Cyberinsurance and Public Policy: Self-Protection and Insurance with Endogenous Adversaries

Fabio Massacci  
University of Trento  
f.massacci@unitn.it

Joe Swierzbinski  
University of Aberdeen  
j.swierzbinski@abdn.ac.uk

Julian Williams  
University of Durham  
julian.williams@durham.ac.uk

April 27, 2015
The growth in corporate insurance contracts that provide liability coverage in the event of a security breach to the firms information systems has been marked.

Lloyds of London reports that the US cyberinsurance market could be as large as $1.5 Billion or 2% of the corporate insurance market.

Cyber is increasingly being bundled with corporate and product liability insurance (CLI & PLI).

However, my coauthors and I will focus our attention on Cyber contracts as a separate product from bundled contracts, however, the claims made herein can be perfectly ported to the bundled case.
Are Insurance Companies Benevolent Risk Managers??

Inducing risk aversion in relation to firms demand for insurance, in particular for property, asbestos and pollution insurance (inherently demanded by corporations) appears to be a regular source of income for insurance companies.

Financial Times reported that a ‘...well-regarded insurance analyst, who declines to be named, says [sic]:’ “The ideal scenario this year is we have some hurricanes.” From: “Struggle to Increase Rates Hits Lloyds”, Alistair Gray, Financial Times, March 28, 2012.

The context of this comment is specifically in relation to the association between the realization of events, perceived increases in threat from liability claims and the subsequent demand for insurance, by firms with a need to satisfy firm level risk aversion.

Cyber-insurance has been seen to have the potential to realise large profits, indeed an industry insider has mentioned that pay-out ratios (from non-health CIPs) are about 10%.
Why is cyberinsurance interesting?

Why is Cyber different?

- The effect of the presence insurance on the behaviour of the individuals or firms purchasing coverage has been of considerable interest in the academic literature for more than four decades.

- However, in most instances the impact of actions on risk is primarily focused on the decisions of the ‘target’ or insured. In cyber, there is another agent, the ‘attacker’ and their decision making will have a significant impact on risk.

- Cyberinsurance and an active market in this area, has been cited as a means for solving many of the return-on-security-investment and cost-of-cyber attack that we are currently struggling to find.

- How might it do this?
Why is cyberinsurance interesting?

The advocating position

1. The presence of a cyberinsurance market allows firms to better control risks.
2. The very action of buying insurance means that firms will take proactive action to ensure their premiums are not too high.
3. By issuing cyberinsurance contracts then paying claims after attacks, insurance companies will begin to identify the frequency of attacks and the resulting distribution of firm losses and hence assist public policy makers in managing risks.
4. Subsequent to this, the insurance industry can then act as information coordinators that improve the management risks and generally reduce the overall frequency of attacks.
5. If this works really well, then we can mandate firms of certain sizes to have insurance and the insurance companies will coordinate security expenditure to better manage cyber security.
So we should all go get Cyberinsurance on top of our CLI?

- The answer to this depends on the ‘we’.
  - The differentiation between an individuals demand for insurance and a firms demand for insurance is addressed in (Mayers and Smith Jr, 1987, JRU).
  - **Individuals** cannot diversify their consumption risk and, as such, need insurance, they are risk averse and prudent.
  - **Firms** by contrast, in a market based economy, corporate stockholders (in diffuse ownership environments) can diversify away insurable risk and, as such, should be risk neutral...**ergo no demand for insurance**.
  
- Indeed, much of the study of the quality of corporate governance [see (Griffith, 2006, Penn.Law.Rev) and (Baker and Griffith, 2007, Chic.Law.Rev.) for examples] uses the magnitude of corporate liability coverage as a proxy for BAD corporate governance.

- As such, we would predict (from classical theory) that smaller firms should buy proportionally more insurance and larger firms less (as they should tend to the market based ideal of a firm)...**we of course do not find this in reality!**
HARA utility functions are always of the form whereby the level of risk aversion is linear in consumption.

From an economist's point of view what is risk aversion?

Let $z \in \mathbb{R}_+$ be a random consumption outcome on a one-dimensional consumption variable (usually an amount of money!).

If we are indifferent between taking this risky outcome and a certain amount $\tilde{z} = \mathbb{E}(z)$ then we are risk neutral.

If we always reject this bet, then we are risk averse. By construction if we are risk averse we have some degree of concavity in our utility function $U : z \rightarrow \mathbb{R}$, where for any $p > q$, $U(p) > U(q)$.

