Cyber-Insurance Revisited

Rainer Böhme

Technische Universität Dresden
Institute for System Architecture
01062 Dresden, Germany
rainer.boehme@inf.tu-dresden.de

Abstract

Cyber-insurance is considered as appropriate means to absorb financial losses caused by computer security breaches. Since insurance markets at the same time create incentives to construct more secure systems, they are regarded as particularly desirable tools. However, this paper argues that the typical market structure in IT businesses may thwart the formation of a proper insurance market for cyber-risks: The worldwide dominance of a few system platforms leads to correlated losses, which require premium surcharges and are thus hard to insure. This paper refers to an indemnity insurance model to evaluate the conditions under which coverage for cyber-risks can be granted despite monocultures of installed platforms. Different premiums for users of dominant and alternative platforms are also addressed. Acting as a counterweight to the market leader's strong economies of scale, a cost advantage for users of less widespread platforms could foster a more balanced market structure.

1 Introduction

It is a commonplace that every year security breaches in computer systems cause immense economic damage, although the true extent is still difficult to quantify [8, 24]. Shortcomings in computer security do not only have economic consequences, but also emerge from economic causes. Ross Anderson [4] explains this by the fact that neither manufacturers nor users have an interest in investing adequately into security measures within their respective sphere of responsibility.

Scholars in computer sciences and related disciplines proposed a vast number of technical solutions for all kinds of computer security issues. However, the blueprints offer protection only if they are effectively employed in practical systems. Apparently, due to a lack of incentives, this does not happen often enough [3]. Hence it is obvious that computer security requires the consideration of both technical means as well as economic principles.

Workshop on the Economics of Information Security (WEIS) 2005.
Kennedy School of Government, Cambridge, MA, USA.

www.manaraa.com

1.1 The Case for Cyber-Insurance

Economist Hal Varian identifies the situation of responsibility attribution as the main source of weak security [35]. He argues that, in a first step, liability for losses due to security breaches should be transferred to the party who could reduce the risk most easily. Accordingly, manufacturers would be liable for vulnerabilities in their products, but also network nodes—up to the end user—could be called to account if they do not comply with their maintenance duties.[1] As a second step, these new *cyber-risks* should be made transferable, so that all parties can buy insurance coverage against possible losses and indemnification claims. In doing so, the valuation of risks is carried out in a market mechanism, which is automatically efficient (sufficient liquidity assumed).

Apart from the obvious benefit of absorbing financial impact of security risks, further reflection on the insurance approach yields three additional advantages: *First*, insurance companies are likely to differentiate premiums according to different classes of risk. This creates concrete incentives to invest in secure technology [36]. It is clear that reductions in premiums can only be granted if actually effective security measures are in place. As a result, it *secondly* becomes possible to express the value (not the cost!) of security measures in monetary metrics. Further implications, such as comparability and the ability to apply well-understood decision methods, are corollaries of this improved quantification. This avoids over-spending up to military level [2] and simultaneously reduces the usage of poorly designed and thus inefficient solutions, which are widely in use out of irrational reasons (subjective feeling of security, visibility of security, or common criteria) [31]. The *third* aspect refers to research and development of security technology. As part of their risk management, insurance companies have to gain information about the characteristics and the extent of individual risks in order to assign adequate premiums. The better they are informed the more competitive they are. Hence, insurance companies have an incentive to reinvest a fraction of their revenues to improve their base of information, which finally leads to ever better supply of coverage. Accordingly, insurance companies demand independent code reviews and laboratory tests, whose results, in turn, yield new insights for more secure products. They can pursue or finance technology development to minimise risks and reduce claim amounts [22, 18]. Eventually, insurance companies are welcome in assumed markets for security vulnerabilities [30] to provide the much-needed liquidity.

In brief, cyber-insurances are quite useful to tackle information security risks. However, the respective literature merely focuses on the perspective of individual insurance holders. This paper, on the contrary, analyses the situation from the perspective of insurance companies that have to bear the entirety of risks. We do this with special regard to the particular market structure of the IT industry.

[1] Note that an enaction of liability for end users seems much more realistic than for manufacturers. The latter still has a touch of gedankenexperiment, although software product liability, at least for security products, is seriously discussed (cf. for example [29]). However, the true extent of liability transfer is not relevant for the validity of the following findings, as it merely affects the dimension of the consequences but not the logic of the argument.

www.manaraa.com

1.2 The Role of Market Structure

When comparing the market structures of the information technology industry to those of other business sectors, we usually find a strong dominance of the respective market leader. Economic theories can explain this concentration of market power by referring to the particularities of the respective industry: Network externalities, negligible marginal costs (especially for software), and interdependencies with complementary markets mutually amplify each other's impact to shift market share to the market leader [32, 4].

These processes ultimately converge in a monopoly. Apart from the known inefficiencies and welfare-decreasing effects studied in economic theories [34], a monopoly also causes a "monoculture", hence a low diversity of installed systems. As a result, a large part of today's computing technology suffers from *the same* weak spots and bugs [14]. Consequently, worms and viruses can systematically exploit these vulnerabilities and thus epidemically cause huge damage by attacking all computers in a network almost *at the same time* [19].

