Cyber Liability

Evolution to Revolution…..

LLOYD'S

Christian Stanley
Underwriting Performance
Lloyd's

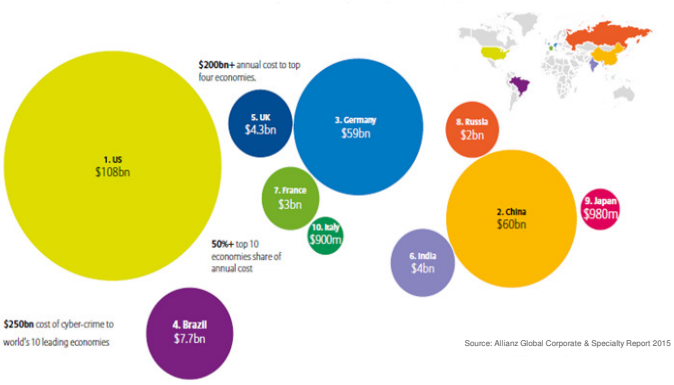
July 2016

Quantifying the Threat….

- "Cyber crime is a bigger threat than drugs"
  (UK Ex-Fraud Police Chief)
- "There are two kinds of big companies in the US. There are those who've been hacked and those who don't know they've been hacked." (2014 FBI director James Comey)
- "We are in the midst of a crime wave unlike any since the 1920s and the age of gangsters"
  (Tom Kellermann, a professor of cyber-security at American University)
- There were 43 million global security incidents detected in 2014…..that's more than 100,000 attacks a day
  (PWC Security Survey 2015)

And the cost is……. ?

- Annual global cost of cyber crime is over $445 bn That's the equivalent of the biggest bank robbery in history (2003's nearly $1bn take from the Central Bank of Iraq) if it were pulled off more than once a day. (Mcafee)

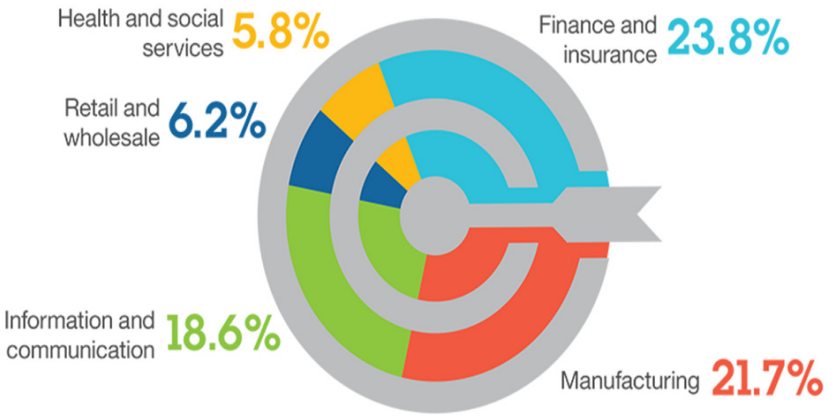


- Cyber crime will cost global business $2.1 trillion dollars by the year 2019 (Juniper Research report)
- Average cost of a data breach is $3.8 million and rising each year. (2015 Cost of Data Breach Study Ponemon Institute)

3 © Lloyd's

Targeted industries

Over 75% of incidents targeted **5 industries**

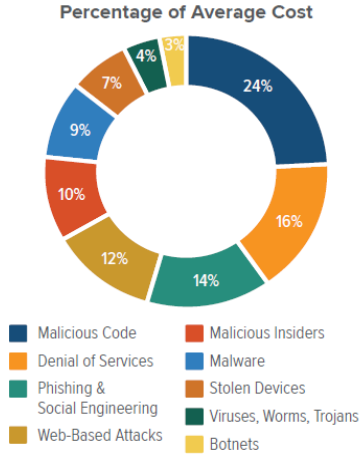


Source: IBM 2014 Cyber Security Intelligence Index Report

4 © Lloyd's

Types of attack

The Most Costly Cybercrimes in the U.S., Fiscal Year 2015



Total may not equal 100% due to rounding.
Source: Ponemon Institute.

