Managing Cyber-Physical Risks
Review and Directions

Galina Schwartz

University of California, Berkeley

Women's Institute in Summer Enrichment (WISE) 2013

June 25th, 2013

Cyber Risk Today

Cyber-threats

"from being the stuff of action movies ....
to the subject of business executivesÕ discussions"

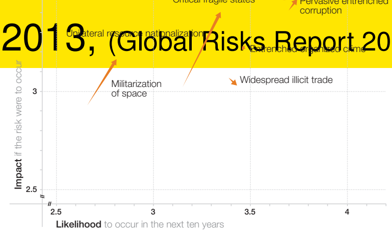
Cyber risk $\neq$ an IT issue

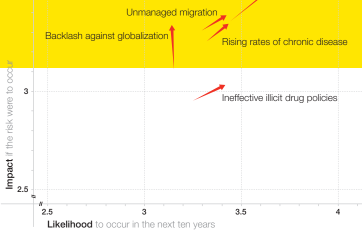
"When you talk to IT people and boards of directors, many of the discussions are about two things: one is that their company has been hit so many times that they feel a need to reconsider their cyber security position, and the other is that cyber risk is no longer just an IT issue – it is a strategic risk management issue."

Erwinn Michel-Kerjan

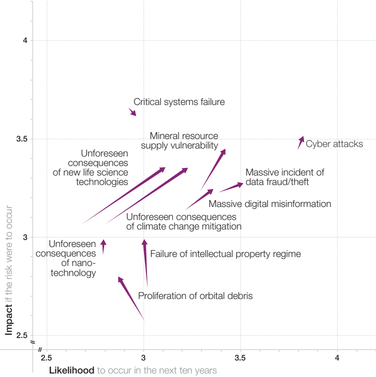
From congressional testimony on Terrorism Risk Insurance Act (TRIA), 2012

2012 to 2013, (Global Risks Report 2013)





Technological



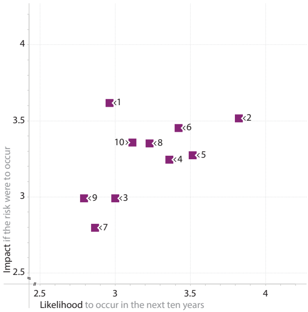
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: World Economic Forum

Technological Risks (Global Risks Report 2013)

7	Unmanaged migration	Mass migration driven by resource scarcity, environmental degradation and lack of opportunity, security or social stability.
8	Unsustainable population growth	Unsustainably low or high population growth rates and sizes, creating intense and rising pressure on resources, public institutions and social stability.
9	Vulnerability to pandemics	Inadequate disease surveillance systems, failed international coordination and the lack of vaccine production capacity.
10	Water supply crises	Decline in the quality and quantity of fresh water combine with increased competition among resource-intensive systems, such as food and energy production.

Technological



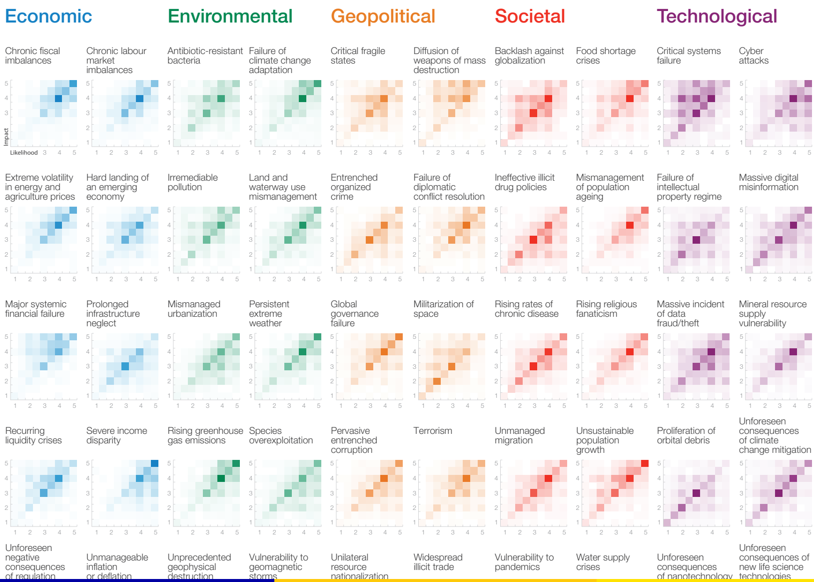
1	Critical systems failure	Single-point system vulnerabilities trigger cascading failure of critical information infrastructure and networks.
2	Cyber attacks	State-sponsored, state-affiliated, criminal or terrorist cyber attacks.
3	Failure of intellectual property regime	The loss of the international intellectual property regime as an effective system for stimulating innovation and investment.
4	Massive digital misinformation	Deliberately provocative, misleading or incomplete information disseminates rapidly and extensively with dangerous consequences.
5	Massive incident of data fraud/theft	Criminal or wrongful exploitation of private data on an unprecedented scale.
6	Mineral resource supply vulnerability	Growing dependence of industries on minerals that are not widely sourced with long extraction-to-market time lag for new sources.
7	Proliferation of orbital debris	Rapidly accumulating debris in high-traffic geocentric orbits jeopardizes critical satellite infrastructure.
8	Unforeseen consequences of climate change mitigation	Attempts at geoengineering or renewable energy development result in new complex challenges.
9	Unforeseen consequences of nanotechnology	The manipulation of matter on an atomic and molecular level raises concerns on nanomaterial toxicity.
10	Unforeseen consequences of new life science technologies	Advances in genetics and synthetic biology produce unintended consequences, mishaps or are used as weapons.

