UNDERSTANDING THE CYBER THREAT

Ian Bloomfield
Managing Director

www.ignite.com.au

February 2018

What will be covered

- Why is cyber security important?
- What is cybercrime?
- The impact of cybercrime
- Cybercrime in action
- How to avoid becoming a victim
- The value of a risk assessment

Why is cyber security important?

Australia's Cyber Security Strategy was released in 2016.

Foreword by Prime Minister Malcolm Turnbull

"While governments can take the lead in facilitating innovation and providing security, businesses need to ensure their cyber security practices are robust and up to date."

Cyber Security Strategy: https://cybersecuritystrategy.dpmc.gov.au

Why is cyber security important?

Law Council of Australia President, Stuart Clark AM talking in 2016 about the Law Council of Australia cyber security initiative.

"Consideration of cyber risks should evolve beyond seeing them as an 'IT issue.' Cybersecurity in legal practices should be managed through a strategic and coordinated approach, and that means making cybersecurity a strategic objective."

Cyber Precedent website: www.lawcouncil.asn.au/lawcouncil/cyber-precedent-home

Why is cyber security important?

Australian Privacy Principles guidelines

"An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure."

Source: Office of the Australian Information Commissioner - Australian Privacy Principles guidelines
https://www.oaic.gov.au/agencies-and-organisations/app-guidelines

Why is cyber security important?

Office of the Australian Information Commissioner Guide to securing personal information

"…the OAIC will refer to this guide when undertaking its Privacy Act functions, including when investigating whether an entity has complied with its personal information security obligations…"

Source: Office of the Australian Information Commissioner - Guide to securing personal information
https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

What is Cybercrime? Definition

- There is a narrow statutory meaning as used in the Cybercrime Act 2001 (Cwlth), which details offences against computer data and systems.

Source: Australian Institute of Criminology

- More generally cybercrime is used as an umbrella term to refer to an array of criminal activity involving electronic data, computer systems, or the internet

What is Cybercrime? Scale & Sophistication

- Cybercrime is big business
- Perpetrators include organised crime, legitimate companies (acting illegally) and nation states
- Many thousands of individual cyber criminals part of a much bigger ecosystem
  - marketable skills
  - commodified products and services

Cybercrime Impact

Australia's Cost

Australia's Cyber Security Strategy 2016

*"Figures vary, but **cybercrime** is estimated to **cost Australians over $1 billion each year**. Worldwide, losses from cyber security attacks are estimated to cost economies around one per cent of GDP per year. On this basis, the **real impact of cybercrime** to Australia could be **around $17 billion annually**."*

Source: Cyber Security Strategy: https://cybersecuritystrategy.dpmc.gov.au

Cybercrime Impact

Small Business

- Data loss – the impact can range from mildly inconvenient through to potentially crippling
- Financial burden – loss of clients, ransom payment, cost of cleaning up
- Reputation – data breach publicity
- Legal action – from OAIC or from clients

Cybercrime in Action

- Theft
  - Stealing data – any information of value
- Extortion
  - Ransomware which involves the encryption of the files on a victim's computer, and a demand for money to decrypt them
- Fraud
  - Social engineering scams - a convincing story to get the victim to send the scammer money

Cybercrime in Action case study 1

- Employee at a law firm received an email appearing to be from Australia Post saying that a parcel could not be delivered and asking for confirmation of the correct address by clicking on a link at the bottom of the email
- Clicking on the link lead to a bogus Australia Post website, identical to the real Australia post website except for the www.auspost.tk address
- After completing the 'Captcha' security and clicking on the 'Submit' button, malicious software was downloaded

Cybercrime in Action case study 1

- The software installed was CryptoWall ransomware
- All of the files on the law firm's server were encrypted and there was a note displayed on the user's computer

WE HAVE ENCRYPTED YOUR FILES WITH Crypt0L0cker !!!

==========

Your important files (including those on the network disks, USB, etc): photos,videos, documents, etc. were encrypted with our Crypt0L0cker. The only way to get your files back is to pay us. Otherwise, your files will be lost.

You have to pay us if you want to recover your files.

Cybercrime in Action case study 1

- The law firm did not pay the ransom, they had all files on the server backed up, so they engaged their IT provider to carry out a restoration
- The cost:
  - 3 hours work by the IT provider to restore the server
  - A days lost work for 7 staff
  - Inability to service clients

Cybercrime in Action case study 2

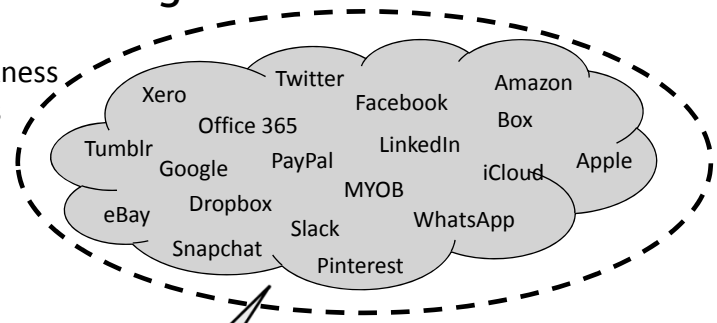
- Law firm defrauded of more that $100,000
- Email correspondence between the law firm and client on a matter involving a settlement
- The scammer had compromised either the lawyer's or the client's email account
- The scammer identified the email conversation as an opportunity