If we then write down the first two derivatives (rates of change of $U$ in $z$) of $U(z)$, denoted $U'(z)$ and $U''(z)$ then the absolute level of risk aversion is given by $\mathcal{A}(z) = -\frac{U''(z)}{U'(z)}$, $\forall z > 0$.

HARA is the most important class of utility functions because $\mathcal{A}(z) = pz + q$ (i.e. it is linear). This class includes the most common constant absolute (CARA) and constant relative (CRRA) risk aversion utility functions. These functions are the foundation of all the asset pricing models we have in finance and the vast majority of the literature in behavioural economics.
Actuarially Fair Insurance

- We term actuarially fair insurance as the price of coverage such that the insuree receives with certainty a consumption value of $\tilde{z} = E(z)$ and the insurer breaks even.

- The easiest way to consider this is to narrow down the distributional assumptions on $z$ to a simple Bernouilli draw, good state versus bad state.

- We do not lose much generality switching to this type of model as an example we can make use of the central limit theorem to construct identical examples using more complex distributions.

- The simplest case is let initial consumption wealth of an agent be described by $W$. After one period, the agent receives either $W$ (good outcome) or $W - L$ (bad outcome), with probability $\sigma$ and $1 - \sigma$ respectively.

- Let $L - \ell$ be a payment from the insurance company if the bad outcome occurs and $q$ be the cost of insurance, if $\ell = 0$ then coverage is complete.

- The profit to the insurer is $\Pi = q - \sigma(L - \ell)$, if the insurance is actuarially fair then $\Pi = 0$.

- Therefore the premium (or quote) is $q = \sigma(L - \ell)$ in the actuarially fair case.
Actuarially Fair Insurance and The Consumer Surplus

Paying more than actuarially fair insurance

- Let \( q \) be the actuarially fair rate of insurance for an excess \( \ell \), whereby \( q = \sigma(L - \ell) \). The insuree now has \( W - q \) in the good state and \( W - q - \ell \) in the bad state, where \( 0 \leq \ell \leq L \).

- Recall then when an agent is risk averse, under Jensen’s inequality we know that \( \mathbb{E}[U(z)] < U(\mathbb{E}(z)) \).

- So there was a premium \( w \) such that \( \mathbb{E}[U(z)] = U(\mathbb{E}(z - p)) \).

- Let us now assume that \( \ell = 0 \), i.e. full coverage, we can do this calculation for any coverage, but this makes it easier as \( q = \sigma L \).

- Therefore, in our example we know that expected utility without insurance is \( \mathbb{E}[U(z)] = \sigma U(W - L) + (1 - \sigma)U(W) \).

- And with insurance it is \( \mathbb{E}[U(z)] = U(\sigma(W - q) + (1 - \sigma)(W - q)) \equiv U(W - q) \).

- Therefore the \( q + \varepsilon \) that satisfies \( U(W - q - \varepsilon) = \sigma U(W - L) + (1 - \sigma)U(W) \) is the highest premium that an insurance company can charge before the individual refuses the contract.
Actuarially Fair Insurance and The Consumer Surplus

