

CENTREPOINT  
ALLIANCE

---

# CYBER RESILIENCE

NOVEMBER 2023



# AGENDA

- Learnings from Centrepont Cyber Incident
- Learnings from Security in Depth
- Actions to take following a cyber incident

# LEARNINGS FROM CYBER INCIDENT

---



# FRAUDULENT WITHDRAWAL FROM CLIENT SUPER - HOW DID IT HAPPEN?

---

- The adviser received an email from a digital signature provider (fake DocuSign) that he used frequently.
- The adviser clicked on the link, was redirected to an Office365 login. The adviser entered their account information.
- The adviser also entered their Multi Factor Authentication (MFA code) when prompted.
- Nothing happened and the adviser forgot about it.
- The bad actor now had access to the adviser's email including the cookie for their MFA.
- The bad actor located a withdrawal form for \$20,000 on an old email. Not password protected.
- The bad actor created a fake email account similar to client's email. For example instead of [Joe@Smith.com.au](mailto:Joe@Smith.com.au) it was [Joe@Smiths-au.com](mailto:Joe@Smiths-au.com)
- The bad actor then sent an email to the adviser requesting withdrawal of \$250,000 stating 'As discussed earlier' and then forwarded that email to the Client Services Officer (CSO)
- The bad actor deleted the emails so the adviser was not aware of the activity.
- From this point the bad actor dealt with the Client Support Officer (CSO) directly using the information gained in the adviser's email. The adviser was not aware of any emails.

## SUPPORT STAFF ACTIONS

---



- The CSO received the email from the adviser and assumed the adviser had spoken with the client.




- The CSO emailed the withdrawal form to the client, replying to the email trail.



- The fake client requested a change of bank account for the payment, which the CSO arranged.



- Immediately after the first withdrawal was successful the CSO received a second request directly from the client requesting another \$250,000 withdrawal.



- The office manager then emailed the client to confirm the withdrawal using the client's email address obtained from their CRM.

# PROCEDURAL AND TECHNICAL WEAKNESSES

---

- The CSO **assumed the adviser had verified** the withdrawal with the client
- The CSO **didn't check the email address**
- There was **no discussion** between the CSO and the adviser
- There were **no phone calls** between the CSO or adviser and the client
- Client **information being sent via emails**
- **Not using secure portals**
- Attachment to email **not password protected**
- The adviser was **vulnerable to a phishing** attack
- The CSO did not pick up on the clues
  - **large withdrawal amount** that was not consistent with previous client behaviour
  - **urgency** in the request
  - **change in bank details**

## RECOMMENDED PROCEDURE CHANGES

---

- Implement a **call back policy**. Always call a client to confirm email instructions.
- Don't **change bank accounts** or update contact details on instructions via email, **always call**
- Check and use the phone number and **email address from your CRM** not those provided in the email
- Keep a **file note** of confirmation phone calls
- CSO should **not act on an email** from an adviser **without verbal instructions**
- **2-person approval process** for withdrawals above \$X – verify the email address, signatures, bank account details
- **Password protect documents** attached to emails and don't put client information directly into email
- Make sure **clients know not to return unprotected documents** via email

## HOW THE BREACH WAS RESOLVED

---

- The product provider was contacted and was able to **stop the second payment immediately**. Only a portion of the first withdrawal was able to be recovered.
- The adviser **contacted their cyber insurance provider** who appointed an expert to ensure the breach was contained and to conduct a **forensic investigation**. The hacker had access for 6 days and reviewed emails containing the personal information of 25 individuals.
- All **25 clients were contacted by phone and received an email** explaining the action they should take to protect their information.
- Reports were submitted to the Australian Cyber Security Centre (ACSC) and the Office of the Australian Information Commissioner (OAIC). The OAIC were satisfied with actions taken.
- The **client was compensated**. Responsibility for reimbursement is being determined.