The central question of this paper addresses the implication of this correlation of attacks on the insurance approach. For this purpose a simple indemnity insurance model is employed to discuss whether it is economically possible to offer insurance coverage for cyber-risks that are subject to correlated claims. In other words, is there a business model for insurance companies to offer coverage against damage caused by worms and hackers at acceptable premiums?

In a second step, we will analyse the case of different premiums for two classes of risk: users of a dominant platform (i.e., the market leader), and users of an independent and considerably less widespread alternative platform (i.e., the challenger). This comparison allows an estimation of the extent to which insurance premiums can motivate diversification and thus counterbalance the above-mentioned forces that accumulate market share.

The remainder of this paper is organised as follows: On the basis of a review of relevant literature given in Section 2, a simple (single-factor two-state) insurance model is developed in Section 3. Section 4 presents the results obtained from the model. The final part, Section 5, addresses further interpretation (5.1), limitations of the method and its implied assumptions (5.2), as well as pointers for future research in this interdisciplinary field.

2 Related Work

In this section we describe three classes of work related to this paper, basic literature on economic aspects of information security, previous proposals of cyber-risk management including case studies and typologies for insurance approaches, and basic literature on actuarial economics and mathematics. Relevant terminology will be introduced during this literature review. Remarkably, we could not find previous publications addressing the specific difficulty to insure correlated cyber-risks.[2]

[2]The author gratefully receives information about relevant work from the reviewers.

www.manaraa.com

2.1 Economics of Information Security

The basics of microeconomics, such as pricing within different market and cost structures, can be found for example in [34]. Selected principles, particularly edited for the special case of IT industry, are presented in [32]. Finally, an application of the general theories of information economy to the narrower field of computer security is given in [4].

These and other authors [7, 35] conclude that insecure software products are underpriced by the market and reveal their true costs in terms of negative externalities. Thus, network security appears to have properties of a public good: Insecure nodes not only risk the sanity of their own systems, but also compromise the security of all users, for instance by spreading worms unintentionally and by irresponsibly tolerating distributed attacks from their computers. Since these public costs are not attributed to the responsible parties, individuals have no incentive to upgrade the security of their systems.

As a reaction to this market failure, a number of solutions have been proposed, largely by calling for regulation: While Camp and Wolfram [7] discuss a tax on insecure network nodes, other researchers come up with financial mechanisms in the software development process and evaluate the pros [30] and cons [20] of vulnerability markets as well as bug auctions [26].

Moreover, there is also literature in the tradition of management sciences, balancing cost and utility of IT security measures for investment decisions [33, 15, 1, 9]. These *Return On Security Investment* (ROSI) models mainly provide guidelines for finding the optimal amount of information security spending—sometimes coupled with bargaining strategies to justify a budget increment [5].

2.2 Cyber-Insurance – A Prospect Market?

The borderline between ROSI models incorporating uncertainty and insurance approaches is somewhat blurred: The acquisition of insurance coverage can be regarded as an investment (although not directly in technology) and buying a policy at reasonable conditions usually implies prior security investment for loss prevention. Early proposals for pure insurance models can be found in [2], subsequent ones in [35, 36, 31, 21]. All these presentations clearly focus on the demand-side, although some of them also address public benefits. The supply-side, however, is characterised as an art instead of a science [10], which is frequently explained by the lack of actuarial data on information security incidents.

Lawrence Gordon et al. [16] describe a procedure to employ cyber-insurance policies as an instrument of risk management. The authors also point to a number of existing offers for cyber-risk coverage, and they distinguish between two classes of risk (compare also [18]).

- *First party risks* cover losses occurring directly to the insurance holder. They include, for example, loss of profits due to spying, destruction of property and data, business interruption due to hacker or virus attacks and software failures, etc.

www.manaraa.com

- *Third party risks* cover financial compensation for losses of third parties that occur due to shortcomings in the insurance holder's field of responsibility. For example: damage caused by forwarded computer viruses, contractual penalties due to IT failures, intellectual property and privacy infringements after data theft.

To comprehensively characterise the particularities of cyber-risks, we add to the classification by loss centre (the insured, third parties) another classification by cause: Computer hardware as well as software is already covered by some policies against "conventional" incidents, such as fire or weather-related perils. This example may also apply to business interruption cases. Still, we clearly have to distinguish the completely different situation when loss of tangible or intangible (e.g., business information) property is caused by logical errors or intentional adversaries. This is the new type of risk—cyber-risk—which currently is rather difficult to insure [18, 10, 21].

At this point it seems reasonable to discuss one more aspect, namely the correlation of claims in conventional insurance business. Actually, correlation of claims is relevant for any insurance branch, though the protection mechanisms employed elsewhere do not apply to cyber-risks: Small local-based insurance companies can survive despite geographic correlation of weather-related perils, such as storms and floods, because reinsurance companies sell coverage for the rare event of very high claim amounts [27]. Secondary coverage is supplied by just a few global companies, which avoid undue risk concentration by intercontinental diversification. However, it seems that cyber-risks are of similar nature all over the globe, meaning that higher-order balancing does not suggest considerable improvement. According to *CSO Magazine* [10], primary insurance companies started to explicitly exclude cyber-risks from existing contracts by January 2002, because their reinsurance companies were concerned about a global "cyber-hurricane", which they would not be able to deal with. To conclude these considerations, since we do not expect additional flexibility from secondary markets for cyber-risk, we can justify that reinsurance is not reflected further in this paper.

