

# Cyber/Privacy

## Cyber/Privacy Insurance



Presented by Matt Prevost  
Product Manager, PHL



PHILADELPHIA INSURANCE COMPANIES

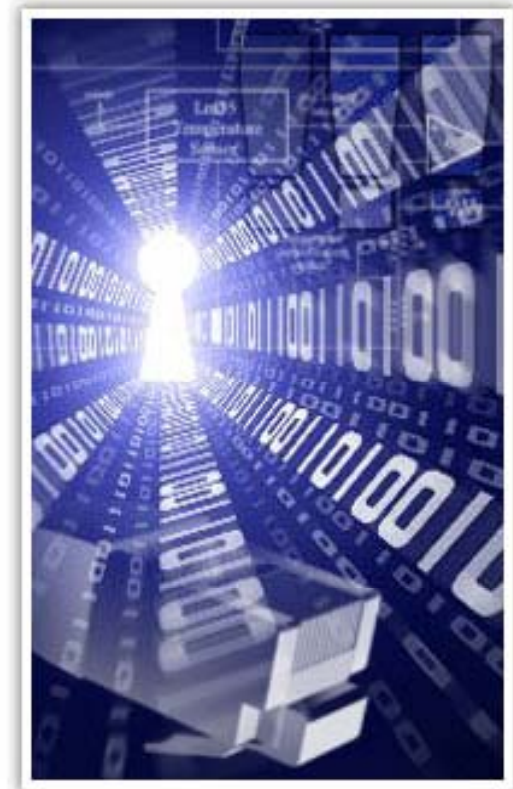
A Member of the Tokio Marine Group

*Focus on the things that matter.  
We'll handle the risk.*

# Cyber/Privacy

## Cyber/Privacy Insurance: Objectives

- Recent breaches/cyber events
- Cyber Liability perils & coverage
- Cyber insurance marketplace
- Privacy trends and future of this ever-changing coverage/exposure



PHILADELPHIA INSURANCE COMPANIES

A Member of the Tokio Marine Group

*Focus on the things that matter.  
We'll handle the risk.*

# Cyber/Privacy Insurance

What does the term “cyber” mean?

Refers to the use of computers, internet, computer networks, and electronic information databases



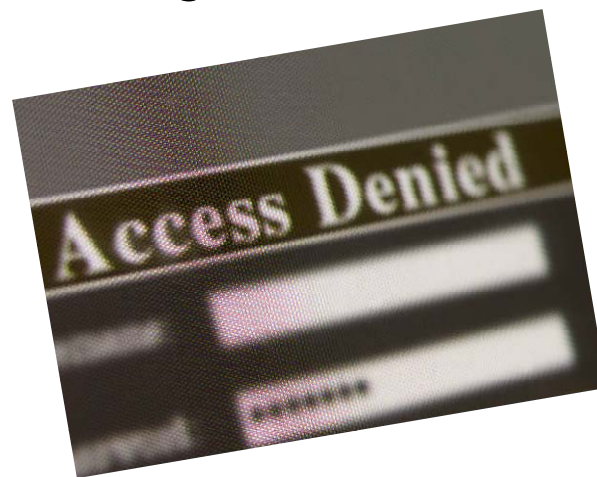
PHILADELPHIA INSURANCE COMPANIES

A Member of the Tokio Marine Group

*Focus on the things that matter.  
We'll handle the risk.*

## What creates cyber risk?

- internet connectivity
- e-commerce
- business websites and internet advertising
- customer forums and support/message boards
- credit card processing/online payment
- data storage, ISP, website design
- providing media content
- paper documents



# Cyber/Privacy Insurance

What clients don't have any exposure?