# LEARNINGS FROM SECURITY IN DEPTH

---



# Why Cybersecurity Matters for You

---



# Statistics



- **552,000 Cyber Crimes in the last 12 months**
- **Approximately 200 Police Officers across all states and law enforcement agencies**
- **\$3.2 Billion dollars lost**
- **\$42 Million dollars recovered**







# Cost of Cybercrime

Reported financial losses:



## STATE BREAKDOWN

WA	11.1%
NT	0.9%
SA	7%
QLD	26.1%
NSW	25.6%
VIC	26.4%
TAS	1.5%

**\$890,000**

In reported losses  
per day

**\$6,000**

average loss  
per report

**\$328**

average loss  
per report



# Where are attacks going to come from?

**OPTUS**

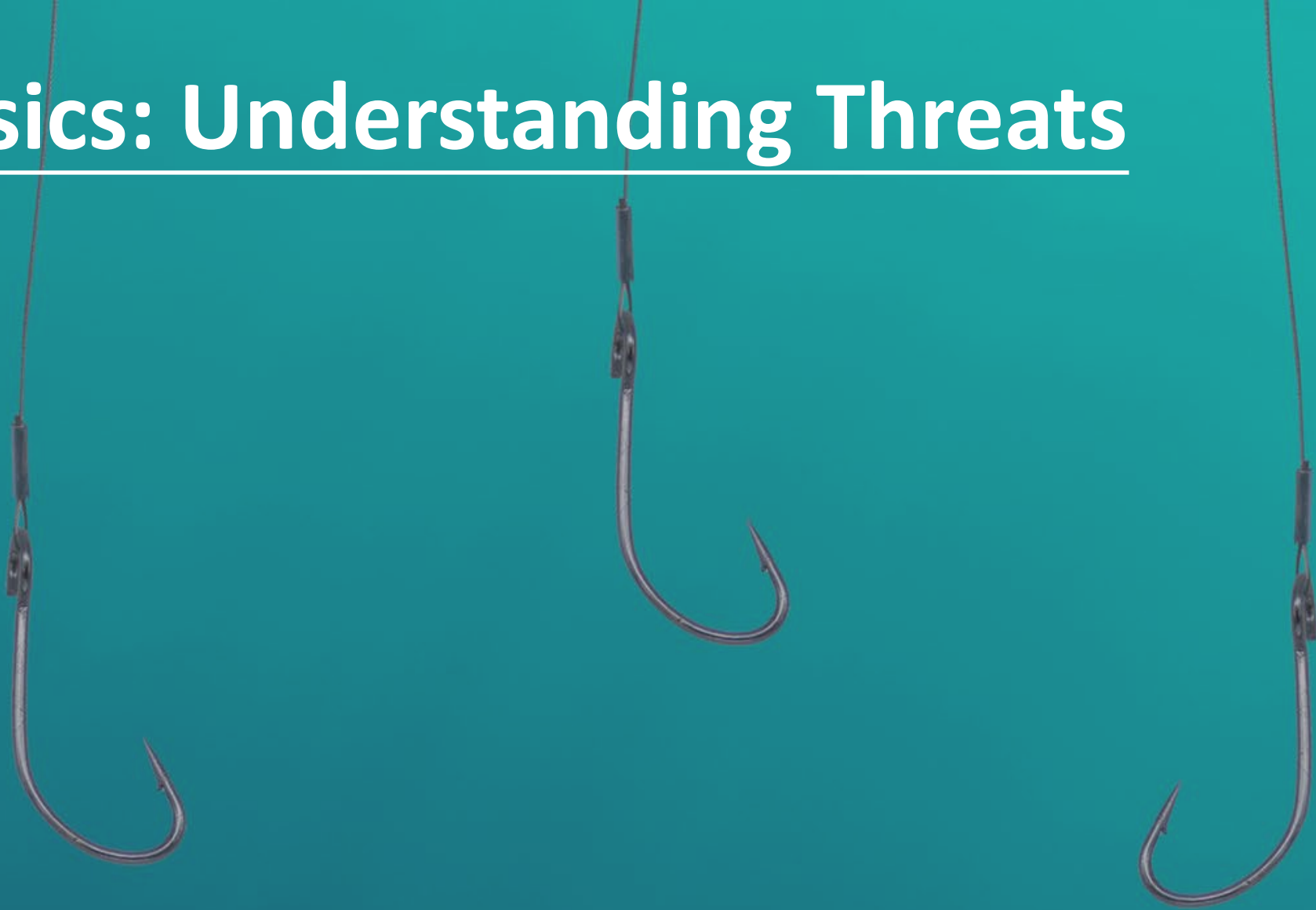
**medibank**

**LATITUDE**



# The Basics: Understanding Threats

---





# Top contact methods



**33%**

Text message

**79,835** reports

**\$28 million**

reported lost



**29%**

Phone

**63,821** reports

**\$141 million**

reported lost



