WELCOME!

CIPR Spring Event:
Insuring Cyber Liability Risk

NAIC Insurance Regulator Professional Designated Program

- This is an NAIC Insurance Regulator Professional Designated program eligible for 4 hours of continuing professional development credit.

- To receive credit, you will need to write down the codes provided periodically throughout the program and provide them in a survey that will be subsequently sent by the NAIC Education and Training Department.

- This survey will be sent to the e-mail you provided during your CIPR event registration.
Following the cyber event, attendees will be able to:

• Describe how cyber risk has evolved and why it is important for businesses to manage and insure against risk of loss from cyber exposures.
• Describe the types of cyber incursions hackers could deliver to business records and web sites.
• Identify the risk management approaches one needs to take to address potential cyber risks.
• Describe recent legal trends affecting business records, web sites and social media.
• State the reasons why an insurer might choose not to insure a business for its cyber risks.
• Identify the elements of the NIST Cybersecurity Framework and describe why it is important for U.S. businesses.
• Describe federal regulatory initiatives related to managing cyber risk.

Introductory Comments
Data Security and Cyber-Liability Issues: The Legal Landscape

Jeremiah Posedel, CIPP/US
Intellectual Property Practice Group
Drinker Biddle & Reath LLP

U.S. Privacy Laws
A Patchwork of State and Federal Laws and Regulations
U.S. Privacy Laws

Some Types of Data At Issue

- Consumer Data
  - Names, Addresses
  - Credit Card Information
  - Financial History
  - Health Information
- Human Resource Records
  - Compensation
  - Social Security Numbers
  - Health Records
- Financial Data
  - Sales Figures
  - Purchasing Costs
  - Inventory Levels
  - Related Data Tracked Into Financial Reports

State Notification Statutes

- 46 of 50 states have adopted some form of security and data breach notification laws – most are similar with slight variation
  - Not Alabama, Kentucky, New Mexico, South Dakota

- All require prompt notification, and some establish penalties and rights of action.

- Statutes typically define “data breach,” the types of protected information, and some set thresholds for the notice requirement, i.e., a reasonable basis to believe the breach will result in harm.
U.S. Privacy Laws

State Statutes

- **Unfair and Deceptive Trade Practices Act**

  - Some variation of this type of consumer protection statute has been enacted by states.

  - Typically enforced by the state’s Attorney General.

Federal Statutes: A “Sectoral” Approach

- Health Care Industry: Health Insurance Portability and Accountability Act (HIPAA) (45 C.F.R. § 160, *et seq.*)
  
  - Applies to healthcare providers and insurers
  - Privacy requirement
  - Security requirement
  - Notice requirement
U.S. Privacy Laws

Federal Statutes: A “Sectoral” Approach

- Financial Industry: Financial Services Modernization Act, a/k/a the Gramm-Leach-Bliley Act (GLBA)
  - Applies to financial institutions
  - Imposes security controls
  - Requires notification

- Sarbanes-Oxley Act (“SarBox”)
  - Applies to U.S. publicly traded companies
  - Section 302
    - Imposes “internal procedures” to ensure accurate financial disclosures
    - Signing officers must certify effectiveness of control procedures and that they have been evaluated within 90 days prior to report
    - External auditors must issue opinion as to whether effective control procedures have been implemented
  - Penalties
    - Civil – same as violations of SEC Act
    - Criminal – up to $1M in fines/10 years in prison
U.S. Privacy Laws

Federal Statutes: A “Sectoral” Approach

• Sarbanes-Oxley Act
  ➢ **Section 404** -- Applies to U.S. publicly traded companies
    ➢ Requires generation of an “internal control report” as part of each report filed with SEC
    ➢ Report must contain assessment of control procedures as of most recent fiscal year
    ➢ Wide discretion to management
    ➢ Management must be knowledgeable about the design and operating effectiveness of the IT control procedures, understand data flows so as to understand points of risk, perform fraud risk assessments, scale any assessments based on the size and complexity of the company

Ramifications as to data security??
Questions as to System Security
Undermine certifications of officers
Undermine reliability of financial reports

Same Issues – Private Companies
Questionable Data Security Systems Undermine Reliability of Financial Reports
“Garbage-In-Garbage-Out”
Same Results w/o Federal Overtones
U.S. Privacy Laws

Federal Statutes: A “Sectoral” Approach

- Others (TCA, COPPA, FACTA, FCRA, etc.)

