LLOYD WRIGHT

2012

www.lloydwrightins.com

Data breach! cyber and privacy risks

Brian Wright
Lloyd Wright Consultants Ltd

LLOYD WRIGHT

Collaborative approach

www.lloydwrightins.com

Objective:

To develop your understanding of a data breach, and risk transfer options to help you understand the exposures and mitigate the risks

In this document:

- What is a data breach?
- How and why do breaches occur
- High profile breach events
- Is your client exposed?
- Why purchase a stand alone policy?
- Coverage's explained
- About the markets
- How to proceed
- Contact us
- Award winning service
- About Lloyd Wright
- Appendix – breach facts
- Appendix - legislation

LLOYD WRIGHT

What is a data breach?

www.lloydwrightins.com

"A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so"

A data breach can vary from state to state as can definitions. Of the 50 US jurisdictions, currently 46 states have regulatory requirements in place for a breach

Are you exposed?

Do you store, hold or even pass onto third parties personal information about clients or employees? If you do then you will have an exposure to the legal and regulatory ramifications of a data breach.

According to Ponemon $214 is the average cost to a company for every stolen or misplaced record.

LLOYD WRIGHT

How and why do breaches occur?

www.lloydwrightins.com

All IT departments will tell you they are invincible, So how does it happen and why? Breaches occur externally or internally.

Small organisations have a higher proportion of cyber crimes relating to malicious code and malware. Large organisations have a higher proportion due to disgruntled employees, stolen or lost devices.

Examples of external breaches

- Hackers
- Organised crime
- Extortion
- Competitors
- Outsourcers

Examples of internal breaches

- Communications transmitted to the incorrect recipient
- Non-encrypted file transfer protocol
- Failure of hardware and/or security software
- 3rd party vendor or contractor
- Lost laptop, PDA or other data storage device
- Rogue employee

LLOYD WRIGHT

High profile breach events

www.lloydwrightins.com

Sony	In May 2011, Sony exposed information from more than **100 million user** accounts. Hackers obtained personal information, including credit, debit, and bank account numbers. Estimates are that the breach could cost Sony and credit card issuers up to a total of $2 billion.
Epsilon	In March 2011, hackers stole millions of names and e-mail addresses with an initial estimated cost of **up to $4 billion**. The high cost was attributed to loss of business and reputation.

LLOYD WRIGHT

High profile breach events

www.lloydwrightins.com

US Veterans Affairs	The names, birth dates and social security numbers of **17.5+ million military veterans** and personnel were stolen from a **laptop an employee took home**. Costs included money for running call centres, sending out mailings and paying for a year of credit-monitoring services for victims. Estimates of the cost are around $25 million. **The VA has had two more breaches since.**
Heartland Payment Systems	In 2009, HPS reserved **$130 million** for lawsuits after malware* was uploaded on systems by hackers.
TJ Maxx	In 2007, the retailer had a data breach where cyber criminals took more than 45 million credit and debit card numbers. **Total cost $250m+.**

*malware = short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour.

LLOYD WRIGHT

Are you exposed?

www.lloydwrightins.com

What information do you have?

Where is it stored?

Is it encrypted?

How easy is it for someone to access?

Are you confident in the security you have?

Do you continually update your security?

Do laptops leave their premises?

See US Veteran Affairs case study

A stolen laptop or one taken home by an employee, is the biggest cause of data breaches at corporations according to the Ponemon 2010 annual study: US cost of a data breach

LLOYD WRIGHT

Why purchase a standalone policy?

www.lloydwrightins.com

Crime, CGL, K&R and property policies may not cover data breaches as they only apply to tangible assets and courts have held that ‘data’ isn’t property.

Standard commercial E&O policies will not cover or respond to the services required and needed for a breach. Loss of income/revenue would similarly not be covered.

Specialist standalone policy forms are a specific approach to an exposure which is volatile and uncertain.

LLOYD WRIGHT

Coverage's explained – 1st party

www.lloydwrightins.com

Business income/dependent business income loss	Reimbursement of loss of income due to a suspension of computer systems (time frame deductible). Reimbursing loss of income due to a data breach to a dependent business partner during the policy period.
Notification and credit monitoring/crisis management	The cost of notifying the individuals whose data has been compromised and the offering of services to monitor suspicious credit activity.
Data asset restoration/forensics	Reimbursement of costs to recover, reinstate and recreate intangible assets destroyed during a cyber attack. Forensics obtained to determine what and whose information was stolen.
Cyber extortion threat	Reimbursing investigation expenses and ransom payments resulting from malicious threats to your organisation’s computer system.

