Cyber Risk Management

Best Practices for Insureds

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

David Ma
Direct: +1.416.596.2895
Mobile: +1.416.625.8229
dma@blaney.com
vCard: http://d-ma.ca/dma1vcf

Overview

- What are cyber risks?
- Losses caused by cyber risks
- Best practices

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

What Are Cyber Risks?

- Harm from failures relating to information technology
- Technology amplifies benefits as well as harm
- Not just about prevention
- Not just about information and data loss

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Some Canadian Examples (1/6)

- 2001 - CIBC mistakenly faxes personal information of hundreds of customers to a scrapyard
- 2005 - Hackers gain access to Equifax and steal hundreds of customer files, including social insurance numbers and financial information
- 2005 - IBM, a service provider to the Alberta government, loses a tape with health information of more than half a million individuals

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Canadian Examples (2/6)

- 2006 - BC government sells backup computer tapes containing sensitive medical information on thousands of individuals
- 2006 - Laptop containing unencrypted financial data of 8,000 clients of MD Management was stolen
- 2006 - Laptop containing files for customers of a branch of the Bank of Montreal was stolen.

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Canadian Examples (3/6)

- 2008 - DaimlerChrysler loses a hard drive containing personal financial information of 240,000 customers
- 2009 - Nurse at Durham Regional Health Department loses an unencrypted memory stick with personal and confidential information of more than 83,000 patients who had received flu shots.

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Canadian Examples (4/6)

- 2007 - Rogue Bank of Nova Scotia employee steals confidential information of customers to commit fraud
- 2011 - Hackers steal personal information of 283,000 customers from Honda Canada's e-commerce websites

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Canadian Examples (5/6)

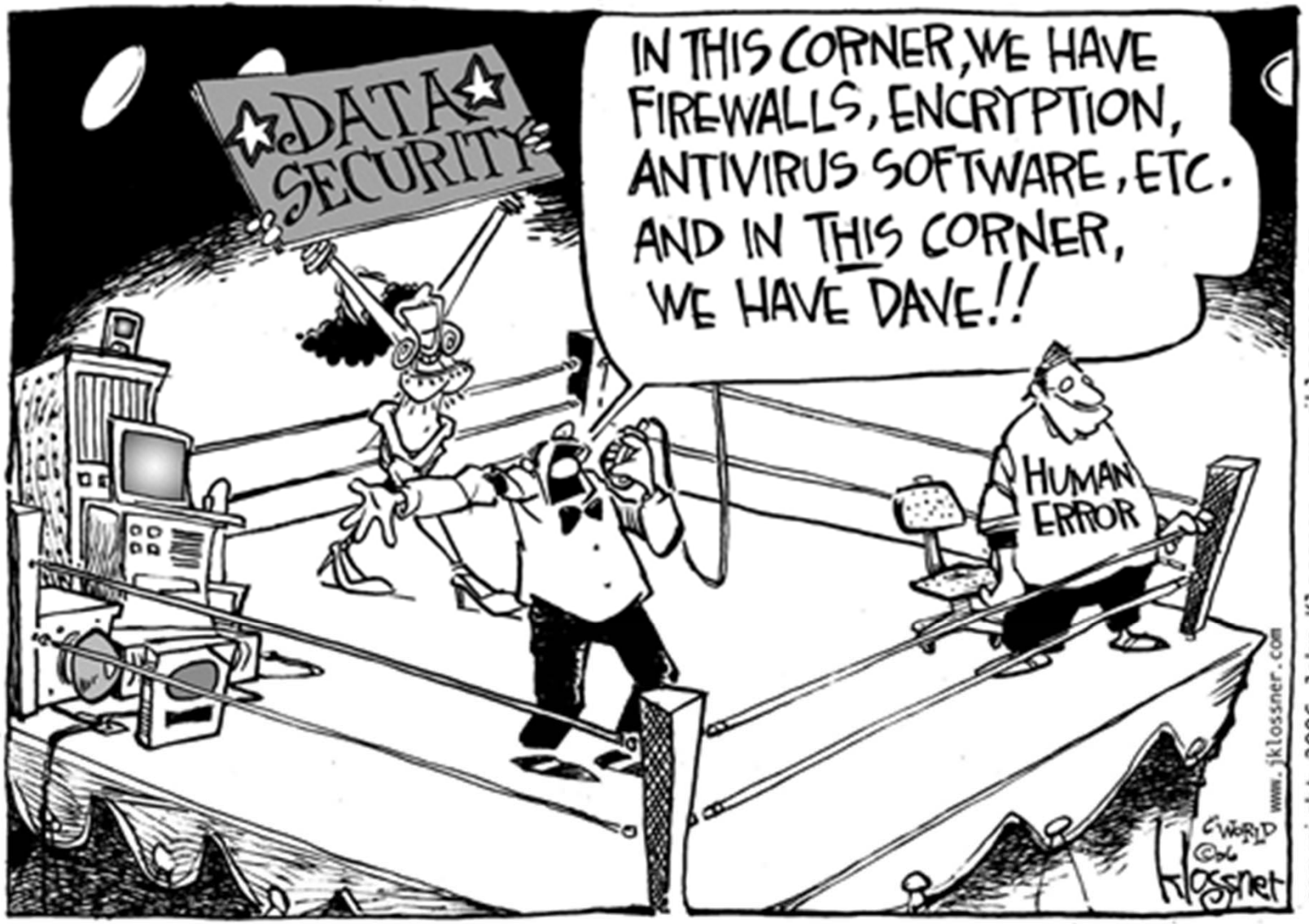
- 2011 - Hospital clerk (who was also an anti-abortion activist) at the Peterborough Regional Health Centre inappropriately accessed records of hundreds of patients who had undergone abortions
- 2012 - Employees at Human Resources and Skills Development Canada lose hard drive and USB key, resulting in the loss of personal information of 583,000 student loan recipients