2.3 Principles of Financial and Actuarial Theory

An insurance contract (*policy*) binds an insurance company in the occurrence of contractually defined *loss events* to pay a specified amount (*claim*) to the insurance holder. In return, the insurance holder pays a fixed sum (*premium*) to the insurance company. Since claim amounts usually depend on the dimension of losses, insurance companies offer uncertain future payoffs for a certain premium at present. This constellation generates three interesting phenomena studied in the literature: *adverse selection* (bad risks are more likely to demand coverage than good ones), *moral hazard* (insurance holders behave careless as they do not have to bear the losses), and *calculation of premiums*. The latter is the subject of extensive literature on actuarial mathematics [6, 27, 23], which can be further classified into life insurance and non-life (indemnity) insurance. However,

www.manaraa.com

some textbooks on these topics still assume independence of losses, which is not deemed realistic when regarding cyber-risks. Therefore we refer to specific work on risk management and extreme value theory (EVT) [12, 13, 17], where dealing with *portfolios* of dependent risks has had a relatively long tradition (the theory goes far beyond the rudimental models used in this paper).

3 An Insurance Model for Cyber-Risks

In this section we present a simplified model for correlated cyber-risks, which illustrates the cost of a monoculture in terms of higher insurance premiums. Therefore we do not directly regard insurance policies, which largely bundle a number of risks, but only individual risks. Each risk is modelled as random variable R with a non-negative distribution of claim amounts. A number of n homogeneous risks results in a portfolio $S_n = (R_1, R_2, \ldots, R_n)$, represented in a random vector of length n.

The following argumentation is confined to one period in time (e.g., one year). We further assume that the individual risks follow a Bernoulli distribution with parameter p as probability of loss. The claim amount in case of loss is assumed to be constant and normalised to a value of 1.[3] Accordingly, after each period, an average fraction p of n risks caused claim events to be compensated with payments by the insurance company.

So holds

$$\mathsf{P}(R = r) = \mathsf{P}(r) = p^r \cdot (1-p)^{1-r}, \qquad r \in \{0, 1\}. \tag{1}$$

From this distribution and from the normalised claim amount we infer that for each period, the claim number x equals the total claims of the portfolio: $L = \sum_{i=1}^{n} R_i$. If the risks $R_1, R_2, \ldots, R_n$ are independent, hence

$$\mathsf{P}(r_i \wedge r_j) = \mathsf{P}(r_i) \cdot \mathsf{P}(r_j), \quad \forall\, (i,j) \in [1;n]^2, \quad i \neq j, \tag{2}$$

then $L \sim \mathbf{B}(n,p)$ follows a Binomial distribution. The probability density function W is given as

$$\mathsf{P}(L = x) = W_p^n(x) = \binom{n}{x} p^x \, (1-p)^{n-x}, \tag{3}$$

with expected value $\mathsf{E}(L) = np$ and variance $\mathsf{Var}(L) = np(1-p)$. Depending on the dimensions of p and n, the Binomial distribution can be approximated numerically either with the Gaussian or the Poisson distribution.

In order to be able to pay the mean claim amount $\mathsf{E}(L)$ in each period from the earnings, a naive insurance company could set the premium so that $\mathsf{E}(L) = np$ is equally divided among the risks. This corresponds to a *net premium*

[3] This implies that losses occur once per period at most, which is plausible for some situations, such as liability for privacy breaches: Once critical information has got public, further distribution will not generate additional harm. Also for other classes of risk, ignoring multiple loss events does not matter much because for small p, multiple losses are very rare.

www.manaraa.com

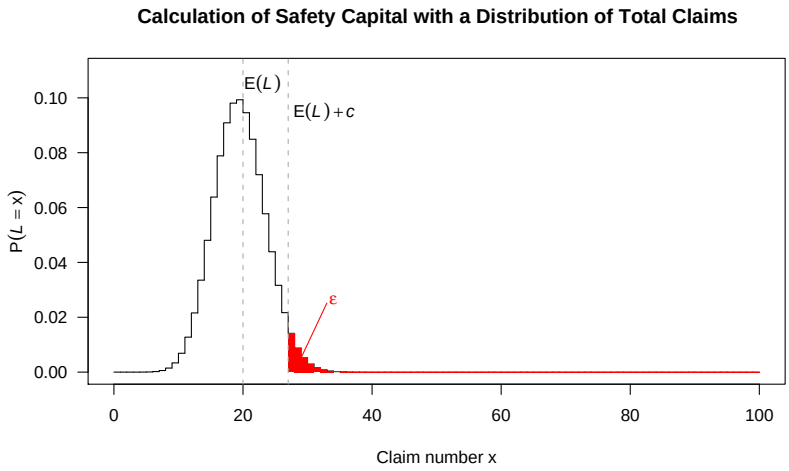

Figure 1: Binomial model: Net premium, safety capital, and probability of ruin

of $\pi_{\mathsf{net}} = p$. As this approach employs a point estimate on the expected value, premium revenues generated by this principle would suffice to settle all claims in only half of the cases. It is obvious that a *probability of ruin* of $\mathsf{P}(L > n{\cdot}\pi_{\mathsf{net}}) = \frac{1}{2}$ is far too high.

