Cyber Security

PRESENTED BY MALCOLM HEATH | LAWCOVER

LEGAL PRACTICE MANAGEMENT WORKSHOP 18 – 20 JUNE 2024

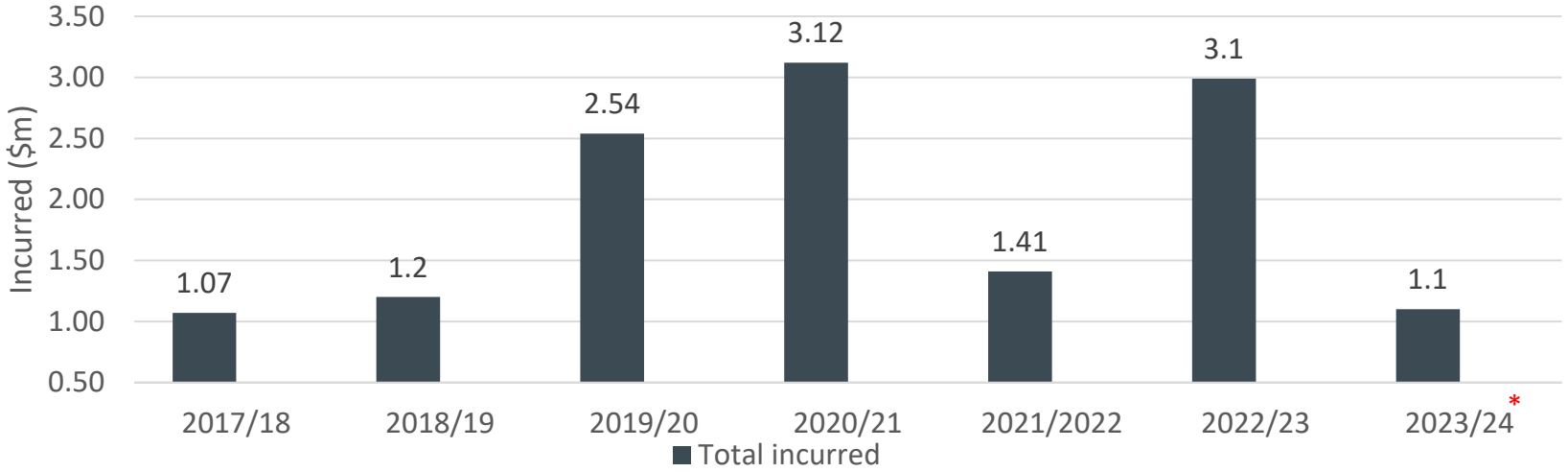
Presentation outline

- A brief history – the relatively new crime impacting private practices
  - Cyber assisted fraud claims
    - Your law practice's cyber risk insurance coverage
      - The main types of cyber crime affecting law practices
        - Resources and Guide to Cyber Security
          - Horizon Gazing – what lies ahead?
            - Opportunities through adversity

Lawcover

Cyber assisted fraud claims

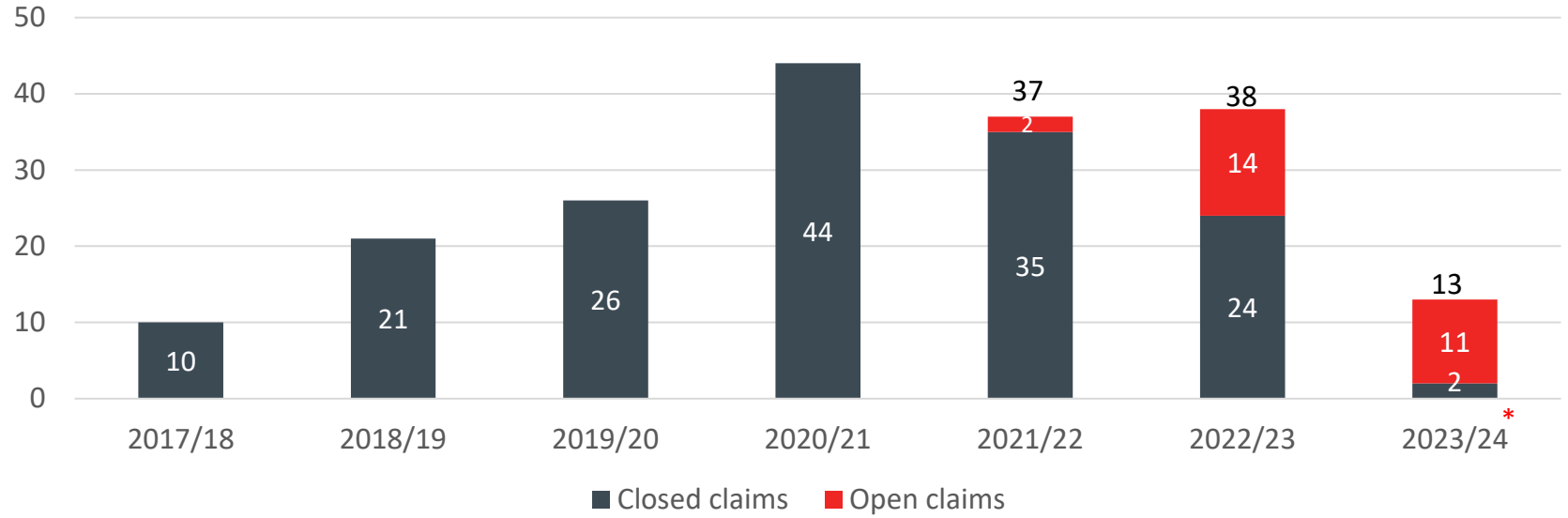
Total incurred - $13.54m at 18 September 2023



