UNDERSTANDING THE CYBER THREAT

Ian Bloomfield
Managing Director

ignite Systems
www.ignite.com.au

26 May 2018

What will be covered

- Why is cyber security important?
- What is cybercrime?
- Impact of cybercrime
- Cybercrime in action
- Effective tactics
- Defence strategy

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?

Angus Taylor, Minister for Law Enforcement and Cyber Security

“This is a very real issue for every Australian, whether you are running a small business, in your home, on the phone, on the street, cyber security is now becoming a critical issue.”

Source: Sky News, 23 April 2018

Why is cyber security important?

Kate Carnell, Australian Small Business and Family Enterprise Ombudsman

“Cyber criminals are becoming more sophisticated and small businesses are particularly vulnerable.

Online threats are just as real as physical threats. Cyber security needs to be taken seriously, like having locks on your doors and a burglar alarm.”

Source: Dynamic Business – 8 January 2018
https://www.dynamicbusiness.com.au/news/small-business-cyber-security-guide-released.html

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 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

- Company defrauded of more that $300,000
- Accounts person received a spear phishing email and was duped into providing their email password
- The email account was compromised and the scammer had access to all email in the account
- The scammer identified an opportunity involving an email conversation between the service provider and a client

Cybercrime in Action
case study 2

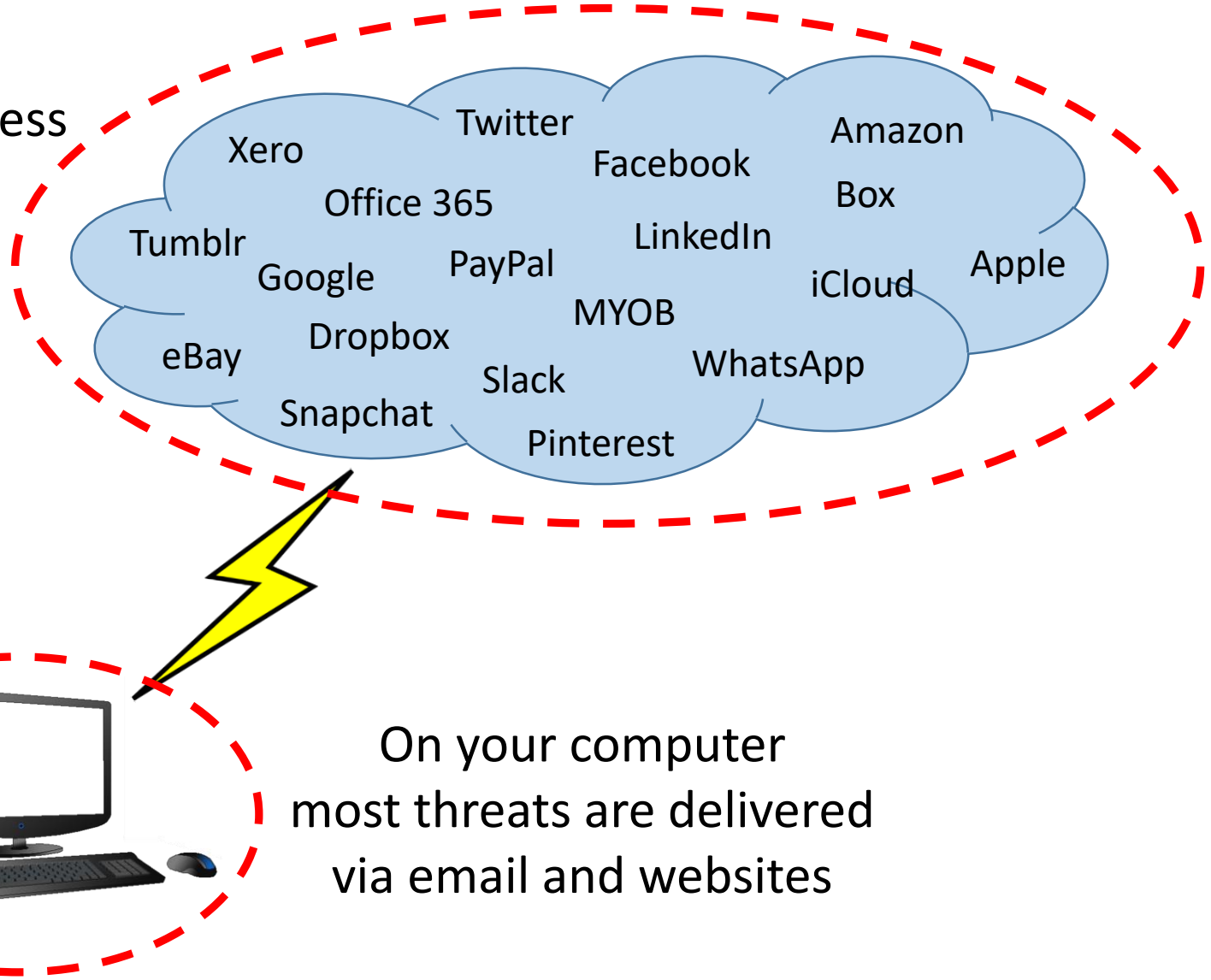
- Scammer waited until the timing was right then sent some grooming emails to the client appearing to come from the service provider
- The ‘service provider’ prompted the client about a due invoice and advised they had some issues with their bank account
- Shortly after the ‘service provider’ advised the client some revised bank account details for payment of future invoices

