



# Cyber Exposure: Mapping Risks, Analyzing Trends and Optimizing Insurance

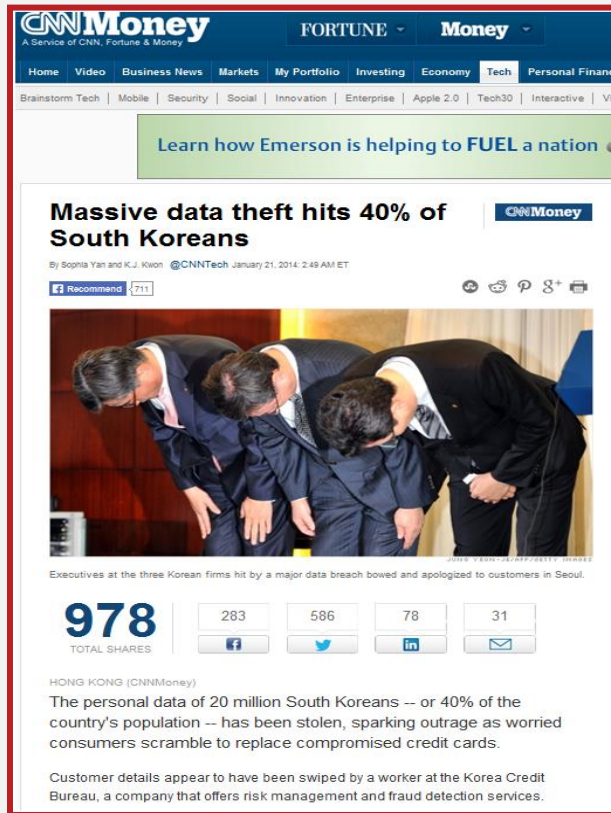
23.05.2014

Belhassen Tonat / Munich Re Seoul

1. Introduction
2. Cyber Risks Origins
3. Dimensions of Cyber Risks
4. Cyber Liability Heat Map
5. Relevance Across Industries
6. Technological Trends
7. Loss Scenarios
8. Regulatory Aspects
9. Cyber Insurance
10. Outlook and trends

# 1. Introduction

Seoul, February 2014



**CNN Money** FORTUNE Money

Home Video Business News Markets My Portfolio Investing Economy Tech Personal Finance


Brainstorm Tech Mobile Security Social Innovation Enterprise Apple 2.0 Tech30 Interactive

Learn how Emerson is helping to FUEL a nation

## Massive data theft hits 40% of South Koreans

By Sophia Yan and K.J. Kwon @CNNTech January 21, 2014 2:49 AM ET

Recommend 711



Executives at the three Korean firms hit by a major data breach bowed and apologized to customers in Seoul.

**978** TOTAL SHARES

|     |     |    |    |
|-----|-----|----|----|
| 283 | 586 | 78 | 31 |
|     |     |    |    |

HONG KONG (CNNMoney)

The personal data of 20 million South Koreans -- or 40% of the country's population -- has been stolen, sparking outrage as worried consumers scramble to replace compromised credit cards.

Customer details appear to have been swiped by a worker at the Korea Credit Bureau, a company that offers risk management and fraud detection services.

Tokyo, May 2011



Sunday 01 May 2011

## The Telegraph

HOME NEWS SPORT FINANCE COMMENT BLOGS CULTURE TRAVEL LIFESTYLE FASHION

Companies Comment Personal Finance Economics Markets Your Business Olympics Business

Banks and Finance Media and Telecoms Retail Transport Construction Industry Energy

Media and Telecoms

### Sony facing profit hit on Playstation security breach

Sony has issued a profuse apology and warned that the cost of winning back customers' trust following its unprecedented PlayStation security breach may whack profits.



Share:

Recommend 20

Tweet 51

Media and Telecoms

Finance »  
News by Sector »  
Business Latest News »  
Technology »  
Rupert Neate »

IN FINANCE

iPad to boost 2011 IT spend to \$3.6 trillion

Crozier: 'ITV must go for acquisitions'

Photo: AP

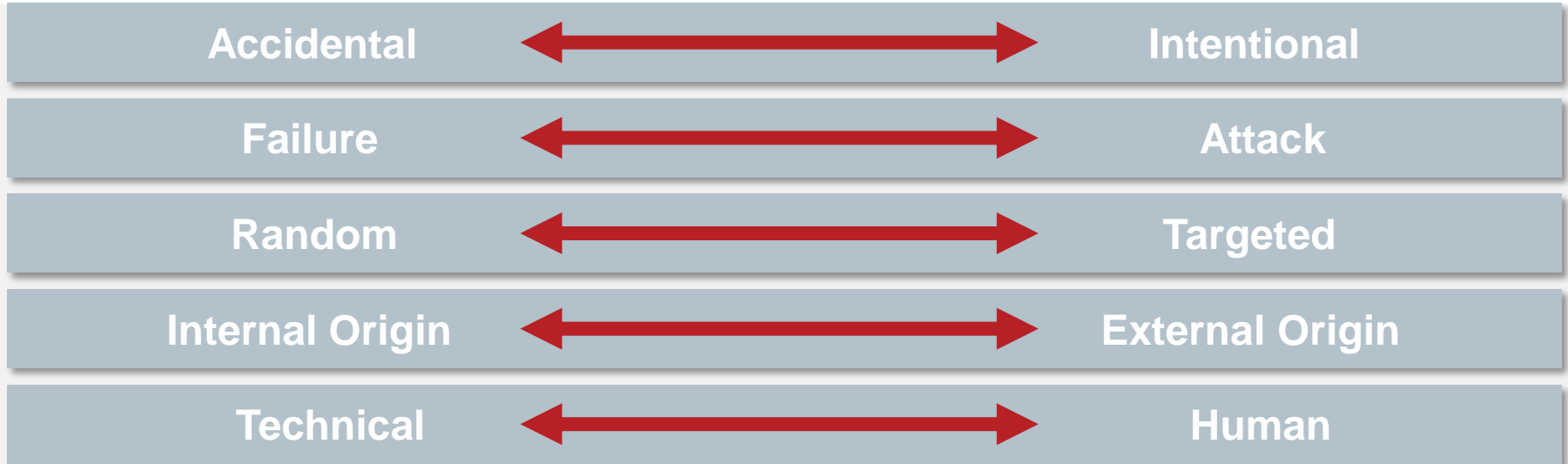
By Rupert Neate 8:16PM BST 01 May 2011

4 Comments

The warning came as Sony executives delivered a dramatic *mea culpa* to 77m PlayStation Network customers, whose personal data and credit card details may have been stolen by hackers.

