Think STRENGTH. Think Chubb.

Cyber Insurance

Andrew Taylor
Asia Pacific Zone Product Manager
Chubb Pro – PI, Media, Cyber

The World Has Changed

Then	Now
1992 first text message	More txt's that the entire planets population
Paper files, carbon paper, photo copiers	Digital files we created 4 exabytes (4x10^19) of unique information in 2010 more than in the past 5,000 years)
1981 first computer virus	3.5 new threats per second
Property, major asset	Knowledge, major asset
Privacy - moral decency	Global concern and legislation in almost every developed country

Or so I heard ….. .

TRENDS

- Targeted attacks grew by 91% in 2013
- Over **552 million identities** were stolen
- 1 in 8 legitimate websites have a critical **vulnerability**
- Ransonware attacks **grew by 500%**
- **1 in 392** emails contain a phishing attack
- NO ONE IS IMMUNE

- Time to compromise time v time to discovery keeps growing
- **They are already inside !!!!**

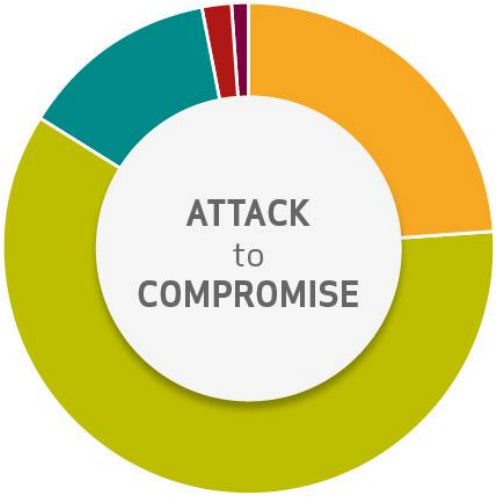
- Costs of cyber crime keep rising
- Legislation is catching up with reality
- Businesses are unprepared
- Nation State boarders are being blurred on-line

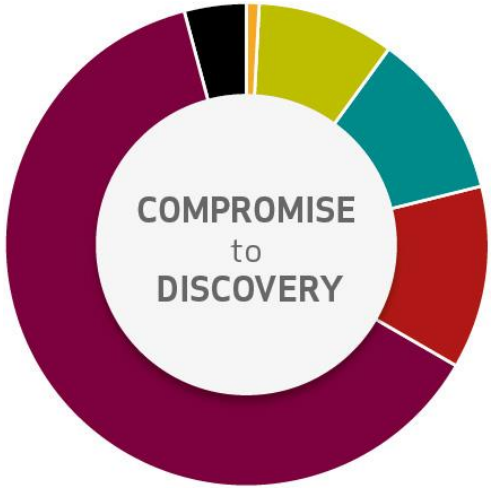
THE REALITY

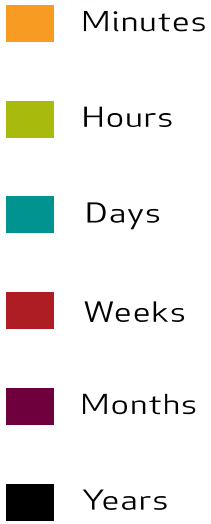
MINIMAL TIME TO COMPROMISE

BUT A LONG TIME TO DISCOVERY

- **IN 84% OF CASES,** INITIAL COMPROMISE TOOK HOURS OR LESS.
- **IN 66% OF CASES**, THE BREACH WASN'T DISCOVERED **FOR MONTHS OR EVEN YEARS.**





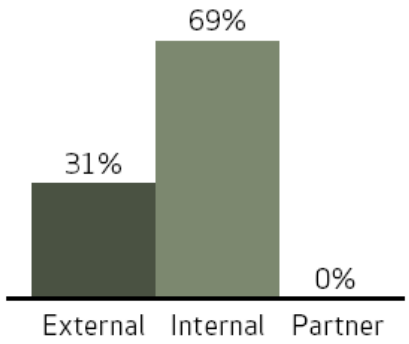


Taken from a AILA Verizon presentation 2013 (Paul Black)

