

The 2023 Intensive Conference

“Staying ahead of
the game”

Conference papers

Deciphering Cyber Security



Get Cybersecurity Ready

Annie Haggart
Cyber GC
ACT Law
Society
March 2023

Go to www.menti.com and use the code 5192 8960

Instructions

Go to
www.menti.com

Enter the code
5192 8960



Or use QR code



Prepare you and your practice

- What are the things you need to know about cybersecurity
- What can you do to prepare yourself, and your practice



Prepare your clients

- What are the cybersecurity challenges facing your clients
- How should you consider cybersecurity issues in your advice



Your presenter

Annie Haggar
Principal
Cyber GC



Accenture - Global Managed Security Legal Lead | Growth Markets Security Legal Lead (2011 – 2023)

Canberra, Australia | 20 years IT and cybersecurity law experience

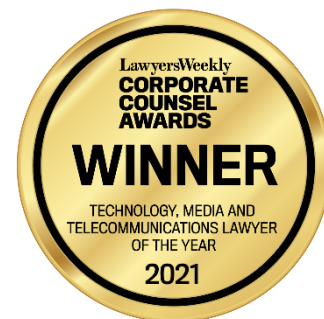
Winner 2021 - Australian In-House Counsel of the Year (Australasian Law Awards)



Winner 2021 – General Counsel of the Year (Australian Law Awards – *Lawyers Weekly* 2021)



Winner 2021 - Technology Media and Telecommunications Lawyer of the Year (*Lawyers Weekly* Corporate Counsel Awards 2021)



About Cyber GC

Cyber GC is a specialist cybersecurity legal and consulting practice based in the ACT, providing services all over Australia. We are dedicated to helping Australian businesses to prepare for and fight cybercrime.

Cyber GC can bring specialist cybersecurity legal skills to complement your existing legal team, or to provide legal advice, strategy, and support to businesses and boards when they need it.

Taking a look at last year's stats

Have you personally ever been the subject of a cyber attack

Mentimeter



Yes



No

Has your firm ever been the subject of a cybersecurity attack?

Mentimeter



Yes - a minor one



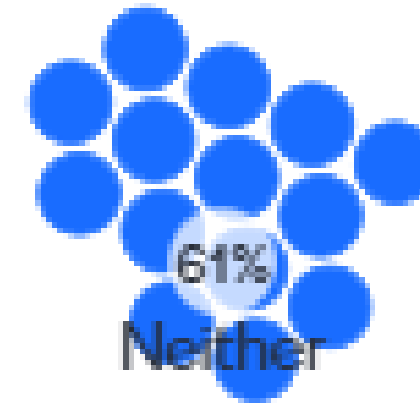
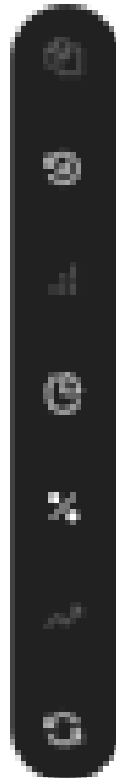
Yes - a major one



No - not yet (that I know of)

Go to www.menti.com and use the code 5192 8960

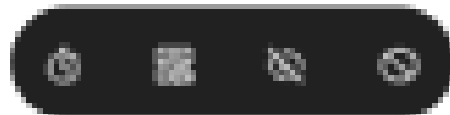
Recent Cyber Attacks



⚡ Lost contact with audience

Unable to synchronise audience with presentation.
Press (Activate slide) to refresh connection.

Activate slide



Some scary numbers

56%

of companies were a victim of a ransomware attack in the last 12 months [^]

39%

of organisations were affected by a third-party cyber incident ^{*}

\$4.35 Million

is the current average cost of a data breach ~

91%

of cyber attacks were business email compromises ^{*}

197.6 Million

emails are sent every 60 seconds ^{*}

13%

rise over the last 2 years in the cost of a cybersecurity data breach ~

80%

Optimism bias – people won't take action because they don't think it will happen to them...#

50%

of companies reported a loss of clients after a ransomware attack [^]

[^] Delinea

^{*} WEF

~ IBM

#PWC

Cybersecurity is in the news

NOTPETYA

Wave of ransomware attacks in network

col
phar
Merc
comp
Russian

Researcher
attack mask
attacks again.