NB: The scatter plots show the average value, across all responses, of the likelihood and impact of the 50 global risks, as measured on the horizontal and vertical axes, respectively.

Source: World Economic Forum

Distribution of Responses (Global Risks Report 2013)

Figure 30: Distribution of Survey Responses



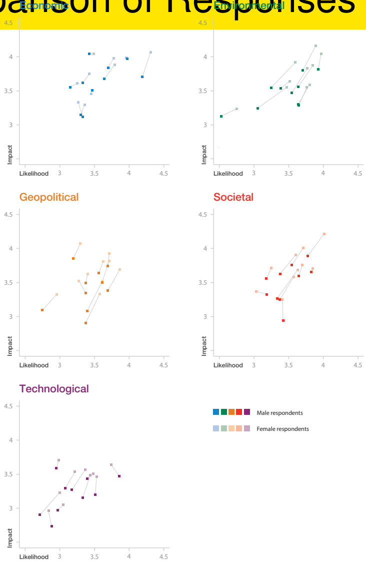
Comparison of Responses (Global Risks Report 2013)

Section 4

Section 5

Section 6

Figure 33: Comparison between Genders

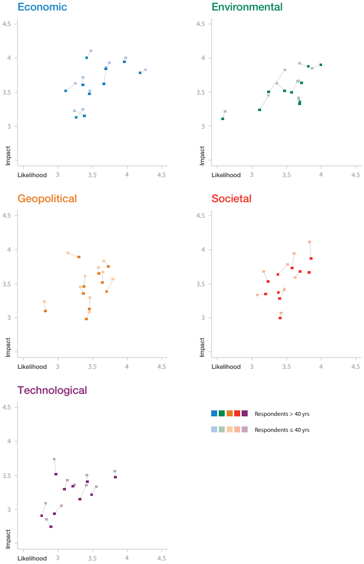


Source: World Economic Forum

xlviii Controlling for other characteristics of the sample, the respective differences would be 0.087 and 0.18 units.

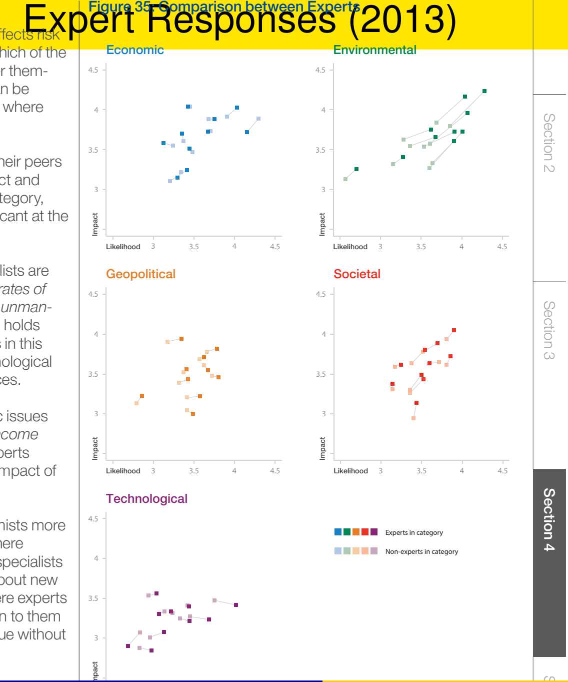
It is interesting that high-level decision-makers tend to be drawn mostly from the group – older males – that the breakdowns by age and gender indicate is least inclined to worry about global risks.