The Push for More Overarching Legislation

- CISPA – Cyber Intelligence Sharing and Protection Act – proposed legislation
- Executive Order 13636 – February 2013
  - Improving Critical Infrastructure Cybersecurity
- Preliminary Cybersecurity Framework – October 2013 (NIST)
- Cybersecurity Framework – February 2014 (NIST)
Fallout From Data Breaches

More Fallout...

Federal Regulatory Agencies

- **Federal Trade Commission (FTC)**
  - *In re TJX Cos., Inc.*, FTC File No. 072-3055 (requiring TJX to implement a comprehensive security program to protect personally identifiable information)

- **Consumer Financial Protection Bureau (CFPB)**

- **Federal Communications Commission (FCC)**

- **Department of Health and Human Services (HHS)**
Still More Fallout . . .

Non-Governmental Regulatory Action

- Financial Industry Regulatory Authority (FINRA)
- Payment Card Industry Council
  - Designed to establish common security guidelines
  - PCI - DSS

Civil Exposure -- Data Breaches

Civil Lawsuits

- State Attorneys General
- Lawsuits by consumers, businesses, banks, or other private entities affected by breach
Civil Fallout (cont’d)

Civil Lawsuits

- Usually Large Numbers Of Plaintiffs
  - Class Actions
    - Reilly v. Ceridian Corp., 66 F.3d 38 (3d Cir. 2011) (plaintiffs sued on behalf of “customers whose sensitive information was stored on the stolen laptops and a subclass of individuals whose identities have been stolen since the laptop theft”)
    - Zurich Amer. Ins. Co. v. Sony Corp. of Amer., et al., Index No. 651982/2011, Supreme Court of New York, New York County (Over 65 class actions filed nationwide implicating over 70 million subscribers)

Civil Action Considerations

Civil Lawsuits

- Standing
  “The complainant must allege an injury to himself that is ‘distinct and palpable,’ as distinguished from merely ‘abstract,’ and the alleged harm must be actual or imminent, not ‘conjectural’ or ‘hypothetical.’”

Civil Action Considerations

Civil Lawsuits

Standing

• Cases continue to be dismissed for lack of standing.

No Standing

• Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 8 (D.D.C. 2007)

However, trend among appellate courts towards finding standing, particularly where stolen data is actually misused or hackers were sophisticated, indicating increased risk of harm.

Standing

• Resnick v. AvMed, Inc., 693 F.3d 1317, 1324 (11th Cir. 2012)
• Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010)
• Ruiz v. Gap, Inc., 380 F. App’x 689, 691 (9th Cir. 2010)
• Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 634 (7th Cir. 2007)
• Lambert v. Hartman, 517 F.3d 433, 438 (6th Cir. 2008)
Civil Action Considerations

Civil Lawsuits

• Causes of Action

  • Significant issue regarding whether there is cognizable injury, risk of harm, or reasonably foreseeable damage


Causes of Action

• Negligence
• Breach of Contract
• Unjust Enrichment
• Negligent Misrepresentation
• Statutory

Civil Action – Legal Theories

Civil Lawsuits

• Requirements:

  (1) the existence of a duty to exercise due care, (2) breach of that duty, (3) causation, and (4) damages. Ruiz v. Gap, Inc., 380 F. App’x 689, 691 (9th Cir. 2010)

• Economic Loss Doctrine

  “Massachusetts, which is not alone, holds that purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage.” In re TJX Companies Retail Sec. Breach Litig., 564 F.3d 489, 498 (1st Cir. 2009); see also Sovereign Bank v. BJ’s Wholesale Club, Inc., 533 F.3d 162, 175 (3d Cir. 2008)
Civil Action – Legal Theories

Civil Lawsuits

- Causation
  - Did the defendant’s alleged harm cause plaintiff’s alleged damages?
  - Did the failure to secure information cause the loss/identify theft?
  - Nexus between the breach and the loss/identity theft – beyond time and sequence. (Resnick: sensitive info on stolen laptops was same info used to steal plaintiff’s identity.)