Therefore, additional *safety capital* c is required in addition to the revenue from the net premiums $\mathsf{E}(L) = n \cdot \pi_{\mathsf{net}}$, so that the probablitiy of ruin never exceeds a given upper bound:

$$\mathsf{P}(L > n \cdot \pi_{\mathsf{net}} + c) \leq \varepsilon \tag{4}$$

The safety capital can be computed for a given ε with the quantile function Q of the Binomial distribution.

$$c = \lceil Q_p^n(1-\varepsilon) \rceil - \mathsf{E}(L) = \lceil Q_p^n(1-\varepsilon) \rceil - np \tag{5}$$

Figure 1 illustrates this relationship for $n = 100$ risks, $p = 0.2$ and $\varepsilon = 0.05$.

As capital c is not spent in the long run, its cost can be expressed in terms of missed yield of an alternative investment of similar risk. Since all risks in the portfolio are homogeneous, the cost of the safety capital shall be equally divided as *safety loading* on all premiums. The gross premium π is calculated as follows:

$$\pi = \pi_{\mathsf{net}} + i^* \cdot \frac{c}{n} + A \ , \tag{6}$$

where i^* denotes the interest rate for an investment with risk not below ε.[4] A is an allocation of administrative costs, which is assumed to be negligible

[4] ε is a lower bound, because—apart from the risk of random fluctuations—insurance companies are exposed to further uncertainties, such as market and operational risks.

www.manaraa.com

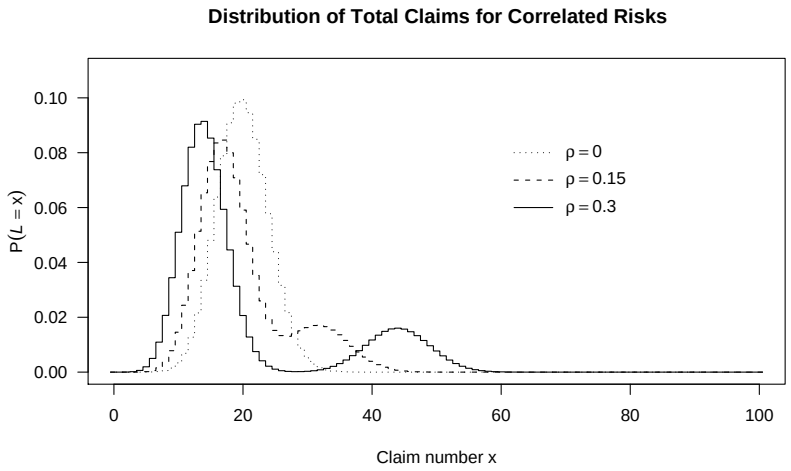

Figure 2: Portfolio of 100 risks ($p = 0.2$) with varying degree of correlation ϱ

in the following. A fundamental element of insurance economics is *portfolio balancing*, a corollary of the law of large numbers. It means that safety loadings decrease with a growing number of *independent* risks in the portfolio. So we face systematic economies of scale: Insurance companies with large portfolios can offer additional coverage more competitively than those with small ones.

For the special case of cyber-risks, we model the presumed co-occurrence of claims as a correlation between the individual risks $R_1, R_2, \ldots, R_n$ and a latent systemic risk $R_0 \sim \mathbf{B}(1, p)$. This simplifying decision reduces the dimensionality of dependence to one latent factor, which can be justified by regarding computer viruses as dominant thread model. A correlation coefficient ϱ is interpreted as a Pearson product-moment correlation:

$$\mathsf{Cor}(X, Y) = \frac{\mathsf{E}(X \cdot Y) - \mathsf{E}(X) \cdot \mathsf{E}(Y)}{\sqrt{\mathsf{Var}(X)\mathsf{Var}(Y)}} \ , \tag{7}$$

with X and Y being arbitrary random variables. Inserting the Bernoulli risks from (1) yields

$$\varrho = \mathsf{Cor}(R_i, R_0) = \frac{\mathsf{P}(r_0 = 1 \wedge r_i = 1) - p^2}{p \cdot (1 - p)}, \qquad i = 1, \ldots, n \ . \tag{8}$$

Now we get the conditional probabilities for R_i in dependence of R_0 as

$$p_{|0} = \mathsf{P}(r_i = 1 | r_0 = 0) \quad = \quad \frac{p - \mathsf{P}(r_i = 1 \wedge r_0 = 1)}{1 - p} = p - p \cdot \varrho \quad \text{and} \tag{9}$$

$$p_{|1} = \mathsf{P}(r_i = 1 | r_0 = 1) \quad = \quad \frac{\mathsf{P}(r_i = 1 \wedge r_0 = 1)}{p} = p + (1 - p) \cdot \varrho \ . \tag{10}$$

www.manaraa.com

It can also be shown that a correlation with a systemic risk R_0 is equivalent to a correlation between each pair of individual risks:

$$\mathsf{Cor}(R_i, R_j) = \sqrt{\varrho}\,, \quad \forall\,(i,j) \in [1;n]^2, \quad i \neq j \tag{11}$$

The construction with a latent random variable R_0, however, enables the probability density distribution of total claims to be written as a sum of two Binomial distributions

$$\mathsf{P}(L = x) = p \cdot W^n_{p_{|1}}(x) + (1-p) \cdot W^n_{p_{|0}}(x)\ , \tag{12}$$

where the parameters $p_{|0}$ and $p_{|1}$ are obtained from equations (9) and (10) in dependence of ϱ. We use a numerical approach to compute the security loading from its cumulative density function:

$$\mathsf{P}(L \leq x) = p \cdot \sum_{k=0}^{x} W^n_{p_{|1}}(k) + (1-p) \cdot \sum_{k=0}^{x} W^n_{p_{|0}}(k) \tag{13}$$

The compound distribution is bimodal for large ϱ and converges to a single Binomial distribution for $\varrho = 0$ (cf. Figure 2).