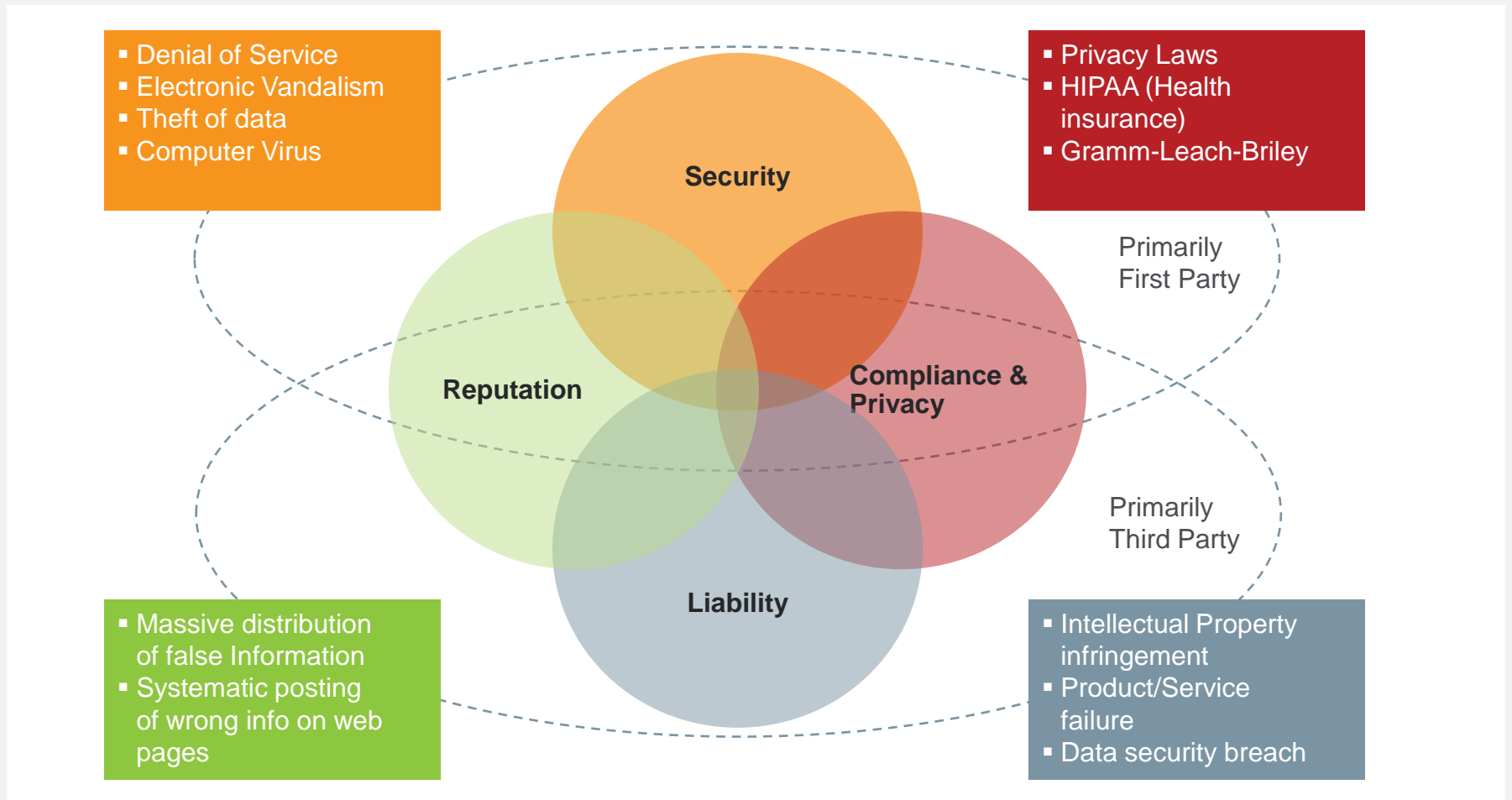
Kazuo Hirai, president of Sony's computer entertainment division and the man widely seen as the leading contender to succeed Sir Howard Stringer as Sony's chairman and chief executive, said: "We apologise deeply for causing great unease and trouble to our users."

## 2. Cyber Risk Origins



Anyone..... Anytime..... Anyplace..... Anyway

### 3. Dimensions of Cyber Risks



**A lot of overlap**

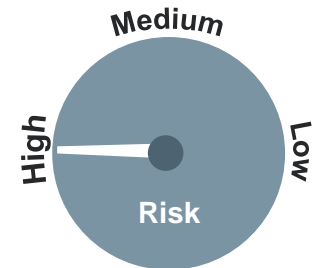


**Adds to complexity**

## 4. Cyber Liability Heat Map

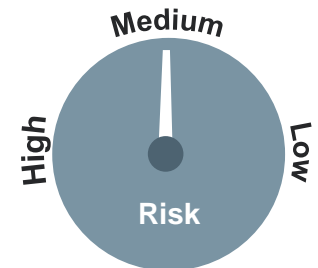
### 1. Security breaches and cyber attacks – High Risk

- The most valuable data to thieves is financial information or information that can be used to perpetrate identity theft
- A cyber attack can also cause disruptions to business operations and other economic harms



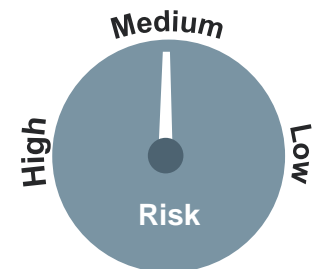
### 2. Unintentional disclosures of sensitive data – Medium Risk

- Many online companies collect, store, and interact with “sensitive data”
- The privacy protections afforded to individuals online is far from comprehensive, however, class action lawsuits have had success and new US legislation appears imminent



### 3. Workplace-related liabilities – Medium Risk

- Employees using social media at work and at home, creating potential secondary liabilities (IP infringement, defamation, harassment, securities fraud, etc.)
- Monitoring employees’ communications and other invasions of privacy
- Online research of current or potential employees (hiring and firing)

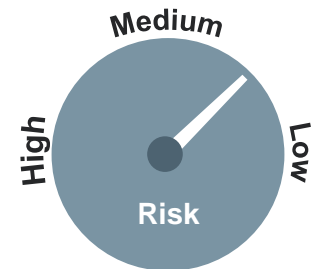


## 4. Cyber Liability Heat Map (cont'd)

### 4. Unintentional loss or destruction of data or services

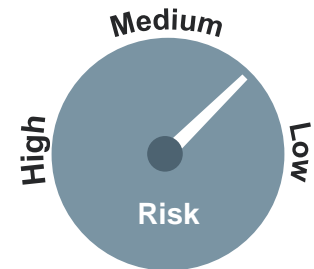
#### – Medium Risk/ Low Risk

- Many companies now offer cloud-based services that allow consumers and businesses to store and interact with data on remote servers managed by the companies. Losing or recovering data assets can be expensive
- Isolated service outages and accidental data loss have raised liability questions related to the maintenance, storage, and accidental destruction cloud-stored data