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Canadian Examples (6/6)

- 2014 - Canada Revenue Agency's website exploited through the Heartbleed security flaw, compromising 900 social insurance numbers
- 2014 - Rogue employees at Rouge Valley Health System steal personal information of more than 14,000 patients and sell it to a financial firm

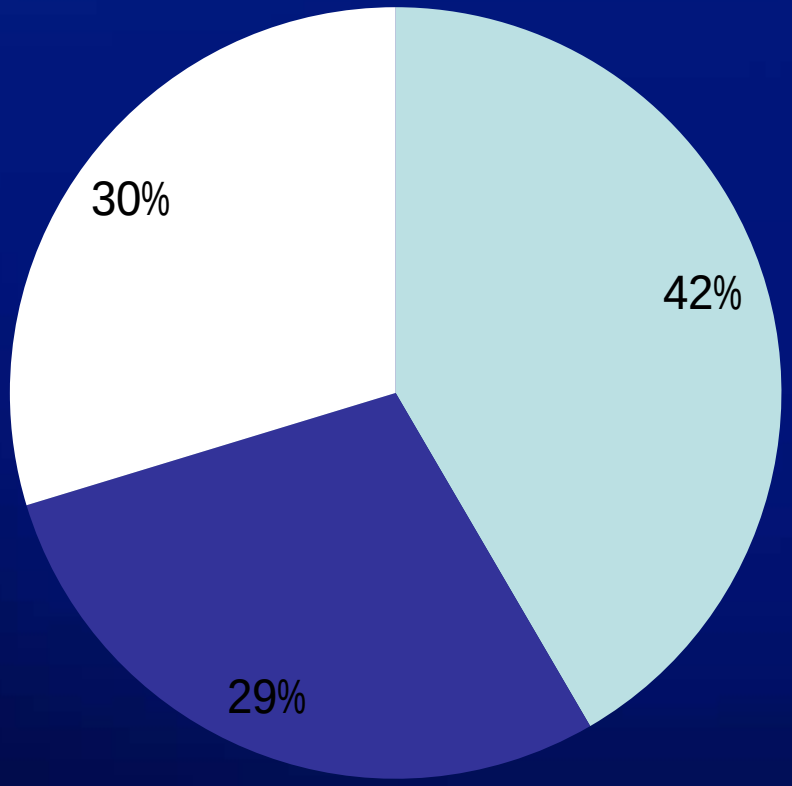
Blaney McMurtry
BARRISTERS & SOLICITORS LLP



Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Root Cause of Data Breach

Ponemon 2014 Cost of Data Breach Study



Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Losses Caused by Cyber Risks

- Third party liability
- First party direct losses
- First party indirect losses

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Third Party Liability

- Mitigation efforts
- Supplier/service provider claims
- Customer claims
- Intrusion upon seclusion
- Legal costs

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

First Party Direct Losses

- Investigative costs
- Remediation of security
- Recovery of data and systems
- Regulatory costs
- Property theft

