RETHINK REINSURANCE

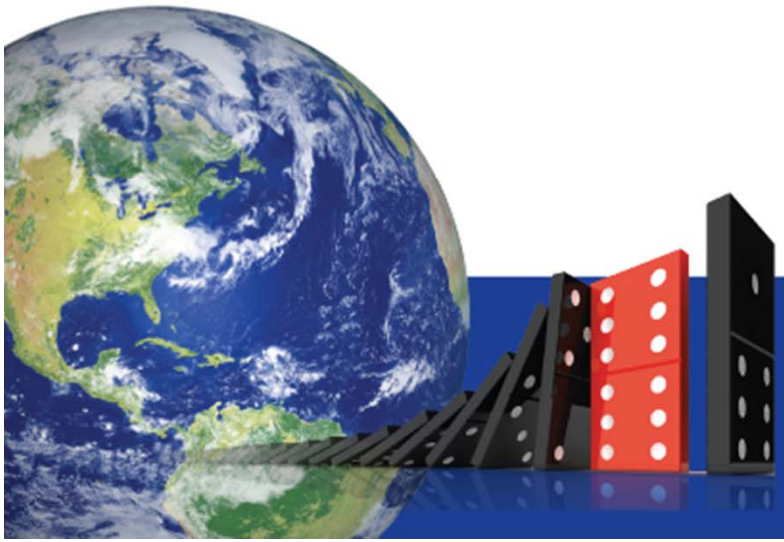
THE 55TH ANNUAL CANADIAN REINSURANCE CONFERENCE

CRD

CANADIAN REINSURANCE CONFERENCE / CONGRÈS CANADIEN DE RÉASSURANCE

RE THINK REINSURANCE

Data Privacy: A modern day Mission Impossible?



THE 55TH ANNUAL CANADIAN REINSURANCE CONFERENCE

CRD

CANADIAN REINSURANCE CONFERENCE / CONGRÈS CANADIEN DE RÉASSURANCE

RE THINK REINSURANCE

Jeffrey Taft
Attorney
Mayer Brown LLP
Washington, DC

THE 55TH ANNUAL CANADIAN REINSURANCE CONFERENCE

CRD

CANADIAN REINSURANCE CONFERENCE / CONGRÈS CANADIEN DE RÉASSURANCE

Data Privacy

- US has a sectoral approach to privacy
  - No comprehensive US privacy law covering all industries or all personal information
  - No privacy commissioner or data protection authority
  - US laws cover specific types of institutions, information and persons
- Gramm-Leach-Bliley Act (GLB Act)
  - Applies to customers of financial institutions
  - Privacy rule
  - Safeguarding rule
- Health Insurance Portability and Accountability Act (HIPAA) and HITECH
  - Covers health information

Data Privacy

- Federal Trade Commission Act
  - Other businesses engaged in interstate commerce
  - Deceptive or unfair acts or practices
- Federal Trade Commission Enforcement Actions
  - Violations of GLB Act safeguarding or privacy rules
  - Unfair or deceptive acts or practices
  - Violation of the disposal rule

Data Privacy

- Fair Credit Reporting Act/FACT Act
  - Credit reports
  - Sharing information with affiliates
- State laws
  - Insurance industry in US is regulated under state law
  - State insurance laws and regulations impose privacy requirements on insurance companies

Data Privacy

- Data breach notice laws (46 states and D.C.)
  - Require notice to consumers in the event of unauthorized access to sensitive customer data
  - Majority allow only government enforcement and penalties
- Data security laws
  - Massachusetts Security Breach Law
    - Written, risk-based security plan
    - Minimum standards and practices: operating system patches, antivirus software, firewalls, passwords, training, etc.
    - Most specific and comprehensive set of data security regulations in US
    - Enforced by Mass. Attorney General with fines up to $5,000/occurrence

Data Privacy

U.S.	Rest of the World (EU, Canada, Australia, Parts of Asia and Latin America)
PI is a corporate asset (customer lists, CRM databases, mailing lists, etc.)	PI belongs to the individual
Collection and use of PI is permitted by law (and usually not by consent of individual)	Collection and use of PI is restricted by law, and requires individual notice and consent
PI is regulated in limited industry sectors, often aimed at protecting privacy and preventing identity theft – compliance with self-regulated fair information principles is encouraged	PI is broadly regulated according to broad prescriptive directives and laws applicable to all industries (e.g., EU)
Regulatory concern is to not impede commerce, and to not prescribe technological requirements that become outdated	Regulatory concern is to ensure that prescriptive privacy laws follow the protected data everywhere around the world
Generally, you can do it if you fairly tell them you are doing it	Generally, you can only do certain things