4 Analysis

Before we can answer the research question with the specified model, we need some preliminary assumptions for reasonable parameter settings. The risk bound ε and the respective interest rate i^* for the safety capital are in reality determined by the capital market. For practical reasons, however, we assume them to be constants with $\varepsilon = 0.005$ and $i^* = 0.1$. The degree of correlation ϱ is indeed very difficult to estimate since there is hardly any empirical data. For this reason, we decided to carry out our further analyses for different values of ϱ. The portfolio size n is deliberately not fixed because it depends on the market power of the system platform to be insured.

4.1 Can We Insure a Monoculture?

The model from Section 3 allows us, for each portfolio S, to compute the premium π at which coverage can be offered, depending on the parameters n, p, and ϱ. As, however, the demand-side determines whether there actually exists a market for this kind of policies, we will employ a simple and well-known model for demand of insurance coverage, which contrasts the expected incomes of utility maximising and risk averse individuals in two states (compare for instance [11, 34]): The *good state* yields an income of I_1 with probability $1-p$, whereas the *bad state* yields $I_0 = I_1 - D$ with probability p. Figure 3 depicts this structure of payoffs.

By buying insurance for complete coverage, an individual can improve his or her utility level from U_1 at point N (no insurance) to U_2 at point Γ_{E} (insurance at net premium solely) on the line of certainty. All points with equal utility are

www.manaraa.com

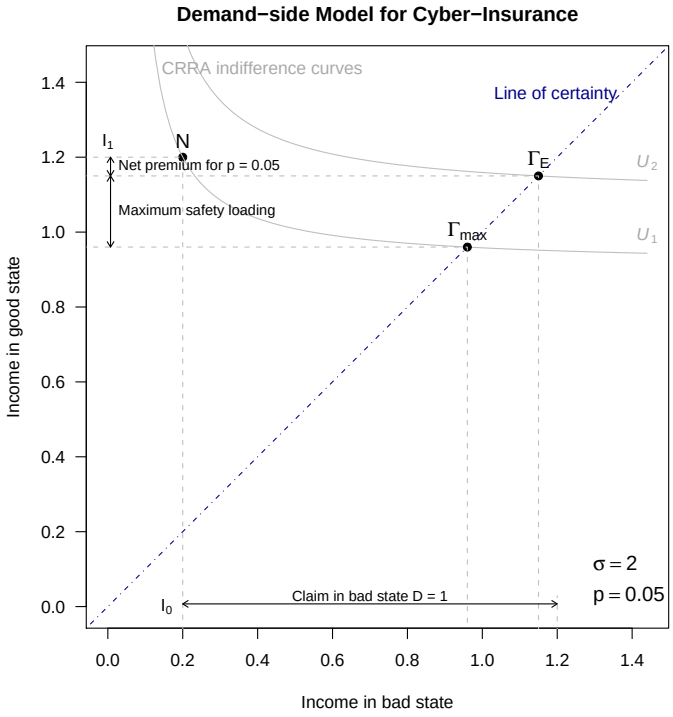

Figure 3: Demand for insurance in a state diagramme: Acquisition of insurance raises the payoff structure from point N to a higher level of utility in point Γ_{E}. The maximum willingness to pay for insurance is given at the intersection point $\Gamma_{\max}$ of the line of certainty and the initial indifference curve U_1.

marked as *indifference curves* in the figure. As in [21], we use a utility function of type CRRA.[5] This strictly monotone mapping assigns utility $u(y)$ to each income y

$$u(y) = \begin{cases} \frac{y^{1-\sigma}}{1-\sigma} & \text{for} \quad \sigma > 0, \sigma \neq 1 \\ \log(y) & \text{for} \quad \sigma = 1 \end{cases} \tag{14}$$

so that

$$\sigma = -\frac{u''(y)}{u'(y)} \cdot y = const, \tag{15}$$

with σ being a measure for risk aversion.

Now we should be able to determine the premium for which people are willing to buy insurance coverage: Rational individuals will demand (partial) coverage as long as they can improve their level of utility. An upper bound for the insurance premium is given in point $\Gamma_{\max}$, where the line of certainty intersects with

[5] *Constant Relative Risk Aversion*, see [28]

www.manaraa.com

the indifference curve of utility level U_1 through N. In combining this demand-side model with the proposed supply-side model for cyber-insurance, we can now numerically determine the maximum correlation ϱ for various parameter settings.

Table 1 shows the results for 2×3 different cases: σ varies between typical values for moderate ($\sigma = 1$) and strong ($\sigma = 3$) risk aversion. Income I_0 is modified in three levels, namely high ($I_0 = 0.2$), medium ($I_0 = 1$) and low ($I_0 = 5$) impact of losses. Note that I_1 is endogenous because we use normalised claim amounts ($D = 1$). As this scenario models a monoculture, we use approximated distribution functions for $n \to \infty$.

