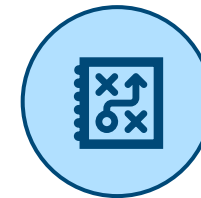
Employee
awareness training



Principle of least
privilege



Stay up to date –
patch regularly &
often



Develop a
response plan for
Ransomware



Get in touch

Noel Kelly

AEI Insurance Broking Group

0466 900 134

noelk@aei.com.au



NATROAD