THE WEAKEST LINK

- Cyber Insurance is needed because of ……. **YOU AND ME**
  - People are the biggest threat to organisations' networks
  - Insiders being *"careless rather than malicious"*

Figure 11: Threat actor categories across 47,000+ security incidents



The list of modern myths just shrunk by one; insider majorities do exist! Bigfoot and Nessie remain unconfirmed. In all seriousness, though, this is an important reminder that confirmed data breaches are a rather exclusive subset amid the plethora of all types of security incidents. As will become more apparent in the Threat Actions section, most of these are insiders acting carelessly rather than maliciously.

- Reality is that external parties present the largest financial threat. BUT people are still the problem not technology.

Source: Verizon 2013 Data Breach Investigations Report Page 20

THE COSTS OF CYBER CRIME

BREACH COSTS (2014 PONEMON STUDY)*

1. **Number of records breached 20,073** Australian Organisations

2. **Cost per records US$135 (US$145 average)**
   - *Healthcare US$359 - Retail $100*

3. **Organisational Costs US$2.7M Australia US$3.5M (globally)**
   - *Root cause Malicious Attacks 37%*

4. **Australian companies experience 3% - 5% abnormal customer churn**

BREACH COSTS (2013 PONEMON STUDY)*

Table 2. Cost changes over four years	FY 2009	FY 2010	FY 2011	FY 2011
Investigations & forensics	26%	27%	28%	32%
Audit and consulting services	11%	10%	9%	8%
Outbound contact costs	10%	12%	12%	11%
Inbound contact costs	9%	8%	7%	7%
Public relations/communications	3%	3%	2%	0%
Legal services - defence	4%	3%	5%	9%
Legal services - compliance	6%	5%	4%	5%
Free or discounted services	1%	1%	1%	0%
Identity protection services	0%	0%	0%	0%
Lost customer business	22%	22%	22%	20%
Customer acquisition cost	8%	9%	10%	8%

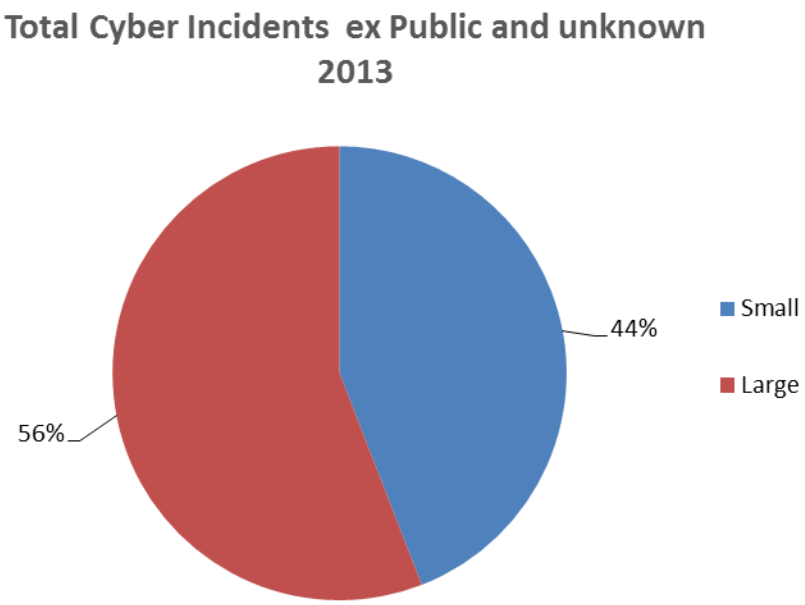
Ponemon Institute Cost of a data Breach Study – Australia Pg 15

WHAT IS CYBER INSURANCE?