The estimated figures represent upper bounds for possible correlation and range between 0 and 1. Values of 1 denote that these types of risks are insurable despite any correlation. Lower numbers, however, indicate difficulties to offer coverage if the correlation in reality exceeds the values given.

When interpreting the results, we notice that in cases of highly risk averse insurance holders and for huge probabilities of losses, we find a potential market for coverage despite a possible correlation of claims. This is plausible and can be explained by the generally high level of premiums for risky ventures and the high willingness to pay of risk avoiding individuals: Here, the additional surcharge for correlated claims becomes a relatively unimportant decision criterion.

But it is even more noteworthy that for orthogonal products, already small correlation of claims can render a market solution unfeasible. It is, however, in particular these products—small policies against relatively unlikely losses—which are supposed to bring volume, liquidity, and thus maturity to the market for cyber-insurance. Regarding the above-mentioned positive outcomes of cyber-insurance in general, this finding can be considered as rather undesirable.

4.2 Different Premiums as Incentive to Diversify

This section takes a look at the effect of varying popularity of system platforms on cyber-insurance premiums. For this purpose we regard two exemplary platforms, representing two different portfolios (since risks differ across systems). The dominant platform $\mathcal{D}$ is characterised by a large portfolio size ($n_\mathcal{D} \to \infty$) and non-negligible correlation of claims $\varrho_\mathcal{D} > 0$. On the opposite, the alternative platform $\mathcal{A}$ suffers from a distinctively smaller portfolio size $n_\mathcal{A}$, but its components cause uncorrelated claims. This assumption is plausible, as, for instance, in a heterogeneous network, virus contagion solely via nodes of $\mathcal{A}$ is very unlikely. In addition, criminals have a notably less incentive to support rare platforms when cooking up computer viruses. For comparison, let both platforms be equally (in)secure in terms of total risk p.

Regarding the premiums, it is interesting to see from which correlation $\varrho_\mathcal{D}$ on upwards the alternative platform $\mathcal{A}$ is less expensive to insure, although it suffers from imperfect portfolio balancing due to the small portfolio size. Figure 4 shows the conditions for equal gross premiums at different probabilities of loss.

All combinations $(n_\mathcal{A}, \varrho_\mathcal{D})$ located right above the depicted lines have lower premiums for the alternative platform $\mathcal{A}$. Hence, the quantitative analysis of

www.manaraa.com

Table 1: Upper bounds for correlation of claims ϱ

		Risk aversion of insurance holder					
		moderate: $\sigma = 1$			strong: $\sigma = 3$		
Risk p	$I_0 =$	0.2	1.0	5.0	0.2	1.0	5.0
0.01		0.11	0.04	0.01	1.00	0.20	0.03
0.05		0.55	0.19	0.05	1.00	0.89	0.16
0.10		1.00	0.37	0.09	1.00	1.00	0.31
0.20		1.00	0.73	0.18	1.00	1.00	0.60

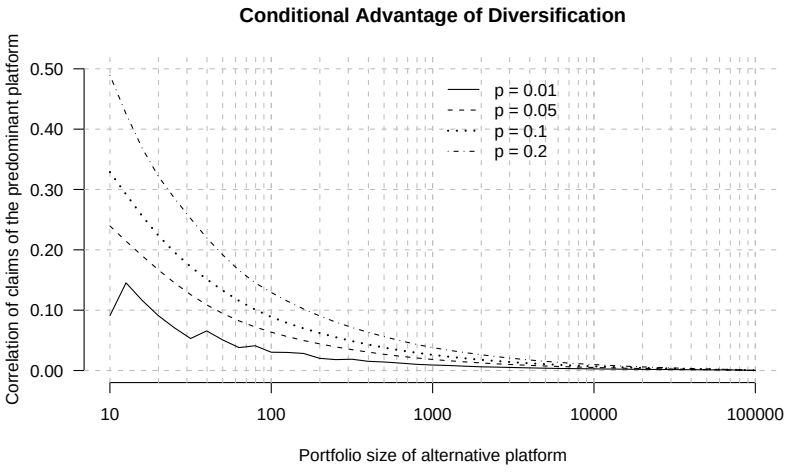

Figure 4: Lines of equal gross premiums $\pi_{\mathcal{A}} = \pi_{\mathcal{D}}$

www.manaraa.com

security aspects for the first time shows a market mechanism that does not imply a competitive advantage in the market leader's cost structure—contrary to the principles discussed in economics of information technology so far. However, it is still an open question whether this diversity bonus suffices to compensate the costs to deviate from a common platform and thus to break the automatism of "natural monocultures." The models given here cannot answer this questions.

Figure 4 further shows that a certain minimum portfolio size has to be reached to render the premiums for $\mathcal{A}$ below the ones of $\mathcal{D}$. We also expect this threshold to raise further when administration costs A are regarded as well, because every new platform requires extensive security assessment before insurance coverage can be issued. This barrier to market entry could effectively prevent a shift of equilibrium from one dominant platform $\mathcal{D}$ to a number of diverse platforms $\mathcal{A}_1 \ldots \mathcal{A}_m$. Again, what we find here seems to be a controversial result.