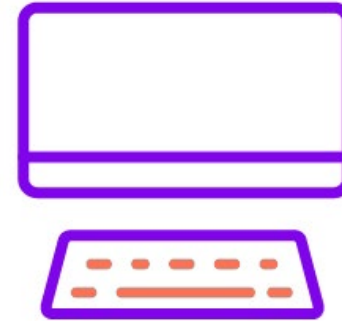
**22%**

Email

**52,159** reports

**\$77 million**

reported lost



**6%**

Email and Internet

**13,692** reports

**\$74 million**

reported lost



**6%**

Social networking

**13,428** reports

**\$80 million**

reported lost

# Top scams by loss as reported to Scamwatch



Investment scams  
**\$377 million**

Dating &  
Romance scams  
**\$40 million**

False billing  
**\$24 million**

Phishing  
**\$24 million**

Remote  
Access scams  
**\$21 million**

Threats to  
Life, arrest  
or other  
**\$13 million**

Identity theft  
**\$10 million**

Jobs &  
Employment  
scams  
**\$9 million**

Online  
Shopping  
scams  
**\$9 million**

Classified scams  
**\$8 million**

1

2

3

4

5

6

7

8

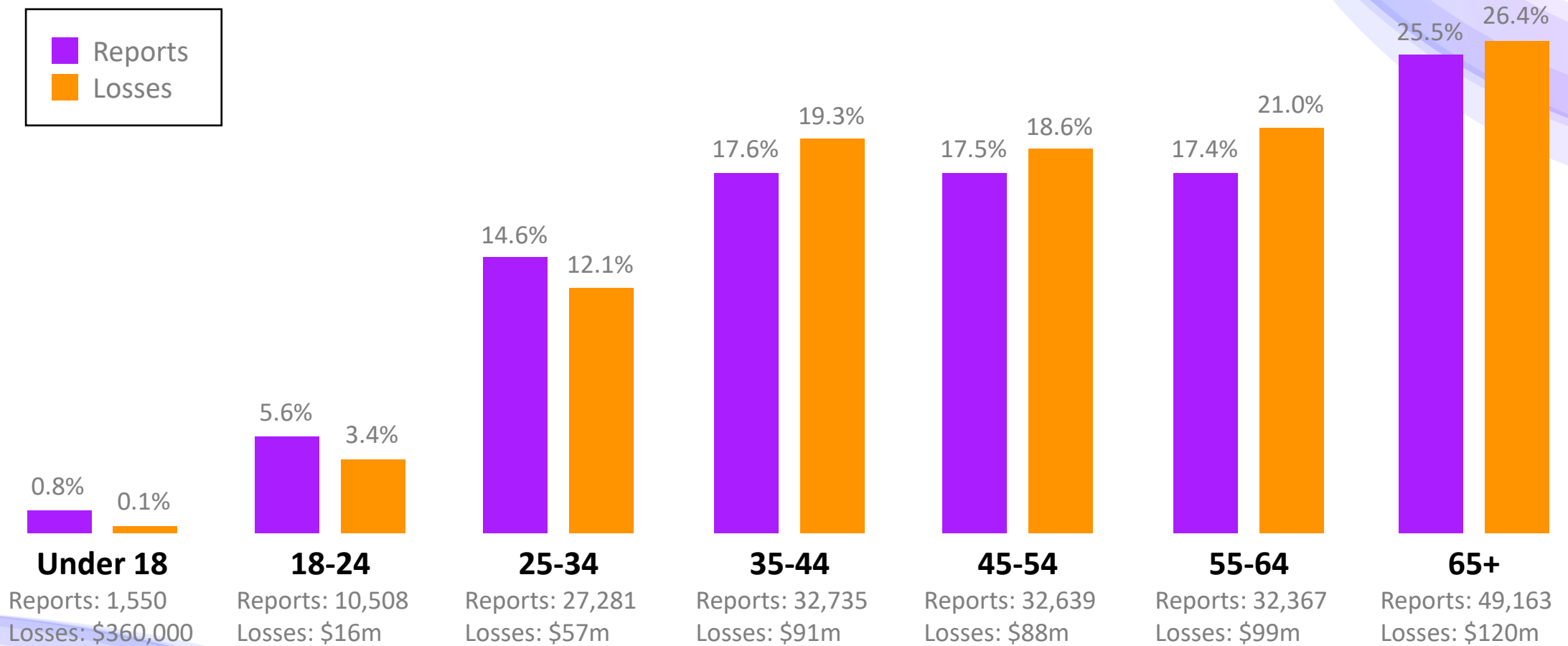
9

10





# Age – Everyone is vulnerable



# The year in review

## CAR review results from hacking

Last year we conducted 1423 CAR reviews and out of that we observed 427 practices under attack – only 8 being successful.