Causes of Action

- Negligence
  - Breach of Contract
  - Unjust Enrichment
  - Negligent Misrepresentation
  - Statutory

Hypothetical Damages

Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 639 (7th Cir. 2007) - “Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.”

“Real” Damages

Anderson v. Hannaford Bros. Co., 659 F.3d 151, 164, 167 (1st Cir. 2011) – “The data was used to run up thousands of improper charges across the globe to the customers’ accounts. The card owners were not merely exposed to a hypothetical risk, but to a real risk of misuse . . . Plaintiffs’ claims for identity theft insurance and replacement card fees involve actual financial losses from credit and debit card misuse.”
Civil Action – Legal Theories

Civil Lawsuits

• Requirements
Requires (1) a contract between the plaintiff and the defendant; (2) rights of the plaintiff and obligations of the defendant under the contract; (3) breach of the contract by the defendant; and (4) damages suffered by the plaintiff. Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1055 (E.D. Mo. 2009)

• Implied Contract
“[A] jury could reasonably find an implied contract between Hannaford and its customers that Hannaford would not use the credit card data for other people’s purchases, would not sell the data to others, and would take reasonable measures to protect the information.” Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011)

Causes of Action

- Negligence
- Breach of Contract
- Unjust Enrichment
- Negligent Misrepresentation
- Statutory

Civil Lawsuits

• Requirements
1) the plaintiff conferred a benefit on the defendant; 2) the defendant has knowledge of the benefit; 3) the defendant accepted or retained the benefit conferred; and 4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying fair value for it. Resnick v. AvMed, Inc., 693 F.3d 1317, 1328 (11th Cir. 2012)

• Unjust Enrichment Permitted
Plaintiffs claimed that their premium payments were partially in exchange for keeping their information secure, and that defendant should not be permitted to retain the money because it failed to protect plaintiffs’ information. The Eleventh Circuit permitted the claim to proceed. Resnick, at 1328

Causes of Action

- Negligence
- Breach of Contract
- Unjust Enrichment
- Negligent Misrepresentation
- Statutory
Civil Action – Legal Theories

Civil Lawsuits

• Requirements

“One who . . . in any [] transaction in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.” In re TJX Companies Retail Sec. Breach Litig., 564 F.3d 489, 494 (1st Cir. 2009)

• Misrepresentation Claim (Barely) Permitted:

Plaintiffs alleged that doing business as a credit card company misrepresented that the defendant complied with security requirements; the court was skeptical, but ultimate found that claim “survives, but on life support.” In re TJX, at 495

Causes of Action

• Negligence
• Breach of Contract
• Unjust Enrichment
• Statutory

Civil Action – Legal Theories

Civil Lawsuits – Where are the Courts going…?

• Resnick v. AvMed (Feb. 2014)

- Negligence, Breach of Contract & Unjust Enrichment claims survive MTD.
- Court approved $3 million dollar settlement.
- Settlement Terms:
  • Individuals on laptops, but no identity theft = $10 for each year paid for coverage (max $30). Intended to compensate for premiums paid relating to security.
  • Actual losses from ID theft “more likely than not” stemming from breach.
  • Internal policy/training requirements.

Causes of Action

• Negligence
• Breach of Contract
• Unjust Enrichment
• Negligent Misrepresentation
• Statutory
Civil Action – Legal Theories

Civil Lawsuits

- Any number of state or federal statutes may be applicable in every case.

Causes of Action

- Negligence
- Breach of Contract
- Unjust Enrichment
- Negligent Misrepresentation

Statutory

Questions?
### History of Risk Management

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000 B.C.</td>
<td>Chinese merchants disperse shipments so as to minimize the risk of total loss.</td>
</tr>
<tr>
<td>1790 B.C.</td>
<td>Code of Hammurabi legalizes practice of canceling &quot;loans&quot; if caravan was robbed.</td>
</tr>
<tr>
<td>916 B.C.</td>
<td>Rhodes instituted &quot;the general average&quot;—a merchant would be compensated by pro rata contribution of all merchants with cargo on a ship, if his goods were thrown overboard.</td>
</tr>
<tr>
<td>1255 A.D.</td>
<td>Venice pooled premiums to pay for loss due to piracy, spoilage, or pillage.</td>
</tr>
<tr>
<td>1688 A.D.</td>
<td>Edward Lloyd opens a coffeehouse in London</td>
</tr>
</tbody>
</table>
What are Cyber Risks?