LLOYD WRIGHT

Coverage's explained – 3rd party

www.lloydwrightins.com

Privacy liability/employee liability	Class actions and suits brought (including employees) which result in a monetary payment due to the disclosure of a persons private and confidential information.
Regulatory defence and civil penalties	Investigation, fines and penalties (where Insurable by law) that you are legally required to pay.
Media liability	Legal liability arising from media content transmitted on any computer system. Harm suffered by others due to an infringement of an intellectual property right. Defamation and slander.

LLOYD WRIGHT

About the markets

www.lloydwrightins.com

Established capacity	Lloyd Wright has access to global privacy markets with London capacity itself of more than $100 million
Market choice	There are 30+ different markets offering primary and excess solutions. London markets can consider full limits, for all cyber coverage's for certain risks.
Worldwide	London markets write privacy worldwide, where regulation does not apply in some jurisdictions, voluntary notification with underwriter consent obtainable for best practices
Tailored to your clients' needs	We tailor policy wordings to best suit your specific requirements.

LLOYD WRIGHT

How to proceed

www.lloydwrightins.com

Discuss exposures

Complete an application form for a non-binding indication

Review coverage

Network security review provided by underwriters

Security recommendations implemented if required

Quote provided

Policy bound

LLOYD WRIGHT

Contact us

www.lloydwrightins.com

For further information, please contact:

