CYBER PRECEDENT

Strengthening the legal profession's defence against online threats

CYBERSECURITY TRAINING TOOLKIT

INTRODUCTION

This toolkit has been compiled by the Law Institute of Victoria, and in particular by members of the Intellectual Property and Information Technology Committee and members of the Technology and the Law Committee.

The key purpose of the toolkit is to provide employers with resources for educating staff members in relation to cybersecurity risks.

It is intended that managers review the material and utilise them to prepare an internal training program for staff. It is noted that, in the context of a legal practice, the duty of client confidentiality is paramount and must be considered in all activities. This duty of client confidentiality should be the overarching consideration that informs any workplace training program in relation to cybersecurity.

The toolkit is up to date as of November 2016. Whilst care has been exercised in preparing the toolkit, the Law Institute of Victoria accepts no liability in relation to any use or modification of the toolkit

The toolkit consists of the following documents:

1. **Manager Handout**
   This provides a broad overview for managers regarding the key cybersecurity issues to raise with employees.

2. **Employee Handout**
   This provides a briefer overview of the information in the Manager Handout - to be reviewed by employees and discussed during a training session. This includes a glossary of basic cybersecurity vocabulary to assist employees understand the key terms.

3. **Essential Cybersecurity Tips**
   This could be used as a handout during a training session, or disseminated to all employees in an organisation to provide them with some key tips in relation to cybersecurity.

4. **Cybersecurity Case Studies**
   It is proposed that these are used as a discussion tool during training, to highlight the practical risks that can arise for an organisation through employee conduct.

5. **Training Outcomes Checklist**
   This is to be used to confirm whether the key issues were covered off during the training session.

6. **Resources for Preparing Cybersecurity Training**
   This provides a range of cybersecurity materials to assist employers prepare training for employees.

MANAGER HANDOUT: CYBERSECURITY STARTER INFORMATION

1. What is cyber security?

As is true of a number of facets of today's digital age, a certain level of hype and jargon impedes understanding of the risks that the legal profession faces in operating in a digital environment. However, as an ever-increasing amount of transactions occur in the cyber sphere, it is critically important for the profession to develop a working knowledge of these risks and have plans in place to prevent such threats.

A "cyber attack" has been defined by the Australian Government as "a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity."[1] As a manager in a legal practice, "cyber security" means having an understanding of these risks and ensuring that you and your employees have the necessary tools and training to guard against them in order to protect your computer systems and the data that you hold on these systems.

2. Why is cyber security important?

Unsurprisingly, recent reporting by the Australian Cyber Security Centre (ACSC) cautions that cyber attacks will continue to increase and pose a threat to Australian business in the coming years. According to the Government's Cyber Security Strategy paper launched earlier this year, the actual cost of cybercrime to Australians is estimated to be approximately $17 billion each year.[2] Evidence shows that it is not only large entities that are targeted by cyber criminals. In 2015, 43% of all targeted cybercrime attacks affected small businesses.[3] Accordingly, irrespective of the size of your organisation, effective cyber security measures are necessary.

In addition to the financial costs of not having mechanisms in place to guard against cyber attacks, there are obvious reputational consequences for legal practices where trust and client confidence in the security and secrecy of their information are of paramount importance. There may also be legal risks to practitioners associated with the disclosure of information and data breaches arising from cyber attacks.

3. What are some common threats?

The following are just a few examples of the kinds of threats targeting Australian business as described in ACSC's 2015 threat report:

- **Malware:** refers to malicious software, which is "designed to facilitate unauthorised access to a system, or cause damage or disruption to a system."[4] Malware disguised in Microsoft Office "macros"[5] are likely to be of particular relevance to legal practitioners often dealing with Word documents[6];
- **Ransomware:** is a form of "extortion through the use of malware that typically locks a computer's content and requires victims to pay a ransom to regain access;"[7]
- **Spear phishing:** describes emails crafted to appear to originate from a legitimate sender (often engineered to look as though they have been sent from a contact of the recipient) which include an attachment or link, which when opened or clicked will seek to download malware onto the recipient system. [8]
- **Distributed Denial of Service ("DDoS") attacks:** involve the use of a number of computers (often being hijacked unwittingly through malware) to interrupt a user's legitimate access to a website by "consuming the amount of available bandwidth or the processing capacity of the computer hosting the online service." [9] The user may then be extorted into paying a sum of money for the resumption of the service to occur.