Examples of cyberinsurance premiums paid in 2014 from a large broker.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Revenue US$</th>
<th>( L - \ell ) US$</th>
<th>q US$</th>
<th>( q/L )</th>
<th>( \sigma: U = C R R A (0.1) )</th>
<th>( \sigma: U = C R R A (1) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare (HC)</td>
<td>25,000,000</td>
<td>1,000,000</td>
<td>12,900</td>
<td>0.01290</td>
<td>0.01287</td>
<td>0.01264</td>
</tr>
<tr>
<td>Education</td>
<td>25,000,000</td>
<td>1,000,000</td>
<td>6,000</td>
<td>0.00600</td>
<td>0.00599</td>
<td>0.00588</td>
</tr>
<tr>
<td>Financial</td>
<td>100,000,000</td>
<td>1,000,000</td>
<td>37,000</td>
<td>0.03700</td>
<td>0.03698</td>
<td>0.03682</td>
</tr>
<tr>
<td>Retail</td>
<td>50,000,000</td>
<td>1,000,000</td>
<td>26,000</td>
<td>0.02600</td>
<td>0.02597</td>
<td>0.02575</td>
</tr>
<tr>
<td>E-commerce</td>
<td>50,000,000</td>
<td>1,000,000</td>
<td>37,000</td>
<td>0.03700</td>
<td>0.03696</td>
<td>0.03664</td>
</tr>
<tr>
<td>Restaurant Chain</td>
<td>50,000,000</td>
<td>1,000,000</td>
<td>10,000</td>
<td>0.01000</td>
<td>0.00999</td>
<td>0.00990</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>100,000,000</td>
<td>10,000,000</td>
<td>50,000</td>
<td>0.00500</td>
<td>0.00497</td>
<td>0.00475</td>
</tr>
<tr>
<td>Health IT Prov.</td>
<td>1,200,000</td>
<td>5,000,000</td>
<td>15,900</td>
<td>0.00318</td>
<td>0.00289</td>
<td>0.00078</td>
</tr>
<tr>
<td>HC SaaS Prov.</td>
<td>1,500,000</td>
<td>5,000,000</td>
<td>30,420</td>
<td>0.00608</td>
<td>0.00553</td>
<td>0.00149</td>
</tr>
<tr>
<td>HC Rec. Prov.</td>
<td>5,000,000</td>
<td>1,000,000</td>
<td>8,010</td>
<td>0.00801</td>
<td>0.00792</td>
<td>0.00718</td>
</tr>
<tr>
<td>Data Hosting</td>
<td>200,000</td>
<td>1,000,000</td>
<td>2,750</td>
<td>0.00275</td>
<td>0.00254</td>
<td>0.00101</td>
</tr>
<tr>
<td>HC IT Cons.</td>
<td>150,000</td>
<td>1,000,000</td>
<td>3,298</td>
<td>0.00330</td>
<td>0.00305</td>
<td>0.00121</td>
</tr>
<tr>
<td>HC Data Analysis</td>
<td>20,000</td>
<td>2,000,000</td>
<td>4,900</td>
<td>0.00245</td>
<td>0.00224</td>
<td>0.00075</td>
</tr>
<tr>
<td>e-Waste Company</td>
<td>1,500,000</td>
<td>1,000,000</td>
<td>3,564</td>
<td>0.00356</td>
<td>0.00340</td>
<td>0.00215</td>
</tr>
<tr>
<td>Psych. Office</td>
<td>1,000,000</td>
<td>1,000,000</td>
<td>1,600</td>
<td>0.00160</td>
<td>0.00148</td>
<td>0.00059</td>
</tr>
<tr>
<td>Doctors Office</td>
<td>700,000</td>
<td>500,000</td>
<td>649</td>
<td>0.00130</td>
<td>0.00123</td>
<td>0.00073</td>
</tr>
<tr>
<td>Online Retailer</td>
<td>500,000</td>
<td>1,000,000</td>
<td>1,100</td>
<td>0.00110</td>
<td>0.00102</td>
<td>0.00040</td>
</tr>
<tr>
<td>Prof. Cons. Serv.</td>
<td>400,000</td>
<td>1,000,000</td>
<td>1,200</td>
<td>0.00120</td>
<td>0.00111</td>
<td>0.00044</td>
</tr>
<tr>
<td>Hospital</td>
<td>170,000,000</td>
<td>5,000,000</td>
<td>42,000</td>
<td>0.00840</td>
<td>0.00839</td>
<td>0.00828</td>
</tr>
<tr>
<td>Data Stor. Cent.</td>
<td>15,000,000</td>
<td>20,000,000</td>
<td>120,000</td>
<td>0.00600</td>
<td>0.00542</td>
<td>0.00111</td>
</tr>
</tbody>
</table>
At present we have assumed that the agent has no control over the probability of a successful attack $\sigma$ and hence the overall expected loss $\sigma L$ is not within the control of the agent, the insurance company or anyone else.

It is useful at this point to specify some notation. Each target $i \in \mathbb{N}_+$ has an endowment of assets $W_i > 0$ and in the event of a successful cyber attack is subject to losses $L_i$, where $L_i > 0$. The utility function of the $i$ target over a random consumption variable $w$, for wealth, is denoted by $U_i(w)$.

The ‘induced’ utility functions for the $i \in \{1, \ldots, N\}$ firm $U_i(w)$ is an at least thrice differentiable von Neumann Morgenstern utility function where for all $w$ it is $U_i'(w) > 0$ and $U_i''(w) < 0$.

We make no presumption on the specific degree of risk aversion of the firms, or the degree of losses.

Each target may make a security investment $x_i$, where $0 \leq x_i < L_i$ and is targeted by a number of attackers $n_i$ where $0 \leq n_i < \infty$.

