Cyber hackers don’t discriminate

Monica Schlesinger & Tina Vuong

Guest Speakers

Monica Schlesinger
Principal Advisory
Boards Group

AdvisoryBoardsGroup

Monica is recognised as a specialist Cybersecurity governance expert who also has extensive Board experience and knowledge. She started her career as an IT architect and systems integrator and managed large projects for a wide range of industries. Her knowledge in security dates back to over 20 years ago. Monica is a Director and Chair on five boards (NFP and for profit).

Tina Vuong
Capability Building
coordinator
ConnectingUp

Connecting Up

In her ConnectingUp role, Tina coordinates the Events grants and Sponsorships &responds to a variety of queries about the company's programs. She helps build capability within the NFP sector.
Tina brings many years of experience from Stratco and m.Net.

Tina will be the webinar moderator asking some of the questions she gathered from the interaction with the ConnectingUp customers about Cyber security.

Topics for Discussion

1. Cyber attacks 101

2. Are NFPs targeted by cyber attacks?

3. Are you prepared for a cyber attack?

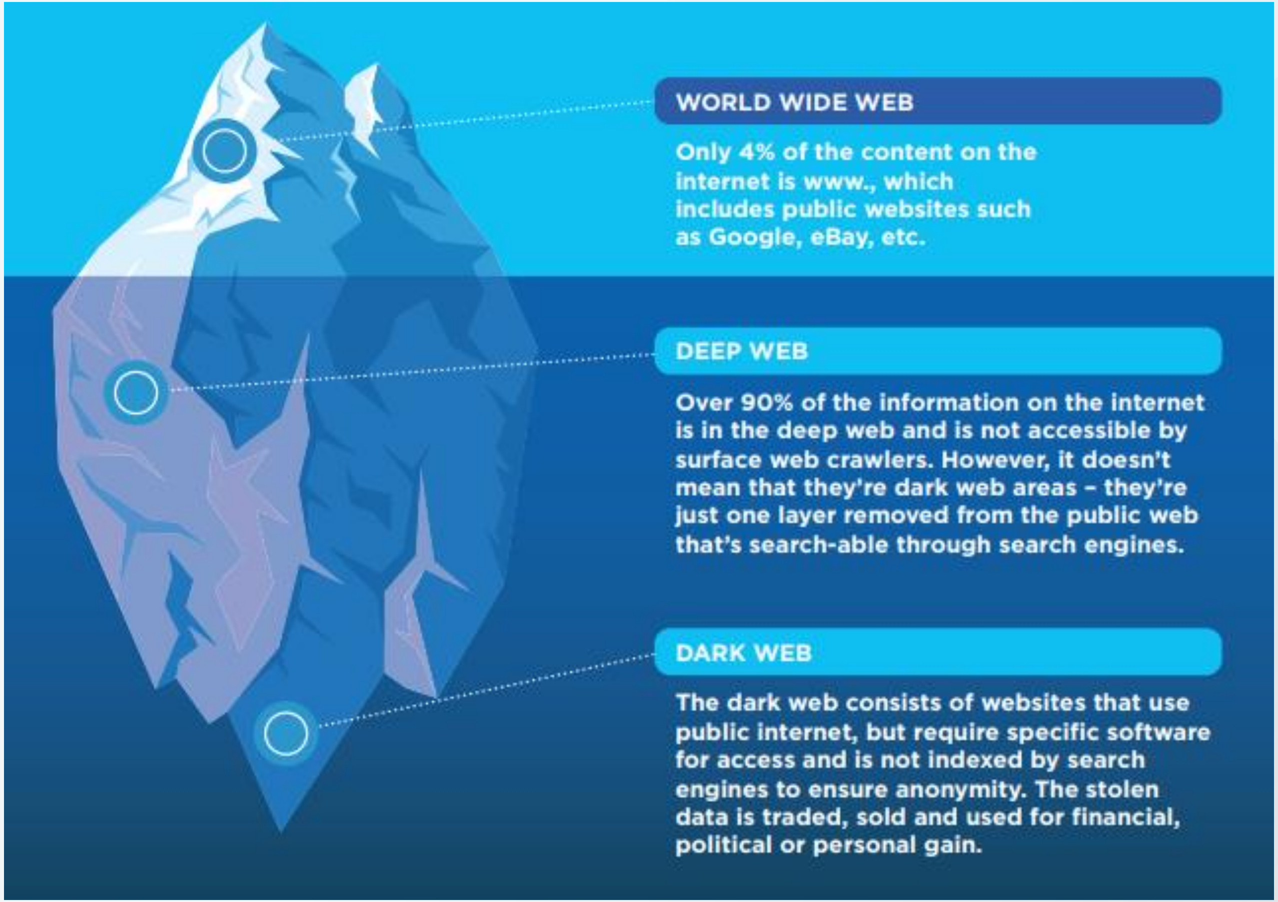
Enter To Win!