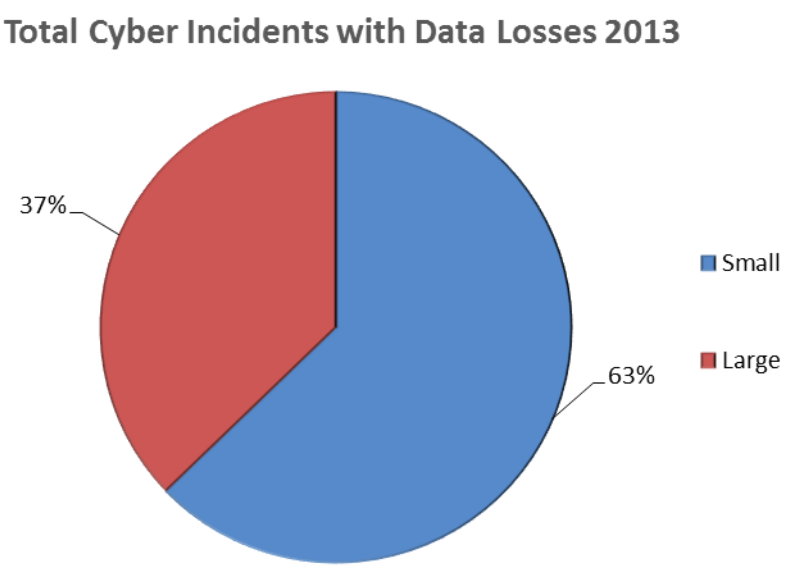
WHAT IS CYBER INSURANCE?

- Cyber Insurance provides
  - first-party expense coverage
  - Business Interruption and extra expense coverage
  - third-party liability coverage
- Cyber Insurance is a blend 1st and 3rd party covers that meet the exposures of a digital age. There are content exposures and privacy / data exposures.
- Cyber Insurance fills the gaps of traditional insurance policies e.g. ISR, CGL, PI, Crime.
- Cyber Insurance offers protection for Network Security and Privacy exposures.
- Chubb's policy is called CyberSecurity by Chubb℠

THE VICTIMS by Size



Size does not matter
All organisations are a TARGET



Source: Verizon Data Breach Investigations report 2014 Pg 6 Figure 2 & 3

WHO ARE THE ATTACKERS?

ACTIVISTS

Aim is to **maximise disruption** and embarrass victims. Very basic methods and are opportunistic.

CRIMINALS

Motivated by **financial gain**, so will take any data that might have financial value. **More calculated and complex** than activists in how they select targets.

SPIES

Often state-sponsored, driven to get **exactly what they want**. Often state-sponsored, use sophisticated tools to commit **most targeted attacks**. **RELENTLESS.**