---

1 Australian Cyber Security Centre (ACSC), "Threat Assessment 2015", p.8 (www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf).

2 Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australia's Cyber Security Strategy, p 15.

3 Symantec - Internet Security Threat Report 2016 https://www.symantec.com/security-center/threat-report

4 Australian Cyber Security Centre (ACSC), "Threat Assessment 2015", p. 14.

5 A "macro" is a type of computing code and is utilised to automate a certain task. See McAfee Solution Brief - Safeguarding Against Macro Malware (November 2015), www.mcafee.com/au/resources/solution-briefs/sb-quarterly-threats-nov-2015-3.pdf.

6 See the Australian Cyber Security Centre (ACSC) Microsoft Office Macro Factsheet (http://asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf).

7 See the Australian Cyber Security Centre (ACSC), "Threat Assessment 2015", p. 16

8 Australian Cyber Security Centre (ACSC), "Threat Assessment 2015", p. 26

9 Australian Cyber Security Centre (ACSC), "Threat Assessment 2015", p. 17

Central to a number of these attacks is the presence of "social engineering" which refers to the process by which a cyber criminal seeks to "manipulate a person into performing actions or divulging sensitive information,"[10] and exploits a number of human tendencies, including our propensity to trust others, our innate curiosity and the desire to help others.

4. Key investments for cyber security?

Experts warn that cyber security should be more than a 'tick box' exercise and is something that should be a whole of business initiative.[11] A priority for any organisation must be training for employees and managers, as evidence demonstrates that a number of cyber crimes rely on social engineering. According to Stephen Day, Head of the Australian Cyber Security Centre, "if you had only one dollar left to spend on cyber security, you should spend it on awareness."[12] Where your workforce is aware of the methods commonly employed by cyber criminals they will be better placed to recognise these threats. Mr Day also recommends implementing the Australian Cyber Security Centre's Top Four mitigation strategies,[13] which can be accessed via the ACSC website.[14] Of course, investment in skilled IT management services should also ideally be a central pillar of any cyber security strategy, which will allow for ongoing monitoring and ensure that the effectiveness of your defences is maintained.

10 Australian Cyber Security Centre (ACSC), "Threat Assessment 2015", p. 26

11 Duca, Sean "Introduction -The Importance of Cybersecurity for Executives in Australia" in Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Australia, p vii.

12 Day, Stephen "Four Questions Executives and Directors Should Ask About Cybersecurity" in Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Australia, p 22.

13 Day, Stephen "Four Questions Executives and Directors Should Ask About Cybersecurity" in Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Australia, p 22.

14 Top four mitigation strategies to protect your ICT system (October 2012) www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf

EMPLOYEE HANDOUT: CYBERSECURITY STARTER INFORMATION

1. What is cybersecurity?

The Oxford English Dictionary defines 'Cybersecurity' as "(t)he state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this",[15] and the Merriam - Webster dictionary defines 'cybersecurity' as "(m)easures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack"[16].

In general terms, cybersecurity is about protecting yourself and your organisation from unauthorised activities that have the potential to compromise computers, associated infrastructure or any electronic information that is the responsibility of your organisation.

2. Why you should care about cybersecurity.

Cybercrime is the 2nd most-reported type of economic crime.[17]

In 2015, 43% of all targeted cybercrime attacks struck small businesses.[18]

The Australian Government estimates the impact of cybercrime in Australia to be around $17 billion annually[19]. The cost of cybercrime to the global economy is projected to reach US$2 trillion by 2019[20].

In 2015, exploiting the human factor was the number one technique employed by cyber criminals to defeat cybersecurity[21]. Your awareness and vigilance regarding cybersecurity is essential in order for your organisation to successfully defend against cybercrime.