File **Message** Help Acrobat Tell me what you want to do

Ignore Delete Archive Reply Reply All Forward Meeting IM More

Junk Delete Archive Reply Reply All Forward Meeting IM More

Share to Teams

Vendors To Manager  
Team Email Done  
Reply & Delete Create New

Move Rules Send to OneNote Actions


Assign Mark Categorize Follow Up

Find Related Select

Read Aloud Immersive Reader Translate

Delete Respond Teams Quick Steps Move Tags Editing Immersive Language

### Please Review: Securityindepth Employees New Payroll Amendment, Paid Sick Leave And New Emergency Loan Application Process

 Securityindepth Notification <michael.connory@securityindepth.com>  
To Michael Connory

Retention Policy SiD (10 years)

Expires 20/02/2033

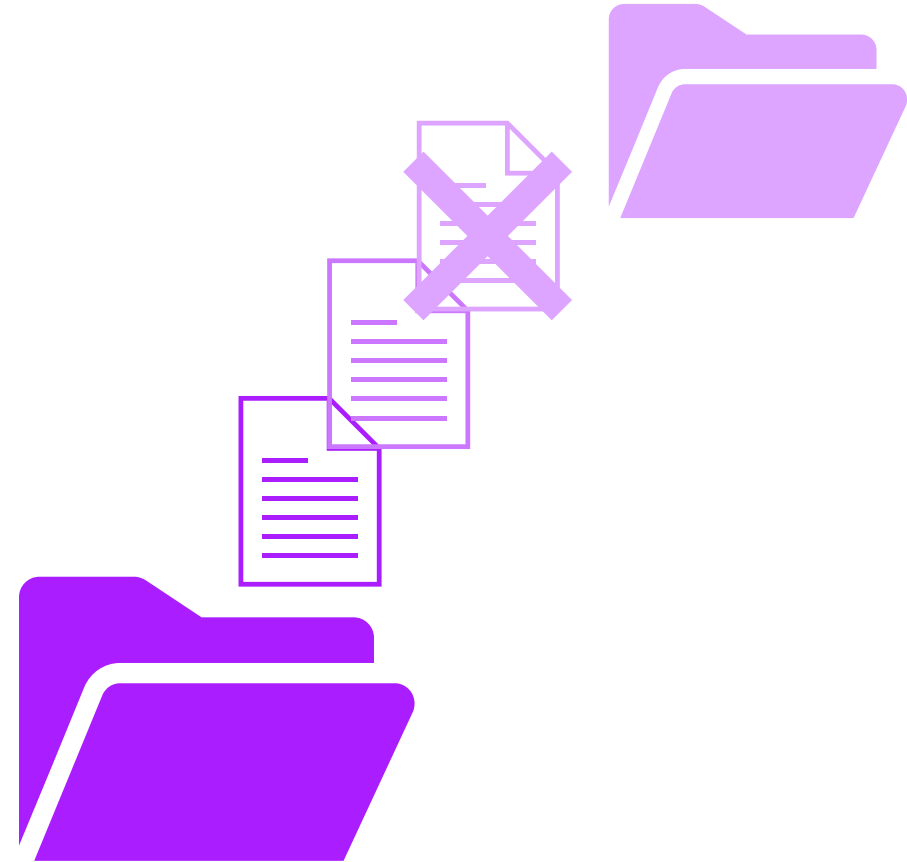
You forwarded this message on 23/02/2023 8:51 AM.