Data Privacy

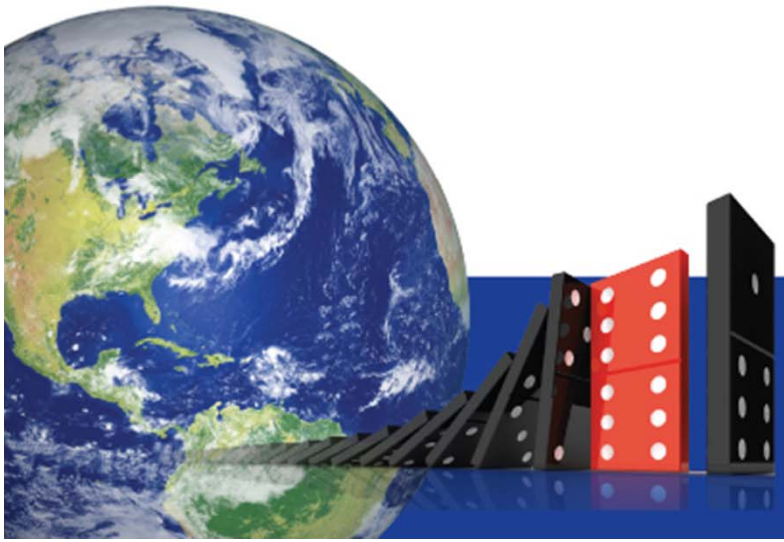
- EU 1995 Data Protection Directive
  - Comprehensive privacy law
  - Directive restricts the processing and transfer of personal data
  - These terms are broadly defined

Data Privacy

- EU Directive: Transfers of Personal Data
  - Transfer within EU and to other countries with adequate level of protections are permissible
  - Possible steps to permit transfer of data to US
    - Elimination of “personal data” from set being transferred
    - US Commerce Department’s “safe harbor”
    - Model contract clauses
    - Binding Corporate Rules (BCRs)

RE THINK REINSURANCE

Thomas Dunbar
Chief Information Risk Officer
XL Group



THE 55TH ANNUAL CANADIAN REINSURANCE CONFERENCE

CRD

CANADIAN REINSURANCE CONFERENCE / CONGRÈS CANADIEN DE RÉASSURANCE

Today's Headlines

Companies beware: The next big leak could be yours

WikiLeaks release highlights risks companies face from poor security policies, angry workers

http://finance.yahoo.com/news/

BP "leaks" data of 13,000 Gulf oil spill victims

http://www.denverpost.com/nationworld/ci_17728919

Security scare as council loses memory stick containing access codes to the homes of thousands of vulnerable people

http://www.dailymail.co.uk/

Report: Cyber-attacks pose a threat to many businesses

http://www.property-casualty.com/

Bank of America settles Countrywide data theft suits

Settling the biggest reported case of data theft by a financial insider, Bank of America Corp. will provide free credit monitoring, identity theft insurance and reimbursement for losses to as many as 17 million consumers who dealt with its Countrywide Financial mortgage unit.

Bank of America settles Countrywide data theft suits - Los Angeles Times

Heartland breach expenses pegged at $140M – so far

http://www.computerworld.com

Data Loss Statistics

- Open Security Foundation
- http://datalossdb.org/
- Office of Inadequate Security
- http://www.databreaches.net/
- Privacy Rights Clearinghouse
- http://www.privacyrights.org/

Data Loss Statistics

Data Loss Statistics

Data Loss Statistics

Data Threats

- Business leaders are beginning to understand that data is the newest form of global currency
- Cybercriminals have already realized this
- Credit cards, chemical recipes, patient records, or phone numbers - all assets have a price
- Loss of assets severely damage the financial well-being of a company
  - Becomes a public relations nightmare when the good reputation of a company is threatened

Data Loss

- Sheer volume of data that "drips" out of an organization is staggering
  - High percentage of data loss is due to employee error, not insider theft
  - Numerous cases where people simply lose their devices
  - Good employees making bad mistakes
    - Sending data to themselves over the Web via personal Webmail sites (e.g., gmail, MSN)
    - Posting to online apps like GoogleDocs, LinkedIn, and the social Web
- Whether at rest, in motion, or in use, data has become a big value item
  - Cost of a data breach can be more expensive than the data itself
  - Strict regulations and policies now surround data - more governments are starting to impose fines for data loss
  - These regulations, policies, and fines that now pertain to data vary greatly between each company, industry, and country involved