### 5. Other secondary liabilities – Medium Risk/ Low Risk

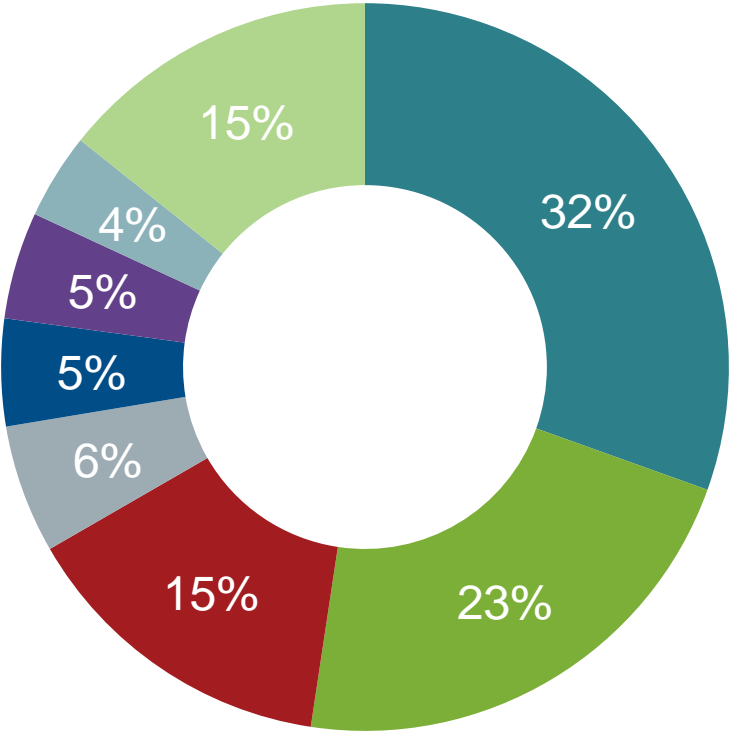
- User-generated content: IP infringement, unlawful speech
- Trademark claims against search engines and auction websites



# 5. Relevance Across Industries

# events

Financial and Healthcare sectors are most affected

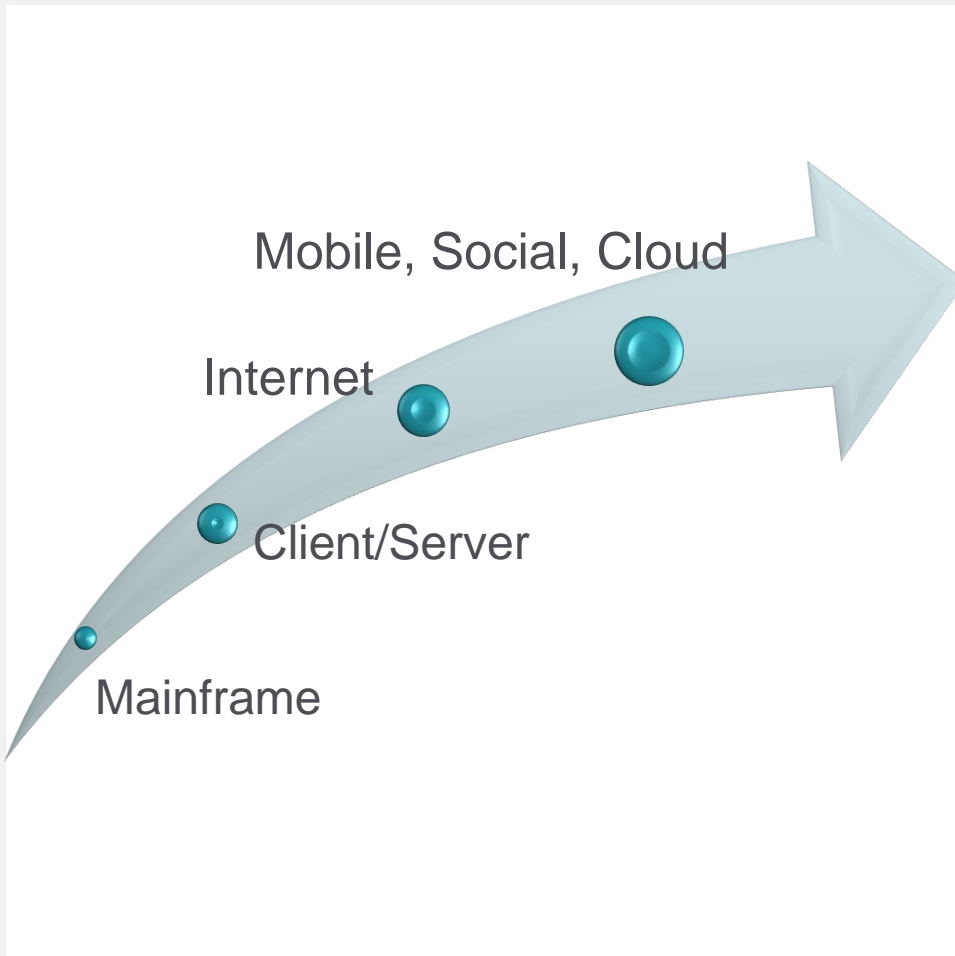


- Financial Services
- Healthcare
- Retails
- Manufacturing
- Tech Services
- Business Services
- Government
- others