3. Main cybersecurity risks you face

Social engineering - Social engineering has always played a part in fraud and it plays a major role in most cybercrime that you will be exposed to. The objective is to manipulate you to carry out an action that will circumvent normal security practices or arrangements. Social engineering exploits simply rely on people's;

- Inclination to trust
- Curiosity
- Readiness to believe a compelling story
- Willingness to assist
- Desire for money or for a bargain

Social engineering is employed in a range of cybercrime activities, including phishing emails and social media scams. It is not only directed at individuals, but may also be directed at businesses, including a scheme called the Business Email Compromise (BEC),[22] which involves the impersonation of someone in authority typically requesting the transfer of money (eg a cybercriminal pretending to be a law firm partner or client requesting the transfer of client monies from a trust account to what appears to be a client account but is in fact the cybercriminal's account).

Phishing - Phishing is the most prolific type of cybercrime and you are likely to see examples on a regular basis. Phishing is an email that contains a link or attachment intended to launch malicious computer code. Typically, a phishing email uses social engineering to convince you to open the attachment, or click on the link. 'Spear phishing' is where the email is targeted at an individual, and could claim to be from someone in your organisation, or someone you know.

---

15 The Oxford English Dictionary definition for cybersecurity https://en.oxforddictionaries.com/definition/cybersecurity

16 Merriam - Webster dictionary definition for cybersecurity www.merriam-webster.com/dictionary/cybersecurity

17 PWC - Global Economic Crime Survey 2016 www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

18 Symantec - Internet Security Threat Report 2016 www.symantec.com/security-center/threat-report

19 Australian Government - Australia's Cyber Security Strategy https://cybersecuritystrategy.dpmc.gov.au

20 Forbes Jan 17, 2016 - www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/

21 Proofpoint - Human Factor Report 2016 https://www.proofpoint.com/us/human-factor-2016

22 AusCERT - www.auscert.org.au/resources/blog/business-email-compromise

Handling information – A lawyer has obligations regarding the need to secure client data, and there is an increasing amount of legislation governing how information must be treated at all stages of its life – creation, storage, retrieval, transmission, and destruction. Whenever client information is sent out of your organisation, or it is stored on mobile devices, there is a risk. Failure to properly take these risks into consideration can open the door to cyber-criminals and have far reaching consequences for both individuals and organisations. The risks from poor information handling include loss of data, identity theft, financial loss, regulatory fines and sanctions, loss of customer confidence, market position and reputation. Individual employees may also be subject to disciplinary action or dismissal.

Passwords – Passwords are the keys for getting access to almost everything in the digital world, so if a cyber-criminal can obtain a password it makes it easy for them to carry out their work. Failure to use strong passwords represents a serious risk to yourself and your organisation.[23] If criminals gain access to a password, it can lead to theft of money or data, fraudulent activity or hacking of computer systems.

4. The essentials to avoid being a victim

Slow down – Never let the implied urgency influence your careful review of an email or a pop-up on a website or on your computer. A phishing email or a bogus antivirus alert will try to get you to act first and think later. If the message conveys a sense of urgency, it is even more reason to be sceptical.

Check the facts – Be suspicious of an unsolicited phone call or email from a service provider and carry out due diligence checks. If it appears to be from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.

Confirm information requests – Ignore any email requesting financial information or passwords, and never provide personal information, unless you expected the request and you can validate the source.

Check website security – When accessing a website for the first time, carry out some basic checks to see if it is safe[24].

- Check the address bar to see whether the site is verified
- Check if HTTPS is used in the web address
- Check the website with Google Safe Browsing www.google.com/transparencyreport/safebrowsing/diagnostic

Reject offers of help – Legitimate companies and organisations do not make contact to provide help. If you did not specifically request assistance from the sender, consider any offer to 'help' a scam.

Be wary of links in emails – Curiosity leads to carelessness. If you don't know what the email is about, clicking a link is a bad choice. If you believe the link is genuine, stay in control; hovering over links in email will show the actual web address. Find the website yourself using a search engine to be sure the link is actually going to take you somewhere safe.

Don't assume an email sender is legitimate – Email hijacking and spoofing is common. Taking over a person's email accounts is common and once someone's email account is compromised, all of that person's contacts are likely to be preyed upon. Even when the sender appears to be someone you know, if you aren't expecting an email with a link or attachment, check with that person before clicking on links or downloading.

