



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 than the entire planet's 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**
- Ransomware 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 !!!!**

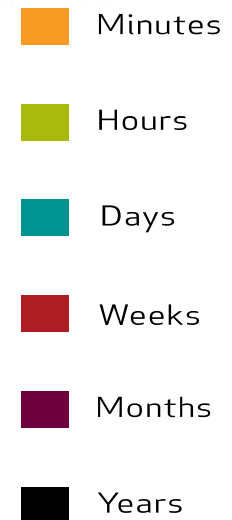
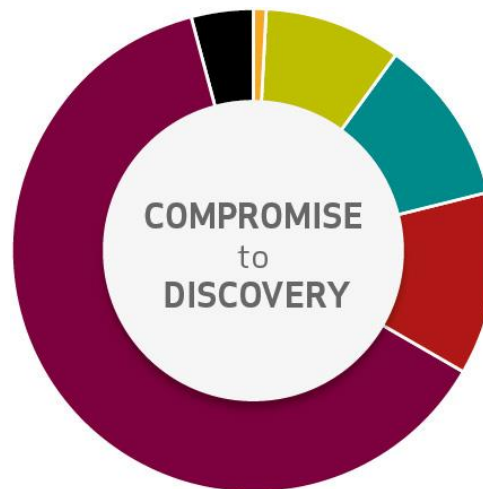
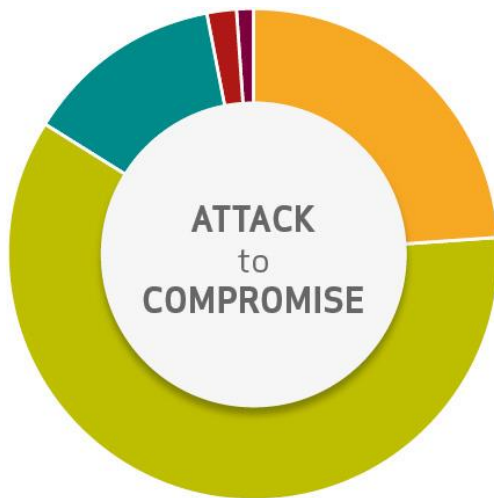
- Costs of cyber crime keep rising
- Legislation is catching up with reality
- Businesses are unprepared
- Nation State borders are being blurred on-line

THE REALITY

MINIMAL TIME TO COMPROMISE

BUT A LONG TIME TO DISCOVERY

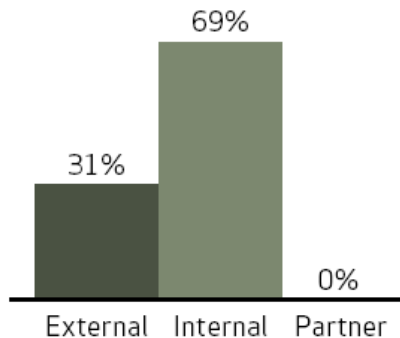
- **IN 84% OF CASES,** INITIAL COMPROMISE TOOK HOURS OR LESS.
- **IN 66% OF CASES,** THE BREACH WASN'T DISCOVERED FOR MONTHS OR EVEN YEARS.



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.

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%

WHAT IS CYBER INSURANCE?

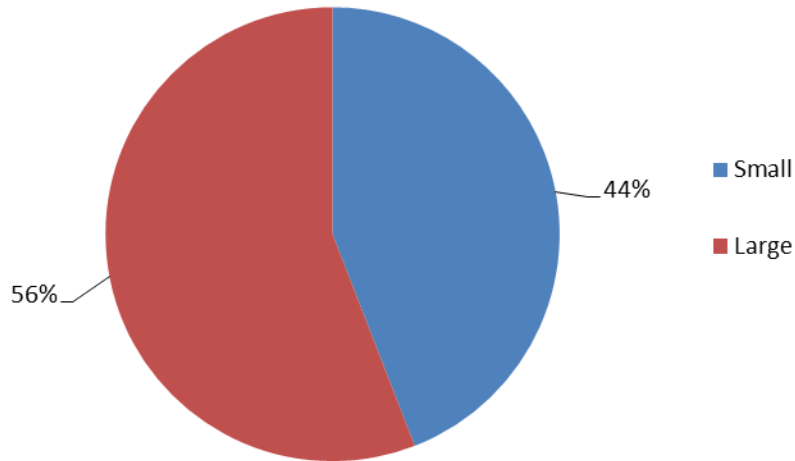


WHAT IS CYBER INSURANCE?