At 8 December 2023, Total Incurred was $1.2m for 2023/24

Cyber assisted fraud claims

By year to 18 September 2023



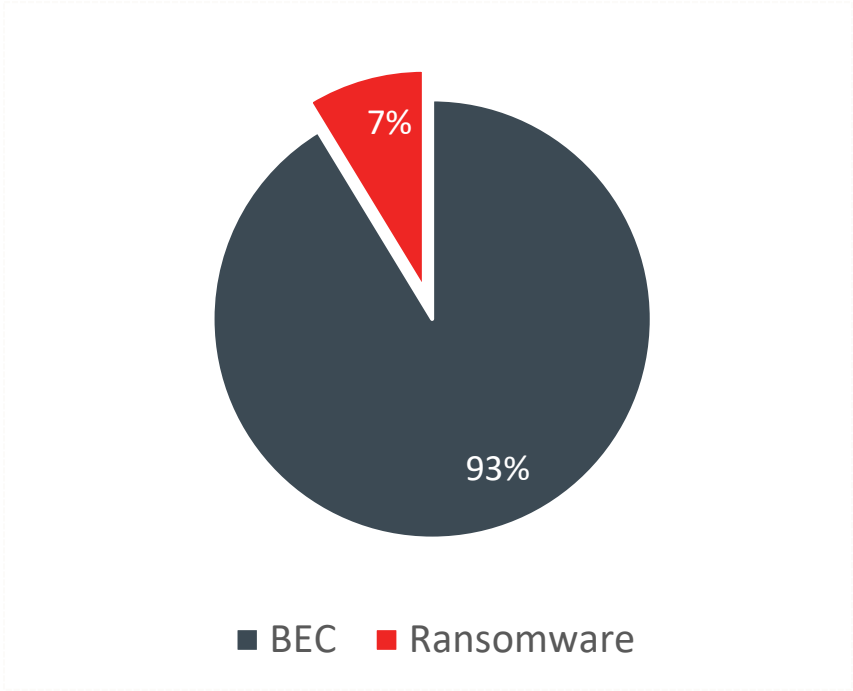
* At 8 December 2023, there were 22 claims for 2023/24

Cyber claims – Lawcover Group Cyber Risk Insurance Policy

Lawcover's group cyber risk insurance policy

- Automatic cover for law practices that purchase Lawcover's PII
  - Up to $50K limit
    - No premium payable by law practices
      - Crisis and claims assistance
        - Subject to terms, conditions & exclusions of the policy wording
          - A per-claim excess applies
            - > 90% are caused by Business Email Compromise

Cyber claims – Lawcover Group Cyber Risk Insurance Policy



HAVE YOU EXPERIENCED A BREACH?

CALL 1800 4BREACH
(1800 427 322)

Cyber claims – Lawcover Group Cyber Risk Insurance Policy

Summary at 31 December 2023

	Jan 18 – Jul 19 (18 months)	2019/20	2020/21	20221/22	2022/23	to Dec 23 (6 months)	Total
Notifications	56	55	73	45	55	38	**322**
Total incurred $'000	249	173	170	244	390	79	**1,307**

How to avoid a double excess

2023/24 Professional Indemnity Insurance Schedule

- Excess: $ *[varies]*
  - EXCEPT THAT, for **claims** arising from any payment or electronic funds transfer made in response to a purported instruction or authorisation, which the **law practice** did not take reasonable steps to verify, **excess** means twice that amount.

