Cyber Insurance February Regional Connect Roadshow

George Kleibert
NSW Insurance Agency Pty Ltd
77 Main St Mittagong NSW 2575

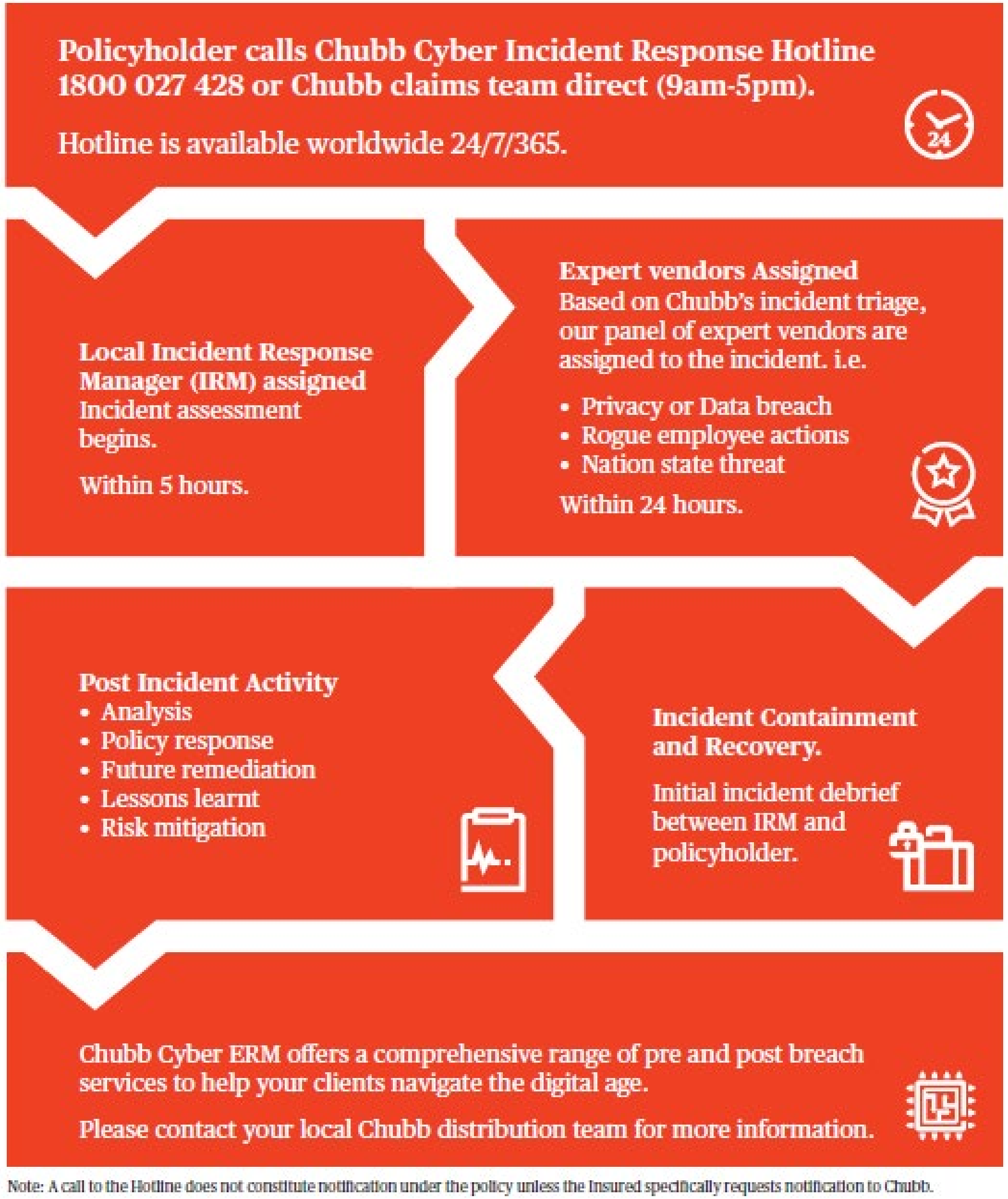
Disclaimer

This presentation has been prepared by NSW Insurance Agency Pty Ltd. The information in this presentation is general in nature and does not constitute personal financial product advice. It does not consider your objectives, financial situation or needs. Before acting on any information, you should seek independent financial advice and read any relevant Product Disclosure Statement (PDS).