- 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 ChubbSM**

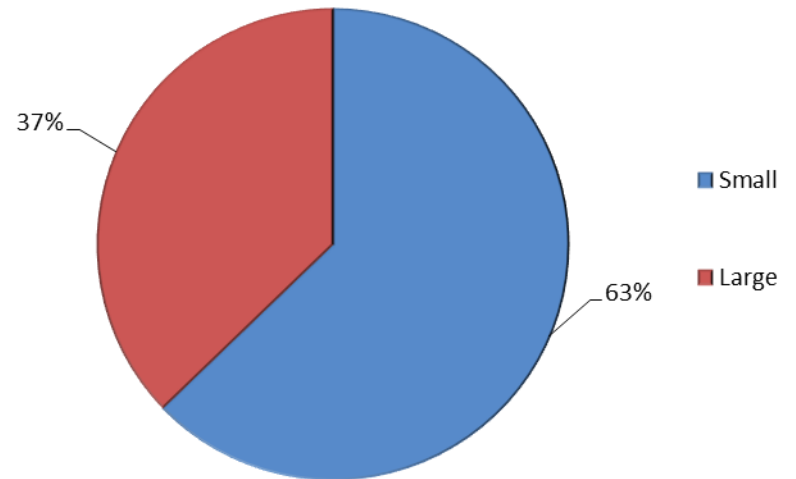
THE VICTIMS by Size

Total Cyber Incidents ex Public and unknown
2013



Size does not matter
All organisations are a
TARGET

Total Cyber Incidents with Data Losses 2013



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
-

eRisk Resources

As part of the eRisk Hub service, we have listed experienced providers of cyber risk management and breach recovery services. Before you engage any of these companies, you should conduct your own due diligence to ensure the companies and their services meet your needs. **Payment for services provided by these companies is your responsibility.**

Cyber Risk Services

Assessments

[Enterprise-wide Cyber Risk Assessment](#)

Breach Response

[General Services for Affected Population](#)

[Notification & Call Center Services Only](#)

[Software](#)

Breach Response Services

Business Continuity / Disaster Recovery

[Business Continuity Planning](#)

Compliance Readiness

[Compliance Management](#)

[GRC – Governance, Risk Management & Compliance](#)

[HIPAA / HITECH](#)

[PCI](#)

[SSAE 16 Services \(SOC 1 / SAS 70\)](#)

Computer Forensics

[Computer Forensic Investigations](#)

[Forensic Accounting](#)

[Software](#)

Denial of Service Attacks



Listed Vendors

[215Secure, LLC](#)

[360 Advanced](#)

[ACT Litigation Services, Inc.](#)

[Avalution](#)

[Baker Hostetler](#)

[Bodman LLP](#)

[Carbon Black, Inc.](#)

[cmdLabs](#)

[Cozen O'Connor](#)

[Crimson Security, Inc.](#)

[Debix, Inc.](#)

[DiFrancesco, Bateman, Coley, Yospin, Kunzman, Davis & Lehrer, P.C.](#)

[Digital Discovery](#)

[DOSarrest Internet Security](#)

[Edwards Anell Palmer & Dodge LLP](#)

[eFortresses, Inc.](#)

[Emerald Data Networks, Inc.](#)

[Experian](#)

[Fleishman-Hillard International Communications](#)

[Hogan Lovells](#)

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

For promotional purposes, Chubb and Chubb Insurance refers to member insurers of the Chubb Group of Insurance Companies. Coverage is issued by Chubb Insurance Company of Australia Limited, ABN 69 003 710 647, AFS Licence Number 239778. This material contains general information only and may not suit your particular circumstances. The precise coverage afforded is subject to the information in the terms and conditions of the insurance Policy when issued. Visit our website for further information www.chubbinsurance.com.au.



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