Optus

9.8 million impacted. 2.1 suffered sensitive information compromise. \$140 million in costs so far.

rogram
nearly
1000 uranium
enriched centrifuges.

MARRIOTT

Hackers had access
of more

Colonial Pipeline

Ransomware attack on Colonial Pipeline - US Oil company causes shutdown of gasoline pipeline across causing shortages

Medibank

9.7 million impacted. 3.9 million suffered data exposure. \$960 million in costs so far (no ransom paid).

Global ransomware attack on utilities & large corporations, temporarily crippled UK's National Health Service.

A sophisticated sup... are hackers compromised Orion... nds product) which was deployed in mid-2020 to 18,000 SolarWinds clients (including FireEye and the US Federal Government) have been affected.

But the issue isn't just overseas... Its local

Law firm accused of losing \$1 million of client's money in email

Law firms lose millions to hackers in 'sophisticated' email scam

This article is but one example of how law firms have taken cyber-security a step further. Instead, all clients have their documents can be exchanged safely.

At least two Queensland law firms have been hit by a scam, prompting an urgent warning from the Queensland Government.

Lawcover Data shows:
- 9% Claims are Ransomware
- 91% are Business Email Compromise
for Australian law firms they cover
All Lawcover PII holders have \$50k coverage to help with incident response – 1800 BREACH

Law Firm Allens Caught Up in Cyberattack

The firm's client data was compromised after a file-sharing system designed by California-based cloud company Accellion was accessed illegally earlier this month.



And I can't remember what email address we used to log in to the account, and the baby's crying-