The probability of a successful attack from the viewpoint of the target, is determined by the level investment and the number of attackers focussing on the particular target and is denoted by $\sigma_i(n_i, x_i)$. 

FM, JS, JW

Cyber Insurance
Investing in security

The impact of security investment and attack intensity on risk

(A) The function $\sigma_i(\cdot)$ should be at least twice differentiable in $x_i$ and $n_i$.

(B) $\sigma_i(\cdot)$ is continuous strictly increasing when the number of attackers against target $i$ increases, for all $n_i$ it is $\partial \sigma_i / \partial n_i > 0$, ceteris paribus. In the absence of attackers the probability of a successful attack is zero, therefore when $n_i = 0$, $\sigma = 0$, $\forall 0 \leq x_i < \infty$.

(C) $\sigma_i(\cdot)$ is continuous strictly decreasing with increasing investment by target $i$ in security investment, for all $x_i$ it is $\partial \sigma_i / \partial x_i < 0$, ceteris paribus.

(D) The rate of reduction in $\sigma_i(\cdot)$ with increasing $x_i$, from (A) is strictly decreasing with increasing defensive expenditure, for all $x_i$ it is $\partial^2 \sigma_i / \partial x_i^2 > 0$. 
Introduction

Primer on the Economics of Insurance

Attack and Defence

The Policy Experiment

Concluding Remarks

References

Modelling Attackers’

We do not know a lot about the motives of cyber-attackers, so we will solve the model under the most general set of assumptions.

- Cyber attacks are conducted by a pool of attackers. In the event of a successful attack, the successful-attacker realizes a reward $R_i$. As with most insurance cases, the reward $R_i > 0$ is assumed to be far lower than the loss $L_i$, however as the unit of account for attackers and targets is assumed to be fundamentally different this assumption does not bind.

- To enter the lottery for the reward $R_i$ each attacker must spend a cost $C_i$, for tractability we assume that all attacks are independent.

- The other complication for attackers is coordination and reward sharing. Our model works at the public policy level so individual target – attacker interactions are of less interest.

- Therefore, we will assume at the macro level choice of target is random and there are technological drivers that suggest this is reasonable too.
Attackers

**Attacker Assumptions**

(A) Attackers have fixed costs of entry $c_i$, are risk neutral and make binary attack or no-attack decisions. We will further assume that when looking at aggregate number of attackers per target $c_i = C$.

(B) Attacker-target matching is fully-degenerate. The probability matching of a given $j$ attacker to the $i$ target is random with a uniform distribution across targets (i.e. the probability is $1/N_T$ where $N_T$ is the total number of targets).

(C) The scalar $R_i \geq 0$ is the reward for the *first-winner-takes-all* attacker to successfully attack target $i$. In the event of a successful attack on target $i$ the successful attacker does not share this reward with other $n_i$ attackers and at this point no further attack will generate any reward. We denote the *rate of return* on $C$ for a given reward $R_i$ for an attack on the $i$ target as $R_i/C = \rho_i$. 
The Policy Experiment

Our objective is to determine the impact of various cyberinsurance markets on the overall level of security as a function of security investment and attacking intensity.

(i) We will look at the unregulated market (solved by a simultaneous Nash equilibrium).

(ii) The case when a benevolent utilitarian social planner coordinates and mandates expenditure.

(iii) A fully competitive cyber insurance market providing insurance contracts at an actuarially fair rate.

(iv) A monopolist insurer extracting the full surplus from targets and mandating defensive expenditure.
Summary of findings

- We predict (and indeed we have anecdotal evidence) that an ‘attacker-externality’ exists.
  
  That is the collective action of targets affects the choice of participation of attackers, more anticipated opportunity and hence greater attacking intensity.

- As such, the highest aggregate welfare is provided by the social planner, driving out that externality by coordinating expenditure across targets.

- Unfortunately, security investment does not increase when there is a fully competitive cyberinsurance market, in fact it may well decrease as targets shift to making risk neutral security investment decisions.

- A monopolist insurer has no incentive to drive down aggregate attacking intensity.