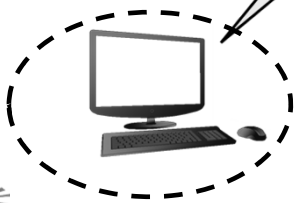
Cybercrime in Action case study 2

- Scammer sent convincing email to the lawyer appearing to come from the client
- The 'client' asked for settlement money to be sent to her bank account as she was 'too busy' to bank a cheque
- The money was transferred and the scam only realised after the client contacted the law firm asking what had happened to the cheque

Avoid Becoming a Victim

In the cloud
the biggest weakness
is passwords





On your computer
most threats are delivered
via email and websites

Avoid Becoming a Victim
Passwords

- Have a password policy
  - Use strong passwords
  - A different one for every account
- Enforce the password policy
- Provide staff with a password manager

Avoid Becoming a Victim
Two factor authentication

- ‘Must have’ for cloud system accounts
- Provides extra layer of protection
- Available for most common cloud solutions, business and personal

Avoid Becoming a Victim
Email

- Use business grade email service with business grade filtering – Office 365 recommended
- Do not use a generic email service such as; Gmail, Bigpond, Optus, iiNet etc.
- Don’t send email from personal email accounts
- Confirm recipient’s email address before sending

Avoid Becoming a Victim Email

"Email is not a secure form of communication and you should develop procedures to manage the transmission of personal information via email." *

- Avoid emailing confidential or Personal Information unless necessary
- Secure any confidential information
  - Use 'end-to-end' email encryption
  - Use encrypted/password protected attachments

* Source: Office of the Australian Information Commissioner - Guide to securing personal information https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

Avoid Becoming a Victim Internet

- Website filtering provides protection from malicious websites and compromised websites
- When you access a website, it's reputation is checked before it loads in your browser
- If the website you want to view doesn't have a good reputation it is blocked

Avoid Becoming a Victim
How it all works

- In the first Case Study the victim received a phishing email
  - Effective email filtering would have blocked this
- If it had got through and the victim then clicked on the link
  - Web filtering would have blocked the bogus Australia Post website

Avoid Becoming a Victim
How it all works

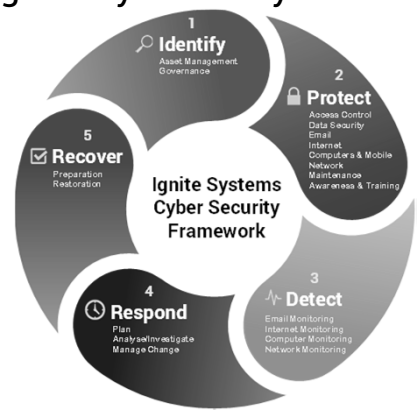
- In the second Case Study the victim had their email account compromised
  - Even though the scammer had the victim's email password, two-factor authentication would have prevented the scammer gaining access
  - Good practice procedures in place for the transfer of money would have prevented the final act of transferring money to the scammer

The Value of a Risk Assessment

- Many businesses consider themselves protected against cyber security risks because they've implemented security 'products' or 'services'.
- BUT - you don't know what you don't know.
- You are not protected if the measures you have in place are not adequate, or not focused on protecting what is important.

The Value of a Risk Assessment

The Ignite Systems Cyber Security Risk Assessment is a comprehensive assessment against the Ignite Systems Cyber Security Framework



Resources

Law Council of Australia Cyber Precedent
http://lawcouncil.asn.au/lawcouncil/cyber-precedent-home

Legal Practitioners' Liability Committee (LPLC) - Bulletin
https://lplc.com.au/bulletins/cyber-security-breach-claims-caused-by-fake-client-email

Queensland Law Society - Alert
www.qls.com.au/Knowledge_centre/Ethics/Resources/Cyber_security/Cyber_criminals_successfully_divert_Qld_Solicitor%E2%80%99s_trust_transfers

Law Institute of Victoria (LIV) - Law Tech Essentials "Cyber security essentials for law firms"
https://www.liv.asn.au/getattachment/Professional-Practice/Areas-of-Law/Technology-and-the-Law/Resources/20171122_LP_LawTechEssentials_CyberSecuirtyFirms-v02.pdf

Guide to securing personal information
www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

Australian Cybercrime Online Reporting Network (ACORN)
www.acorn.gov.au

Australian Cyber Security Centre
www.acsc.gov.au

SCAMwatch
www.scamwatch.gov.au

Stay Smart Online
www.communications.gov.au/what-we-do/internet/stay-smart-online

Ian Bloomfield
03 9379 4360
ian.bloomfield@ignite.com.au
www.ignite.com.au