Modeling Cyber-Insurance
Towards a Unifying Framework

Rainer Böhme*, Galina Schwartz†

* Networking Group, ICSI Berkeley   † EECS, UC Berkeley

Workshop on the Economics of Information Security, Harvard, 8 June 2010
Talks on Cyber-Insurance at WEIS

2002 2003 2004 2005 2006 2007 2008 2009 2010

enthusiasm obstacles
Outline

1. Characteristics of Cyber-Risk

2. Framework Overview

3. Selected Features
   - Network topology
   - Unified approach to interdependent security and correlated risk

4. “Results” and Conclusion
1

Characteristics of Cyber-Risk
What Is Specific to Cyber-Risk?

**success factors of ICT**
- distribution & interconnection
- universality & reuse

**risk properties**
- interdependent security
  - own risk depends on other parties’ actions
- risk propagation & correlation
  - incidents cause further incidents

+ complexity

→ imperfect information

WEIS, Harvard, 8 June 2010
Examples

Conventional risks in the economic insurance literature

*neither interdependence nor correlation*

Airline baggage security

*interdependence, but no correlation*

Natural disasters in the actuarial literature

*spatial correlation, but no interdependence*

Cyber-insurance

*both interdependence and correlation, but never modeled together*
Talks on Cyber-Insurance at WEIS

- interdependent security (IDS)
- correlated risk
- information asymmetries

Enthusiasm and obstacles over time:

- 2002
- 2003
- 2004
- 2005
- 2006
- 2007
- 2008
- 2009
- 2010
Risk Properties in the Cyber-Insurance Literature

- Böhme, 2005
- Böhme & Kataria, 2006
- Bandyopadhyay et al., 2009
- Shetty et al., 2009
- Radosavac et al., 2008
- Ogut et al., 2005
- Hofmann, 2007
- Bolot & Lelarge, 2008
- Lelarge & Bolot, 2009
Framework Overview
Framework

1. Network environment (nodes)

2. Demand side (agents)

3. Supply side (insurers)

- Design
- Utility
- Risk
Framework

1. network environment (nodes)  
   - design
   - utility

2. demand side (agents)

3. supply side (insurers)
   - risk
   - risk
Framework

1. network environment (nodes)
2. demand side (agents)
3. supply side (insurers)
Framework

1. Network environment (nodes)
2. Demand side (agents)
3. Supply side (insurers)
4. Information structure
5. Organizational environment
## Overview of Model Attributes

### 1. network environment
- defense function
- network topology
- risk arrival
- attacker model

### 2. demand side
- node control
- heterogeneity
- agents’ risk aversion
- action space
- time

### 3. supply side
- market structure
- insurers’ risk aversion
- markup
- contract design
- higher-order risk transfer

### 4. information structure
- IA in conventional insurance
- IA specific to cyber-insurance
- timing

### 5. organizational environment
- regulator
- ICT manufacturers
- network intermediaries
- security service providers

WEIS, Harvard, 8 June 2010
Variables of Interest

**Breadth of market**

*Under which conditions will a market for cyber-insurance thrive?*

**Network security**

*Can we expect fewer attacks if cyber-insurance is broadly adopted?*

**Social welfare**

*Will the world be a better place with cyber-risk reallocation?*
Selected Features
Network Topology

Examples

- Ideosyncratic
- Fully connected
- Single-factor model
- Erdoes-Renyi graph

- Hardware failure
- Email spam
- OS vulnerability
- Inter-organizational dependence

→ Comprehensive insurance policies represent bundles of contracts.
Unified Approach to IDS and Correlation

**Defense function** for node $i$:

$$P(L_i = l) = D(l, w_i, s, G, x)$$

- $l$: size of loss (random variable $L_i$)
- $w_i$: initial wealth
- $s$: vector of security investments: $s = s_i \cup s_{j\neq i}$
- $G$: network topology as model of interconnectedness

Simplification: fix $w$ and normalize $l = 1$, then let $p_i$ be the probability of a loss at node $i$ and $X \in \{0, 1\}^n$ be a random vector of realized losses per node.

Proposition: interdependent security and correlated risk can be modeled jointly by making $s$ and realizations $x$ of $X$ parameters of $D$. 
Risk propagation is hard to tract: the modeling requires recursive methods or approximations and it may lead to dynamic equilibria.
“Results” and Conclusion
Dependent Variables
in the Cyber-Insurance Literature

- Social welfare
  - Shetty et al., 2009
- Breadth of market
  - Bandoopadhyay et al., 2009
  - Böhme, 2005
  - Böhme & Kataria, 2006
- Network security
  - Ogut et al., 2005
  - Hofmann, 2007
  - Radosavac et al., 2008
  - Bolot & Lelarge, 2008
  - Lelarge & Bolot, 2009
Discrepancy between Statements and Models

*Cyber-insurers will improve information about security levels;*

… but relevant parameters not included in the model.

*Cyber-insurers will positively affect agents’ decisions in shaping the network environment;*

… but existing models of contracts do not reflect these choices.

*Broad adoption of cyber-insurance will change the market structure and behavior of ICT manufacturers;*

… but never modeled parametrically.
Endogenize!

Future modeling approaches should endogenize key parameters of the network environment, information structure, and organizational environment.

Example:
endogenous network formation to model platform switching dynamics
Framework

1. network environment (nodes)
2. demand side (agents)
3. supply side (insurers)

4. information structure

5. organizational environment
Endogenize!

Future modeling approaches should endogenize key parameters of the network environment, information structure, and organizational environment.

Example:
endogenous network formation to model platform switching dynamics

Policy recommendations need better foundations in analytical models.
Talks on Cyber-Insurance at WEIS

- enthusiasm
- obstacles
Talks on Cyber-Insurance at WEIS

- 2002
- 2003
- 2004
- 2005
- 2006
- 2007
- 2008
- 2009
- 2010

enthusiasm

obstacles
Thank you for your attention.

Rainer Böhme* *, Galina Schwartz†

* Networking Group, ICSI Berkeley † EECS, UC Berkeley

Workshop on the Economics of Information Security, Harvard, 8 June 2010