Keep client information secure – Ensure that client information sent externally is only ever sent to an appropriately authorised entity. It is preferable to utilise email encryption or some form of rights management so that an email with client information can only be accessed by the intended recipient. Keeping client data on mobile devices should be avoided wherever possible and where it is necessary to keep client data on a mobile device, the data should always be encrypted.

Before sharing information – Consider the following before sharing information:

- Is this information sensitive?
- What is it going to be used for?
- Do you have permission to share this information?
- Is it legal to share?
- Are you only sharing what is necessary?
- Is sharing the information in line with your organisation's policy?

---

23 Legal Insight - http://insight.thomsonreuters.com.au/resources/resource/password-protection-legal-practice-infographic/

24 Engadget, Is This Website Safe? The A-Z to Safer Browsing - www.engadget.com/2016/09/29/is-this-website-safe-the-a-z-to-safer-browsing/

Adopt strong password best practice:

- At least 15 characters long
- Use a combination of special characters, numbers, and letters, or consider using a phrase
- Make it random; avoid using repetition, dictionary words or usernames
- Maintain a different password for each account
- Change passwords regularly
- Use multi-factor authentication if it is available

Keep passwords safe – Do not share passwords, write them down or send them via email. Consider using a reputable password manager – as well as securely storing passwords, most password managers will also generate strong passwords.

Installing programs or apps is risky – Only install authorised programs or apps, and if your organisation does not have a stated policy on the installation of programs or apps, make sure you do a search or ask someone knowledgeable to be 100% sure it is safe before proceeding.

Public Wi-Fi is unsafe - Data over a public Wi-Fi network is often unencrypted and unsecured. If you must use a public Wi-Fi hotspot, also use a virtual private network (VPN) to secure your connection – a VPN creates a "secure tunnel" where data sent to and from your device is encrypted, making all that data secure. Don't log into password-protected websites that contain sensitive information when using a public Wi-Fi connection.

Basic cybersecurity vocabulary

Term	Definition
Access rights	The permission or privileges granted to users, programs or computers to create, change, delete or view data within a system. Typically defined by a security policy.
Adware	A type of software that automatically displays advertising material on a computer, usually as pop-ups. In most cases the adware comes bundled with other software, and this is done without any notification to the user or without the user's consent. The adware term may also refer to software that displays advertisements as an alternative to shareware registration fees.
Anti-malware	Software used to prevent, detect and remove many categories of malware. Usually used in connection with antivirus products, the anti-malware abilities can also include anti-spyware, anti-phishing or anti-spam solutions.
Antivirus software	Software designed to detect and potentially eliminate viruses, and to repair or quarantine files that have already been infected. Typically today antivirus programs protect users from more advanced online dangers, like ransomware, rootkits, Trojans, spyware and phishing.
Attack vector	A path or means by which an attacker gains access to the person or computer system.
Authentication	A mechanism for confirming the claimed identity of an individual user, typically via provided credentials (e.g. username and password).
Backdoor	A method, often secret, of bypassing normal authentication in a computer system. Backdoors are often used for securing unauthorised remote access to a computer
Biometrics	A security technique that verifies an individual's identity by analysing a unique physical attribute, such as a fingerprint or iris scan.
Blacklist	A blacklist is a list of entities that are considered to be unacceptable and are denied access or privileges.
Botnet	A term derived from "robot network;" is a large network of compromised (infected) computers that can be simultaneously controlled to launch large-scale attacks such as a denial-of-service attack on selected victims
Brute force attack	An exhaustive password-cracking procedure that tries all possibilities one by one.