## 6. Technological Trends

Where we are...and where we're going



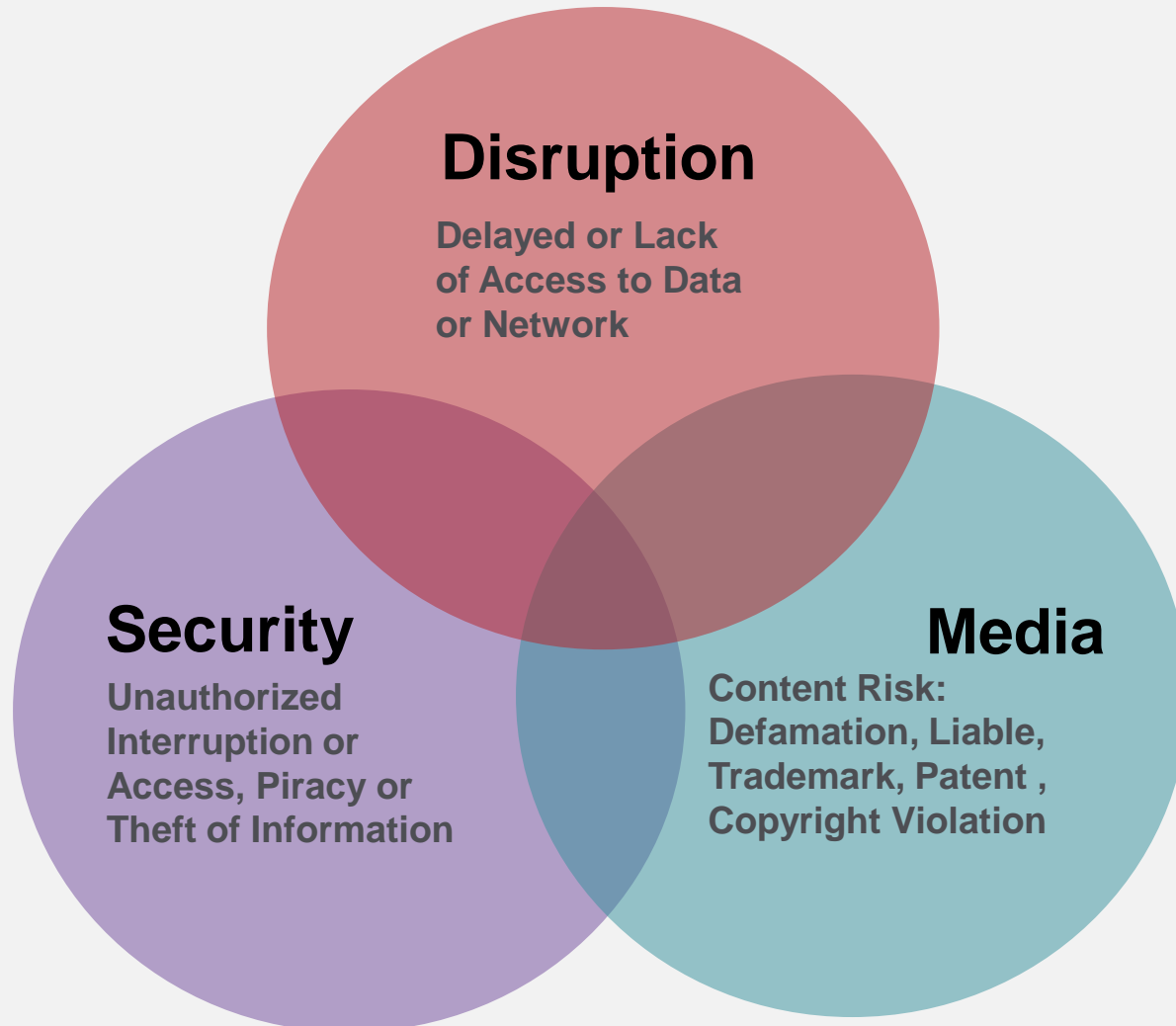
### Every 60 Seconds

- **98,000+** tweets
- **695,000** status updates
- **11 million** instant messages
- **694,445** Google searches
- **168 million+** emails sent
- **38 tons** of e-waste

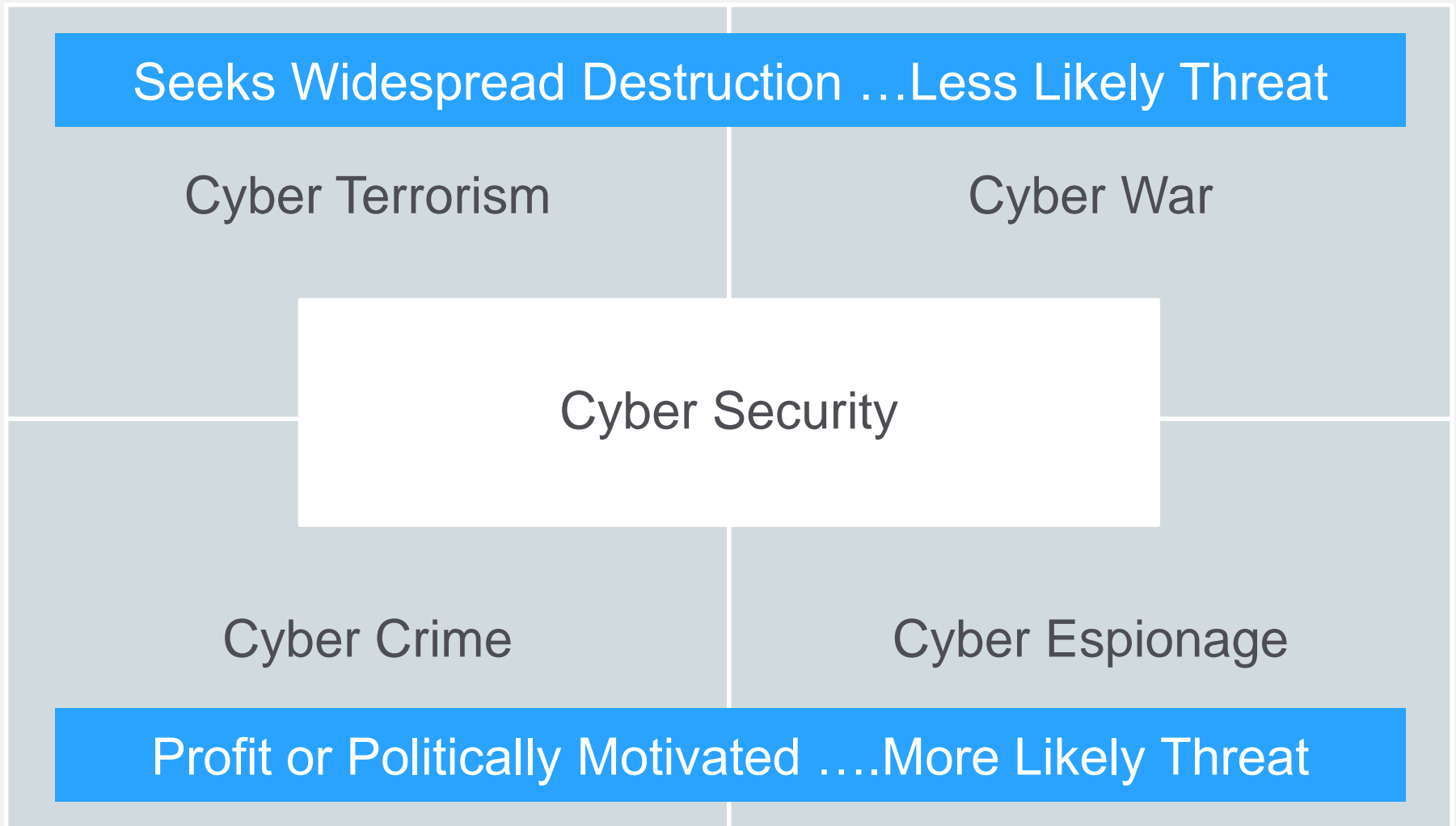
**Subject to change without notice**

# 7. Loss Scenarios

## Three Main Categories

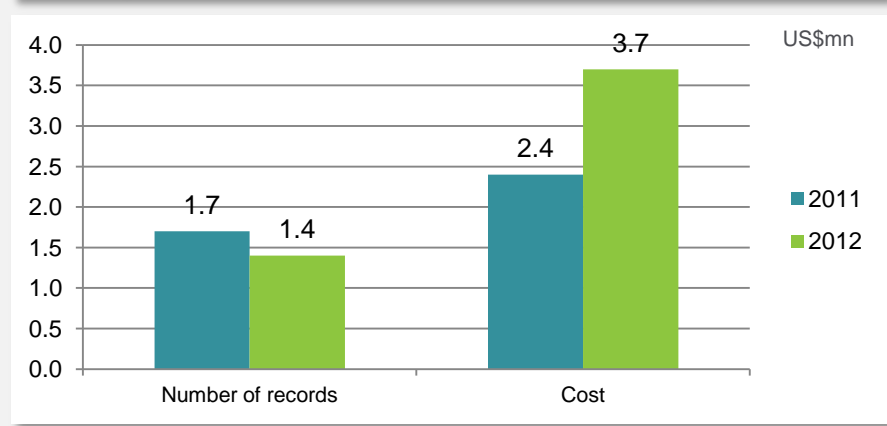


## 7. Loss Scenarios Security



# 7.1. Data Breach Special Security Risk - Trends

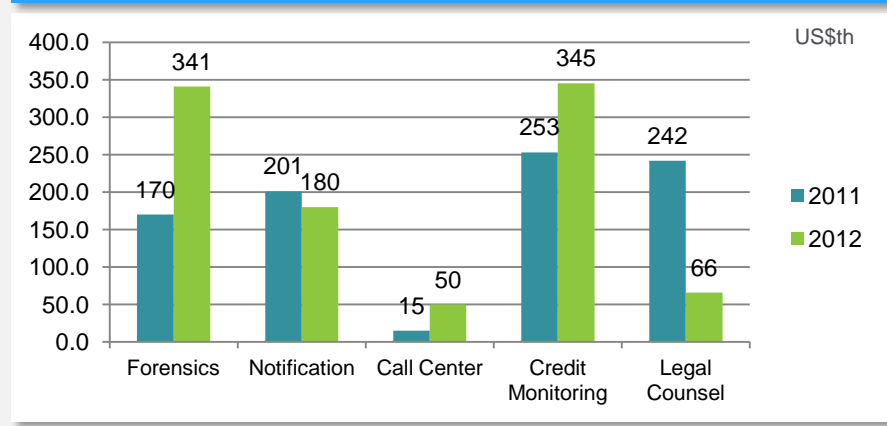
**Comparing 2012 & 2011 Findings**  
Average number of records exposed and average cost