4. Survey & prize

5. Q&A

1. Cyber attacks 101

The entire web



WORLD WIDE WEB

Only 4% of the content on the internet is www., which includes public websites such as Google, eBay, etc.

DEEP WEB

Over 90% of the information on the internet is in the deep web and is not accessible by surface web crawlers. However, it doesn't mean that they're dark web areas – they're just one layer removed from the public web that's search-able through search engines.

DARK WEB

The dark web consists of websites that use public internet, but require specific software for access and is not indexed by search engines to ensure anonymity. The stolen data is traded, sold and used for financial, political or personal gain.

Cyber attacks 101

- Identity theft fastest growing crime in US
- 2016/2017 – more than 75% of Fortune 500 were breached
- By 2020 more than 25% of identified attacks in enterprises will involve IoT (Internet of Things)
- 2016/2017 - Consumers globally lost $180 billion US to cybercrime
- 75% of the top 20 US banks are infected with malware
- Nearly half of all crime in the UK is cybercrime.
- Ransomware attacks have increased 300% in 2016/2017

Regulatory environment - Australia

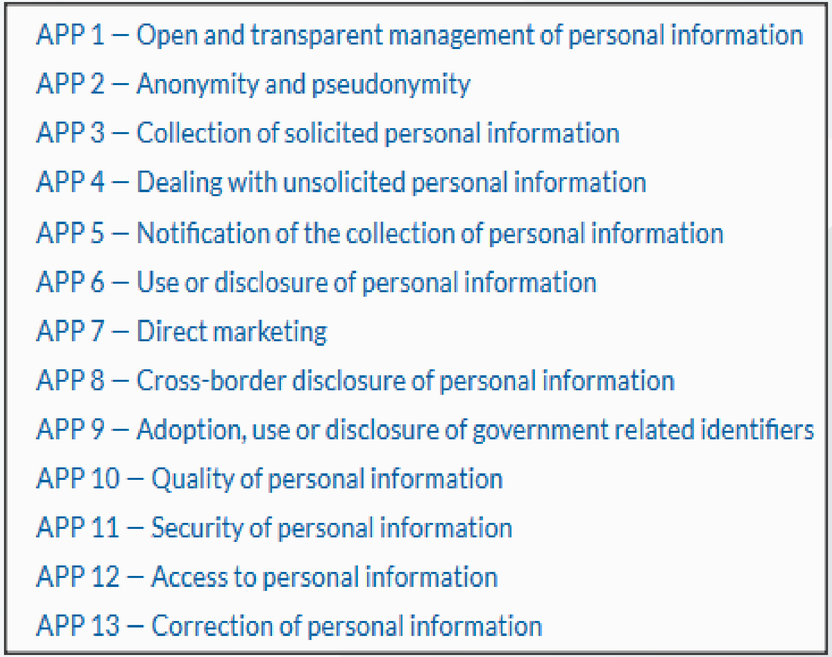
- **Privacy Act Part IIIC** commenced 22 February 2018.
- **A scheme for mandatory data breach notifications** applies to all entities subject to the Privacy Act:
  - **Agencies** – most government agencies
  - Organisations whose **turnover is greater than $3 million**
  - Organisations which can have lower turnover:
    - Organisations who are **Health services providers, Entities trading in personal data**, etc
  - Other Categories: **Credit providers, credit reporting bodies, TFN recipients**, etc