Why Do I Need A Cyber Liability Policy

- Covers Financial Loss – Financial Loss Hiring of Expert Consultants
- Costs of replacing records and in some cases hardware
- Legal Defence Costs in defending a claim
- Crisis Management
- Notification and Monitoring Expenses
- Report Completion & Mandatory Data Breach Notification
- *Can be extended to include social engineering

- **Social Engineering is effectively the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes**



Policyholder calls Chubb Cyber Incident Response Hotline 1800 027 428 or Chubb claims team direct (9am-5pm).

Hotline is available worldwide 24/7/365.

Local Incident Response Manager (IRM) assigned
Incident assessment begins.

Within 5 hours.

Expert vendors Assigned
Based on Chubb's incident triage, our panel of expert vendors are assigned to the incident. i.e.

- Privacy or Data breach
- Rogue employee actions
- Nation state threat

Within 24 hours.

Incident Containment and Recovery.

Initial incident debrief between IRM and policyholder.

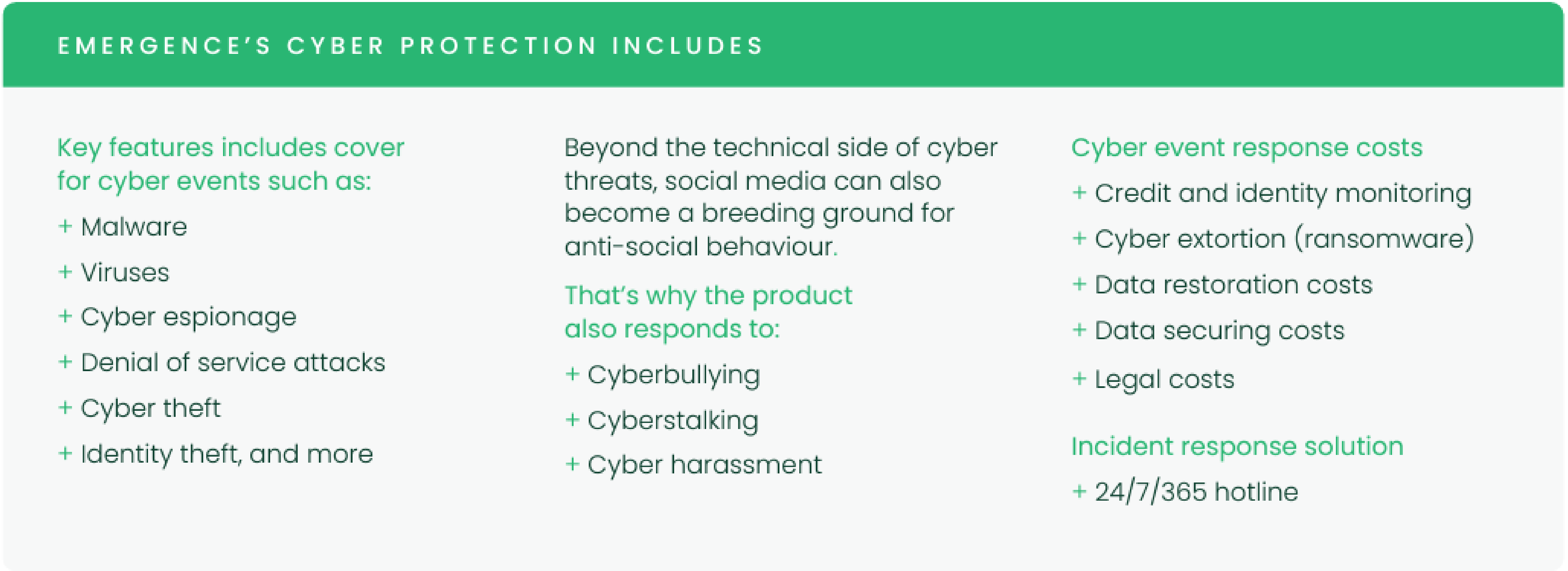
Post Incident Activity

- Analysis
- Policy response
- Future remediation
- Lessons learnt
- Risk mitigation

Chubb Cyber ERM offers a comprehensive range of pre and post breach services to help your clients navigate the digital age.