**Comparing 2012 & 2011 Findings**  
Average cost by type



**Comparing 2012 & 2011 Findings**  
Average cost for crisis services



- Number of records exposed is lower, but average cost is higher
- Legal settlements drive the costs
- Forensic costs and credit monitoring up

# 7.1. Data Breach

## Special Security Risk - Trends

- Employee behaviors, both intentional and accidental are a fundamental cause
- Small/Midsize businesses (SMBs) are at a greater risk (81% to 78%)

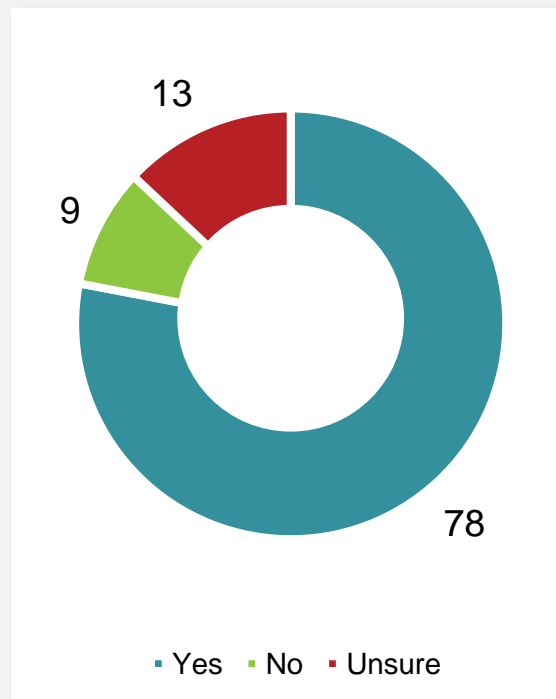
### SMBs More Likely to:

- Open spam
- Leave computers unattended
- Visit off-limit websites

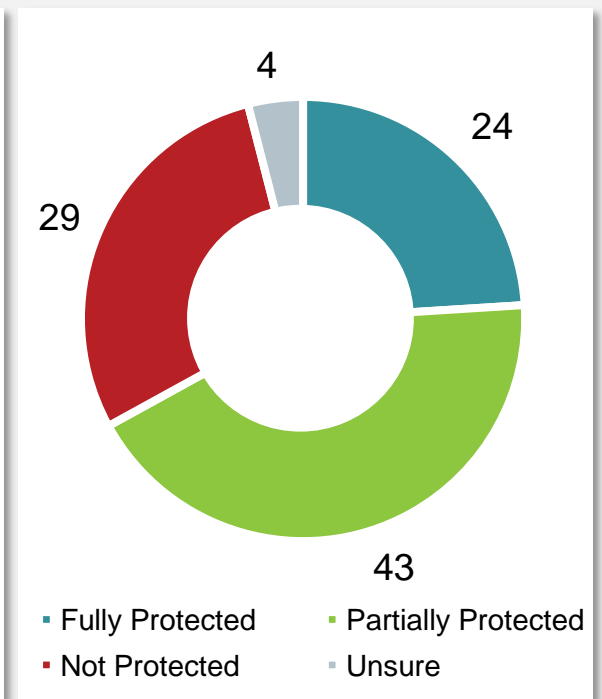
### Data Breach Top 3 Causes

- Loss of laptop /mobile devise (35%)
- 3<sup>rd</sup> party vendor mishaps
- System glitches

Has your organization ever experienced a data breach as a result of negligent or malicious employees or other insiders?



In general, is your organization's sensitive confidential business information protected by encrypted or other data protection technologies?



# 7.1. Data Breach

## Special Security Risk - Trends

### Increased Exposure

- Increased use - Social Media; Transactional Activity , Mobile Activity
- Rapid Technological evolution and development ; E.g., Wi-Fi, Hand Held devices, Cloud Computing

### Workplace Trends

- Nontraditional work arrangements
- Qualified IT staff
- Information technology budgets
- Customer demands

### Workplace Technology Trends

- Increase in high-speed Internet lines
- Software trends –Microsoft dominance
- Increasing sophistication of computer programs
- Internet and e-mail trends

### Increased System and Data Vulnerability

## 7.2. Data Breach

### Special Security Risk– Loss Examples

#### Hannaford Brothers Supermarkets

- Dec. 2007 breach...Made public March 2008
- 4.2m credit/debit card numbers exposed – Est. 2,000 subject to fraud... Litigation pending

#### TJX (TJ Max, BJ Warehouse Club, Marshals, etc. )

- 45.6m customer credit cards breached in 2007
- \$256m (Cost to companies, banks and insurers)
- \$200m class action (incl. \$177m for Credit monitoring)

#### Heartland Payment Systems (Credit Card Processor)

- 2008/2009 credit card breach – Partial settlement as of 2010 for \$114m – 139m
- 100m transactions per month - 40% are small / mid-sized businesses (e.g. restaurants)
- 130m credit card records breached

#### RockYou (Social Media Application Developer)

- 2009 breach
- Hackers gained access to 32m email addresses and passwords
- Claims include company was slow to respond

## 7.2. Data Breach

### Special Security Risk– Loss Examples

#### Epsilon

- 2011 breach
- Email marketing – 40 billion emails per year
- 2% of database invaded
- Names and email addresses of customers of thousands of name brand business exposed (Citigroup, Capital One, Best Buy, Target, etc.)

#### SONY On Line Entertainment

- 2011 Breach of Sony PlayStation On-line Gaming System
- Potential costs could reach \$50m or more in revenue and remediation costs

#### ZAPPOS (Subsidiary of Amazon)

- 2012 Breach by hacker
- On line shoe and clothing retailer
- 24 million customers information accessed (names, addresses.... But company says actual credit card information was not breached
- Class action has commenced



## 7.2. Data Breach Special Security Risk– Loss Examples

### LinkedIn (Social Network)

- Breach reported in June 2012 (UPI)
- Possible 6.4m members data breached (Reuters)
- Total members = 161m globally (61% in the US)

### Global Payments (Credit Card Processor)

- March 2012 reported breach = \$94m
- 1.5m credit/debit cards breached
- Co still not sure what was actually stolen but customer names, addresses, SS #, driver license # and bank account information was exposed

### Yahoo (Web Service)

- July 2012 breach
- 400,000 user names and passwords stolen
- Yahoo, Gmail, Hot mail, Comcast impacted
- Committed by a group of hackers known as D33D just to show that the system is not secure

## 7.2. Data Breach Special Security Risk– Loss Examples

### Wyndham Hotels

- 2012 breach of global hotel chain
- 600,000 credit cards

### eHarmony

- 2012 breach of on line dating service
- 1.5Million passwords

### Texas Attorney General's Office

- 2012 breach
- 6.6 Million records

### Gamigo

- 2012
- On line game developer
- 3 million records

## 7.2. Data Breach Special Security Risk– Loss Examples

### Hamilton County Court Clerk (OH)

- County Website breached – Hundreds of county residents' data stolen
- 1.3mm records: tax, medical, bank account, etc.