Brian Wright
brian.wright@lloydwrightins.com
+44 (0)20 3397 0951

LLOYD WRIGHT

Award winning service

www.lloydwrightins.com

2008
UK Broker Awards

2002
The British Insurance Awards

2000
The British Insurance Awards

1999
The British Insurance Awards

2001
The Insurance Times Awards

1999
Insurance Industry Awards

1999
Insurance Industry Awards

LLOYD WRIGHT

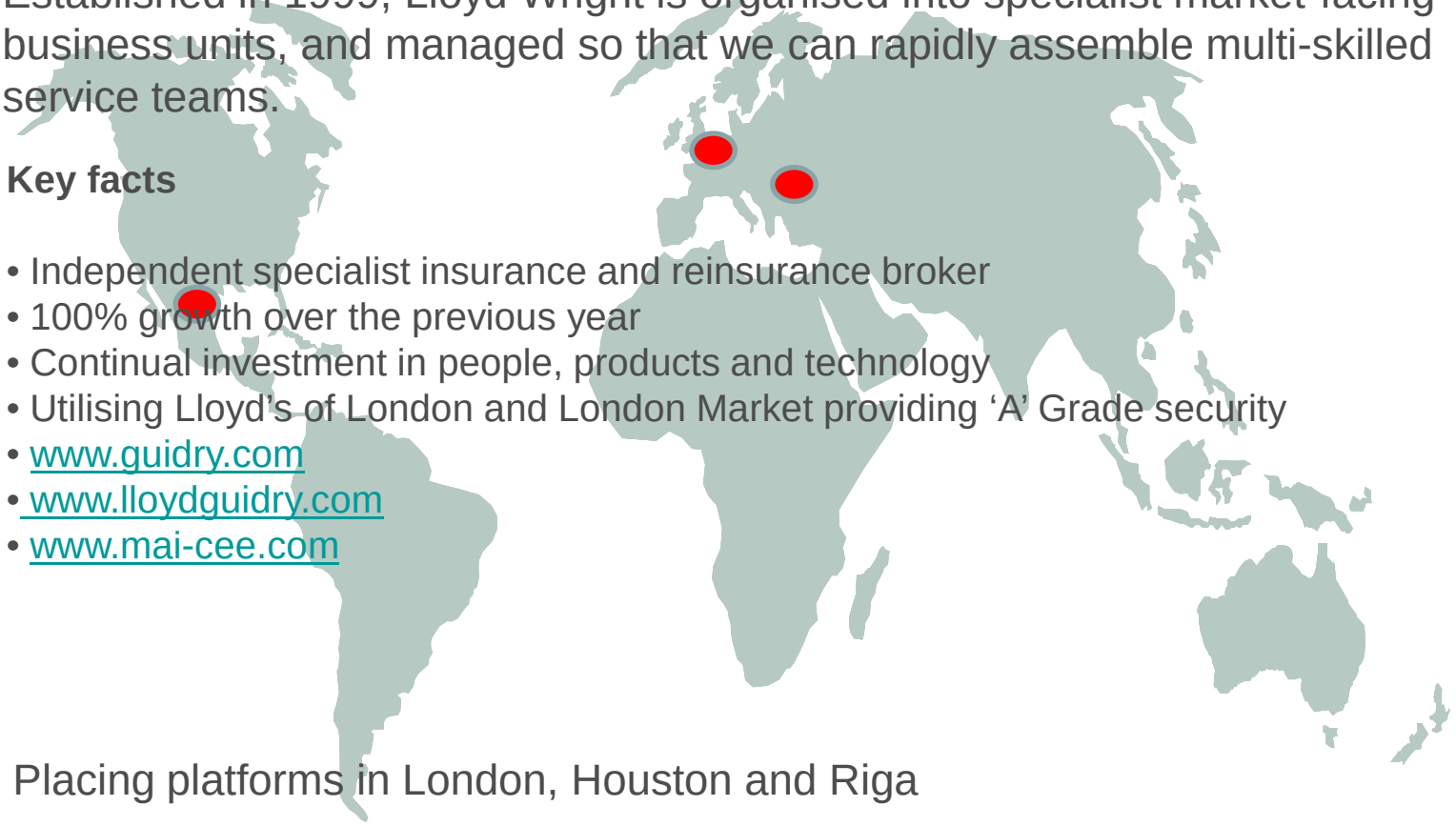
About Lloyd Wright Consultants

www.lloydwrightins.com

Established in 1999, Lloyd Wright is organised into specialist market-facing business units, and managed so that we can rapidly assemble multi-skilled service teams.

Key facts

- Independent specialist insurance and reinsurance broker
- 100% growth over the previous year
- Continual investment in people, products and technology
- Utilising Lloyd's of London and London Market providing 'A' Grade security
- www.guidry.com
- www.lloydguidry.com
- www.mai-cee.com



Placing platforms in London, Houston and Riga

LLOYD WRIGHT

Appendix - other breach events

www.lloydwrightins.com

Gucci	A disgruntled ex-employee gained access, deleted files and shut down the server for 24 hrs. This cost Gucci an estimated $200,000.
BP	A laptop was lost which contained 13,000 Louisiana oil spill claimants information.
Briar Group	A group of restaurants in Boston who failed to patch a security hole. The were fined $110,000 plus ordered to improve data security by implementing a password management system.
Kaiser Permanente	150 patient names, address and medical files were posted online and accessible for 4 years. The company was fined $200,000.

LLOYD WRIGHT

Appendix - case studies

www.lloydwrightins.com

Potential event	How a policy responds
Disgruntled employee posting on a blog/social networking site	Slander Defamation
Malware permitted entry to a banks online banking system	Forensics
Hacker breaks into network, steals customer data, threatens to post publicly or sell it	Cyber extortion Liability
An employee's laptop or USB is stolen containing customers information	Notification Credit monitoring
Foreign hackers penetrate defence networks in an attempt to steal information on an unmanned aircraft	Cyber terrorism

LLOYD WRIGHT

Appendix – data breach facts

www.lloydwrightins.com

Source: Ponemon 2010 annual study: US cost of a data breach

- For the fifth year in a row data breach costs have continued to rise
- Breaches by third party outsourcers are becoming slightly less common but more expensive
- Breaches involving lost or stolen laptops computers or other mobile devices remain a constant and expensive threat
- ‘First timers’ pay the highest breach costs

LLOYD WRIGHT

Appendix – data breach legislation

www.lloydwrightins.com

- Gramm Leach Bliley Act (GLBA)
- Health Insurance Portability Accountability Act (HIPAA)
- ISO 17799
- PCI DSS
- Sarbanes Oxley Act
- COBIT
- FFIEC Guidelines
- COPPA
- Amendment to S.B. 1386 (California) effective January 1st 2012
- Red Flags Rule Amendment
- Privacy Act of 1974
- CAN SPAM Act