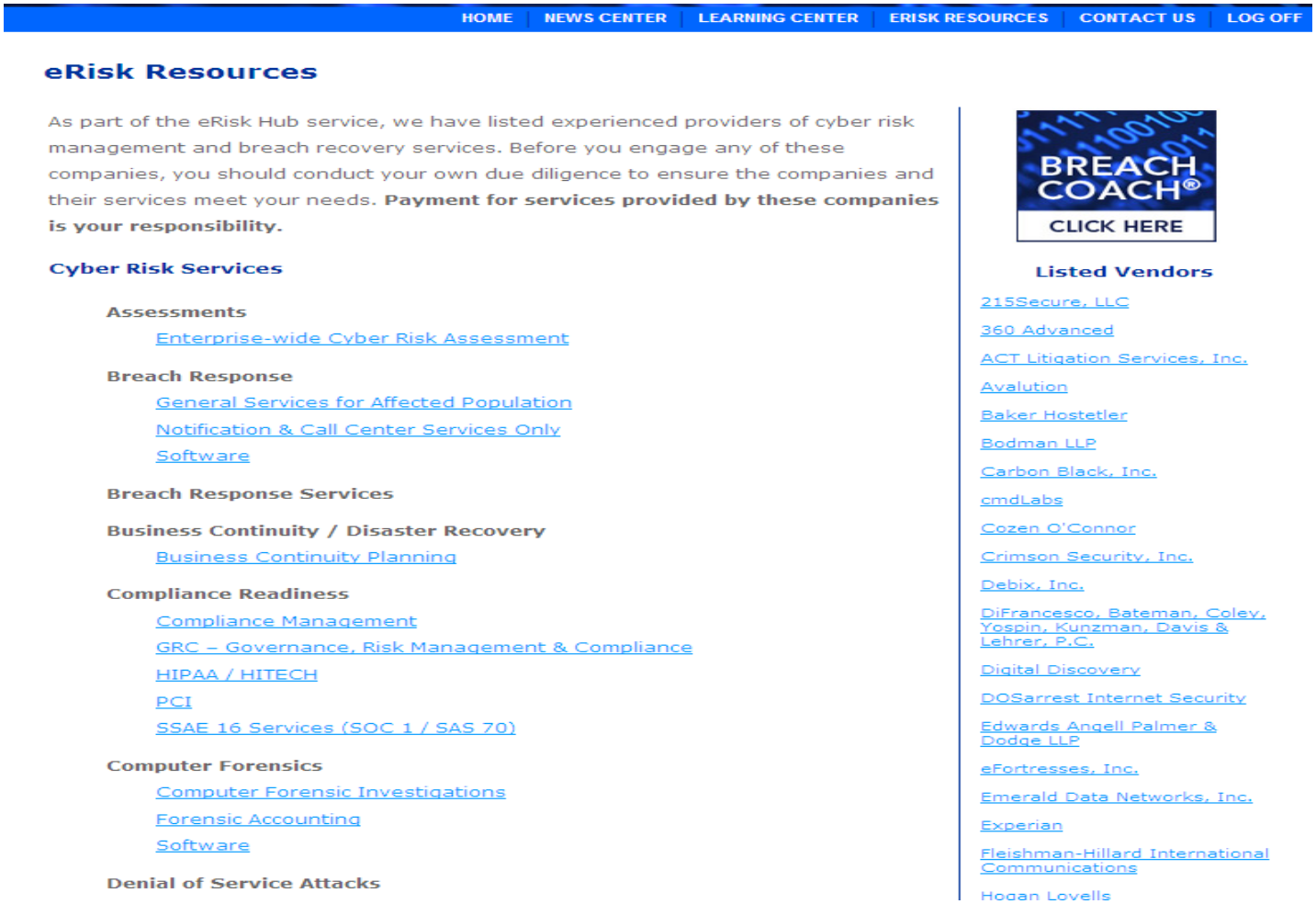
APPETITE
and VALUE ADD

RISK MANAGEMENT / COMMON QUESTIONS

Size	• Revenue, • IP addresses • Geographic location
PCI DSS compliance	• What is it ? • Levels of compliance
Internal Policy and Procedures	• IT policies, BCP, IRP • Passwords, Penetration testing , network monitoring • Back-up / web Servers • Encryption
3rd Party Vendors	• Cloud service providers • Outsourced IT providers • Trusted partners
Claims / Incidents	• DDoS, Malware, Viruses • Personal information • Employee Records

E-Risk Hub for Chubb Insureds

https://eriskhub.com/chubb.php



SUMMARY

- Cyber Insurance is a blended speciality insurance policy that meets the needs of a **digital age.**
  - 3rd and 1st party cover can be offered
  - Cyber Insurance is not an IT errors and omissions policy
- It is **people not technology** that create the weaknesses
  - An **assumed breach** risk methodology should be considered
  - This is an **enterprise wide issue**. Boards should be engaged not just IT departments
- The costs of a cyber attack can be crippling and **incident response plans** and risk mitigation tools need to be revisited.

THANK YOU FOR YOUR TIME

QUESTIONS / CONTACT DETAILS

Andrew Taylor
Asia Pacific Zone Product Manager
ChubbPro PI, Media, Cyber
ajtaylor@chubb.com
02 9273 0456 ph
0418 600 238 m