### Chicago Board of Elections

- 100 computer disks were inadvertently shared
- 1.3mm Chicago residents SS # exposed
- Class action filed

### Texas Attorney state controller's

- In 2011 unencrypted state employee retirement data posted on the states public website
- 3.5mm state employees exposed

### Texas State Comptroller

- Student break in - Teacher, student, taxpayer personal information stolen
- Over 16,000 residents, 15,000 students impacted

## 7.2. Data Breach Special Security Risk– Loss Examples

### Sutter Medical Foundation

- 2011 burglary of computers containing patient information dating back to 1995
- Information on 4mm patients at risk

### EMCA

- Student identity theft
- Office break-in resulting in 3.3 mm college students' personal information data stolen

### Diocese of Providence

- Vandals broke into church offices and physically stole unlocked computers – Personal data on 5,000 current/former employees exposed

“Cyber attacks now 2<sup>nd</sup> most common economic crime (asset misappropriation is #1” (Financial Planning 3/27/12)

## 7.3. Data Breach Takeaways

High Tech  
High Profile

**Don't have to be Targeted**

Low Tech  
Low Profile

**Everyone is at Risk**

- Automated programs search for unprotected computers on the internet...doesn't care if it finds a Fortune 500 computer or the local pizza parlor computer or a church computer or another computer
- Located vulnerable computer accessed to install malicious software:

Identity Theft

Malicious Mischief

Vandalism

**FTC : 2010 Identity Theft is Most Frequently Reported Complaint 250,000 or 19% (11th Year in a row)**

**Towers Watson 2012 Study:  
72% of Commercial Insurance Buyers Do Not Have Cyber Insurance**

## 7.4. Social Media/Blogging Special Media Risk

**Beyond Increased Breach Exposure.....**

**“Open” Communication  
Platform**

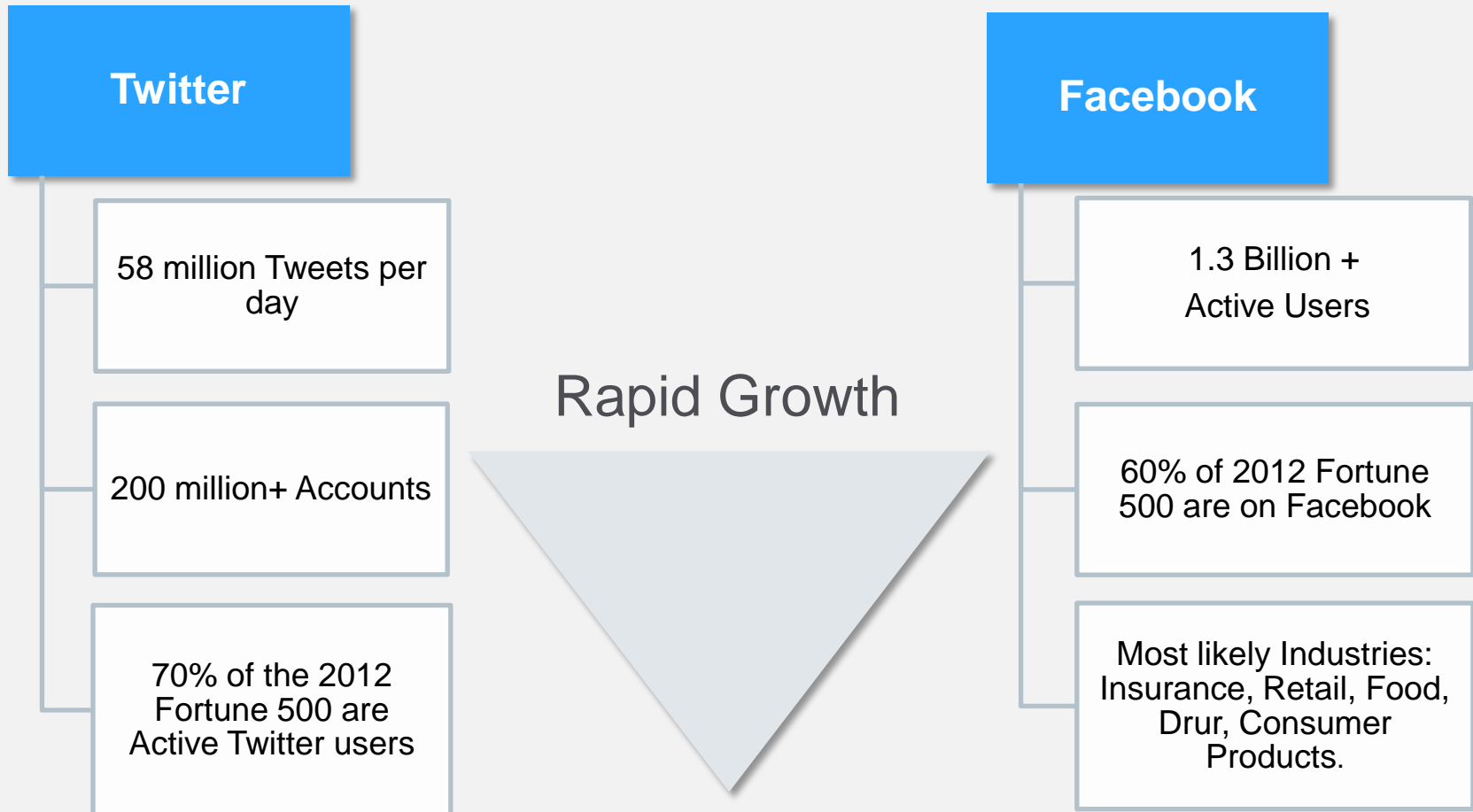
**Social Media**

**Content Risks**

**Everyone is in the Publishing Business  
Any person or organization, not just media companies,  
can be sued for media content**

## 7.4. Social Media

Some Quick Numbers (Already outdated!)



**Widespread Personal and Commercial Use**

### Commercial Risks: Social Media Exposure varies by Predominant Usage

Internal  
Employees Focus (Employment  
Practices Liability)



#### Discrimination or Harassment

- Hiring, Treatment, Termination
- Liable/Defamation
- Invasion of Privacy
- Cyber Stalking

External  
Public, Customers, Students,  
Constituents



#### Operational

- Antitrust Violations
- Data Security (Breach)
- Trade Secrets
- Copyright/Trademark Infringement
- Consumer Fraud/Deceptive Practices

Speed and global reach  Greater Impact



## 8. Regulatory Aspects US perspective

### Notification Legislation – fluid & complex laws and regulations

- State and federal laws – include penalties for failure to notify possibly affected persons
- Law follows the victim – most losses extend over multiple states

### State laws are extensive

- 46 States plus DC and Puerto Rico have individual Laws –
- MA and NV have the most stringent privacy laws setting the standard for other states
- CA and WA recently passed revised laws

### Federal legislation recently passed includes

- 2/17/10 – HITECH Act Protecting Health information – Expanded application of HIPAA
- 2/22/10 – Full Enforcement of Health Data Breach Notification Rules
- 12/31/10 – Broad Federal “Red Flag Rules” instituted