Please contact your local Chubb distribution team for more information.

Note: A call to the Hotline does not constitute notification under the policy unless the Insured specifically requests notification to Chubb.



EMERGENCE'S CYBER PROTECTION INCLUDES

Key features includes cover for cyber events such as:

- Malware
- Viruses
- Cyber espionage
- Denial of service attacks
- Cyber theft
- Identity theft, and more

Beyond the technical side of cyber threats, social media can also become a breeding ground for anti-social behaviour.

That's why the product also responds to:

- Cyberbullying
- Cyberstalking
- Cyber harassment

Cyber event response costs

- Credit and identity monitoring
- Cyber extortion (ransomware)
- Data restoration costs
- Data securing costs
- Legal costs

Incident response solution

- 24/7/365 hotline

Security to succeed

Our strength and security is 100% Lloyd's - insuring risks for hundreds of years.

Help is at hand

Cyber protection for the whole family. Our dedicated team is knowledgeable, experienced and ready to lend support to help give peace of mind when you need it.

Cover with confidence

Assure families with confidence that they'll be protected in the event of a cyber attack. Cyber attacks include; identity theft, cyberbullying, cyberstalking, personal cyber crime, hacking, malware, ransomware and cyber harassment.

Cost effective for families

Premiums start from $99. Policy limits from $50,000 to $1,000,000 available.

Online portal

Seamless acquisition process. Quote and bind policies in as little as 30 seconds.

Incident response solution

Local presence. Global expertise on call 24/7/365 to manage claims and help families when they need it most.

Year in Review 2022-2023

- Average cost of cybercrime per report, **up 14 per cent**
- small business: **$46,000**
- medium business: **$97,200**
- large business: **$71,600.**
- Nearly **94,000** cybercrime reports, **up 23 per cent**
- on average a report **every 6 minutes**
- an increase from 1 report **every 7 minutes.**
- Answered over **33,000** calls to the Australian Cyber Security Hotline, **up 32 per cent**
- on average **90 calls per day**
- an increase from **69 calls per day.**
- **Top 3 cybercrime** types for **individuals**
- identity fraud
- online banking fraud
- online shopping fraud.
- **Top 3 cybercrime** types for **business**
- email compromise
- business email compromise (BEC) fraud
- online banking fraud.
- Publicly reported common vulnerabilities and exposures (CVEs) **increased 20 per cent.**

I already have insurance??