Cleartext	Data that is not encrypted. Also known as plaintext.
Countermeasure	Any process that directly reduces a threat or vulnerability
Cryptography	Techniques used to encode and decode messages, in order to protect their security.
Cyber attack	An attack, via cyberspace, intended to disrupt, disable, destroy, or maliciously control a computing environment/infrastructure; steal information or destroy the integrity of data.
Cybersecurity	The protection of computer systems and the information contained therein.
Cyberspace	The notional environment in which communication over computer networks occurs.
Data Breach	An incident that results in the disclosure of potential exposure of sensitive information.
Decryption	A technique used to recover the original plaintext from the ciphertext so that it is intelligible. The decryption is a reverse process of the encryption.
DDoS (Distributed denial of service)	An assault on an internet service or website that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate. This type of attack uses multiple compromised systems (Botnet) to target a single system causing a Denial of Service (DoS).
Domain name system (DNS)	A database that is distributed across the Internet that allows domain names (web addresses) to be resolved into IP addresses (and vice versa), to locate services such as web and e-mail servers.
Encryption	The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext)
Exploit	A tool designed for use in exploiting a specific vulnerability within an IT system.
Freeware	Software available free of charge.
Hacker	A person who gains or attempts to gain unauthorised access to a computer system
Incident	An occurrence that constitutes a violation or imminent threat of violation of security policies, resulting in adverse consequences to a system or the information that the system processes, stores, or transmits.
Internet service provider (ISP)	A company that provides access to the Internet and related services.
IP address	A unique identifier in the form of a binary number that is assigned to each device connected to a network.
Keylogger	Software that usually runs hidden in the background and automatically captures and records the keystrokes of a computer user.
Malware	Short for malicious software, and is a general term referring to all types of malicious software, including computer viruses, worms and Trojans.
Man-in-the-middle attack	An attack in which a cyber criminal inserts themselves into communication between the victim and an internet service (such as online banking), then either replaces or alters the traffic between the two parties, typically to circumvent encryption and to enable capture of authentication information and then uses this information to impersonate the victim.
Multifactor authentication	A combination of more than one authentication method, typically a password in combination with a token, a biometric device, an SMS, or a code generator on a smart phone.
Password	A secret sequence of characters that is used as a means of authentication to confirm your identity when accessing a computer system.
Payload	This refers to that part of the malware that performs the malicious action.

Personally Identifiable Information (PII)	Information that could be used to identify an individual, either directly or indirectly.
Phishing	This is a type of email attack that attempts to acquire sensitive information by masquerading as a trustworthy entity - information such as usernames, passwords, and credit card details, etc.
Ransomware	A type of malicious software that installs covertly on a victim's computer or mobile device then either blocks access completely, or blocks access to files and demands payment to restore access. The most common form is categorised as crypto-ransomware, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.
Rootkit	A type of malicious software that gives the attacker privileged access to a computer and is able to conceal processes or programs associated with it so as to avoid detection by security software.
Security software	A generic term referring to any computer program that secures a computer system or computer network; the two main types of security software are virus protection software and software that removes adware and spyware (both require regular updating to remain effective).
Social engineering	An attack based on manipulating users in order to bypass security controls.
Spam	Unsolicited emails sent indiscriminately to a large lists of email addresses. Spam is often used to spread malware or carry out phishing.
Spear phishing	A type of personalised phishing where an attacker targets an individual, masquerades as a trusted party and uses social engineering techniques to obtain sensitive information, such as passwords, from the victim. Spear phishing uses a sense of urgency and familiarity to manipulate the victim.
Spoofing (email)	This is where an attacker uses a forged sender address in order to deceive the recipient. Email spoofing is a common tactic used in conjunction with phishing, where the attacker poses as one of the victim's contacts.
Spyware	Software whose purpose is to covertly collect information (e.g., web sites visited) and pass this information to a third party, without the informed consent of the computer user. It is often packaged with software that is intentionally downloaded, and even when that software is later uninstalled, the spyware may remain.
Threat	Anything that has the potential of becoming a security violation.
Trojan horse	A type of malicious software that is hidden within what appears to be a legitimate file or computer program, in order to trick users into downloading it, and unknowingly give unauthorised access to their computer.
Two-factor authentication	The use of two independent mechanisms for authentication e.g. requiring a smart card and a password.
Virtual private network (VPN)	A method of securely connecting two local private networks (e.g. your home and your office) over a public network (e.g. the Internet), enabling systems to safely send and receive data as if they were directly connected.
Virus	A piece of malicious software hidden within a program, specifically designed to replicate to other connected resources or systems once the program is installed on a computer.
Vulnerability	A flaw in software that has the potential to be exploited by an attacker. Vulnerabilities are often resolved by patches or security updates issued by the software creator/ vendor.
Whitelist	A list of entities that are considered to be acceptable and are granted access or privileges.
Worm	A type of malicious software that is standalone (unlike a virus, which is attached to another program) and spreads via computer networks by replicating itself without requiring interaction from the victim.
Zero-day attack	An attack that exploits a vulnerability before the software creator/vendor is even aware of its existence.