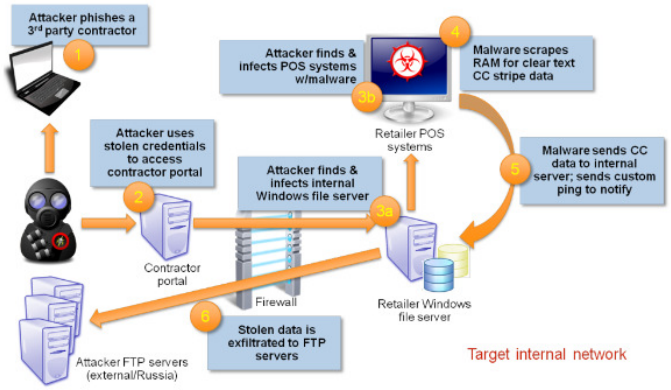
5 © Lloyd's

Who are the bad guys ?

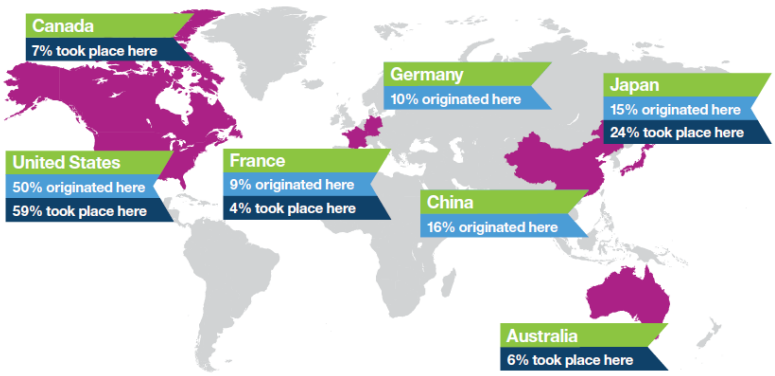
Source: IBM 2015 Cyber Security Intelligence Index Report

6 © Lloyd's

Claim case



Where are the attacks coming from and where are they taking place ?



Source: IBM 2015 Cyber Security Intelligence Index Report

So Should Individuals be worried about attacks on businesses and govt. ?

- The answer is a definitive yes:

  Big organizations hold caches of individual information (which is useful for identity theft and other crimes), they make tempting targets for cyber criminals.

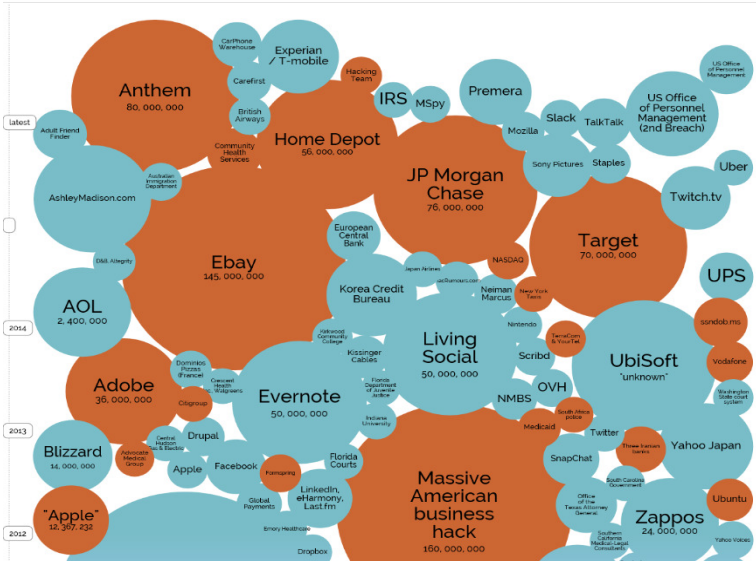
- In 2013, 43% of companies had a data breach in which hackers got into their systems to steal information.

- In 2014, 47% of American adults had their personal information stolen by hackers, primarily through data breaches at large companies.

- Data breaches targeting consumer information are on the rise, increasing 62% from 2012 to 2013, with 594% more identities stolen. That added up to a staggering total of $18,000,000,000 in credit card fraud for the year.