Business Email Compromise

What is it and how does it work?

1. Cybercriminals collect information to create a profile of key targets. (e.g. Does the target conduct regular financial transactions?)
2. Using a fake or hacked email address, an email impersonating an individual or entity is sent to the target. Emails may request a change in details (e.g. bank account details) or urgent payment of an invoice
3. The victim is convinced they are conducting a legitimate transaction and transfers funds (for example) to the requested bank account or pays the urgent invoice
4. Funds are transferred unknowingly to the cybercriminal

Lawcover

Ransomware

What is it and how does it work?

1. Victim receives email containing Malware
2. Malware downloads malicious files (codes)
3. Malicious codes encrypt victim's files
4. Ransom notice with deadline and instructions for payment sent
4. Demand ransom payment to unlock/decrypt files

Business Email Compromise and Ransomware - Causes

1

Weak passwords

- Use of the same password for different accounts
- Use of a password that is easily guessed (e.g. birth dates)
- Passwords recorded in a notebook
- Use of a variation of the same password for different accounts

2

Malicious links and attachments

- Decision and skill-based errors, (e.g. opening malicious email or attachments or clicking a malicious link)
- Lack of or inadequate protective software to block malicious emails
- Lack of staff training and awareness of cyber security and threats

Lawcover

Business Email Compromise and Ransomware - Causes

3

Risks with WiFi and USB drives

- Use of WiFi available in public places
- Use of portable storage devices that are not your own or are unprotected
- Failure to protect your own portable storage devices

4

Poor protection software and data backups

- Little or no protection software to safeguard your system
- Disabled software protection alerts
- Failure to perform updates when alerted
- Failure to perform frequent data backups
- Failure to check efficacy of data backups