Public & Product Liabilty – Covers Damage to people or property

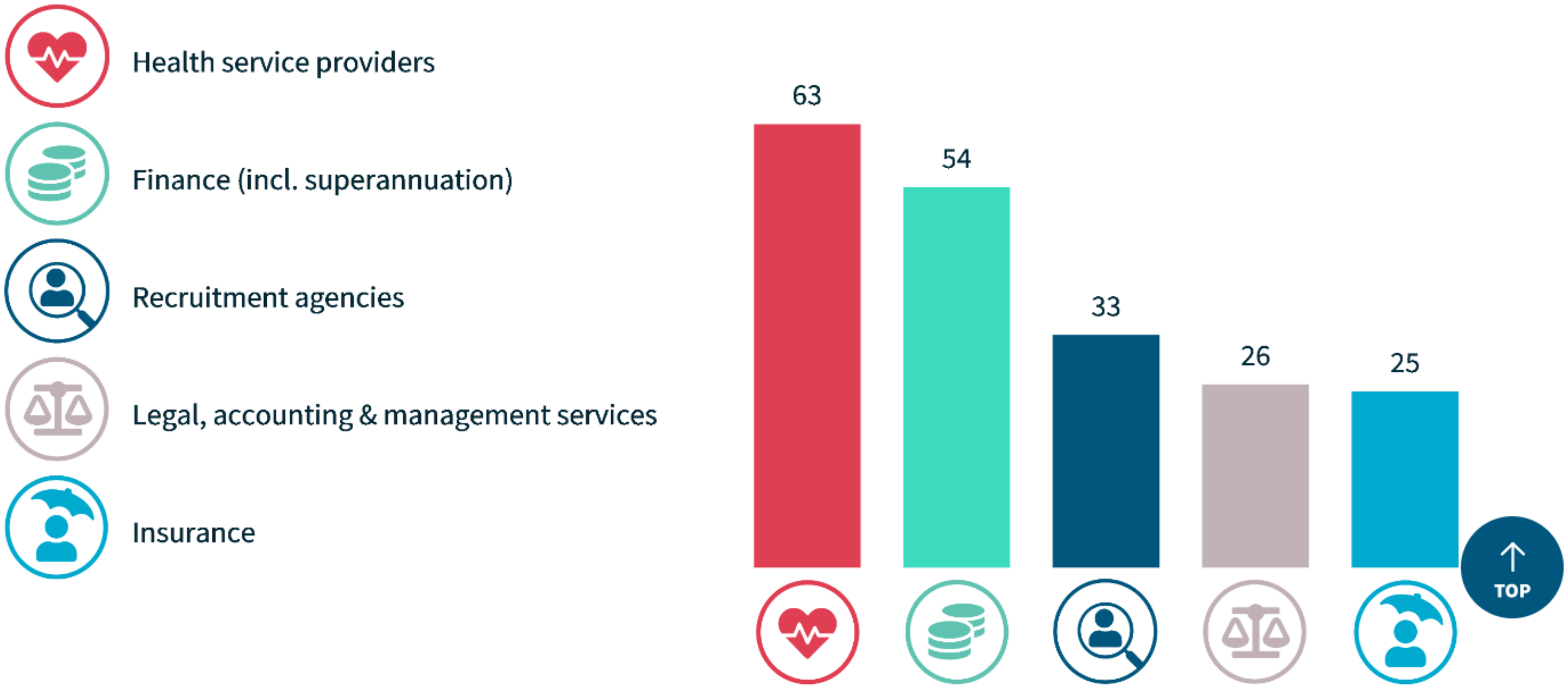
Professional Indemnity – Covers Financial loss caused by professional negligence

Cyber Liability A Separate insurance which covers costs, damages & remediation in the event of hacking & unauthorised access to electronically stored personal information