### Litigation still Evolving, but fertile ground for Class Actions

- Costs include: Civil Penalties, Damages, Remediation/Notification/Recovery Expenses, Lost Business

## 8.1. Specific Laws of Interest

### A Quick Reference (1/2)

#### Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999)

- Mandatory Compliance – Broad governance of consumers non-public information

#### Sarbanes-Oxley Act of 2002 (SOX)

- Sets tough standards for all US public companies

#### Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Title II of the Act sets requirements for the administration of electronic health care information

#### Health Information Technology for Economic and Clinical Health (HITECH)

- Modified the penalties that could be imposed for violations of HIPAA

#### Payment Card Industry Security Standard (PCI DSS)

- Worldwide security standard for credit/debit cards

#### Computer Fraud and Abuse Act

- Passed in 1986 to reduce computer hacking

#### Basel II

- EU Recommendations on Banking Laws & Regulations – requires enterprise risk standards

#### Genetic Information Nondiscrimination Act of 2009 (GINA)

- Protects employees from discrimination if an employer accesses their genetic information

## 8.1. Specific Laws of Interest

### A Quick Reference (2/2)

#### Identity Theft and Assumption Deterrence Act

- Makes identity theft a Federal crime with severe penalties Establishes that the person whose identity was stolen is a true victim (previously was only the credit grantors)

#### California On-Line Privacy Protection Act

- Requires strong privacy practices for e-commerce sites be posted and fully complied with

#### Fair Credit Reporting Act (FCRA)

- Governs the collection, dissemination, and use of consumer credit information

#### Fair and Accurate Credit Transactions Act (FACTA) – Strengthens FCRA

- Added new sections to the Fair Credit Reporting Act (FCRA) intended to fight identity theft

#### Multiple Federal legislation has been/is being developed

- List of major proposed laws on next slide

#### Most States (44 and counting) have Anti-Bullying Statutes related to Electronic Bullying

**All involve Significant Fines, Penalties and/or Prison**

## 8.2. Federal laws - Proposed .....A Quick Reference

### Specific Cyber Laws Proposed

|  |  |
|--|--|
| <b>CISA Act of 2012 (S 2102)</b>           | Improve the sharing of cyber security information among entities in the private sector and between the private sector and the government.                          |
| <b>PRECISE Act of 2011 (HR 3674)</b>       | Establishes the National Information Sharing Organization (NISO) to serve as a collector of information relating to cyber threats.                                 |
| <b>SAFE DATA Act (HR 2577)</b>             | Establishes uniform national standards for data security & data breach notification.   |
| <b>CISPA Acts of 2011 (HR 3523)</b>        | Intended to protect business from intellectual property theft by hackers; Exemption from liability for sharing the information with the government.                |
| <b>Cyber Security Act of 2012 (S 2105)</b> | Gives the Department of Homeland Security <u>broad powers</u> to require that “critical” computer systems meet minimum security standards.....Defeated August 2012 |
| <b>SECURE IT Act of 2012 (S 2151)</b>      | Competing version of the Cyber Security Act with less force; Gives the DHS less authority than the Cyber Security Act.   |

## 8.2. Federal Laws – CISPA ..... .....A Quick Reference

### The CyberSecurity Act of 2012 (S 2105)

- Introduced February 14, 2012
- Gives the Department of Homeland Security broad powers....Most of the provisions implemented as an Executive Order by President Obama in 2013 to require that “critical” computer systems meet minimum security standards
- Requires that “company” computer systems involved in “vital” functions meet standards set by the Homeland Security Department and industry
- Imposes a new regulatory scheme and risk-based security requirements upon owners of critical infrastructure
- **KEY => What is Deemed “CRITICAL” = DHS determines : Life Sustaining Services, Damage to Economy or National Security**

Couldn't get Through Congress....  
2013 Executive Order by President Obama implemented most of the provisions ...  
.....while more permanent legislation continues to be developed.

**New standards established by the Bill could become a measuring stick for cyber security risk management for all public companies.**

## 8.3. Regulatory Aspects

### EU perspective



**2009:** Introduction of Data Breach Notification Requirement for the Electronic Communication Sector (Directive 2009/136/EC)

**2012:** On January 25th, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules, including:

- Notification within **24 hours** applicable to all industries
- Appointment of **Dedicated Data Protection Officer** for companies with more than 250 employees
- **Financial Penalties up to 2% of the Global Annual Turnover** of a company which violates EU data protection rules

Applicable for all companies which handle personal data of EU citizens.

To be enforced in 2014.

# 9. Cyber Insurance

## Unique Character – Unique Challenges

### “Commercial” Use

- The internet should never be considered fully secure
- Fundamental to business, not a “nice to have”

### Technology

- Complex and rapidly changing
- Risk management more challenging

### Accumulation

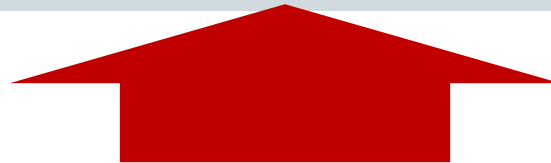
- Broad, simultaneous access and usage
- Global, instantaneous transmission

### Legal Landscape

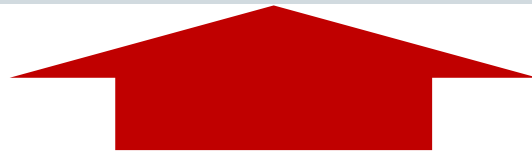
- Challenge - proving facts in court
- Rise in multi-jurisdictional disputes
- Determination of applicable law – Global and even state differences

## 9. Cyber Insurance “Commercial” Insureds

Profitable Growth Opportunities ?  
(If Risks are Fully Appreciated and Underwritten)



Risk Management and Coverage is Essential



Growing Risks: Technology and legal aspects are rapidly evolving



Broad Based, Global Use of the Internet



# 9. Cyber Insurance

## Cyber Risk - Specialized Coverage

### Wide Variety of Non-Standardized Coverage - 1<sup>st</sup> and 3<sup>rd</sup> Party.....A Common Sampling

|   |   |
|---|---|
| <b>Privacy Regulatory Defense &amp; Penalty</b>                 | Covers defense costs, fines/ & penalties for violations of privacy regulations, including but not limited to HIPAA and the new Hi-Tech Act.   |
| <b>Data Privacy/Security</b>                                    | Covers third party claims as a result of a network security/privacy breach. Covers both online /offline information, virus attacks, denial of service & failure to prevent transmission of malicious code.  |
| <b>Internet Media Liability</b>                                 | Covers both online and offline media. Website content (copyright/trademark infringement, libel/slander, plagiarism and personal injury ).   |
| <b>Intellectual Property</b>                                    | Theft/use/disclosure of proprietary, advertising, technology, trademarks, etc.  |
| <b>Information Asset Protection &amp; Business Interruption</b> | Covers expenses and costs required to recover and/or replace data that is compromised, damaged, lost, erased or corrupted. Coverage also includes business interruption and extra expense coverage for income loss as a result of the total or partial interruption of the insured's computer system. |
| <b>Cyber Extortion</b>  | Covers investigation costs and extortion demand.  |
| <b>Cyber Terrorism</b>  | Terrorist acts covered by the Terrorism Risk Insurance Act of 2002. In some cases, may be further extended to terrorist acts beyond those contemplated in the Act.  |
| <b>E&amp;O Coverage</b>   | Inadvertent loss or disclosure of data, employee error resulting in deletion of data or spreading of virus, etc.  |
| <b>Reputational Coverage</b>                                    | Covers reputational harm resulting from adverse media activity - pays for crises management expenses (via dedicated crisis management and public relations professionals) and pays for loss of revenue resulting from adverse media activity.   |