- We are not saying cyberinsurance is ‘bad’, but that it cannot be used in place of public policy coordination of security.
(i) Unregulated Markets

Let $x_i$ and $n_i$ be given exogenously. The expected utility of target $i$ for a given pair $(x_i, n_i)$, denoted $\mathbb{E}[U_i(x_i, n_i)]$, is therefore described by the following

$$\mathbb{E}[U_i(x_i, n_i)] = (1 - \sigma_i(x_i, n_i)) U_i(W_i - x_i) + \sigma_i(x_i, n_i) U_i(W_i - x_i - L_i)$$  \hspace{1cm} (1)

If the target $i$ is risk neutral and therefore $U_i(w) = w$, its expected utility for a given level of security expenditure is simply the expected net monetary value of its assets

$$\mathbb{E} [U_{\text{risk neutral}_i}(x_i, n_i)] = W_i - x_i - \sigma_i(x_i, n_i)L_i$$  \hspace{1cm} (2)

The optimal level of defensive expenditure for a risk neutral target is obtained by maximizing the expected utility (point B in the figure). Since $W_i$ is constant, in presence of a given number of attacker, this value is obtained by setting to zero the first order condition which leads to the following condition

$$L_i \frac{\partial \sigma_i(x_i, n_i)}{\partial x_i} = -1$$  \hspace{1cm} (3)

The choice of the optimal expenditure is denoted: $x^\star$. 
The Nash Equilibrium

- In a symmetric Nash equilibrium \((x^*, n^*)\) each target \(i\) selects the same level of defensive expenditure \(x^*\) that optimizes the expected utility of the target whereas the number of attackers per target \(n^*\) is determined by

\[
x^* = \arg \max_x \{ \mathbb{E}[U(x, n^*)] \}
\]

\[
n^* = \rho \cdot \sigma(x^*, n^*)
\]

- we will now show that the presence of a public policy acting as a benevolent social planner the socially optimal level of investment \(x_{i}^\dagger\) will be greater than \(x_{i}^*\).
(ii) A Utilitarian Social Planner

Before introducing the insurance market, it is useful to ascertain the optimal investment policy that a fully informed benevolent social planner would mandate.

- By ‘benevolent’ we will adhere to a classical utilitarian definition.
- The planner’s action is to ‘mandate’ security investments for each target denoted \( x_i^\dagger \) and we will assume that \( x_i^\dagger \) is binding, measurable and enforceable.
- Let the social planner’s preferences regarding the risks of cyber-attacks be described by an aggregate von Neumann-Morgenstern utility function of the form

\[
U_P = \sum_{i=1}^{N} \nu_i U_i
\]  

(4)

- Without loss of generality, we normalize the weights so that

\[
\sum_{i=1}^{N} \nu_i = 1.
\]  

(5)

In practice the social planner is not necessarily a public-policy maker.
A Utilitarian Social Planner

A Stackelberg Equilibrium

Let us assume that the policy maker moves first and that all other actors (targets and attackers) make their choices in a second stage after observing the choice of the policy maker. The expected utility of the social planner is now:

$$\mathbb{E}[U_P] = \sum_{i=1}^{N} \nu_i \mathbb{E}[U_i],$$

(6)

The utilitarian social planner then chooses a vector $x^\dagger = [x_i^\dagger]$ for all targets such that $\frac{\partial \mathbb{E}[U_P]}{\partial x_i} = 0$.

Solving for the first order condition and dividing by $\nu_i$ and illustrates how the incentives of the policy maker may differ from the incentives of individual unregulated targets.

$$0 = \frac{1}{\nu_i} \frac{\partial \mathbb{E}[U_P]}{\partial x_i} = \frac{\partial \mathbb{E}[U_i]}{\partial x_i} + \frac{\partial \sigma_i}{\partial x_i} \left( \Delta U_i(x_i) - \frac{1}{\nu_i} \Delta U_P(x_i) \right)$$

(7)

$$- \frac{\partial n^*}{\partial x_i} \left( \mathbb{E} \left[ \frac{\partial U_i(x_i)}{\partial n^*} \right] - \frac{1}{\nu_i} \mathbb{E} \left[ \frac{\partial U_P(x_i)}{\partial n^*} \right] \right)$$

(8)

We can show that $x_i^\dagger > x_i^* \forall i \in \{1, \ldots, N\}$ always.
What happens when we add Cyberinsurance Markets?

- Let the $i$ target have an available insurance contract described by a pair $(q_i, \ell_i)$, which specifies the premium, or quote, $q_i$ paid by the target $i$ in the event of a loss, and the amount of the deductible, or excess, $\ell_i \leq L_i$ that will be left to be paid by the target if the successful attack takes place.