Cybercrime in Action
case study 2

- The invoice was paid by transferring the money to the ‘new’ bank account
- The scam was only realised after the service provider queried the client about non-payment of the invoice

Tactics to Avoid Becoming a Victim

In the cloud
the biggest weakness
is passwords



On your computer
most threats are delivered
via email and websites

Tactics to 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

Tactics to 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

Tactics to 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

Tactics to 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

Tactics to 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

How the tactics work – case study 1

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

How the tactics work – case study 2

- Service provider received a spear phishing email
  - Effective email filtering may have blocked this
- If the email had got through and the victim then clicked on the link
  - Web filtering would have blocked accessing the website that captured the email password
- Even if the scammer had the password to the service provider's email account
  - Two-factor authentication would have prevented the scammer gaining access

The Cyber Security Solution

- Tactics are useful, but they are band-aids and not a solution for a business
- You are not protected if the measures you have in place are not adequate, or not focused on protecting what is important
- You are not protected if you are relying on technology alone
- The solution is a strategy

4 Step Defence Strategy

1. Governance
2. Risk
3. Culture
4. Training

Defence Strategy - Step 1: Governance

It starts at the top

- Cyber security is not just an IT issue, it is a business issue
- Cyber security is relevant to everyone and everything that connects to the internet
- Cyber security cannot be effective if management does not take responsibility

Defence Strategy - Step 2: Risk

Know what you are facing

- Cyber security has to be designed around an understanding of your risks
- There is no simple or single fix to cyber security
- Cyberattacks are constantly changing and becoming evermore sophisticated
- Understanding risks allows prioritising of actions to maximise protection

Defence Strategy - Step 3: Culture

Get everyone on board

- Start with cyber security policies and procedures
- Make them relevant by involving people
- Make them readily available
- Make them known by actively promoting them
- Compliance - observe and respond, don't ignore

Defence Strategy - Step 4: Training

People are the best defence

- Technology alone is not enough
- Cyber security is not a business skill, it is a life skill
- The end-game is to change habits
- People need to understand why they should change, followed by ongoing reinforcement

Strategy at Work - AIC (Victorian Division)

1. Governance

   Jill Ludwell and Ann Kinnear recognised that cyber security was a critical business issue requiring action from the top

2. Risk

   Ignite Systems conducted a Cyber Security Risk Assessment

3. Culture

   Ignite Systems has been engaged to provide cyber secure technology management services

4. Training

   Cyber security awareness training for AIC-Vic Executive

   Developing cyber security awareness training for AIC members

Ian Bloomfield

03 9379 4360

ian.bloomfield@ignite.com.au

Presentation resources available at
www.ignite.com.au/aic