Figure 34: Comparison between Age Groups



Source: World Economic Forum

Expert Responses (2013)



Outline

1. Today
   - Now
   - Public goods and public bads
   - Dangers
2. Tomorrow
   - A roadmap (IMHO)
   - High Hopes
3. CPS resilience: building blocks
4. Economic Incentive (EI) Mechanisms

Security Incentives

Questions

How security decisions are made by corporations, governments, individual users? How much to invest?

Security Decisions: Practices

- 1. to improve security technologically and organizationally
  [invest to reduce security risks]
- 2. to manage residual security risks
  [redistribution, reallocation, hedging]
- Combinations of 1 and 2
  [how to choose between 1 and 2?]

$\Rightarrow$ Micro- perspective dominates

Public goods and externalities: Definitions & Connections

Public Goods

Informal definition: see public goods, wikipedia.
Formally, we define "public good" as Varian (2002), "total effort".
"Total effort" = public good level is a function of total user contributions

Externalities

Formally, *externality* is the effect of some users' action(s) on well-being (utility) of other users, beyond the effects reflected by price changes, see Besanko (2005), Microeconomics, p. 355.

Private optimum $\neq$ Social optimum

Important: for public goods, private and social optima differ! Mathematically, this disparity is the same as the presence of externalities
Externalities $\equiv$ Public goods

Public goods and externalities: Definitions & Connections

Public Goods

Informal definition: see public goods, wikipedia.
Formally, we define "public good" as Varian (2002), "total effort".
"Total effort" = public good level is a function of total user contributions

Externalities

Formally, *externality* is the effect of some users' action(s) on well-being (utility) of other users, beyond the effects reflected by price changes, see Besanko (2005), Microeconomics, p. 355.

Private optimum $\neq$ Social optimum

Important: for public goods, private and social optima differ! Mathematically, this disparity is the same as the presence of externalities
Externalities $\equiv$ Public goods

Public goods and externalities: Definitions & Connections

Public Goods

Informal definition: see public goods, wikipedia.
Formally, we define “public good” as Varian (2002), “total effort”.
“Total effort” = public good level is a function of total user contributions

Externalities

Formally, *externality* is the effect of some users’ action(s) on well-being (utility) of other users, beyond the effects reflected by price changes, see Besanko (2005), Microeconomics, p. 355.

Private optimum $\neq$ Social optimum

Important: for public goods, private and social optima differ! Mathematically, this disparity is the same as the presence of externalities
Externalities $\equiv$ Public goods

Public goods and public bads

Two distinct types: public goods and public bads

(i) goods [*positive* externalities]
(ii) bads [*negative* externalities]

For efficiency one should: *subsidize* public “goods” and *tax* public “bads”

Positive externalities (*“goods”*)

- PBC
- Info / news sharing (web)

Negative externalities (*“bads”*)

- network congestion; highway congestion
- pollution
- reliability of electricity

Public goods and public bads

Two distinct types: public goods and public bads

(i) goods [*positive* externalities]
(ii) bads [*negative* externalities]

For efficiency one should: *subsidize* public "goods" and *tax* public "bads"

Positive externalities (*"goods"*)

PBC
Info / news sharing (web)

Negative externalities (*"bads"*)

network congestion; highway congestion
pollution
reliability of electricity

Modeling vs Reality

Game Theoretic Models vs. Reality

Game theory misfits business realities
Game theorists are [too] smart. A problem?

Complex & Abstract Games

Complex: Games are subtle [hard to popularize]
Abstract: Many constraints & conditions [unrealistic]

Implications

In many cases, results are trivial and/or irrelevant

Outline

Key properties of [macro] security (games)

Network Security: a Global Perspective

1. Info is a public good

   Information Structure ⇔ Technology AND Incentives

   - low costs of information ⇒ local is global
     but "*X*" knows *ABC* does not imply this knowledge is used
     [meager incentives to use information]

2. Security is a public good

   equilibrium incentives: social ≠ individual

3. Marginal vs Aggregate ⇔ Micro vs Macro

   [dangers of partial equilibrium analysis]

   - Player outside option(s)
   - Multiple parties (not two, but very many!)

Thinking Realistically?