5 Discussion

The economic perspective to information security in general, and the idea of cyber-risk insurance in particular, are promising approaches to identify and tackle current security issues, leading to a reliable communication infrastructure for the information society. This paper—as well as many others—attempts to point out that proven concepts from "offline economics" do not always apply seamlessly to "online economics". We show in particular that losses generated by security breaches must not be treated in the same way as traditional indemnity insurance risks, because the structure of today's installed computer systems produces unwanted correlation of claims.

5.1 Possible Implications

The emerging of an insurance market for cyber-risks is presumed to have a number of positive consequences: (1) improved quantification of the security value of technical measures; (2) additional incentives to run current systems more securely and to develop ever more secure systems; (3) motivation to innovate for suppliers of alternative solutions due to reduced indirect costs. Along these immediate benefits, an evaluation of the ultimate effects on welfare and growth remains an open question to future research.

However, before the desirable consequences come into effect, a number of preconditions have to be fulfilled. *First*, a binding regulation of the responsibility and liability for security breaches is a key element for the development of a wide market for cyber-insurance [35]. *Second*, the analysis in this paper shows that coverage for a large part of the market cannot be supplied because of correlated claims due to the market structures in the IT industry.

Hence, it is possible that the positive consequences for the entire market can only be achieved with complementary subsidies of individual market segments. According to [21], this kind of regulatory intervention is already dis-

www.manaraa.com

cussed in the U. S., however for reasons different from correlation of claims. In addition, the considerations show that the development of a market for cyber-insurance—whether self-supporting, subsidised, or enforced by compulsory insurance—might go along with shifts in the market structure in relevant equipment markets.

Last but not least, we can easily imagine that manufacturers will react to the new situation and adapt their products: Computer systems may be designed deliberately to reduce co-occurrence of failures by technical means. This, in turn, will result in interesting connections with the research fields of fault tolerance and safety.

5.2 Limitations of the Model in Hand

Given the variety of possible implications from the reported findings, a critical view on the methodology and the underlying assumptions is particularly important. The model employed suffers from strong simplifications. It does not cover all relevant aspects of reality, for instance, varying claim amounts and different probability of losses for systemic and individual risk are left out. What is more, all parameters are arbitrarily chosen and the design as an individual risk model impedes the inclusion of empirical data [27]. Moreover, the literature is still controversial on the issue of whether the backward-looking—in terms of relying on historical data—insurance approach is generally suitable to deal with losses caused by strategic adversaries [30]. In addition, correlation-based measures of dependency are regarded as unsuitable for general risk management and should be replaced by alternative concepts, such as copulas [13].

The demand-side model used in Section 4.1 is based on some strong assumptions, which would have to be subject to critical investigation as well. For example, we must consider the robustness of the results towards modifications of the utility function. The same applies in case the individuals demand only partial coverage for their risks [25]. The comparison of platforms $\mathcal{D}$ and $\mathcal{A}$ (Section 4.2) is unrealistic because both platforms show the same probability of loss. Differences in financial and human resources between manufacturers determine the quality of their R&D and might eventually lead to further correlates between market structure and probability of loss. Also, considering the transaction costs for administration and information procurement could alter the above-shown relationship (presumably in favour of the market leader). For a comprehensive analysis, additional aspects of information economics have to be regarded as well: moral hazard, adverse selection, and regulation [6].

Therefore the interpretation and generalisation of the presented findings should always reflect the reservations and limitations addressed in this section. At the same time, this enumeration provides a number of unsolved questions for interdisciplinary research. Probably the most salient field for new research consists in empirical analyses to estimate the actual amount of claim dependency in monocultures. Delivering insights on the true dimension of the problem, this would allow for a clearer view on the relevance of further steps.

www.manaraa.com

5.3 Conclusion

A careful interpretation of the preliminary findings suggests that correlation of claims may indeed hinder the development of a mature market for cyber-insurance. Policies attempting to support cyber-insurance should simultaneously consider supporting a diversity of systems. Regulatory interventions, such as compulsory insurance, even if limited to certain segments, imply a change to the existing market mechanisms and could eventually lead to a shift in market structure. Against the background of these arguments, the following principle Ross Anderson [2] formulated in 1994, gains a new meaning:

> *"A trusted component or system is one which you can insure."*

References

[1] Roger Adkins. An insurance style model for determining the appropriate investment level against maximum loss arising from an information security breach. In *Workshop of Economics and Information Security (WEIS)*, Minneapolis, MN, 2004. Online available at `http://www.dtc.umn.edu/weis2004/adkins.pdf`.

[2] Ross J. Anderson. Liability and computer security: Nine principles. In Dieter Gollmann, editor, *Computer Security (ESORICS '94)*, LNCS 875, pages 231–245, Berlin Heidelberg, 1994. Springer Verlag.

[3] Ross J. Anderson. Why cryptosystems fail. *Communications of the ACM*, 33(11):32–40, 1994.

[4] Ross J. Anderson. Why information security is hard – an economic perspective, 2001. Online available at `http://www.cl.cam.ac.uk/~rja14/econsec.html`.

[5] Lawrence D. Bodin, Lawrence A. Gordon, and Martin P. Loeb. Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, 48(2):79–83, 2005.

[6] Karl H. Borch and Knut K. Aase. *Economics of Insurance*. North-Holland, Amsterdam, 1992.