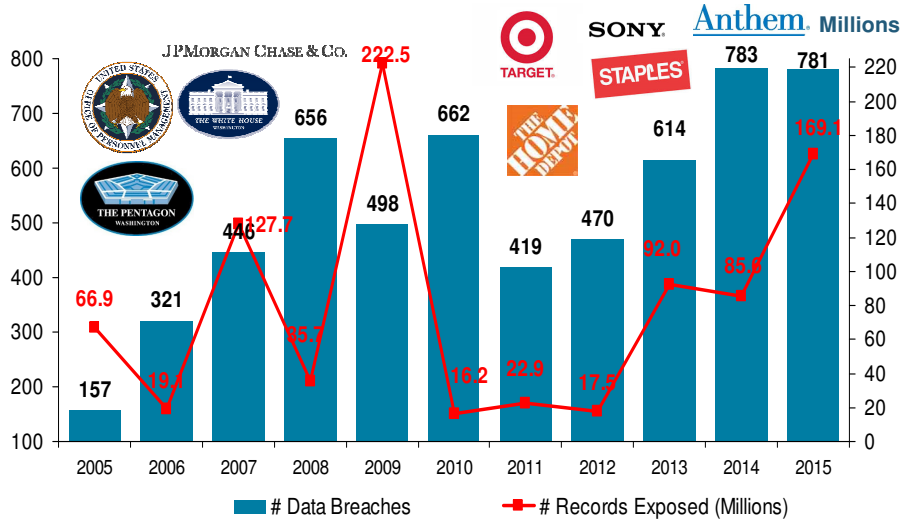
9 © Lloyd's

The High profile breaches



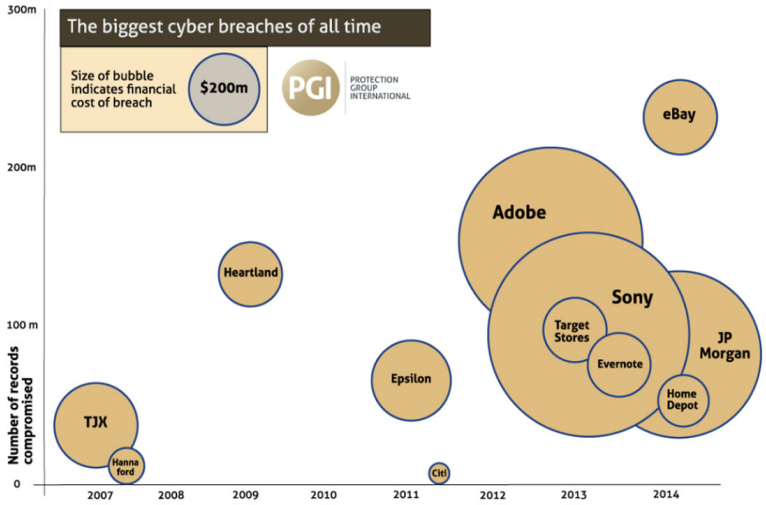
10 © Lloyd's

Data Breaches/Millions of Records Exposed



Source: Identity Theft Resource Center (updated as of Jan. 6, 2016);
http://www.idtheftcenter.org/images/breach/ITRCBreachReport2015.pdf

the cost of some high profile Breaches



Source: Protection Group International

the cost of some high profile Breaches

- **2013 Sony $1,500m** - 100m personal credentials of Sony customers were stolen, including credit card data, phone numbers and emails and passwords. The company was hit with 65 class actions suits and substantial fines
- **2013 Target Stores $248m** - payment card readers are infected with malware that had been harvesting credit card details. Customer's records were compromised in the attack forcing the CEO to resign and costing the company $248 m. ($100m Insurance reportedly) 70 Class Actions
- **2013 Adobe Systems $1.5bn** - Adobe, makers of Photoshop and other high end graphics software, lost credentials for 150 million user accounts in a cyber-attack in 2013.
- **2014 Home Depot $161m** - point-of-sales systems had been infected with malware that was masquerading as anti-virus software but was actually stealing credit card details. Some 56 million cards were compromised, initially 57 lawsuits brought against them
- **2014 JP Morgan $1bn** - Russian hackers stole details of 76 million client accounts from this premier US Bank. The criminal gang stole gigabytes of sensitive data over a two month period. The cost to the bank is estimated at $1bn, despite spending a $250m annual budget on cyber security.
- **2014 eBay $200m** - It took this online retailer six months to discover that they had been hacked with 230m customer's credentials being compromised. Class action suits and regulatory fines will probably cost the company around $200m