Focus: From Micro to Macro

1. Info: Technology vs Incentives
   - Effects of Info
   - How to Improve Info?
2. The disparity of social and private optima
   - Our games alone CANNOT resolve the disparity
   - Formulation and assessment
   - How to: Developing tools to reduce the disparity
     [public policy tools: regulations, rules, laws, trust, reputation, ...]

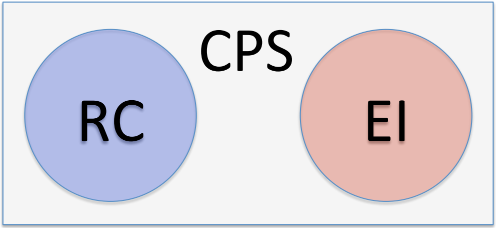
Outline

1. Today
   - Now
   - Public goods and public bads
   - Dangers
2. Tomorrow
   - A roadmap (IMHO)
   - High Hopes
3. CPS resilience: building blocks
4. Economic Incentive (EI) Mechanisms

A dichotomy in CPS

Resilient Control (RC) tools

Primarily driven by the technological developments with a view of distributed sensing of phenomena, change detection and fault diagnosis, and closed-loop control over sensor-actuator networks.



Economic Incentives (EI) tools

Primarily driven by the strategic interactions of human decision makers within systemic societal institutions with a view of aligning individually optimal allocations with socially optimal ones.

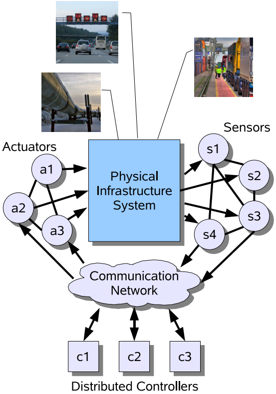
From Past → Into Future

New functionalities

- State awareness
- Real-time closed-loop control
- Demand management
- Incident management

Need for RC + EI integration

1. Off-the-shelf IT devices
   ⇒ software bugs & hardware flaws
2. Open networks
   ⇒ accessible by strategic attackers
3. Multi-party management
   ⇒ incentives for misbehavior
4. Large # of field devices
   ⇒ increased attack surface



Large-scale critical infrastructures are Cyber-Physical Systems (CPS)

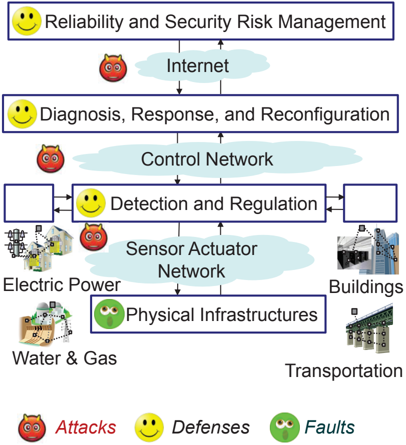
In direction of high-confidence CPS

Theory of robust control

- Assessment, diagnosis, & response
- Stealthy attack diagnosis
- Attack-resilient control

Theory of incentive mechanisms

- Information deficiencies
- Individual vs. social incentives
- Interdependent network risks



Dichotomy of RC and EI is no longer suited for ensuring resilient CPS.

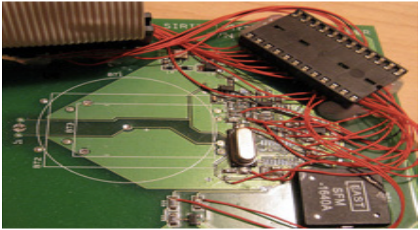
Critical infrastructure domains

CPS Environments	RC	EI
Road traffic operations	Distributed traffic control (metering & control)	Congestion pricing and traveler incentives
Airport and airspace operations	Robust air traffic scheduling and routing	Strategic allocation of airport & airspace resources
Electricity transmission & bulk-power operations	Wide-area monitoring, state estimation, and MPC	Transmission planning & cost allocation
Electricity distribution & demand management	Distributed load control, control of smart appliances	Incentives for peak-shaving & reducing price volatility

Cyber-attacks to transportation infrastructures

Hackers: Road signs near MIT *(2008)*

Insiders: LA traffic control *(2008)*



Hackers: Tolling system*(2008)*

UCSD-UW Demo: Car hacking *(2011)*

Claim #1: Cyber attacks $\neq$ Random faults

Attackers

- Malicious insiders
- Computer hackers
  - cyber criminals, cyber warriors, hacktivists, rogue hackers, spies

Attacker may manipulate CPS data

- Time between telemetry requests can be used for malicious traffic injection
- Both malicious and legitimate traffic can travel through encrypted tunnels