## Recent Cyber Events / Privacy Breaches

Family Planning Council in Philadelphia: computer storage device containing the personal and medical records of approximately 70,000 patients was stolen in December and remains missing. Philadelphia Inquirer, April 9 2011

Gucci: disgruntled former employee deleted servers, shut down a storage network and deleted a disk containing the corporate mailboxes from an email server. Estimated at \$200,000 in damages MSNBC.com April 5 2011

Briar Group: restaurant group(Ned Devines, Green Briar, Lenox) paid \$110,000 to resolve allegations by the MA attorney General over malware that was installed on their POS system for 9 months. Boston Globe March; Settled April 2011

BP: employee lost laptop containing the personal data of 13,000 Louisiana residents who filed compensation claims after the Gulf oil spill. Information was not encrypted. Nearly a month elapsed before BP notified. Notification was sent to 13,000 people. March 29, 2011: EVERY NEWS ORGANIZATION IN THE USA

## 1<sup>st</sup> Party perils

- Data storage (loss or corrupted)
- Business interruptions (DoS, system failure)
- Fraud & theft (ee theft, computer fraud)
- Extortion (former ee's, rogue ee, criminal extortion)
- Crisis Management (costs to notify, investigate, if theft monitoring)



## 3<sup>rd</sup> Party perils

- Intellectual property: trademarks, trade secrets, patents, copyright infringement
- Privacy & customer data: data theft, security breach, notification requirements
- Errors and omissions: negligence & evolving standards
- Defamation: global, email, site, etc.
- Malicious code: transmission of viruses and/or BOTNET attacks



## Why do Cyber Liability Policies Exist?

A lack of affirmative coverage for these perils in “other” liability policies:

- Comprehensive GL (CGL): electronic data?
- Commercial Crime(Intangible assets)
- Kidnap & ransom, E&O and D&O exclusions

## Underwriting for Cyber Insurance

### Common carriers:

- Primary up to \$20M+ Limit of Liability
- Capacity for individual risks can exceed \$100M

### Most Active Markets:

Ace	CNA	Philadelphia
Arch	Chubb	Safeonline
AWAC	Endurance	Travelers
AxisPro	Hartford	ThinkRisk(GA)
Beazley	Hiscox (Lloyds)	XL
CFC(ClickforCover)	USLI	Zurich
Chartis	Kiln (Lloyds)	Brit(Lloyds)

## Typical Insuring Agreements for Cyber Liability

### Third party liabilities:

- Technology E&O
- Employee Privacy
- Intellectual Property(electronic media)
- Network/Privacy Liability
- Denial of Service
- Transmission of malicious code

### First party losses:

- Unauthorized access
- Cyber extortion and cyber terrorism
- Unauthorized use
- Loss of digital assets
- Business interruption(non CGL)
- Security event costs

## Underwriting for Cyber/privacy Insurance

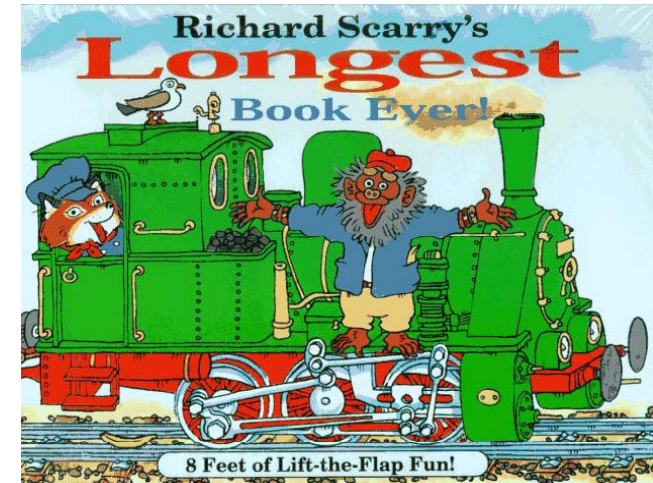
### **Underwriting standards / requirements:**

- Revenue/assets
- Security(audits)
- Other factors, to include:
  - Loss history
  - Years in business
  - Location(most active cities)
  - Clients
  - Website review
  - Privacy
  - Subcontractors
  - Contracts
  - Employees
  - Loss assessments

## Why are the 1<sup>st</sup>/3<sup>rd</sup> party applications so long?

### Carrier and length of application

- Chubb Cyber Security: 6 pages
- Philadelphia Cyber Liability: 8 pages
- C.N.A. Net360: 8 pages
- Hiscox TMT Privacy: 5 pages
- ACE Privacy Protection: 13 pages
- ThinkRisk Converging Risk: 9 pages
- Chartis: 8 pages
- SafeOnline Safe Enterprise(AceGlobal Markets): 5 pages
- CFC Underwriting: 8 pages



\*All information obtained from online public websites. Potentially changes according to the risk.