 Please Review: Securityindepth Employees New Payroll Amendment, Paid Sick Leave And New Emergency Loan Application Process  
Outlook item

**CAUTION:**This email originated from outside of the organization. This message might not be safe, use caution in opening it. If in doubt, do not open the attachment nor links in the message.



# What are the main types of cyber security threats?





# Phishing attacks

This year we have seen a significant increase in phishing attacks— last year we saw an increase of reported phishing attacks (successful) from **4744** to **6288** from June to July 2022 – mainly focusing on Tax and tax savings.....and August it continued with a slight increase to **6301**

# Cyber attacks come in all shapes and sizes...



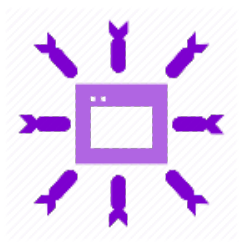
Ransomware



Phishing



Password attacks



Denial of Service



Man-in-the-middle

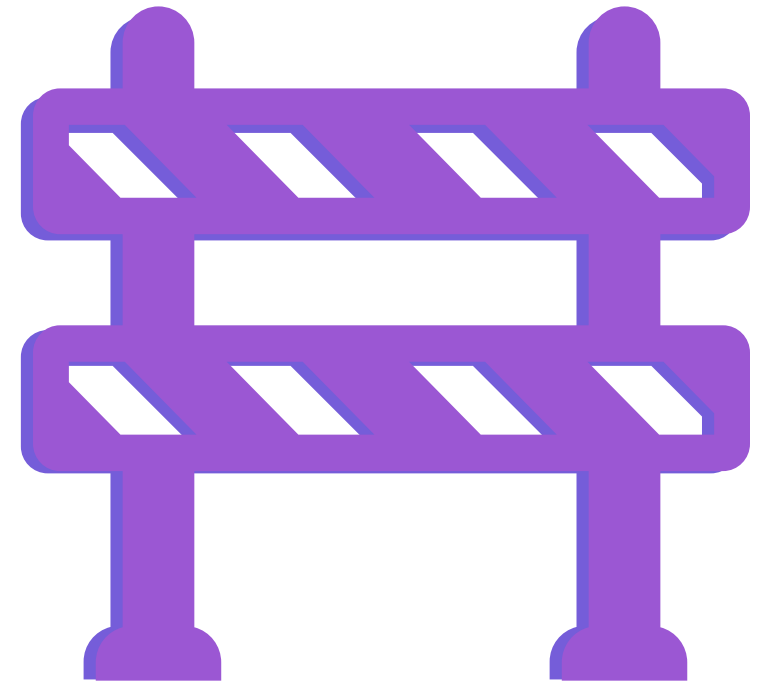


Malware



# Be Warned!

- No two incidents are identical
- No one-for-all solution, tailor it for your need
- Many types of incidents
- Focus on a hacking scenario
- But the principle remains the same!