A. Cárdenas, S. Amin, S. Sastry, et al. [ASIACCS]

S. Amin, X. Litrico, S. Sastry, A. Bayen. [HSCC '10]

Claim #2: IT security is necessary but not sufficient

Missing:	• How is data collected by NCS used? • Resilient control & anomaly detection for NCS
System Design	• Least Privilege Principle • Separation of Duty
Software Validation	• Correct implementation of system design • Minimize vulnerabilities and bugs
Network Security	• End-to-end integrity, confidentiality, availability • Network intrusion detection
Device Security	• Trusted Platform Modules (TPM): device integrity

A. Cárdenas, S. Amin, S. Sastry. [HotSec '08]
A. Cárdenas, S. Amin, G. Schwartz. [HiCoNS'12]

Claim #3: CPS operators underinvest in security

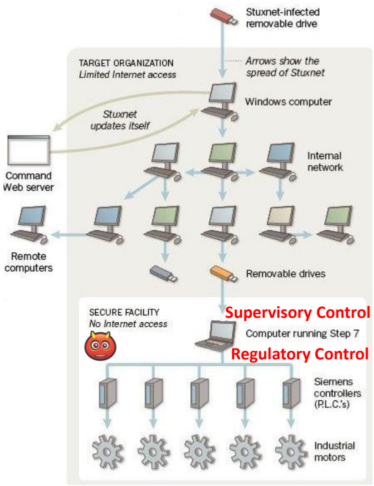
Stuxnet worm ['10-'11]

- Targets SCADA systems
- Four zero-day exploits, windows rootkit, antivirus evasion, p-2-p updates, network infection routines
- Reprograms PLC code
- Information stealing: Duqu ['11-'12]

Network induced risks

- Security is a public good
- Infrastructures are privately managed
- Individual & social incentives differ

S. Amin, G. Schwartz, S. Sastry.
GameSec '10, CDC '11, Automatica



Source: Symantec, NYT

Claim #4: Reliability-Security failures are non-isolable

Hacker Apparently Triggers Illinois Water Pump Burnout

Attack illustrates the extent to which industrial control systems are Internet-connected, yet lack basic password checks or access controls.

By **Mathew J. Schwartz** InformationWeek
November 21, 2011 11:45 AM

Federal authorities are investigating a hack that resulted in the burnout of a water pump at the Curran-Gardner Township Public Water District in Illinois. Located west of Springfield, Ill., the utility serves about 2,200 customers.

A hacker apparently exploited a supervisory control and data acquisition (SCADA) system that managed the water pump and set the pump to continually turn on and off. Only after the pump failed, earlier this month, did plant operators discover that their systems had been exploited, apparently in September. The attack appeared to have been launched from a server based in Russia.

DHS, FBI Dispute Illinois Water Hack

Feds say their preliminary investigation finds no evidence of stolen credentials or foreign attackers.

By **Mathew J. Schwartz** InformationWeek
November 23, 2011 12:41 PM

The Department of Homeland Security and FBI on Tuesday issued a joint statement disputing that an Illinois water utility's industrial control systems were recently hacked.

The DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the FBI cautioned that findings issued by the DHS Illinois State Fusion Center--aka the Illinois State Terrorism and Intelligence Center (STIC)--"were intended to be initial raw reporting and not conclusive in nature."

TJ·maxx
Marshalls.

(click image for larger view)

Slideshow: 10 Massive Security Breaches

G. Schwartz, S. Amin, et al. [Allerton '11], S. Amin, G. Schwartz, S. Sastry. [CDC'11]

Claim #5: Security legislation needs a scientific base

Cybersecurity Act S.2105 *vs.* SECURE IT Act S. 2151

- S.2105 [Lieberman et al.]: DHS to access risks and vulnerabilities to critical infrastructures. Recommends a *regulation* that requires private companies owning designated critical infrastructure to *certify* that their cybersecurity capabilities rise to an appropriate level.
- S. 2151 [McCain et al.]: Federal contractors *required* to inform the government about cyber threats. Provides *liability protections* for the private sector to share cyber threat information through established channels and the Department of Commerce.

Big questions: Regulations? Incentives? Privacy laws?

R. Böhme, G. Schwartz. [WEIS'10]

G. Schwartz, B. Johnson, S. Sastry [Work-in-progress]

Outline

Interdependent security (IDS) & incentives to secure

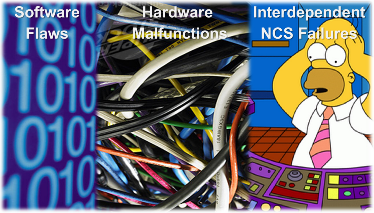
A problem of incentives

Due to presence of network-induced interdependencies, the individually optimal [Nash] security allocations are sub-optimal.