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

First Party Indirect Losses

- Business interruption
- Loss of Goodwill

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

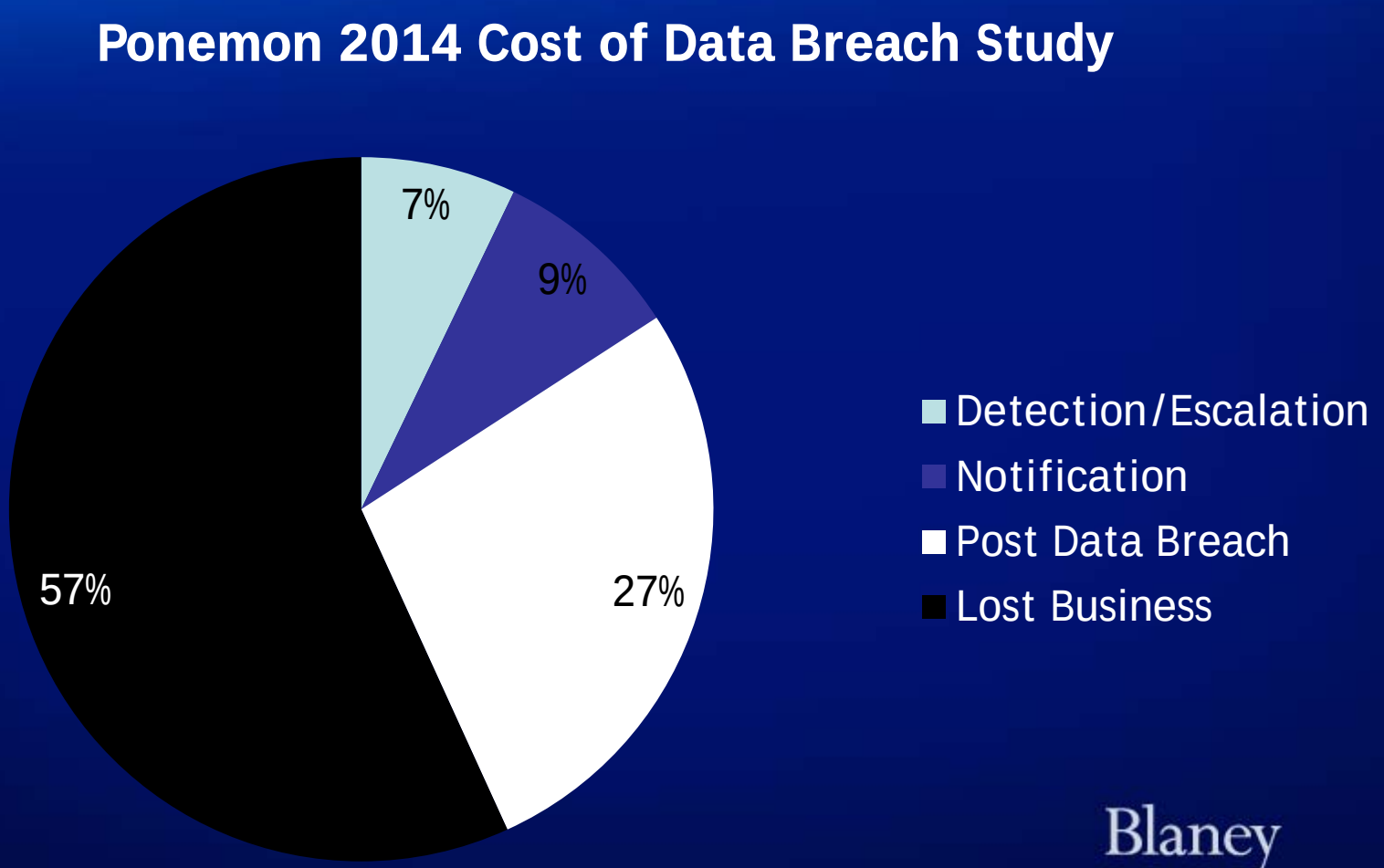
Some Figures

- Average total cost per breach: $3.5 million
- Average cost per record: $145
- Factors that decrease cost (per record):
  - Strong security posture – $14.14
  - Incident response plan – $12.77
  - Chief Information Security Officer - $6.59
- Factors that increase cost (per record):
  - Breach caused by lost/stolen device + $16.10
  - Third party involvement in breach + $14.80
  - Quick notification + $10.45
  - Engagement of consultants + $2.10

Ponemon Institute 2014 Cost of Data Breach Study

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Breakdown of Losses (US)



Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Best Practices

- Standards and Guidelines
- General Principles

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Standards and Guidelines (1/5)