**Rapidly Growing and Evolving!**

## 9. Cyber Insurance

### Cyber Risk - Specialized Coverage - ISO Form

#### ISO E-Commerce Package

Designed for Commercial Enterprises, including Non-Profit Organizations that have some form of Web Presence

**Intent : Fill Gaps/Expand Coverage of the CGL Policy**

**Coverage : 8 Separate Insuring Agreements**

1. website publishing liability — copyright, trademark, trade dress, or service mark; defamation against a person or organization; or violation of a person's right to privacy
2. security breach liability — unauthorized acquisition or disclosure of client information held within a computer system or otherwise (for example, hard copy); transmission of a virus to a third party by e-mail or other means
3. programming errors and omissions liability — programming errors or omissions that ultimately disclose clients' personal information held within a computer system
4. replacement or restoration of electronic data — expenses incurred to replace or restore electronic data or computer programs affected directly by a virus
5. extortion threats — ransom payments and other expenses incurred resulting directly from cyber threats
6. business income and extra expense — loss of business income and/or extra expenses
7. public relations expense — expenses incurred to restore the insured's reputation
8. security breach expense — expenses incurred to notify parties affected by a security breach .

## 9. Cyber Insurance Specialized Coverage

Terms, Definitions and Conditions  
of similar Coverage can vary significantly, for example....

- Explicit Trigger (e.g., Claims Made; Failure to Secure Data, etc) rather than “Occurrence”
- Named peril rather than All Risk: Remediation, response costs, Regulatory fines, Penalties ( Defense costs only)
- Often Defense in Limit
- Most have been Developed since 2000 – Largely untested in Court
- Scope of Coverage varies including:
  - Indemnity v Pay on behalf;
  - Aggregate Limits;
  - Duty to Defend;
  - Definitions of key terms (“Claims”, Computer System”, “Damages”. Etc.);
  - Exclusions, Sub-limits, Expense Coverage, etc.

**Coverage is Growing and Evolving Rapidly  
A Growth Area for insurers.**

## 9. Cyber Insurance

### Hartford Steam Boiler (Member of Munich Re Group)

#### Identity Recovery Coverage

- Enhancement to various Personal coverage
- Coverage: Expense Reimbursement for Legal Expenses, Lost wages, Child/Elder care, Miscellaneous Expenses
- Services: Access to Identity Restoration Services

#### Data Compromise Coverage

- Enhancement to various Commercial Coverage
- Coverage: Expense Reimbursement (1<sup>st</sup> Party) including: Legal, Restoration, Forensic IT, Credit Monitoring, Notification
- 3<sup>rd</sup> Party Coverage is available

#### Cyber Risk

- Enhancement to various Commercial Coverage
- 1<sup>st</sup> Party Coverage – Data Restoration and Recreation, System Restoration, Business Income, Public Relations
- 3<sup>rd</sup> Party Coverage – Breach of 3<sup>rd</sup> Party Business data; Unintended Malware propagation, Unintended Denial of Service

## 9. Cyber Insurance

### Korea: Phishing and Hacking insurance

#### Covered risk

- Economical loss of the insured.
- Arising out of phishing and hacking.
- Due to the leakage of personal information.

#### Form of coverage

- Beneficiary is the individual.
- Mostly bought by an institution to cover its members.

#### Original terms and conditions

- Limit of Liability: KRW1mio. - 10mio. per insured
- Deductible: ~ KRW100,000 per insured

#### Covered Loss

- Economical loss of the insured
- Caused by false withdrawal of savings or misuse of credit card

## 9. Cyber Insurance

### Korea: Phishing and Hacking insurance (cont'd)

#### Period

- Loss occurrence : during the policy period
- Accident (financial fraud of phishing or hacking): also during the policy period

#### Coverage basis

- Occurrence basis policy and doesn't have any “extended reporting period” provision.

#### Most important Exclusion

- Economical loss during the policy period because of “accident” which took place before the beginning of the policy period.

## 9. Cyber Insurance

### Underwriting considerations

1. Which jurisdiction agreement?
2. Worldwide 193+ countries (multiple jurisdiction possible)
3. EU - "Freedom of Service" policy (FOS)
4. Premium tax requirement's („Kvaerner-judgement“)
5. Recommended limitations: patent infringement / penalties / Biz interruption.
6. Penalties from \$100 to \$1 million+ for "Payment Card Industry Data Security Standard" (PCI DSS violations) possible
7. Jurisdictions and policies define "data" differently: tangible property or pure financial loss?
8. Not all Cyber risks are excluded from commercial liability covers
9. Clients expectation for additional services / reputation protection in case of a claim
10. Potential risk of class action suits in the U.S./ EU

## 9. Cyber Insurance

### Takeaway Thoughts – Balance Risk/Reward

Take Advantage of Opportunities

Internet is central to commerce, it's fundamental to business operations

**Goal:** optimize the benefits and growth potential of Internet and provide proper, profitable coverage

Growth Potential

Diligent, Informed Underwriting  
Proactively manage the risks  
Develop proper coverage and underwriting expertise  
Focus on Risk Selection

Respect and Manage the Risks



- Emerging and Rapidly Evolving – Technology and Increased Use
- Coverage being developed to meet the challenges – Wide Variety
- May be a Common Coverage in the Future
- Significant Opportunities for Knowledgeable Underwriters



# 9. Cyber Insurance

## Munich Re Seoul - Service Portfolio

Data mining/ Portfolio analysis



Cycle + Market Analysis



Product Advice + Development



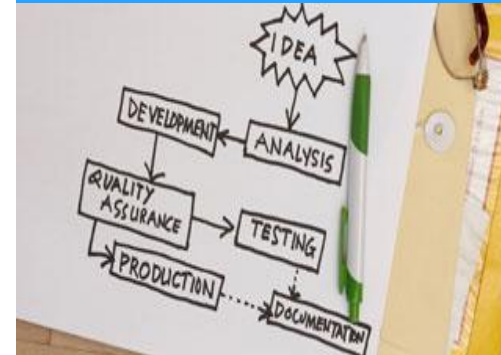
Rating advice



Underwriting Support



Business Administration  
(Underwriting + Claims)





Thank you for your attention

23.05.2014

Belhassen Tonat / Munich Re Seoul

© 2014 Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München ("Munich Re"). All rights reserved.

The content of this presentation (including, without limitation, text, pictures, graphics, as well as the arrangement thereof) is protected under copyright law and other protective legislation. These materials or any portions thereof may be used solely for personal and non-commercial purposes. Any other use requires Munich Re's prior written approval.

Munich Re has used its discretion, best judgement and every reasonable effort in compiling the information and components contained in this presentation. It may not be held liable, however, for the completeness, correctness, topicality and technical accuracy of any information contained herein. Munich Re assumes no liability with regard to updating the information or other content provided in this presentation or to adapting this to conform with future events or developments.