Regulatory environment - NZ

- **Privacy Act 1993 (http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html)**

- **New Zealand** currently falls into a group of countries in which breach reporting **is not mandatory**. Breach notification is **voluntary** but **that is likely that will change in the future**. The Government has indicated that a mandatory requirement to report data breaches is going to be part of the **changes made in a new Privacy Act**.

Privacy Principles - Australia



APP 1 – Open and transparent management of personal information

APP 2 – Anonymity and pseudonymity

APP 3 – Collection of solicited personal information

APP 4 – Dealing with unsolicited personal information

APP 5 – Notification of the collection of personal information

APP 6 – Use or disclosure of personal information

APP 7 – Direct marketing

APP 8 – Cross-border disclosure of personal information

APP 9 – Adoption, use or disclosure of government related identifiers

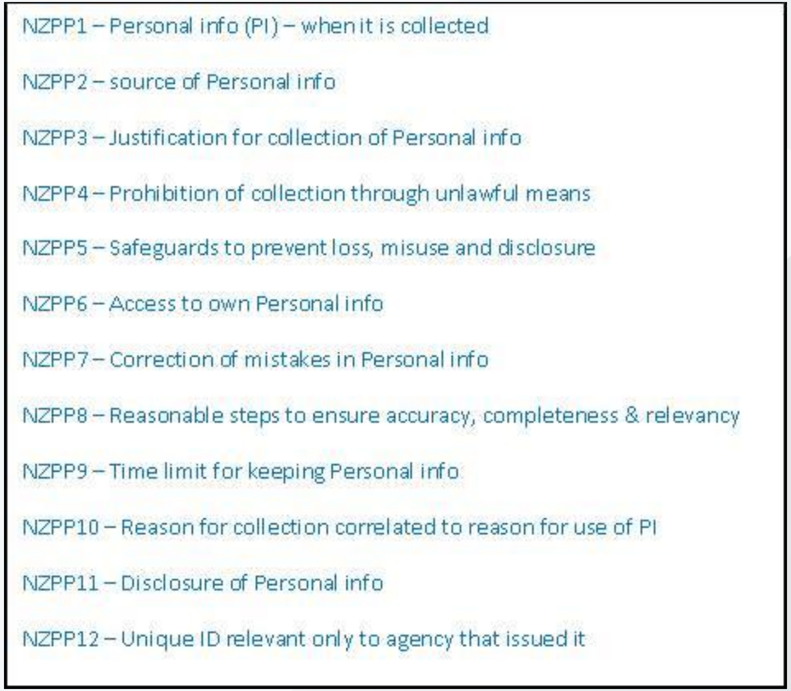
APP 10 – Quality of personal information