If a company uses technology in its operations or handles/collects/stores confidential information—it’s got Cyber risk

- Legal liability to others for computer security breaches
- Legal liability to others for privacy breaches of confidential information
- Regulatory actions, fines and scrutiny
- Cyber-extortion
- Cyber-terrorism
- Loss or damage to data / information
- Loss of revenue due to a computer attack
- Extra expense to recover / respond to a computer attack
- Loss or damage to reputation

Supply Chain Disruptions

A cyber event could disrupt the supply chain & cause damage

- Unplanned outages of IT/telecoms is the most significant cause of supply-chain disruption, outpacing adverse weather, which placed second.¹

Some possible scenarios² …

- A virus infecting the systems of a key supplier destroys essential records, forcing the supplier to shut down systems for several days. Once systems are restored, customers must resubmit their orders, causing further delays.
- An attack on a large commodities exchange interrupts the flow of essential materials resulting in price volatility in markets.
- A malicious attack on a shipper disrupts freight management and logistic systems, resulting in delays in shipments.

¹ Business Continuity Institute’s 2013 Supply Chain Resilience Survey
² Managing Cyber Supply Chain Risks (Advisen May 2013)
Data Privacy and Network Security: A Multi-Threat Environment

**Technology**
- Viruses, SQL Injections, DDoS attacks, etc.
- Structural vulnerability
- Social Media/Networking
- Phishing

**Internal**
- Rogue employees
- Careless staff

**External**
- Business Associates
- Vendors/Suppliers
- Foreign and domestic organized crime
- Hackers/Hacktivists

**Regulatory**
- HHS, HIPAA & HIPAA HITECH
- Identity Red Flags
- SEC, FTC, state attorney generals
- 47 State Breach notification laws
- DHS/NIST developing Cyber Framework
- Foreign Laws: Canada, South Korea, Spain
- EU General Data Protection Regulation

---

What Are the Gaps in Traditional Policies?

Traditional insurance does not respond to all cyber liability.

- **Errors and Omissions (E&O):** Even broadly worded E&O policies remain tied to “professional services” and often further tied to a requirement that there be an act of negligence.

- **Commercial General Liability (CGL):** CGL covers only bodily and tangible property—Advertising Injury / Personal Injury (AI/PI) section has potential exclusions/limitations in the area of web advertising.

- **Property:** Courts have consistently held that data isn’t “property”—“direct physical loss” requirement not satisfied.

- **Crime:** Requires intent and only covers money, securities, and tangible property.

- **Kidnap and Ransom (K&R):** No coverage without amendment for “cyber-extortion.”
Cyber Coverage Overview

- **Network Security Liability**: liability to a third party as a result of a failure of your network security to protect against destruction, deletion, or corruption of a third party's electronic data, denial of service attacks against internet sites or computers; or transmission of viruses to third party computers and systems.

- **Privacy Liability**: liability to a third party as a result of the disclosure of confidential information collected or handled by you or under your care, custody or control. Includes coverage for your vicarious liability where a vendor loses information you had entrusted to them in the normal course of your business.

- **Regulatory Investigation Defense**: coverage for legal expenses associated with representation in connection with a regulatory investigation, including indemnification of fines & penalties where insurable.

- **Crisis Management and Event Response Expenses**: expenses incurred in responding to a data breach event, including retaining forensic investigator, crisis management firm and law firm. Includes expenses to comply with privacy regulations, such as communication to impacted individuals and appropriate remedial offerings like credit monitoring or identity theft insurance.

- **Cyber Extortion**: ransom &/or investigative expenses associated with a threat directed at you that would cause an otherwise covered event or loss.

- **Network Business Interruption**: reimbursement of your loss of income and / or extra expense resulting from an interruption or suspension of computer systems due to a failure of technology. Includes coverage for dependent business interruption.