Lawcover

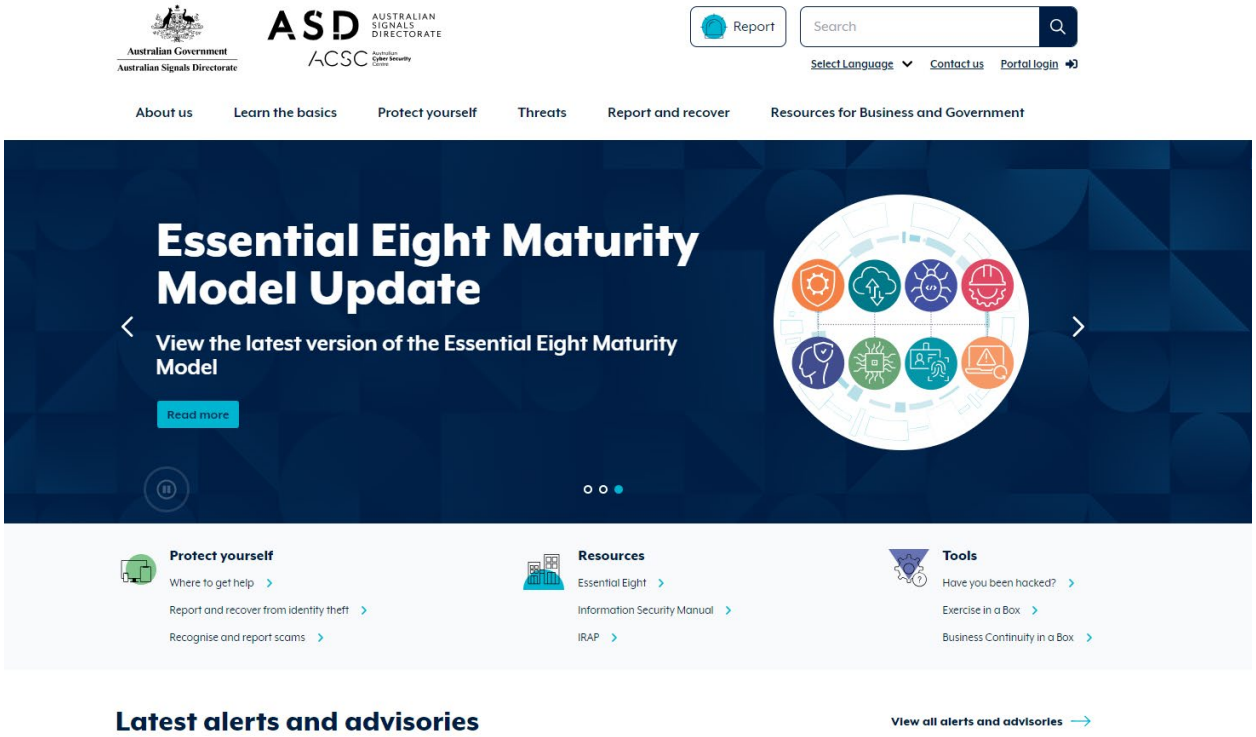
Ransomware scenario

Ransomware scenario

- The solicitor contacted the Cyber response Team on 1800 427 322
  - The legal practice had been diligently backing up their files to the backup server
    - There was and urgent need to retrieve the law practice's data from its backup servers
      - It was discovered that the backups were corrupted, and the last readable backup was three years old
        - The Cyber Response Team's security consultants were able to identify the type of ransomware without paying the ransom

Lawcover

cyber.gov.au


Australian Government
Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre
Report
Search
Select Language
Contact us
Portal login
About us
Learn the basics
Protect yourself
Threats
Report and recover
Resources for Business and Government
Essential Eight Maturity Model Update
View the latest version of the Essential Eight Maturity Model
Read more
Protect yourself
Where to get help
Report and recover from identity theft
Recognise and report scams
Resources
Essential Eight
Information Security Manual
IRAP
Tools
Have you been hacked?
Exercise in a Box
Business Continuity in a Box
Latest alerts and advisories
View all alerts and advisories

Lawcover's Cyber Resources

Podcasts

Risk On Air

View

Videos

Short Minutes

View

FAQ's

View

Cyber Risk Assessment

Click here to start

Policy Wording

View

Cyber Security Guide

View

Lawcover's Guide to Cyber Security

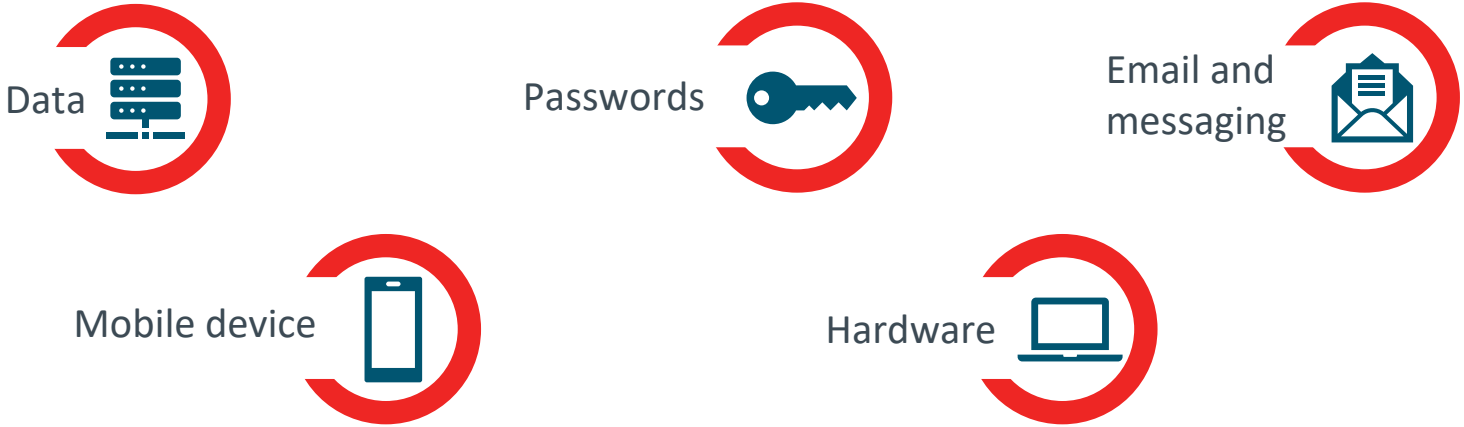
Designed to help legal practices navigate the world of cyber security; identify and prioritise their security needs and implement effective defense systems, ongoing protection and appropriate response plans in their own practice.

Lawcover

lawcover.com.au/cyber-security-guide

Lawcover's Guide to Cyber Security

Supplementary materials with step-by-step instructions to help protect critical aspects of your practice.



Lawcover

lawcover.com.au/cyber-security-guide

Cyber Security: Risks, Reality and Remediation

Malcolm Heath, Practice Risk Manager, Law

Lawcover

Law Society of the Australian Capital Territory
Level 4, 1 Farrell Place, Canberra City ACT 2601
Phone 02 6274 0333 | memberconnect@actlawsociety.asn.au

actlawsociety.asn.au