[7] Jean L. Camp and Catherine Wolfram. Pricing security. In *Proc. of the CERT Information Survivability Workshop*, pages 31–39, Boston, MA, October 24–26 2000. Online available at `http://www.cert.org/research/isw/isw2000/papers/54.pdf`.

[8] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9:69–104, 2004.

www.manaraa.com

[9] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. A model for evaluating IT security investments. *Communications of the ACM*, 47:87–92, 2004.

[10] Daintry Duffy. Safety at a premium. *CSO Magazine*, December 2002. Online available at `http://www.csoonline.com/read/120902/safety.html`.

[11] Isaac Ehrlich and Gary S. Becker. Market insurance, self-insurance, and self-protection. *Journal of Political Economy*, 80:623–648, 1972.

[12] Paul Embrechts, Claudia Klüppelberg, and Thomas Mikosch. *Modelling Extremal Events for Insurance and Finance*. Springer Verlag, Berlin Heidelberg, second edition, 1999.

[13] Paul Embrechts, Alexander McNeil, and Daniel Straumann. Correlation: Pitfalls and alternatives. *Risk Magazine*, pages 69–71, May 1999.

[14] Dan Geer et al. CyberInsecurity – The cost of monopoly, 2003. Online available at `http://www.ccianet.org/papers/cyberinsecurity.pdf`.

[15] Lawrence A. Gordon and Martin P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457, 2002.

[16] Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3):81–85, 2003.

[17] Stefan Huschens, Konstantin Vogl, and Robert Wania. Estimation of default probabilities and default correlation. In M. Frenkel, U. Hommel, and M. Rudolf, editors, *Risk Management*, pages 239–259, Berlin Heidelberg, 2005. Springer Verlag.

[18] Insurance Information Institute. Computer security-related insurance issues, 2004. Online available at `http://www.iii.org/media/hottopics/insurance/computer/`. (Last access on February 24th, 2005).

[19] Peder Jungck and Simon S. Y. Shim. Issues in high-speed internet security. *IEEE Computer*, pages 36–42, July 2004.

[20] Karthik Kannan and Rahul Telang. An economic analysis of markets for software vulnerabilities. In *Workshop of Economics and Information Security (WEIS)*, Minneapolis, MN, 2004. Online available at `http://www.dtc.umn.edu/weis2004/kannan-telang.pdf`.

[21] Jay P. Kesan, Ruperto P. Majuca, and William J. Yurcik. The economic case for cyberinsurance. *Illinois Law and Economics Working Paper Series*, 2004. Online available at `http://ssrn.com/abstract=577862`.

[22] Robert Kneuper and Bruce Yandle. Auto insurers and the air bag. *Journal of Risk and Insurance*, 61:107–116, 1994.

www.manaraa.com

[23] Thomas Mack. *Schadenversicherungsmathematik [Mathematics of indemnity insurance]*. Number 28 in Schriftenreihe Angewandte Versicherungsmathematik. Verlag Versicherungswirtschaft, Karlsruhe, Germany, 1997.

[24] Rebecca T. Mercuri. Analyzing security costs. *Communications of the ACM*, 46:15–18, 2003.

[25] Jan Mossin. Aspects of rational insurance purchasing. *Journal of Political Economy*, 76:553–568, 1968.

[26] Andy Ozment. Bug auctions: Vulnerability markets reconsidered. In *Workshop of Economics and Information Security (WEIS)*, Minneapolis, MN, 2004. Online available at `http://www.dtc.umn.edu/weis2004/ozment.pdf`.

[27] Harry H. Panjer and Gordon E. Willmot. *Insurance Risk Models*. Society of Actuaries, Schaumburg, IL, 1992.

[28] John W. Pratt. Risk aversion in the small and in the large. *Econometrica*, 32:122–136, 1964.

[29] Daniel J. Ryan and C. Heckmann. Two views on security software liability. *IEEE Security & Privacy*, 1:70–75, 2003.

[30] Stuart E. Schechter. *Computer Security Strength & Risk: A Quantitative Approach*. PhD thesis, Harvard University, Cambridge, MA, 2004.

[31] Bruce Schneier. Hacking the business climate for network security. *IEEE Computer*, pages 87–89, April 2004.

[32] Carl Shapiro and Hal R. Varian. *Information Rules. A Strategic Guide to the Network Economy*. Harvard Business School Press, 1998.

[33] Kevin J. Soo Hoo. *How Much Is Enough? A Risk-Management Approach To Computer Security*. PhD thesis, Stanford University, CA, 2000. Online available at `http://cisac.stanford.edu/publications/11900/`.

[34] Hal R. Varian. *Intermediate Microeconomics – A Modern Approach*. W. W. Norton & Company, New York, 5th edition, 1999.

[35] Hal R. Varian. Managing online security risks. *New York Times*, June 1st, 2000. Online available at `http://www.nytimes.com/library/financial/columns/060100econ-scene.html`.

[36] William Yurcik and David Doss. Cyberinsurance: A market solution to the internet security market failure. In *Workshop on Economics and Information Security (WEIS)*, Berkeley, CA, 2002. Online available at `http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurit%y/`.

Acknowledgement The author wants to thank Ivan Alves and Karen Kreutel for their helpful comments.

www.manaraa.com