- The premium is paid upfront and its cost is incurred in both of the outcome states. Individual targets can freely choose a level of defensive expenditure $x_i$ the level of defensive expenditure as well as whether to purchase an insurance contract specified by the tuple $(q_i, \ell_i)$.

- As such the $i$ target’s expected utility is therefore given by:

\[
\mathbb{E}[U_i(q_i, \ell_i, x_i, n_i)] = (1 - \sigma_i(x_i, n_i)) U(W_i - x_i - q_i) + \\
+\sigma_i(x_i, n_i) U(W_i - x_i - q_i - \ell_i). 
\]  

(9)

For the purposes of our analysis herein, it is useful to impose certain assumptions on the information set and range of actions available to a provider of insurance.
The cost of insurance:

- An insurer provider issues a cyberinsurance contract that pays out and amount $L_i - \ell_i$ in the event of loss from a cyber attack.

- If insurance markets are efficient, the insurer does not make a profit on the equilibrium path and must therefore charge

$$q_i = \sigma_i(x_i, n_i)(L_i - \ell_i) \tag{10}$$

- IMPORTANT PREDICTION: For a given number of attackers per target $n > 0$, let $x_i^{\star}$ be the optimal security investment for the risk averse target with actuarially fair insurance quote $q_i^{\star} = \sigma_i(x_i^{\star}, n_i)L$. The optimal security investment $x_i^{\star}$ of the risk averse target, in the absence of any available insurance contracts, will be higher than $x_i^{\star}$, in almost all cases.

- That is, if a target has access to actuarially fair insurance, they will, in the majority of plausible cases, substitute some of their security investment with insurance.

- Attackers react to this reduction in security investment and the overall level of risk increases. For correctly priced insurance contracts the insurer will be economically indifferent to this adjustment.
We have illustrated that the perfectly competitive cyberinsurance does not result in aggregate risk reduction in most cases.

- We now consider the case where a single insurer who can set a required level of defensive expenditure as part of the insurance contract.
- The monopolist wishes to offer an insurance contract which all targets will be willing to purchase.
- For the targets to be willing to accept the insurer’s offer, they must be indifferent between accepting or not accepting and at the same time the insurer will try to extract the maximum possible rent from the target.
- This in effect means charging the actuarially fair rate plus the premium $\epsilon$ we discussed before.

In the reactive set-up this means that the premium $q_i$ charged to each target must satisfy the following incentive compatibility constraint:

$$
\mathbb{E}[U_i(q_i, \ell_i, x_i^\#(x_i^\#))] \geq \mathbb{E}[U_i(0, L_i, x_i^*(n^*(x_i^\#))), n^*(x_i^\#))].
$$

(11)
What if the monopolist insurer can mandate security expenditure?

- The insurer optimizes its profit function by taking the usual first order condition on the profit under the implicit expression for $q(X_i)$ defined by the attackers entry condition.

$$\frac{\partial \Pi}{\partial x_i} = 0$$  \hspace{1cm} (12)

$$U_i(W_i - x_i - q_i) = \mathbb{E}[U_i].$$ \hspace{1cm} (13)

- The outcome is stark: The optimal security expenditure $x^*_i$ chosen by the unregulated targets who cannot purchase insurance is always larger than the above security expenditure $x_i^\#$ mandated by the monopolist insurer if the marginal (first derivative) change in the expected loss at $x_i^\#$ is smaller than -1.

- That is the bigger the change in risk the less the monopolist mandates as they control precisely the exposure, this increases the risk premium and hence their profits.
The Good

Implications

- The only way that insurance markets provide a global benefit to targets is when security investment is separately mandated by a social planner (usually government) whose sole objective is to maximise the targets global utility.

- If insurance is provided without a social planner then the effects almost unambiguously indicate a aggregate drop in security investment.

- One of the key drivers is the ability of attackers to enter and exit the market for attacks in a flexible manner, this is mediated by the technology of attack, which appears to be relative diffuse (exploit kits and markets, hacker forums etc).
The worst case is always when the social planner delegates coordination to the insurance sector (as has been suggested in some circles in the United States) and a dominant monopolist appears.

The monopolist insurer has no incentive to manage security risks away and as risks and losses increase the need for targets to substitute security expenditure with insurance becomes more acute.

Targets can not even utilise informal alliances! Insurance companies can offer individually welfare improving contracts and targets will eventually diffuse to a completely insured state at which point the degree of risk is controlled by the insurance sector.