REAL PL TUNE

The threat landscape is ever evolving

EXTERNAL THREAT ACTORS



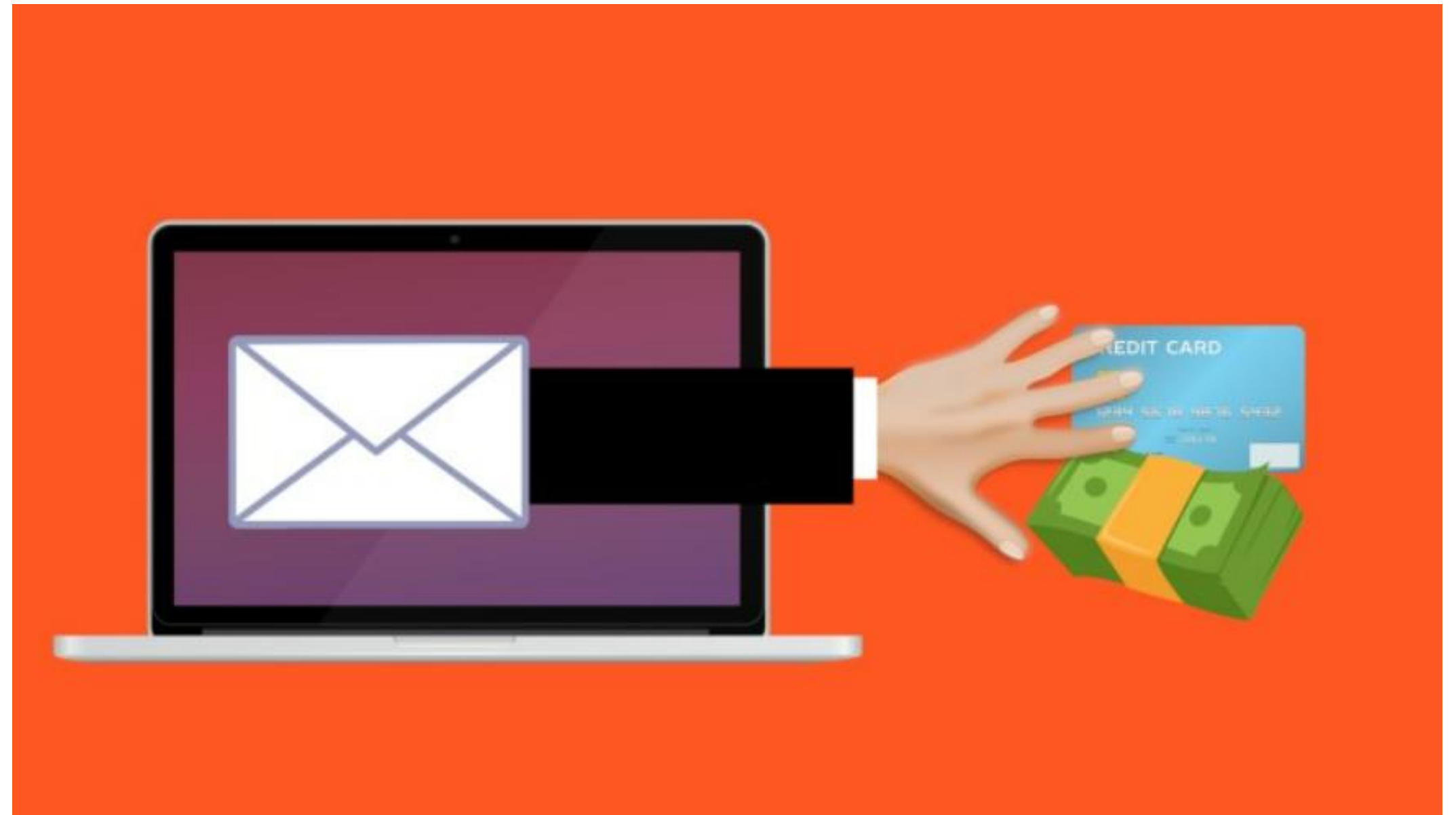
INTERNAL THREAT ACTORS



There are now ~**15 billion** IoT devices

Types of security attacks

1. Business Email Compromise
2. Ransomware
3. Malware
4. Phishing/Social Engineering
(SMSishing, Vishing)
5. Man-in-the-Middle (MitM) attacks
6. Denial-of-Service (DDOS) attacks
7. SQL Injections
8. Zero-Day Exploit
9. Password attack
10. Cross-site scripting
11. Root kits
12. Internet-of-Things (IOT) attacks



Go to www.menti.com and use the code 5192 8960



⚡ Lost contact with audience

Unable to synchronise audience with presentation.
Press [Activate slide] to refresh connection.

Activate slide



Press **ENTER** to show answers



New Task



I am thinking of implementing an employee incentive program to show our employees we care about them. I would like to surprise them and put a smile on their faces today. Can we purchase some gift cards (Google Play/Apple Store) from the store?

Which of the cards can you easily buy from the store? You are to keep this surprise package strictly CONFIDENTIAL until we give it out to them.

Thanks
Vanessa Smith

Sent from my iphone

⚡ Lost contact with audience

Unable to synchronise audience with presentation.
Press [Activate slide] to refresh connection.

Activate slide



Press **ENTER** to show answers



AN Alex Nicholls
lessaowenn@gmail.com

To You [redacted]@lawyerbank.com.au

Tuesday, 14 June, 10:33 am

Hello [redacted]

are you doing today? Well I'm in a conference
ng right now,
talk on phone, but let me know if you got my
age and if you
idly send me your personal number.



Thanks,

Alex Nicholls
Director and Co-Founder at lawyerbank - lawyers you
can bank on.

⚡ Lost contact with audience

Unable to synchronise audience with presentation.
Press [Activate slide] to refresh connection.