# What can you do now?

- a. Ensure that you use MFA on all data holding applications
- b. Stop reusing passwords and start using a password manager
- c. Implement DMARC
- d. Ensure Policies and Governance is up to date
- e. Follow the standards



# HOW TO RESPOND TO A CYBER INCIDENT


---



# WHAT TO DO IF YOU HAVE A CYBER INCIDENT

---

- Immediately notify your **Licensee Privacy Officer**
- If Licensed through Centrepont, notify via [ProfessionalStandards@cpal.com.au](mailto:ProfessionalStandards@cpal.com.au) or complete [Data and Cyber Breach Notification Form](#)
- Take immediate action to contain the breach and mitigate any future breaches, including:
  - change passwords or remove security access
  - contact any impacted institutions or individuals
  - notify relevant technology services
  - notify your cyber insurance provider



**You will need technical expertise. It is important not to destroy evidence needed to investigate.**

# CYBER INSURANCE


---

## **Cyber insurance policies may cover:**

- Third party claims for failure to keep data secure
- Third party losses from funds transfer fraud and social engineering
- Reimbursement of your costs to respond to and recover from a cyber incident or data breach
- Cyber extortion costs
- Business interruption compensation

## **Additional benefits may include:**

- Incident response handling by experts
- Free security upgrades



**If you have a cyber policy, contact the provider immediately so that you do not invalidate the policy.**

# PSC INSURANCE – CYBER INSURANCE POLICY PRICING

Total Cost including charges based on VIC, WA, NT

## Option A - \$1,000 Excess

	\$	250,000.00	\$	500,000.00	\$	1,000,000.00
<\$100k		\$777.48		\$1,078.13		X
\$100k-\$250k		\$947.47		\$1,170.73		X
\$250k-\$500k		\$1,015.97		\$1,234.16		\$1,617.26
\$500k-\$1M		\$1,092.08		\$1,326.76		\$1,801.20
\$1M-\$1.5M		\$1,191.03		\$1,563.98		\$2,068.87
\$1.5M-\$3M		\$1,316.62		\$1,783.44		\$2,250.27
\$3M-\$5M		\$1,671.80		\$2,313.70		\$2,955.58

## Option B - \$2,500 Excess

	\$	250,000.00	\$	500,000.00	\$	1,000,000.00
<\$100k		\$745.48		\$1,031.10		X
\$100k-\$250k		\$906.98		\$1,119.06		X
\$250k-\$500k		\$972.05		\$1,179.32		\$1,543.27
\$500k-\$1M		\$1,044.35		\$1,267.30		\$1,718.01
\$1M-\$1.5M		\$1,138.36		\$1,492.65		\$1,972.30
\$1.5M-\$3M		\$1,257.67		\$1,701.15		\$2,144.64
\$3M-\$5M		\$1,595.09		\$2,204.88		\$2,814.67

## KEY CONTACTS

---

### PSC Insurance Brokers

#### David Withers

Managing Principal

M: 0423 489 847

E: [dwithers@pscinsurance.com.au](mailto:dwithers@pscinsurance.com.au)

#### Brooke Gunasti

Account Executive

M: 0448 765 286

E: [bgunasti@pscinsurance.com.au](mailto:bgunasti@pscinsurance.com.au)

### Security in Depth

#### Michael Connory

[www.securityindepth.com.au](http://www.securityindepth.com.au)

P: 1300 041 042

E: [support@securityindepth.com](mailto:support@securityindepth.com) or

[Michael.Connory@securityindepth.com](mailto:Michael.Connory@securityindepth.com)

CENTREPOINT  
ALLIANCE

---

**QUESTIONS**