Management Liability – Some policies include cover for Social Engineering

Top five sectors

Top Sectors to Notify Data Breaches

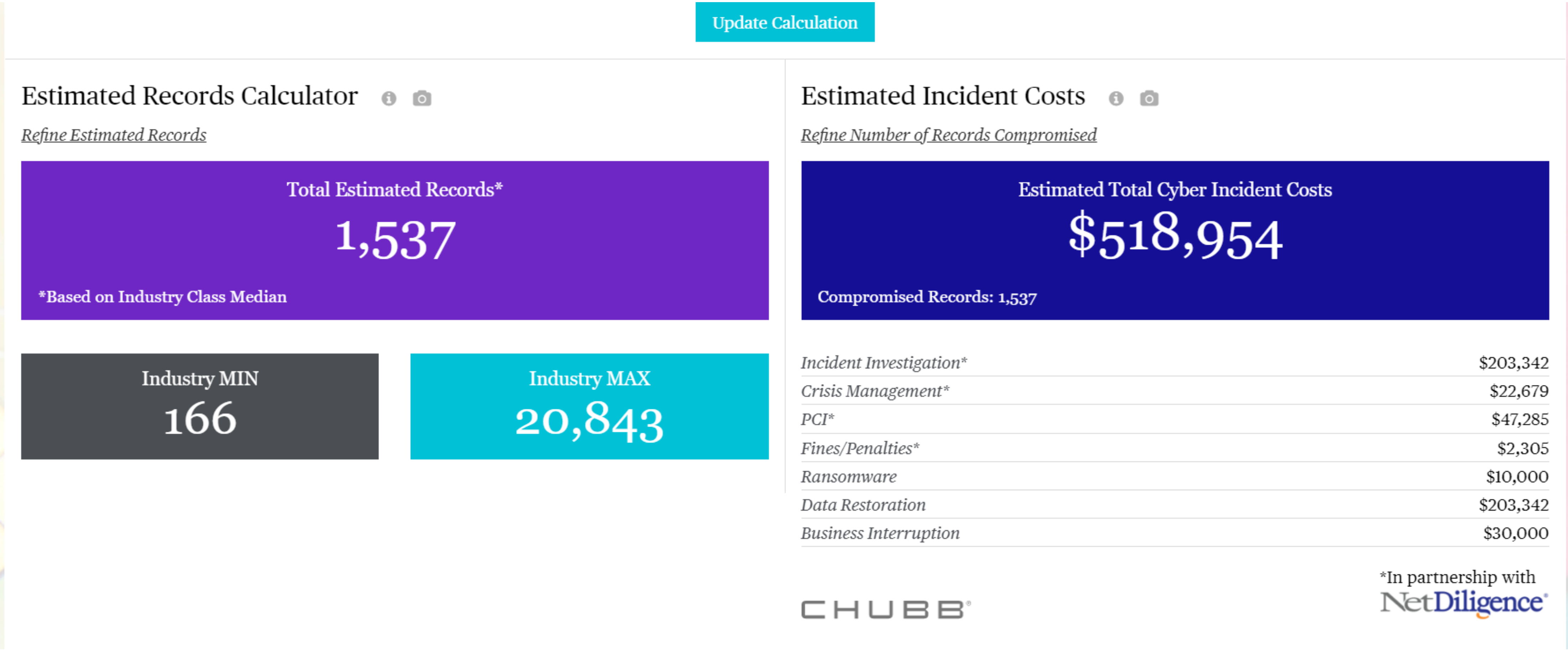


How Much Do I need to Insure for ?

Tools are available to forecast a loss amount

https://chubbcyberindex.com/#/cyber-risk-calculators

Retail $1 Mill T/o Less than 25% Online Sales



Estimated Records Calculator

Refine Estimated Records

Total Estimated Records*

1,537

*Based on Industry Class Median

Industry MIN

166

Industry MAX

20,843

Estimated Incident Costs

Refine Number of Records Compromised

Estimated Total Cyber Incident Costs

$518,954

Compromised Records: 1,537

*Incident Investigation**	$203,342
*Crisis Management**	$22,679
*PCI**	$47,285
*Fines/Penalties**	$2,305
Ransomware	$10,000
Data Restoration	$203,342
Business Interruption	$30,000