- **Data asset protection**: recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., software applications) that are corrupted or destroyed by a computer attack.

NOTE: Some Carriers offer elements of Risk Mitigation and Loss Prevention services, like the Crisis Management & Event Response Expenses as a service bundled with the insurance coverage but not eroding the policy’s limits.

---

Privacy Liability

Why is it Different From Cyber Liability?

- **Breach of privacy:**
  - Disclosure of confidential information:
    - Personal
    - Commercial
  - Cause doesn’t matter:
    - Negligence
    - Intentional acts
    - Computers
    - Vendors
    - Dumpsters
    - Phishing
    - Employees

- **Damages / covered loss:**
  - Legal liability
  - Defense and claims expenses
  - Regulatory defense costs
    - Fines & Penalties
  - Vicarious liability when control of information is outsourced

- **Crisis coverage:**
  - Credit remediation, credit monitoring, and ID Theft investigation
  - Forensic expenses
  - Cover for crisis and public relations expenses
  - Cover for notification costs
**Where Risk Management meets Risk Transfer**

- Placement of coverage is the last step in the process
- Insurance is never a valid alternative to good risk management
- However, technology is not a "silver bullet" that will defend against all risks
- “Best Practices” approach to the privacy and cyber risks combines elements of:
  - **Assessment**;
  - Remediation;
  - Prevention;
  - Education; and
  - **Risk transfer**.

---

**The Path to Coverage**

- **Privacy and Information Security Assessment.** Helps your company evaluate internal policies and procedures related to human, physical, and network security, privacy, and breach preparedness
- **Risk Mapping:** Identify potential exposure —this includes a scorecard, a gap analysis of your breach response policies and procedures, and a risk map identifying and evaluating both the severity and probability of key privacy and information security risks.
- **Benchmarking & Modeling:** Going beyond simple matching you against what your peers do, Adds a layer of benchmarking that details the costs and expenses associated with likely risk scenarios, including an analysis of a catastrophic privacy and information security event
- **Coverage gap analysis:** Review your current insurance policies to determine what coverage may be already respond to claims and losses in the event of network disruption, breach of privacy, or loss of confidential information.
This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are intended solely for the entity identified as the recipient herein (“you”). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.
Cyber Insurance: Barriers and The Issue of Setting Premiums in Context

Professor Lance J. Hoffman
lanceh@gwu.edu 202 994-4955
The George Washington University
NAIC Orlando
March 28, 2014

A word about CSPRI

• Multi-disciplinary
• Research, education, platform development and management
• Network of researchers within GWU (30+)
• Impartial engineering, social science, and policy experts
Why I am Here

Eric Nordman at the National Association of Insurance Commissioners’ Center for Insurance and Policy Research contributed his insights to this report in an interview with one of the authors.

We thank you by now sharing the results of the report.

It is available online at
http://is.gd/cyber_ins

Toregas/Zahn paper

• Reviewed papers (previous work) defining cyber insurance market
• (Re)stated barriers hindering market development
• Presented dialogue highlights with market actors
• Suggested collaborative research agenda that would move world closer to a viable market for cyber insurance
  – Policy, Management and Technology strategies
  – Information security metrics
  – Risk management in an expanded Internet framework
## Insurance for Cyber Attacks: The Issue of Setting Premiums in Context

- Over 17 million personal records breached in 2012
- Average financial impact of a cyber attack is $9.4M
- Many companies exhibit unwillingness or inability to invest in adequate IT security
- Businesses store massive amounts of data electronically, often outsourcing our using third-party software
- Many technologies exist

---


---

## Arguments for Cyberinsurance
- Transfers risk
- *Insurers can incentivize investments in cybersecurity*
- As demand spreads, best practices spread throughout the economy

## Arguments against Cyberinsurance
- Risks are not quantifiable and thus not insurable
- It’s an easy out that doesn’t fix security flaws in systems

---

The Issue of Setting Premiums in Context: Market Appears to be Growing

Insurance for Cyber Attacks: Challenges Like Those in Other New Markets

• “Traditional” insurance market challenges
  – Information asymmetry
  – Moral hazard
  – Adverse selection

• Cyberinsurance challenges
  – Legal Framework
  – Conceptual Issues
  – Setting Premiums