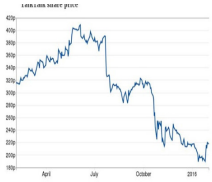
13 © Lloyd's

True Cost of a breach……



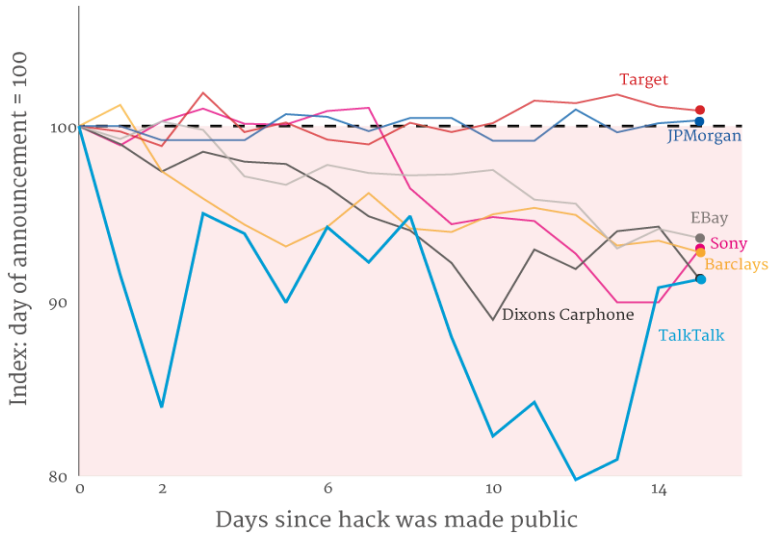





CONFIDENTIAL: Market update - November 2013 14 © Lloyd's

How share prices fare, post breach



Source: City A.M.

15 © Lloyd's

Evolution of the insurance solution

- Origins in late 1990's following increasing reliance on information technology within business world, and fuelled by the 'dot com' boom
- Traditional Property and Casualty policies were inadequate
- Early Cyber policies pioneered by Lloyd's and AIG, for US clients, focussed on Business Interruption from being 'hacked'
- Evolved into a 'privacy issue' with the 2003 establishment of US data breach/notification laws
- Cyber coverage widely packaged with Technology E&O insurance
- 2014, specific policies created to offer cover for physical damage and bodily injury caused by a Cyber attack.

16 © Lloyd's

Todays Insurance product

- Cyber policies can now cover a suite of 1st and 3rd party, Non Physical and Physical exposures relating to:-

  - Data Breach
  - Privacy Breach
  - Network Security Liability
  - Cyber Extortion

  - Crisis Management Costs
  - Business Interruption/Contingent Business Interruption
  - Reputational Harm Expenses
  - Regulatory Defence Costs and Fines/Penalties

  - Multi-Media Liability
  - Intellectual Property Theft

  - Environmental Damage
  - Physical Damage
  - Bodily Injury

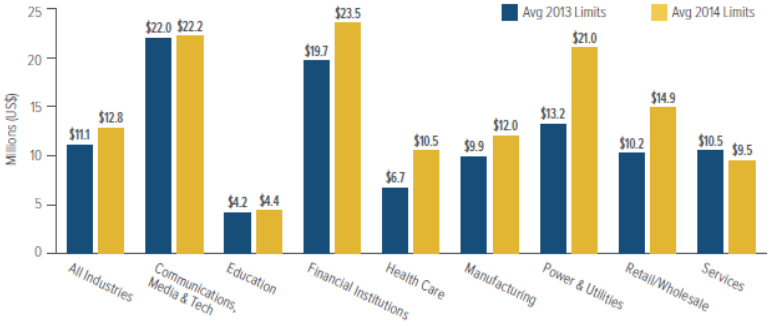
- Risk audits and post claim assistance/services from specialist vendors

17 © Lloyd's

Who's buying ?

Fig. 12

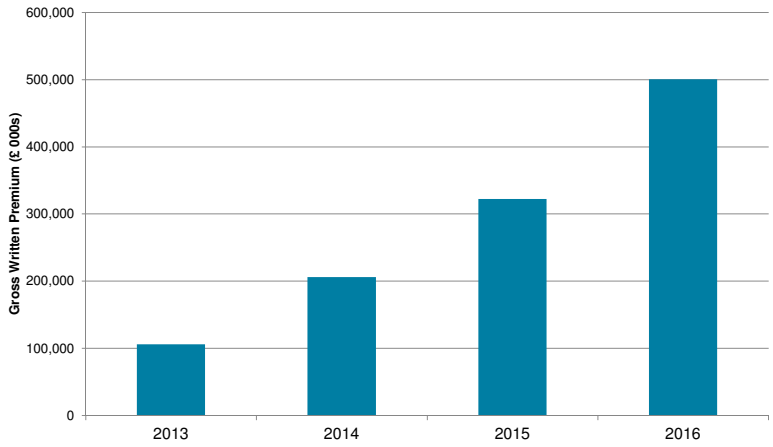
Marsh: Total Limits Purchased, By Industry – Cyber Liability, All Revenue Size



Source: *Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise*, Marsh Risk Management Research Briefing, March 2015.