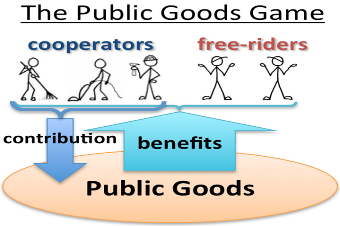
Interdependencies due to

- Network induced risks ⇒ vulnerability to distributed DOS attacks
- Negative externalities
- Goal: Develop mechanisms to reduce CPS incentive sub-optimality

[Amin, Schwartz, Sastry, CDC '11, Automatica]



Courtesy: C. Goldschmidt (Symantec)



Cyber-attacks and privacy threats

Integrity: A1 & A3

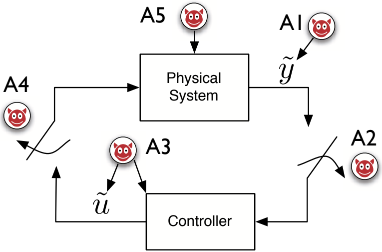
- Deception causes lack of integrity
- Trustworthiness of CPS data

Availability: A2 & A4

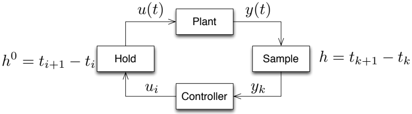
- Denial-of-service (DoS) causes lack of availability
- Accessibility of CPS components

Privacy

- Disaggregate usage data collection causes lack of privacy
- Minimization of privacy-sensitive data

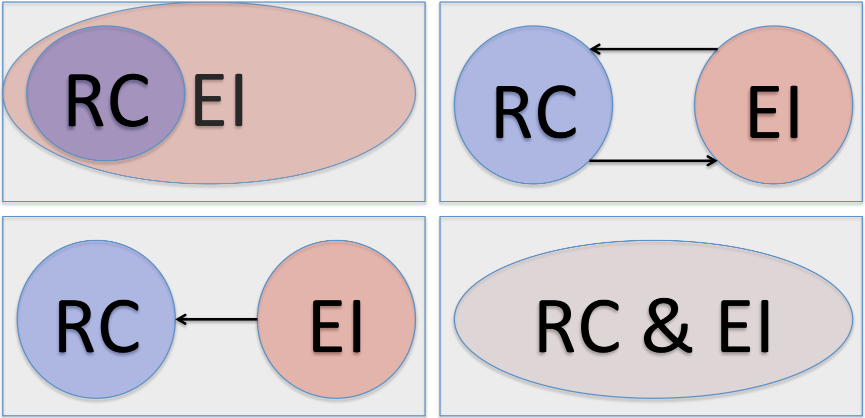


Deception & DoS attacks to CPS



Privacy-preserving sampling of CPS

Looking forward into tomorrow



1. Why cyber-insurance?

Questions

1. Q1 How does cyber-insurance differ from conventional one?
2. Q2 Why should society care of cyber-insurance?
3. Q3 Why should engineers / researchers care of cyber-insurance?

... and Answers

1. A1 As network environments differ from conventional ones, cyber-insurance differs from conventional insurance.
2. A2 Insurance is widely used to manage risks. Obviously, network risks are important: they cause many billions of losses. Thus, cyber-insurance should be used to manage network risks.
3. A3 Network risks importantly depend on the choices of engineers [ex. network structure; security tools employed in it].

2. Conventional insurance: the basics

Definition of Risk

- What is Risk?
  - $Risk = R = pL$, or $R = p(\cdot)L(\cdot) = p(a, E) \times L(a, E)$, where
  - $p(\cdot) = p(a, E)$ – the prob. of loss
  - $L(\cdot) = L(a, E)$ – the amount of loss
  - a – actions [affecting the prob. and / or the amount of loss]
  - E – parameters of environment
- Who are the relevant actors (players)?
  - the insurer
  - the insured
  - and other parties affecting risk $R = R(a, E)$ via p or/and L

3. Conventional insurance: insurer profit

Contract (ρ, L_c, a_{min}), where

- ρ – insurance premium
- L_c – the amount paid by the insurer to the insured if loss occurs
- a_{min} – min requirements on the insured