ESSENTIAL CYBERSECURITY TIPS

1. Password Protection

- Use strong passwords or adopt a passphrase that are hard to guess
- Use a different password for each website/device/log-in of any type
- Change passwords regularly, at least four times per year (set mandatory reminders)
- Keep passwords secure, including not stored anywhere without encryption
- Consider using multi-factor authentication (eg password + SMS code)

2. Email links and attachments

- Don't click on links or open attachments in emails from unknown senders
- Don't click on links or open attachments in emails that seem suspicious, even if you think you know the sender
- A single instance of poor grammar or spelling in an email can sometimes be an indication that it is a scam (however it is also possible that a scam email cannot be detected in this way)
- Be wary of .zip or .exe files, which may install malware on devices when opened
- Hover over links without clicking to verify whether they are for legitimate websites
- Run an anti-virus scan on attachments before opening
- Report suspicious emails to IT

3. Confidentiality and privacy

- Use passwords and/or encryption to protect confidential files
- Don't access confidential information from an unprotected computer, such as a shared public computer
- Don't respond to unsolicited emails requesting confidential information or personal information
- Verify email requests from known sources for confidential information or personal information (eg by a phone call)
- Don't post confidential information and limit personal information posted on social media
- Don't allow others to read your screen, including on public transport

4. Devices

- Use password protection on devices such as computers, USB drives and phones
- Install a laptop lock on laptops while they are in the office
- Install trusted security software on all devices
- Limit persons with administrative privileges
- Don't run computers with administrator access
- Lock device screens after a period of inactivity
- Log off devices when not in use
- Do not plug personal devices into work devices without permission and anti-virus scanning
- Keep devices physically secure by avoiding loss and not leaving them unattended outside of the office
- Remotely erase lost or stolen devices in accordance with firm procedure
- Destroy storage devices before equipment disposal, including fax machines and photocopiers
- Back up data on devices regularly
- Store back-ups separately and securely

5. **Programs and apps**
    - Don't install unauthorised programs or apps on work devices
    - Install vendor security updates to programs and apps
6. **Websites**
    - Limit browsing to trusted websites
    - Type the website address into the browser address bar rather than clicking on links
    - Ensure that the website address does not contain typographical errors, additional characters or unusual extensions
    - Always log out of secure website sessions when you are finished
    - Do not be enticed by 'clickbait', which may lead to the inadvertent download of malware
    - Look for the padlock symbol and "https" in the browser address when performing transactions or providing personal information online
7. **Use of public wi-fi**
    - Consider whether employees should avoid completely, or whether your organisation considers use acceptable with appropriate encryption
8. **Additional materials**
    - Consider company/law firm policies and procedures relating to cybersecurity
    - Consider relevant conditions of any relevant cyber threat insurance.
    - Consider any recent threat patterns in the relevant industry
9. **Remain alert and report suspicious online activity**
    - Trust your gut feeling – if it doesn't look right, don't click/respond
    - Report suspicious online activity or anything 'weird' in your computer systems to management and IT as quickly as possible, following processes outlined in relevant materials.

TRAINING OUTCOMES CHECKLIST

1. What is cybersecurity?

Participants will be able to explain what cybersecurity is and what it is intended to achieve.

2. The impact of cybercrime

Participants will recognise cybercrime as a real and present danger that could seriously damage their organisation.

3. The important role of employees

Participants will be able to identify how they contribute to cybersecurity.

4. Awareness about the main types of cybercrime

Participants will be able to explain in broad terms how the main types of cybercrime are carried out e.g. ransomware, phishing, identity theft, scams, hacking.