18 © Lloyd's

Cyber insurance premium at Lloyd's



No of syndicates:	22	42	67	63

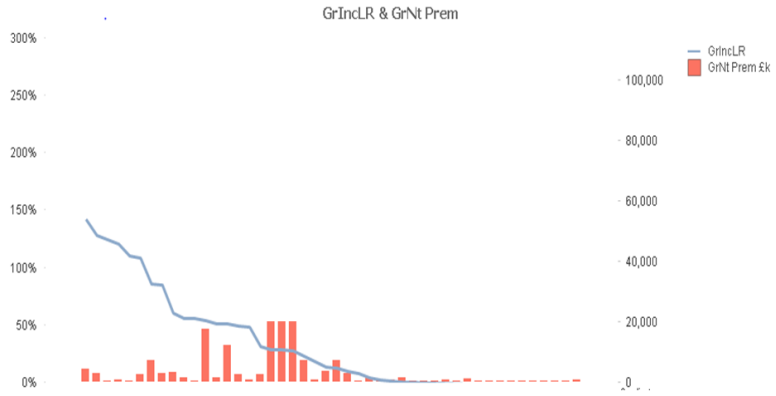
19 © Lloyd's

Market size

- 2016 global gross premiums widely estimated to be approx. $2.5-$3bn with predictions of continued growth to $7.5bn by 2020
- 65 Lloyd's Synds. writing $750m GWP in 2016, being approx. 25% of estimated global market
- Lloyd's aggregate limit available approx. $400m
- 50+ Carriers W/W (includes MGA's)

20 © Lloyd's

Lloyd's 2013 and 2014 performance



NB - Aggregated data over two years of account.
- Premium income capped off at £20m

21 © Lloyd's

Underwriting Hurdles

CONFIDENTIAL: Market update - November 2013 22 © Lloyd's

Drivers of future growth

- 'The Internet of Things'
- Increasing Attacks
- Business Interruption / Supply Chain
- Industry and Government sponsored standards and information sharing of claims data and threat analysis.
- Legislation

Standards, frameworks and sharing

- Cyber Essentials (2014 UK government scheme encouraging organisations to adopt good practice in information security)
- ISO 27001 (an information security standard that was published on the 25th September 2013)
- IASME (an information assurance standard that is particularly suitable for SME's)
- COBIT (1996Control Objectives for Information and Related Technology)
- CiSP (UK - Cyber Security Information Sharing Partnership)
- NIST Framework (US - National Institute of Standards & Technology)
- CISA (US - Cybersecurity Information Sharing Act 2015)

EU Legislation - 2018

- Network & Information Security Directive
  - Industries who are deemed 'Operators of Essential Services' will have security and notification requirements (Penalty fines of 2% of global turnover)
- Data Privacy Law Reform
  - General Data Protection Regulation (GDPR)

    The GDPR will replace the Data Protection Directive 95/46/EC and therefore the UK Data Protection Act 1998 and will be directly applicable in all Member States without the specific need for governments to implement legislation. (Penalty fines of 4% of global turnover)
  - Data Protection Directive

    Legislation for the police and criminal justice sector to ensure protection of data of victims, witnesses and suspects

Key features are mandatory reporting of breaches and penalty fines

25

Lloyd's oversight

- Lloyd's main areas of concern:-
  - Traditional lines of business intentionally covering cyber risk
  - A malicious electronic attack causing a systemic loss
  - Claims aggregating across multiple lines of business across the market
- Underwriting Performance monitoring: -
  - Establishment of specific Cyber risk codes :-

    Effective 2013: **CY** - Cyber security data and privacy breach
    Effective 2015: **CZ** - Cyber security including property damage
  - Syndicates must have: - Defined Cyber risk appetite
    - Cyber risk management framework
    - Three Cyber attack scenarios
  - Analysis and development of various 'Realistic Disaster Scenarios'

26