CHUBB®

*In partnership with NetDiligence®

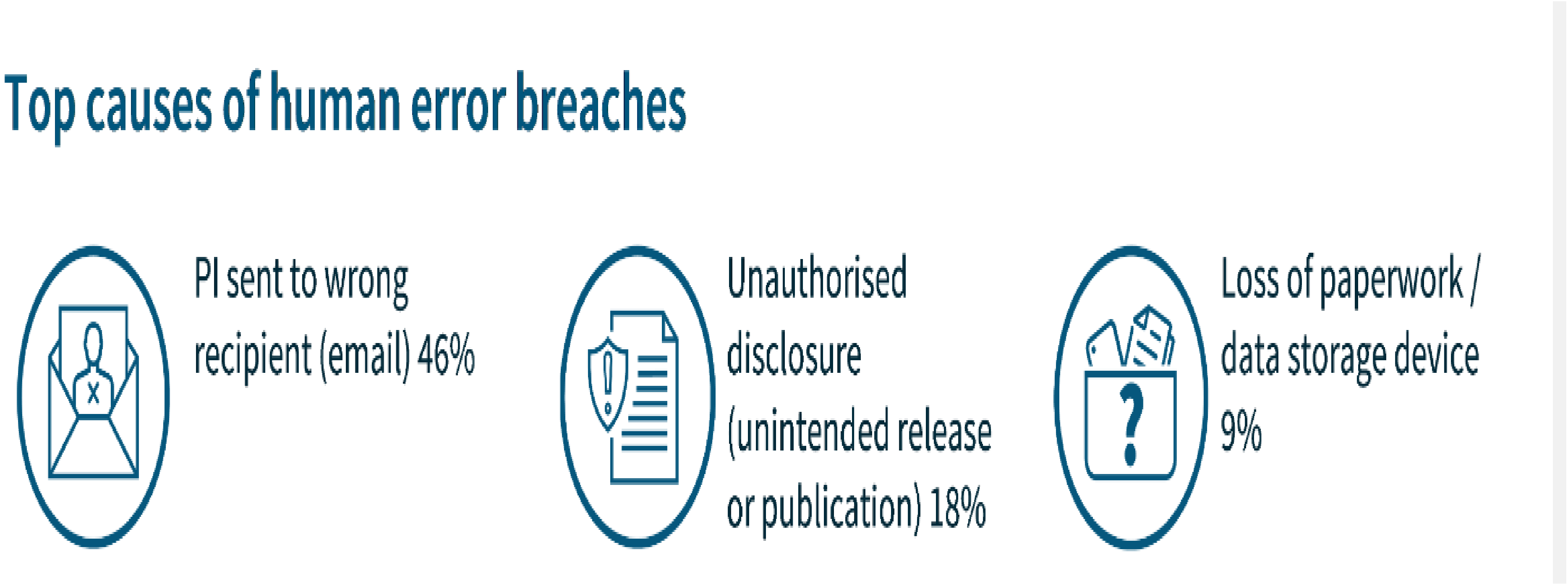
Mandatory Data Breach Legislation

A data breach happens when personal information is accessed or disclosed without authorisation or is lost.

The MNDB Scheme requires public sector agencies to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information that are likely to result in serious harm. As part of the Scheme, agencies are required to publish a data breach policy, which outlines an agency's overall strategy for managing data breaches. Agencies must also maintain an internal register of eligible data breaches.

- Under the Notifiable Data Breach (NDB) scheme an organisation or agency must notify affected individuals and the OAIC about an eligible data breach.
- An eligible data breach occurs when:
- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
- this is likely to result in serious harm to one or more individuals, and
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action.

A Breach must be Disclosed to the Privacy Commissioner within 30 Days



Top causes of human error breaches

- PI sent to wrong recipient (email) 46%
- Unauthorised disclosure (unintended release or publication) 18%
- Loss of paperwork / data storage device 9%

How much does it Cost ?

- Patch Software. When Immediately Upon release. Cost Free
- Update & Change Passwords Regularly. Use a Password Manager, Google or check your anti-virus provider. subscriptions from a few Dollars per month or free
- Backup Data. Minimum 2 copies off site. Isolated from your network 5TB Drives are <$300
- Don’t click on any text message links. Do not scan QR Codes Free
- Encryption Software – Plans start from a few dollars a month

Nordlock $30 p/m, Axcrypt from $5p/m

Cyber Liability premiums vary depending upon security industry and turnover.

Expect premiums to generally start around the $2k++ mark

Tips to Minimise Cyber Breaches

1. Complete the Healthcare Business IT Guide
2. Use a full-service internet security suite
3. 2. Use strong passwords At least 10 characters A password management application can help you
4. 3. Keep your software updated. Update software as soon as patches are available
5. 4. Manage your social media settings Keep your personal and private information locked down
6. 5. Strengthen your home network
7. 7. Keep up to date on major security breaches If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.
8. Use 2 Factor Authentication as much as possible
9. Spend some time on https://www.staysmartonline.gov.au/

DUAL

10 TIPS

TO HELP PREVENT A CYBER ATTACK

DUAL Australia has partnered with Cyber Incident Management Team (CIMT) to manage all cyber incidents from initial notification through to a resolution. In the first instance, if you experience a cyber claim or incident, notifications should be made via the following methods to ensure that security / privacy breaches are managed efficiently and effectively:

24/7 monitored email at cyber.incident@canopius.com or the Cyber Incident Reporting hotline on +64 483 10243.

Backup Data

Backup data frequently with the backups stored off the insured's premises and not connected to the insured's network.

Staff Training

Ensure all staff have frequent cybersecurity training so they are aware of the potential risks.

Firewall & Anti-Virus Protection

Use operating systems with embedded firewalls and anti-virus protection software (such as Windows or MAC OS X), or run separate commercially licensed firewall or anti-virus protection software.