Insurance for Cyber Attacks: Cyberinsurance Challenges

- Legal Framework
  - Uncertainty about liability
  - Spotty coverage and insurance loopholes
  - Lack of standards or “bad” standards
- Conceptual Issues
  - Quantification of risks and costs
  - Cyber risk not seen as a business problem (or underestimated)
  - Correlated, interrelated, and global risks
  - Lack of re-insurance
- Setting Premiums
  - Lack of actuarial data
  - Uncertainty about normative standards
  - Premiums Too High


My thoughts from reading Toregas/Zahn paper

- Look back to history with insurance driving change in various verticals
- Could similar impact be in the future with cybersecurity?
  - Currently many vendors say “Choose our product to have better protection”
  - With the right data elicited from networks and organizations and careful studies of it, insurance rates can be set more rationally, without companies tempted to buy the latest hot (but unproven) product but rather driven by insurance industry to better risk-related decisions
- Is cybersecurity’s border-crossing nature an impediment or an opportunity for cyber risk insurance?
Is There a Third Way Beyond Actuarial and Predictive Approaches?

- Rates based on actuarial or predictive approach
  - Actuarial difficult, given reluctance to share data (or to even identify or measure losses)
  - Predictive difficult, given current state of cyber security understanding as a system
- Is there more to consider?

More Risk-Based Methods Adopted in DoD

DOD replaces longstanding information assurance process with NIST’s holistic "built-in, not bolt-on," risk-focused security approach.

- DoD replacing its longstanding DOD Information Assurance Certification and Accreditation Process (DIACAP)
- Adopting instead a risk-focused security approach developed by NIST
- DOD Instruction memo (8510.01), aligns for the first time the standards the Defense Department and civilian agencies use for approved information assurance and risk management controls in IT.
- Shifts from DIACAP compliance, which prescribes a standard set of activities and a management process to certify and accredit DOD information systems before implementation and every three years thereafter
- New approach is more heavily risk-management-focused, including standards for assessment and authorization, risk assessment, risk management, and dynamic continuous monitoring practices.
- The change in policy reflects a “move away from unique DOD standards …”
- “we were concerned we’re driving up our costs by virtue of having companies have to fit our standards as well as to other national standards.”

Many Verticals in the Internet of Things (IoT)
Much Need for Better Design Standards/Guidelines, Metrics, Governance Models

Example Medical Vertical in IoT

http://chipdesignmag.com/display.php?articleId=5323

http://www.flamingosshanghai.com/blog/2012/07/02/the-internet-of-things-the-robopocalypse-starts-with-your-toothbrush/
Software Mistakes Can Generate Significant Liability

- Early example 1985-87 from Medical Vertical
- Therac-25 Radiation Therapy Machine from Atomic Energy of Canada, Ltd. (ACEL)
- Physical fail-safes replaced by software that was not tested adequately.
- 3 or 4 patients died
- Total compensation from settled lawsuits estimated to be over $150M (c. 1989 dollars) = $283 million in 2014

How to Arrive at a (Big Data-defined) price

- Both actuarial and predictive approaches are currently difficult
- Should work with a broad-based group to figure out best (hybrid/other?) approach, BEFORE a possibly underresearched “solution” is imposed, since right now it is not clear what risks the underwriter is actually assuming
- Group participants
  - Insurance Industry
  - Government
  - Academe
  - Law
  - Computer Science
  - Economics
  - Public Policy
- A workshop is a tested solution
  - Low-cost
  - Inclusive
  - Quick turnaround
  - Identifies areas of agreement
  - Identifies hard problems where more research is needed
  - Can prioritize these and even schedule due dates
- Examples of similar work
  - Workshop on Integrating Social Sciences into the Design of Cybersecurity Systems
  - 2013 Cybersecurity SFS Workforce Development Workshop
Example of Similar Platform Building

A First Cut at Applying This to Insurance

Make “Social Science” \(\rightarrow\) “Cyber Insurance” and similar relevant substitutions below.
What we as academics seek in research partners

- Experience in related cybersecurity areas
- Expertise in insurance risk analysis
- Open minds for interdisciplinary research
- Funding to explore new frontiers