Possible Costs

- Failure to comply with regulatory requirements
  - Fines levied by regulatory bodies such as EU Data Privacy laws and US state laws
  - Allow affected shareholders and individuals to seek action, including financial penalties
  - Substantial fines: $15M (Choicepoint); £3.25M (Zurich Insurance); $110K (Briar Group)
- Reputation risk
  - Loss of customer confidence
  - Lower stock price
- Cost of data breaches is steadily increasing*
  - 2010: average data loss incident = $7.2M
  - average cost per compromised record = $214
  - 2006: average data loss incident = $4.8M
  - average cost per compromised record = $182

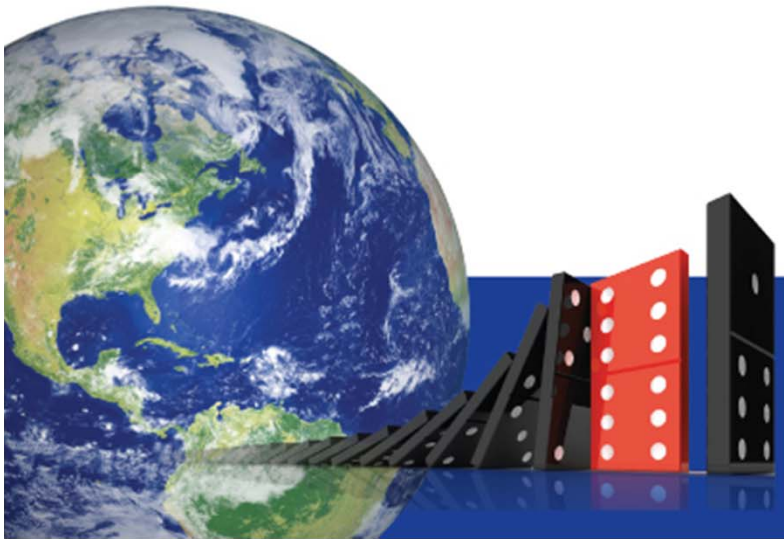
*Ponemon Institute

Solutions

- DLP Software (Data Loss Prevention)
- Entitlement Reviews
- Secure (encrypted) email
- Secure File Transfer
- Password/Encrypt File Attachments
- Paper Shredders and Secure Disposal
- Awareness & Education
- Virtual Desktops

RE THINK REINSURANCE

Pauline Wilson
Head of Customer Services
Hannover Life Reassurance (UK)



THE 55TH ANNUAL CANADIAN REINSURANCE CONFERENCE

CRD

CANADIAN REINSURANCE CONFERENCE / CONGRÈS CANADIEN DE RÉASSURANCE

Data Privacy - Operational Perspectives

- Changing environment in the UK
- Impacts on Reassurance Treaties
- Data transmission
- Data handling
- Data storage/destruction
- Working with third parties
- Risk assessment and mitigation

Changing Environment in the UK

- Increased regulation and oversight driven by the EU Directive through the FSA
- Greater focus on the security of personal data throughout it's lifetime
- Greater onus on Companies to ensure data security at all times, even when the data is in the control of third parties, including Reassurers
- More stringent penalties for non compliance with heavy fines imposed for loss of policy data
  - DP breaches must be reported

Impacts on Reassurance Treaties

- Reassurers are data driven organisations; increased awareness of how data is used and protected by all parties, impacts the standard treaty terms
- Tightened clauses around DP and confidentiality
- Incorporation of specific schedules for data handling
  - Classification of data
  - Sharing data internally
  - Security of data for BAU
  - Clear desk policies

Impacts on Reassurance Treaties (Cont)

- Specific requirements for staff vetting
  - Existing/new staff
  - Financial and criminal checks
- The treaty puts the onus to ensure the security of data on the Reassurer while it is in their possession and when they have passed it to others
  - Third party service providers
  - Retrocession partners

Impacts on Reassurance Treaties (Cont)

- Treaties now have more focus on due diligence and governance requirements
- Often detailed due diligence questionnaires and meetings must be completed before the treaty can be signed
- On going access and audit rights are incorporated into the treaty

Data Transmission

- All personal data must be protected
- Every company has its preferred methods for the secure transfer of it's data
  - Encrypted using increasingly complex passwords
  - Server to server links/Secure mail systems
- Secure transmission must also be observed by the Reassurer when returning information to the Ceding Company
  - Raising queries on the policy data
  - Communicating underwriting decisions