Insurer profit [expected] from the contract (ρ, L_c, a_{min})

$$\Pi = \rho - R$$

Min requirements aim to decrease risk $R \Rightarrow$ increase profit Π

- examples of a_{min}: fire insurance requires every room to have
  - a fire alarm
  - a fire extinguisher
- in equilibrium, Π is non-negative:
  - $\Pi \geqslant 0 \Rightarrow \rho \geqslant R$
- with perfectly competitive insurers $\Pi = 0$
  - $\rho - R = 0 \Rightarrow \rho = R = p(a, E) \times L_c(a, E)$

4. Conventional insurance: examples

Example 1: Insurance against an accident (ex. broken leg)

- Contract (ρ, L_c)
  - Insurer: receives ρ from the insured; pays L_c if accident occurs
  - Insured: pays ρ; receives the amount L_c if his leg is broken

Example 2. Auto insurance

- Contract $(\rho, L(\cdot))$
  - Insured: pays ρ; receives $L(\cdot)$ if accident occurs and repairs $L(\cdot)$ are needed

Example 3: Fire insurance [with min requirement on the insured]

- Contract (ρ, L_c, a_{min})
  - Insured: pays ρ; receives L_c if his house burns and a_{min} were in place (ex. fire alarms were installed)

5. Adverse selection

ADVERSE SELECTION PROBLEM
aka ex ante information problem (before the contract is signed)

Let bad drivers have higher incident probability than good ones:

$$p_{bad} > p_{good}$$

With perfectly competitive insurers:

$$\rho_{bad} = p_{bad} L > p_{good} L = \rho_{good}$$

If insurers cannot differentiate driver types, contract is identical for all:

$$\rho_{bad} > \rho > \rho_{good}$$

Adverse selection

Good drivers might find such premiums too high and avoid signing such a contract. But if only bad drivers buy insurance contracts, insurers would lose money. This is called *adverse selection problem*.

6. Moral hazard

MORAL HAZARD PROBLEM
aka ex post information problem (after the contract is signed)

Does having insurance affects risks? Yes, it does. The insured have weaker incentives to reduce their risks.
For example, a driver with auto-insurance is less worried of damaging his car than an uninsured driver. Thus, the insured driver is more likely to be careless, i.e., he has higher probability of incidents.

Moral hazard

Ceteres paribas, having insurance worsens insurer's incentives. If an insurer cannot observe the quality of driving, the insured drivers have higher prob. of incidents then these drivers would have had with no insurance. This is called *moral hazard problem*.

7. Conventional insurance and problem of information

INSURANCE: IMPERFECT INFORMATION IS AN IMPORTANT PROBLEM

- ex ante information deficiency = before the contract is signed
  - aka adverse selection problem
- ex post information deficiency = after the contract is signed
  - aka moral hazard problem

EXAMPLES OF RISKS

- earthquake
- car accident
- fire
- burglar's attack
- cyber attack

8. Cyber-insurance vs conventional insurance

- What information is needed to evaluate Risks?
- What are the distinctive features of cyber-risks?

Cyber-risks: the specifics

- CPS systems interdependencies
- network features (topology)
- cyber laws
- lack of actuarial data

Cyber insurers & network security

Hypothesis: cyber insurers = improved security [incentives $\Uparrow$], but

Without Insurance

With Insurance

Thus, insurance also has a tendency to worsen incentives [incentives $\Downarrow$]

- How could insurers improve incentives?
- What do insurers change?

Insurers and information

1. Perfect information = perfect security
2. Imperfect information: two cases
   - 2A. Symmetric info – easy
     - E.g.: Insurance against cold weather (for agricultural firms). Insurers (i) Diversify (Florida, California, ...), (ii) Base premium on known probabilities (historical data)
   - 2B. Asymmetric info – hard (2001 Nobel to Akerlof, Spence, Stiglitz)
     - Insurance worsens incentives
     - NCS = a lot of asymmetric info