Insurance Industry and the Cybersecurity Community

- Insurance (and re-insurance) can benefit from engagement with cyber security research community
  - Technology is important
  - Hardware and software solutions
  - Research labs and commercial product developers can be at the table with users
  - Risk analysis (and model building) is important
- Two areas, so naturally culture, language, and incentives different
- Still, necessary to find common ground to solve the problem
Developing Possible (Risk Analysis, Implementation, Research) Agendas for the Industry

• Industry can set standards, or else:
• Tech firms will build their own devices, with little or no privacy and security built in
• Also, no audit logging will be built in
• But it could be:
  — Just like Black Boxes
Developing Possible (Risk Analysis, Implementation, Research) Agendas for the Industry

- Industry can set standards, or else:
- Tech firms will build their own devices, with little or no privacy and security built in
- Also, no audit logging will be built in
- But it could be:
  - Just like Black Boxes

- Realistic data metrics have to be developed
- We are already at the stage in cybersecurity where we want them and don’t have them. Help us help ourselves (and you).
Suggestions for a Research Agenda

• **Policy**
  
  – Establish a better understanding of CEO attitudes towards cyber risk and preferences towards mitigation strategies by engaging social science, cyber security and finance experts
  
  – Study regional variations in approaches to cyber insurance across the globe and identify common patterns and features
  
  – Investigate differences between insurance and reinsurance regarding national vs. global approaches – US insurer acts on state level but risk to be insured is global – is this a problem? Business model has to take this into account

• **Management**
  
  – Explore feasibility of constructing a causal model of cyber threat/response mechanism at enterprise level
  
  – Develop a “big data” strategy linking actual cyber losses and specific variables under the control of management
  
  – Analyze potential of a global cyber loss data base with proper privacy controls and a business model that would make such a data base viable and sustainable

• **Technology**
  
  – Map cyber risk variations for different technology platforms (both in house and Cloud) and provide insights on IT industry perspectives as these platforms change and become more interlinked
  
  – Review Computer Science curricula and identify courses dealing with technology approaches to cyber risk and risk management as an explicit strategy

• **Additional “Food for thought”**
  
  – Metrics for information security cost
  
  – More descriptive surveys to gather more data
  
  – Further investigate the role of different legal frameworks and regulatory regimes
  
  – Further investigate the impact of technologic characteristics, e.g. should the global nature of the Internet change the way we approach risk management? Does the lack of attribution of cyberattacks increase the risk of insurance fraud? How can insurance companies keep up with fast-paced technological innovation?
  
  – What private and public initiatives could address cyberinsurance market challenges, e.g. the lack of reinsurance?


Thank You!

Professor Lance J. Hoffman

lanceh@gwu.edu  202 994-4955

The George Washington University
A word about CSPRI

- Multi-disciplinary
- Research, platform development and management, education
  - Research
    - Privacy and Civil Liberties Project
    - Internet of Things, Economics, and Privacy
    - Malware Markets
    - International Trade and Malware
  - Platform development and management
    - Secure and Trustworthy Cyberspace Principal Investigator Meeting Program Development
    - Workshop on Integrating Social Sciences into the Design of Cybersecurity Systems
    - National CyberWatch Center
    - 2013 Cybersecurity SFS Workforce Development Workshop
  - Education
    - Scholarship for Service Program
    - Speaker series
    - Sea to Shining Sea Interactive Video Library
    - Teaching Cybersecurity to the Next Generation from Sea to Shining Sea
- Network of researchers within GWU (30+), I3P (25 institutions) beyond from various disciplines
- Impartial engineering, social science, and policy experts

Who was Surveyed?

- To complement the literature review, a handful of experts and professionals were asked to provide input. The information they provided is referenced as Questionnaire. The small sample of eight people included an insurance lawyer, two insurance companies that offer cyberinsurance policies, a commissioner from the National Association of Insurance Commissioners, a representative at the Insurance Services Office, a representative from a defense contractor, a private sector CISO, and an academic. A snowball-sampling was used starting from an initial sample of publicly available contacts. Given resource constraints, the purpose of the sampling was not to be representative, but to get as many different perspectives on the issue as possible within a reasonable time frame.