Never pay Ransom

Its not always wise to pay a ransom as you are not able to determine where the money will go (i.e funding terrorism without knowing) or if the hacker will repeat this attack.

Mobile Device Encryption

Protect your data with encryption including mobile phones, laptops and other portable devices.

Credit Card Storing

Do not store your credit card details on websites – do not keep them saved on notes or documents on your computer system.

Password Protection

Keep passwords strong and secured and set up two factor authorisation (2FA).

Third Party Vendor Management

Any requests to alter supplier and customer details including bank account details, independently verified with a known contact for authenticity.

Two Person sign-off

Ensure that at least two members of staff authorise any transfer of funds, signing of cheques and the issuance of instructions for the disbursement of assets, funds or investments.

Incident Response Plan

Have a well-planned approach to addressing and managing a cyber attack to help respond to, and recover from network security incident.

SYDNEY | MELBOURNE | PERTH | BRISBANE
Tel: 1300 769 772 | www.dualaustralia.com.au
DUAL Australia Pty Limited Part of the DUAL International Group Registered in Australia under ABN No. 16 107 553 257

The information contained in this fact sheet is meant as a guide only. DUAL Australia does not accept any liability arising out of any reliance on the information in this fact sheet. We urge you to consult your insurance broker, the Insurance Council of Australia or the Australian Financial Complaints Authority (AFCA) for further information.

Medical Services 6 Staff $3.2 Million T/o

- Medical Services
- 6 staff
- $3.2M turnover

- Background
- The Insured's system, which held confidential medical information on their patients, was compromised by a ransomware attack. As the Insured could not access their patients' medical data, they were unable to operate.
- Outcome
- The Insured's policy was triggered and DUAL appointed an IT Forensic Consultant to fix the damage to the Insured's system and investigate if the hacker still had access to the system. A law firm was also appointed to assist the remediation process and advise if the client had to report the matter to the Privacy Commissioner. Payment was made in relation to business interruption loss, forensics and legal costs.

- **Payment:** $63,000.

Hairdresser 5 Staff $3 Million T/o (Phreaking)

- Hairdresser
- 5 staff
- $3M turnover

- Background
- The Insured uses a VoIP telephone system. A hacker gained access to the telephone system and made multiple unauthorised calls to a premium number over the course of a month. At the end of the month, the Insured received their invoice, which included $30,000 of unauthorised calls.
- Outcome
- The Insured made a claim on their Cyber policy which triggered the optional Social Engineering cover. The client was covered for their direct financial loss as a result of the phreaking attack.
- **Payment:** $30,000.

Media Co 12 Staff $3 Million T/o (Invoice Doctoring)

- Media
- 12 staff
- $3M turnover

- Background
- A hacker impersonated a client of the Insured, using an identical email address. The hacker emailed the Insured advising that future payments should be made to a new bank account. When the Insured was due to pay the client, they paid $41,000 into the fraudulent account.
- Outcome
- The Insured claimed against their Cyber policy which triggered the optional Social Engineering cover. Indemnity was granted for the direct financial loss suffered by the Insured.
- **Payment:** $41,000.

Accountant $2 Million T/O (System Comprimise)

- Accountant
- 5 staff
- $2M turnover

- Background
- The Insured's director noticed that some documents on their server had been deleted. Further investigations were undertaken and it was discovered a hacker had been accessing the Insured's system for the past 2 months.
- Outcome
- The Insured notified DUAL who hired an IT Forensic Consultant to review the Insured's systems. It was discovered 800 client files had been accessed which included private details such as driver's licenses and passport numbers. DUAL appointed a specialist firm to monitor whether any client identities were stolen or sold as well as a law firm to advise on the data breach issues and draft a notification letter to all affected parties. It was determined that the Insured had to report the incident to the Privacy Commissioner and the appropriate steps were taken to secure the information they held. Remediation costs were also covered to rectify any issues with the Insured's system.
- **Payment:** $90,000.

Reference Links

www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

George Kleibert – Authorised Broker
M 0478 155 581
E gk@wgib.com.au
A 77 Main St Mittagong NSW 2575

NSW INSURANCE AGENCY

NSW Insurance Agency Pty Ltd