Data Handling

- Data classification policy ensures the organisation considers the type of data it is using and how it uses it
  - Medical details – strictly confidential
  - Policy holder details – confidential
- The classification dictates the strength of security around the specific data; not all data is treated the same

Data Handling (Cont)

- Once received onto the secure server network, access to data should be controlled on a ‘needs’ basis
- Access granted should be reviewed regularly
- Where data is shared within the organisation, the purpose of the activity should be considered and non essential data should be removed before sharing
  - Personal details such as policy holder name are not required for experience analysis or setting reserves

Data Handling (Cont)

- Working practices are changing, bringing changing risks for handling data
  - Mobile or home working
  - Social net working sites and access to the internet
  - Portable data storage devices (USB)
- To mitigate these risks Companies must consider how and when they grant permission for these to be accessed
- Web filtering or blocking software can be utilised to monitor or block activity

Data Storage

- Data security must be embedded within the organisation and should also influence data storage
- Data held in physical format, as well as electronic must be protected
- Clear desk policy must be practiced when the data is not in use, especially at the end of the business day
- Storage should be in lockable cabinets with controlled access

Data Destruction

- Data must be maintained securely throughout its lifetime; even to the point where it is destroyed
- A secure data destruction policy must be in place, and should be regularly reviewed to ensure effectiveness
- The destruction process should include an agreed timetable and acceptable evidence that the activity has taken place securely

Working with Third Parties

- For a Reassurer passing data to third party suppliers raises further issues
  - Third party service providers
  - Retrocessionaires
- In today's environment the onus is on the Reassurer to ensure security of data at all times, even when passed to a trusted Retrocession partner
- The transmission of data between the parties must be secure at all times

Working with Third Parties (Cont)

- The UK/EU rules surrounding the protection of data still apply irrespective of where the data is transmitted to
- Many countries, including Canada have equivalent standards of DP
- The 'gentleman's agreement' approach is no longer good enough; Retrocession treaties now mirror the requirements imposed on the Reassurer
- Governance still needs to be observed; due diligence questionnaires need to be completed, even for Retrocession partners of many years standing

Working with Third Parties (Cont)

- The security of systems to be used to analyse the data or to store it must be assessed
- Business practices and policies for the day to day handling of data must be reviewed with a focus on
  - How much data is required?
  - What is it used for?
  - How many people have access to it?
  - How is it stored?
  - How and when is it destroyed?

Risk Assessment and Mitigation

- Set up a process whereby the risks associated with data security are regularly assessed to deal with changing working practices, changing technology and changing regulations
- Assess the continued effectiveness of mitigation strategies
- Review access rights and authorities to ensure relevance
- The concept of data security must be embedded into all aspects of the organisation's working practices and enforced

Risk Assessment and Mitigation (Cont)

- Everyone in the organisation must understand and buy into data security procedures, training and communication needs to be regularly refreshed
- Activities involving any third parties need special care and the business practices of the third party must be regularly reviewed and assessed
- The amount of data being shared internally and with external parties, and its use, should be regularly reviewed
- Data held in test and development environments is still data and should not be forgotten

Data Privacy 'Top 10 Tips'

1. Privacy is now part of the daily news - Enforcement and Litigation are steadily increasing and laws continue to evolve; Follow changes to the law and other developments.

2. You cannot have privacy without security – Review risks and mitigation strategies - technology and regulations change all the time, risks do too.

3. Well drafted policies are not enough - The policies need to be policed and appropriate evidence collected.

4. Create a 'Privacy Culture' within the organization - Educate your employees through Training and Awareness programs. Training needs to be ongoing and keep pace with changes in technology and regulations.

5. Most data breaches are caused by third (and fourth) party providers - Perform due diligence and oversee vendors. Your partners data security ethos and data handling practices need to be aligned with yours.

Data Privacy 'Top 10 Tips'

6. Negligence, lost devices and human error are still the most common causes of data breach and if you are breached, respond quickly to both your customers and to the regulators.

7. You can outsource systems and technology but you are still responsible to customers and regulators for compliance with laws and protection of data.

8. Think about your whole business process – even data destruction needs to be secure.

9. Review access rights and use data is put to on a regular basis – people's roles and needs for data change over time.

10. Don't forget to consider any data you use in systems development, your test and development environments will still use data – data is data and still needs to be protected.

Q&A

- Opportunity for questions from the attendees