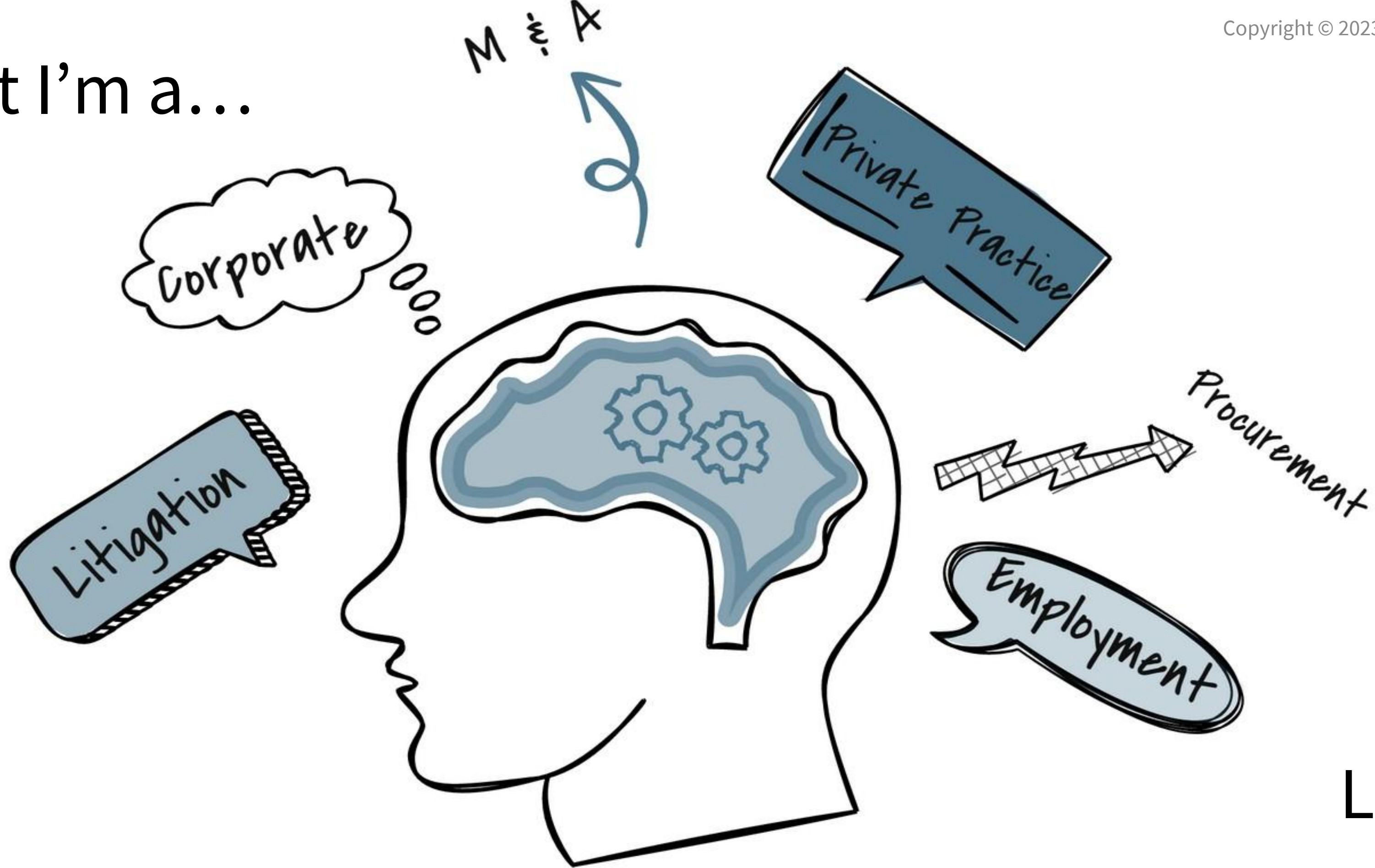
Activate slide



Press **ENTER** to show answers



But I'm a...



Lawyer.

What do I need to know about cyber security?

SO WHERE DO I START?





UPSKILL

Train yourself -
Train your team

What can you do to upskill?

- Read
- Listen
- Practice

What should your firm/company be doing to upskill its employees?

Courses and Subscriptions | Guidance, Simulations & Training tools

<https://www.institutedat.a.com/courses/cyber-security-program/>

<https://www.cybersecurityconnect.com.au/>



Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

BUSINESS AUSTRALIA



SECURITY CENTRIC
Engineered Information Security

KnowBe4
Human error. Conquered.

Phriendly Phishing



CROWN JEWELS

Know what it would take to bring your company/your client to its knees. Start there.



Who might be interested in attacking your business – and why?

Who are your enemies?

What is your 'secret sauce'?

Who are your clients (eg might you be a target of a supply chain attack)?



FIND IT. SECURE IT.

Know where your data is.

Prioritise securing it.



What processes do you have for checking changes to data (eg account payment details)?

Where is your data held and how secure is that? What backups do you have, and where are they held?

Copyright © 2023 Cyber GC. All rights reserved.

Who in your supply chain has access to your systems and data?

If you had a ransom attack that threatened to release your data – who is impacted by this?

Do you know who you would have to tell if which individuals, which regulators – and when)? you had a data breach (eg

What types of data do you hold?

If you had a data breach – would you know what data had been accessed?

Do you have a ‘dual approval’ or multifactor authentication or warning email system that you can use to confirm changes?