APP 11 – Security of personal information

APP 12 – Access to personal information

APP 13 – Correction of personal information

Privacy Principles - NZ



NZPP1 – Personal info (PI) – when it is collected

NZPP2 – source of Personal info

NZPP3 – Justification for collection of Personal info

NZPP4 – Prohibition of collection through unlawful means

NZPP5 – Safeguards to prevent loss, misuse and disclosure

NZPP6 – Access to own Personal info

NZPP7 – Correction of mistakes in Personal info

NZPP8 – Reasonable steps to ensure accuracy, completeness & relevancy

NZPP9 – Time limit for keeping Personal info

NZPP10 – Reason for collection correlated to reason for use of PI

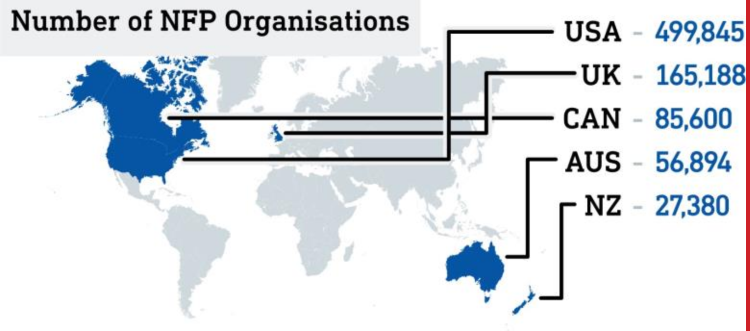
NZPP11 – Disclosure of Personal info

NZPP12 – Unique ID relevant only to agency that issued it

Best practice - NFPs

- Organisations that are not subject to the Privacy Act
- Definitions and assessment of Serious Harm
- What about the Stakeholders?

2. Are NFPs targeted by Cyber attacks?



Nature of cyber attacks

- State sponsored
  - 2017 – Australian Minister Marise Payne (Defence) stated that over 400 companies were hacked by Russian state-sponsored cyber attacks
  - 2017 – NZ Director Gen Hampton (Gov Communications Security Bureau) blames Russia for 122 incidents

- Hackers:
  - Motivation
  - Tools
  - Ease of mounting attacks

- What about the Stakeholders?

Examples

- 2017 – Cyber attack exposed the personal information of 8000 Family Planning NSW clients (Australia)

- 2015 – National Centre for Charitable Statistics (US) – hackers obtained info on more than 700,000 US not-for-profits from the 990 database

- 2016 – Australian Red Cross personal data breach

2017 WannaCry – hackers don’t discriminate

336,856
Infection rate USA

100,448
Other countries combined infection rate

54,841
Infection rate UK

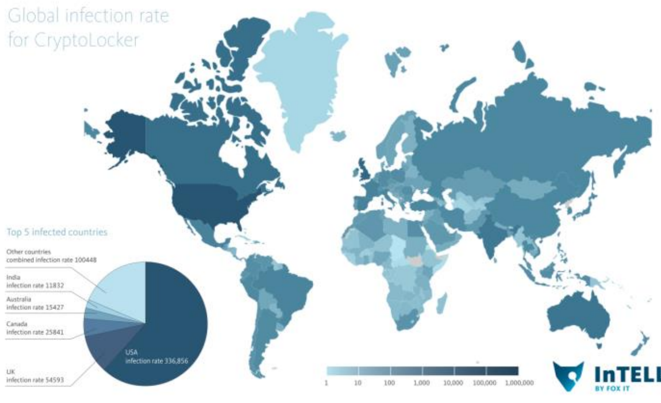
25,841
Infection rate Canada

15,427
Infection rate Australia

11,832
Infection rate India

130,634
Paid by victims as of 14 June 2017

4 billion
According to Cyence – cyber risk modelling firm



Computers were hacked due to lack of up-to-date Patches

Most of them were running Windows 7

Payload(attack)done through scanning the Internet

3. Are you prepared for a Cyber attack?

Cyber readiness & resilience

- What measures can you take to prepare?
- Board level involvement
- First steps

Cyber products

- Cyber Governance Course for Directors & Officers
- Cyber Risk Management Workshop
- Cyber security governance Healthcheck/Audit
- Cyber Mentoring Program for CEOs/Directors/Managers
- Cyber Security Newsletter (admin@advisoryboardsgroup.com)

http://advisoryboardsgroup.com/services.html

Survey

- Please go to the link provided to fill in the Survey

- The winner will benefit from a 30 minute discussion with Monica over the phone about their organisation's readiness for Cyber attacks

4. Q&A

NEXT STEPS

To find out more about the necessary steps to protect the organisation, please contact us at:

monica@advisoryboardsgroup.com

AdvisoryBoardsGroup

Connecting Up