Participants will be able to explain and provide examples of how social engineering is employed in cybercrime.

5. Competency in preventing cybercrime

Participants will be alert to the use of social engineering and be able to recognise when it is being employed.

Participants will know how to identify a possible phishing email and be able to carry out checks to determine if it is a genuine email or not.

Participants will know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source.

Participants will be able explain the types of information that should not be shared on social media.

Participants will know not to install programs on their computer without first getting approval.

Participants will know and follow good password practices.

Participants will exercise due care and carry out appropriate checks before sending sensitive information externally.

Participants will know to raise concerns or issues regarding cybercrime, and will know the appropriate way to go about this.

6. Reference material

Participants will be provided with reference information including;

- Employee handout
- Policies e.g. Acceptable Use policy, Cybersecurity policy, Mobile Device policy, Access Control policy, Password policy, Remote Access policy.
- Link to the Law Council cybersecurity website

CYBERSECURITY CASE STUDIES

Case Study 1

John, the Managing Partner of a law firm, receives an email from an irate client.
The client alleges that one of the young lawyers, Zach, has billed for work that was never performed. The client has provided a number of documents further explaining the matter, as attached in the .zip file. Although John is not familiar with the client, Zach has been reprimanded for attempting to overcharge a client before, so he is not surprised to see this type of email. John downloads the attachments to review.

Once John opens the attachment, a program called CryptoWall is automatically installed on his computer. All his files have been encrypted – he has 48 hours to pay 2 bitcoins (approx. $1,800) for the files to be unlocked.

How could this be avoided?

- Treat any email attachments with high suspicion.
- John should have checked their internal client register to see if the 'client' is in fact a client. If it was a registered client, he should have called them to confirm the email's veracity.

Case Study 2

Max recently synchronised his work emails and calendar to his mobile phone, although the phone is owned and paid for by Max. He is a big fan of HBO's latest series, and regularly streams content illegally on his commute home. Max visits a number of sites to find the show he is after. The sites are flooded with advertising content. As a busy lawyer, Max has not had the chance to update his phone's software to the latest version released a few months ago. One advertisement on a site contains malware, which exploits an unpatched section of the phone's software. Max's phone is infected with ransomware. Rather than reporting this embarrassing incident to the firm, Max decides to simply buy a new phone.

What action should have been taken?

- Law firms should have detailed knowledge of the mobile devices its employees are using to access client information. All software should be updated regularly.
- Consider using a mobile data management product, which would allow the firm to remotely manage application on a phone and remove content from a phone.
- It is important that all cybersecurity incidents are reported. In Max's case, the extent of the intrusion was not known. The malware may have extracted client information. By failing to investigate further, Max may have placed the firm in breach of mandatory data breach notification obligations (legislation pending).
- Law firms have a paramount duty to protect client confidentiality and failure to do so could expose the firm's partners and employees to regulatory consequences (i.e. charges of unprofessional conduct, fines etc). By failing to report the potential breach means that the firm has no opportunity to mitigate the consequences of any breach.

Case Study 3

Pauline is a property lawyer, holding $2 million of client money in the firm's trust account from a recent settlement. The client is travelling abroad and is communicating via email. Pauline has not worked with this client before, but is aware he controls various entities throughout the world. One morning, Pauline receives an email from the client, requesting a transfer of the $2 million, to be split across a three different accounts. One of these matches the account details the client had previously provided, although the 'tone' of the email was not quite right.

Having recently joined the firm, Pauline recalled her cyber security induction session. Although she had the client's instructions in writing, she was uneasy and decided to phone the client. The client could not recall sending any such email. On closer inspection, somebody has gained unauthorised access to the client's email account.

It is essential to carry out due diligence before acting on information to transfer money. You cannot assume an email is safe just because it appears to be sent by someone who is known and trusted. Always be alert for the possibility of social engineering and if any doubts, carry out appropriate checks to confirm an email's veracity.

Case Study 4

One morning, a lawyer found that she could not open Word and Excel files on her computer, and the files appeared to be corrupted. The IT Department investigated further and found that the files had been encrypted – she could not access any of them.