HAVE A PLAN AND PRACTICE IT

Like a fire evacuation plan...

How do I make a cyber security plan?

- Get some professional help
- Consider different attack scenarios
- Include all the key parts of your business and external advisors (Executive, Board, Legal, IT and infosec, Marketing and Comms)

How do I practice a cyber security plan?

- Table top and role play
- 'Live Attack' test (Adversary simulation or 'red teaming')
- 'Live defense' test (supporting your defense team to spot a live attack)

Who should practice?

- Executive/Board
- Legal
- IT and infosec
- Marketing and Communications staff



How often should we practice?

- Regularly!
- 6 monthly at a minimum



INVEST AND PROTECT

Insurance, technology, training, planning, support.

It's an investment in your resilience and your recovery.

For yourself

- Password manager
 - Lastpass
 - Dashlane
 - Keeper
- 2 factor authentication – on everything.
- Identity monitoring
- Encrypt portable storage. Even better – don't use it. Put your documents in the cloud.
- Use complex passwords – on your phone, your laptop, your home network
- Check if your details are already breached -

LastPass

<https://lastpass.com>

dashlane

<https://dashlane.com>

KEEPER

<https://keepersecurity.com>

For your firm

- Mandate personal protections for employees
- Good IT support
- Secure cloud solutions
- Secure document storage solutions
- Cybersecurity Vulnerability Assessment
- Training regime
- Breach Coach
- Insurance



INVEST AND PROTECT

Some useful and free resources!

KnowBe4
Human error. Conquered.

PRODUCTS & SERVICES ▾ **FREE TOOLS ▾** PRICING ▾ RESOURCES ▾ ABOUT US ▾ CONTACT ▾

Phishing Tools

- Phishing Security Test
- Phishing Reply Test
- Phish Alert Button
- Second Chance
- Social Media Phishing Test

Security Awareness Tools

- Automated Security Awareness Program
- Training Preview

Password Tools

- Weak Password Test
- Browser Password Inspector
- Password Exposure Test
- Breached Password Test
- Multi-Factor Authentication Security Assessment

Email Security Tools

- Email Exposure Check Pro
- Domain Spoof Test
- Mailserver Assessment
- Domain Doppelgänger

Malware Tools

- Ransomware Simulator Tool
- USB Security Test

Compliance Tools

- Compliance Audit Readiness Assessment

Phishing Security Test

Free Phishing Security Test Results

Phish-Prone Percentage

25% Your Test

1.6% Industry Average

What percentage of your users are Phish-prone™?

[Phish Your Users](#)

FORRESTER RESEARCH

THE FORRESTER WAVE™

Security Awareness And Training Solutions

2020

Challengers Contenders Strong Performers Leaders

Stronger current offering

Weaker current offering

Weaker strategy Stronger strategy

[All Free Tools >](#) [Featured Tool : MASA >](#)

Emerging technologies

New technologies are being implemented at speed, increasing risk scope

New tech with the greatest influence on cyber risk strategies

1. Artificial Intelligence (AI) and machine learning (Chat GPT)
2. Cloud technology
3. User identity and access management

Jan 1984



Jan 2007



Oct 2020



ChatGPT

- + New chat
- New chat
- Princess Dragon Adventure He
- Request Bank Info Change Con
- Wedding Hair Salon Ad
- Cybercrime Definition In Austr
- Gilbert & Tobin's 2022 Rev
- MOU for Sharing Software Cod
- MOU for Code Sharing
- Apple Gift Card Request
- Update Bank Account Details R
- Clear conversations
- Upgrade to Plus **NEW**
- Dark mode
- Updates & FAQ
- Log out

Examples	Capabilities	Limitations
"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally produce harmful instructions or biased content
"How do I make an HTTP request in Javascript?" →	Trained to decline inappropriate requests	Limited knowledge of world and events after 2021

Questions?



WEBSITE
cybergc.au



EMAIL
info@cybergc.au



LinkedIn
Annie Haggar



PHONE
+61 466 257 154



EMAIL
annie@cybergc.au

actlawsociety

the law society of the australian capital territory
a member of the law council of australia
ABN 60 181 327 029
02 6274 0300 | mail@actlawsociety.asn.au
www.actlawsociety.asn.au