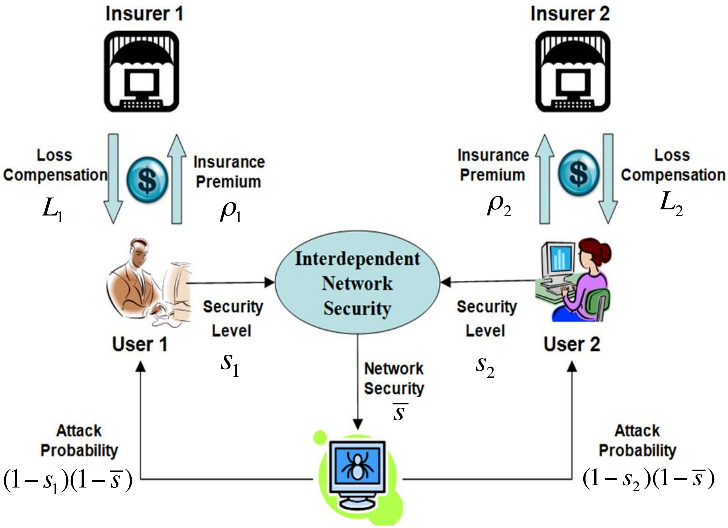
Insurers and imperfect info [asymmetric case]

- Asymmetric Info: two problems for insurers
  - Adverse selection [before the contract is signed]
  - Moral hazard [after the contract is signed]

- Conventional results:
  1. *Ceteris paribus*, under asymmetric info, with insurers security incentives worsen; i.e., a firm invests less in IT security if it has cyber insurance
  2. Insurers could improve security only when (i) overweighs (ii), where
     - (i) Insurers know more about security than the insured (reversed info asymmetry): Clients views of insecurity are downward biased and insurers have superior info about security practices
     - (ii) Insignificant levels of adverse selection and moral hazard

- Our model: extends conventional results to interdependent security in networks

Model



Insurer 1
Insurer 2
Loss Compensation
L_1
Insurance Premium
ρ_1
Insurance Premium
ρ_2
Loss Compensation
L_2
Interdependent Network Security
User 1
Security Level
s_1
Security Level
s_2
User 2
Network Security
$\overline{s}$
Attack Probability
$(1-s_1)(1-\overline{s})$
Attack Probability
$(1-s_2)(1-\overline{s})$

Network with interdependent security (IDS)

- Modeling N Users:
  - one user type [N identical users]
  - two user types [M malicious users and $(N - M)$ normal users]
- Insurers: perfectly competitive (i.e., zero expected profit)
- Probability of successful attack p_i for user i depends on
  - user's security $s_i \in [0, 1]$ ("private good") AND
  - network security $\bar{s}$ ("public good") [externality]
- IDS = externality:
  - Individual users: no effect on network security, BUT
  - But in aggregate, user choices affect security

$$p_i = (1 - s_i)(1 - \bar{s}), \text{ where } \bar{s} = \frac{1}{N} \sum_{i=1,\ldots N} s_i$$

Expected user utility [no-insurance case]

Expected user utility for the case of no insurance and single user type

$$E[u_i] = p_i U(W - L) + (1 - p_i) U(W) - h(s_i),$$

where p_i: probability of successful attack, W: wealth, L: loss in case of successful attack, $h(s_i)$: cost of security level s_i.

Assumptions

1. Standard assumption on utility (decreasing marginal utility)

$$U' > 0 \text{ and } U'' < 0$$

2. low cost of initial security improvements

$$h(0) = h'(0) = 0$$

3. prohibitive cost of complete risk elimination

$$\lim_{s_i \to 1} h(s_i) = \infty$$

User utility [with perfectly competitive insurers]

I. Noncontractable user security: Contract (ρ, L_c), where ρ is insurance premium when insured amount is L_c

$$E\left[u_i\right] = p_i U(W - \rho - L + L_c) + (1 - p_i) U(W - \rho) - h(s_i)$$

II. Contractable user security: Contract $(s_{\min}, \rho, L_c)$, where $s_{\min}$ is minimum security level by the insurer for the contract to be valid

$$E[u_i] = p_i U(W - \rho - L + L_c \cdot 1_{s_i \geqslant s_{\min}}) + (1 - p_i) U(W - \rho) - h(s_i)$$

Due to the assumption of perfect insurer competition:

$$\rho = L_c \cdot p_i,$$

That is, expected insurer profit is zero.

Modeling cyber-insurance

Theorem [N identical users]

For any contract $(s_{\min}, \rho, L_c)$, equilibrium is unique and it is symmetric. With insurance contract and no minimum security imposition: $(s_{\min} = 0)$

1. There is a unique social optimum, where users invest $s^{soc} > s^*$.
2. Nash equilibrium security decreases with insured amount L_c.

□

Theorem [Two user types]

Any equilibrium insurance contract offered by the competitive insurers has no minimum security imposition

1. That is, only one equilibrium contract exists, and it has $s_{\min} = 0$.
2. Security level is lower in the presence of competitive insurers than when no insurers present.

□