All of the encrypted files were in a Dropbox folder. The lawyer had synchronised the files between her work computer and her personal computer at home. Further investigation uncovered that the lawyer's home computer had been subjected to a ransomware attack. Malicious software had gained access to her home computer and encrypted all of her files, including the files in the Dropbox folder. Dropbox had diligently synchronised these encrypted files back to her work computer.

What are the lessons here?

- All business files must be centrally stored, properly secured and backed up on a daily basis. In this case there were important business files being stored locally on the lawyer's work computer.
- Using file sharing software like Dropbox is a risk, as it allows files to be taken into an uncontrolled environment. In this case it was the lawyer's home computer, which did not have up to date security software installed.

Case Study 5

A principal of a law firm has been expecting a parcel from overseas. He received several emails appearing to be from Australia Post and eventually thought the emails might be about the parcel he was waiting on. He opened one of the emails and it said his parcel could not be delivered. He was instructed to download and print the attached label and take it to Australia Post. When he clicked on the link it opened a white page and nothing more.

About three minutes later all the icons on his screen went white and he had a message flash up that the crypto locker virus had locked his computer. The message said he had to pay $640 in bitcoin by a certain time to have his computer released and if he didn't pay by then it would go up to $1280 with again a limited time to pay.

After consulting with his IT team, he decided not to pay the ransom. Most client information was stored on the cloud and had not been affected. He did, however, lose several documents that had taken weeks to draft.

This could easily have been avoided. The practitioner could have checked the email address of the Australia Post email by hovering over the sender's address or copying it into Google to look for fraud warnings.

RESOURCES FOR PREPARING CYBERSECURITY TRAINING

Australian Resources:

Legal Practitioners' Liability Committee (LPLC) – *"Key Risk Checklist: Cyber Security"*
https://lplc.com.au/wp-content/uploads/2016/10/LPLC-Key-Risk-Checklist-Cyber-Security.pdf

Logic Plus IT Solution – *"Cyber Security Checklist – Do You Fail to Secure Your Business"*
http://logicplus.com.au/cyber-security-checklist-do-you-fail-to-secure-your-business/

UNSW – *"Cyber Security"*
http://guides.lib.unsw.adfa.edu.au/cybersecurity/add_resources

Australian Government, Department of Defence - *"Cyber Security, It's Your Move"*
www.asd.gov.au/partners/cybersecurity.htm

Australian Government, Australian Cyber Security Centre (ACSC) – *"2016 Threat Report"*
https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

Australian Government, *Stay Smart Online Guides*
www.staysmartonline.gov.au/guides

ASIC – *"Cyber security and directors"*
http://asic.gov.au/regulatory-resources/corporate-governance/corporate-governance-articles/cyber-security-and-directors/

ASIC – *"Cyber resilience health check"*
http://asic.gov.au/regulatory-resources/corporate-governance/corporate-governance-articles/cyber-resilience-health-check/

International Resources:

National Association of Corporate Directions – *"Cyber-Risk Oversight"*
https://na.theiia.org/standards-guidance/Public%20Documents/NACD-Financial-Lines.pdf

American Institute of CPAs (AICPA) - *"'Top 20' Cybersecurity Checklist"*
www.aicpa.org/InterestAreas/PrivateCompaniesPracticeSection/QualityServicesDelivery/InformationTechnology/Pages/cybersecurity-checklist.aspx

Bic Idea Technology – *"Top 10 Cyber Security Training Tips for Your Company's Employees"*
www.bigideatech.com/top-10-cyber-security-training-tips-for-your-companys-employees/

Financial Industry Regulatory Authority (FINRA) – *"Cybersecurity"*
www.finra.org/industry/cybersecurity

utah.gov – *"Cyber Security Controls Checklist"*
www.utah.gov/beready/business/documents/BRUCyberSecurityChecklist.pdf

Security Standards Council – *"Information Supplement: Best Practices for Implementing a Security Awareness Program"*
www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Sophos – *"IT Security Do's and Don'ts"*
www.sophos.com/en-us/security-news-trends/it-security-dos-and-donts/training-tools.aspx