## Regulatory Environment: Who/what regulates the cyber world?

- Federal Trade Commission Act
- Fair and Accurate Credit Transaction Act, 2003
- Gramm-Leach-Bliley Financial Services Modernization Act, 1999
- HIPAA (Health Insurance Portability and Accountability Act), 1996
- Sarbanes-Oxley Act, 2002
- Digital Millennium Copyright Act, 2000
- State Privacy Breach Legislation
- World Intellectual Property Organization Copyright Treaty, 1996
- Lanham Act, 1946
- Data Protection Directive, 1998
- China?

## Regulation specific to Pennsylvania...

Pennsylvania Law & Effective Date: 73 PA. Cons. Stat. 2302(6/22/2006)

<http://government.westlaw.com/linkedslice/default.asp?SP=pac-1000>

- Triggering event: unauthorized access & Acquisition of computerized data that *materially* compromises security or confidentiality of PERSONAL INFORMATION in database and causes or could be reasonably believed to cause loss or injury.
- Timing of notification: “without reasonable delay”
- Civil or criminal penalties: yes(insurability? PA goes in line with punitive damages-directly assessed not insurable; vicariously assessed are).
- Exceptions: criminal investigation or publicly available information
- If 1,000 or more individuals effected, notification of Consumer Reporting Agencies is mandatory

## Handling Cyber Insurance Claims

1. Claim is reported
2. Claim is evaluated
3. Counsel selected. Claim investigated & strategies for litigation or settlement are evaluated.
4. *Claim resolved through settlement/litigation*

### **Unique to Cyber...**

- Study allegations to determine 1<sup>st</sup> party or 3<sup>rd</sup> party
- Immediate response is often necessary
- Damage & loss analysis involves specialized experts & counsel
- Unfamiliar case law.
- Valuation of business loss is complicated in cyber situations
- Other policy forms
- Need for specialists/vendors
- Post-incident requirements(PR, notification required, etc)

## How much do these cost an Insured?

### Costs of a Breach\*

- \$204 average cost per record(worldwide average is 142)
- \$6.75mm average cost per breach.

Source: \* Ponemon Institute 2010: Five Countries: Cost of Data Breach, Sponsored by PGP Corporation  
AVERAGE AND PER CAPITA COST SUMMARY IN UNITED STATES:

US Dollars	Detection & escalation	Notification	Ex-post response	Lost business	Total
US 2009	264,280	500,321	1,514,819	4,472,030	6,751,451

US Dollars	Detection & escalation	Notification	Ex-post response	Lost business	Total
US 2009	8	15	46	135	204

## Emerging privacy risks

- \*85% of U.S. organizations experienced at least one security breach in 2009
- \*497 million records containing PII were breached in the US from 2005-2009
- Organized criminal groups responsible for 85% of all stolen data in 2009
- Defamation: global, email, site, etc.
- Annual hacker / security expert DEFCON

➤ \*Ponemon Institute annual study

## Best Practices In Cyber Risk\* NetDiligence, Mark Greisiger

1. Vigilant employees: security mentality
2. Prepared internal security and privacy teams
3. senior management(budget is important)
4. network asset policies
5. legal vetting process for contracts
6. system change and patch management
7. network priveleges
8. emergency response and business continuity plans
9. baseline controls: firewall, acces controls, anti-virus, event/security logs, backup data, encryption
10. redundancy/mirror systems

## Top 10 Trends for 2011?

- More small scale data breaches in news
- “low-tech” theft will increase
- Lost devices will continue to dominate
- Data minimization will increasingly be seen as essential
- Increased exchange and collaboration will increase risk
- More social networking policies implemented
- Data encryption = golden ticket
- Business associates
- Privacy awareness training
- Overarching federal law?

\*Kroll Fraud Solutions, Top Ten Data Trends for 2011



## Cyber / Privacy Breaches

“We keep seeing these breaches but we don’t see the call to arms... They’re (companies) not taking care with that data. If you’re going to earn a profit on it, you need to protect it.”

Adrian Lane, CTO of IPLocks in response to his company’s estimation that the TJ Maxx breach will cost them \$4.5 billion. 

PHLY



## Q&A/Lunch



PHILADELPHIA INSURANCE COMPANIES

A Member of the Tokio Marine Group

Focus on the things that matter.  
*We'll handle the risk.*