- International Organization for Standardization/International Electrotechnical Commission Standards
  - Information technology - Security techniques - A framework for IT security assurance - ISO 15443
  - Information technology - Security techniques - Information security management systems - Requirements - ISO 27001/27002
  - Information technology – Security techniques – Information security risk management, ISO/IEC 27005

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Standards and Guidelines (2/5)

- Government of Canada policies - developed by the Treasury Board
  - Policy on Government Security
  - Operational Security Standard: Management of Information Technology Security (MITS)
  - Guidelines for Privacy Breaches
  - Privacy Breach Management Toolkit
- Canadian Get Cyber Safe Guide for Small and Medium Businesses
- Protection of Canada's Vital Cyber Systems Act (forthcoming)

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Standards and Guidelines (3/5)

- Ontario eHealth Guide to Information Security for the Health Care Sector
- US National Institute of Standards and Technology
  - Framework for Improving Critical Infrastructure Cybersecurity
  - Federal Information Processing Standards 200 - Standard for Minimum Security Requirements for Federal Information and Information Systems
- US Computer Emergency Readiness Team - Cyber Resilience Review

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Standards and Guidelines (4/5)

- Software Engineering Institute - Governing for Enterprise Security (GES) Implementation Guide
- US Financial Industry Regulatory Authority - Report on Cybersecurity Practices
- US Federal Financial Institutions Examination Council (FFIEC) - Information Security Booklet
- SANS Institute - Critical Security Controls

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Standards and Guidelines (5/5)

- Information Systems Audit and Control Association (ISACA) - Control Objectives for Information and Related Technology (COBIT)
- The International Association of Privacy Professionals - Managing Your Data Breach
- Payment Card Industry Data Security Standards
- OSFI Cyber-Security Self-Assessment Guidance

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

General Principles – Key Functions

- Identification
- Protection
- Detection
- Response
- Recovery

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Identification

- Governance
- Inventory
- Risk assessment

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Protection and Detection

- Security policy
- Skills assessment and training
- Consequences
- Access controls and limitations
- Data security lifecycle
- Activity records
- Security reviews
- Contractual protections

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Response and Recovery

- Response and recovery plan
- Identification and assessment
- Containment and mitigation
- Preservation and analysis
- Report and communicate
- Recovery and improvement
- Incident response team
- Breach coach
- Insurance

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Conclusion

- Growing market
- Insurers as subject matter experts
- Improved underwriting
- Informing and improving standards

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Thank you!

David Ma

TEL 416. 596.2895| DIRECT FAX 416.594.5081

DMa@blaney.com

Blaney McMurtry LLP

2 Queen Street East, Suite 1500

Toronto, Canada M5C 3G5

www.blaney.com

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Lawyer Profile

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

EXPECT THE BEST

David Ma

Direct 416.596.2895 Direct Fax 416.594.5081
dma@blaney.com

Called to the Bar of Ontario, 2000

Called to the Bar of New York, USA, 2000

LL.B., McGill University, 1998

B.C.L., McGill University, 1998

B.Comm. University of Toronto, 1991

Qualified as a Chartered Accountant and a Chartered Financial Analyst

Member, Canadian Bar Association (Ontario)

Board of Directors, Canadian IT Law Association

Member, International Technology Law Association

David Ma is a member of the firm's Corporate/ Commercial group.

David maintains a practice focusing on commercial transactions involving technology (including outsourcing, development, licensing, distribution, service provision, procurements, electronic commerce and related matters) as well as corporate matters involving companies that develop, market and exploit technology (including shareholder agreements, corporate structures and reorganizations, financings and acquisitions and divestitures).

David leverages both his experience in dealing with technology and the business of technology and a strong background in accounting and finance to deliver practical, sensible and cost-effective advice. He advises a broad variety of clients - from start-ups to large national and multi-national corporations and financial institutions.

David is member of the Canadian IT Law Association, the International Technology Law Association, the Information Technology and E-Commerce Section of the Ontario Bar Association, the Licensing Executives Society, the Toronto Computer Lawyers Group and the American Bar Association.

David was called to the Bars of Ontario and New York in 2000. He obtained his common law and civil law degrees from McGill University (with Distinction) and during his time there was the recipient of the Stikeman, Elliott Tax Prize and the Patricia Allen Memorial Prize for contribution to student life. David is also qualified as a Chartered Accountant and Chartered Financial Analyst, and holds a B.Comm. from the University of Toronto (Distinction, Double Specialist: Commerce & Finance and Economics).