Bartholomae, Florian W.

Working Paper

Networks, hackers, and nonprotected consumers

Volkswirtschaftliche Diskussionsbeiträge, No. 2013,3

Provided in Cooperation with:
Bundeswehr University Munich, Economic Research Group

Suggested Citation: Bartholomae, Florian W. (2013) : Networks, hackers, and nonprotected consumers, Volkswirtschaftliche Diskussionsbeiträge, No. 2013,3, Universität der Bundeswehr München, Fachgruppe für Volkswirtschaftslehre, Neubiberg

This Version is available at:
https://hdl.handle.net/10419/81127

der Bundeswehr
Universität München

Fachgruppe für Volkswirtschaftslehre
Economic Research Group

VOLKSWIRTSCHAFTLICHE DISKUSSIONSBEITRÄGE

WORKING PAPERS IN ECONOMICS

Florian W. Bartholomae

Networks, Hackers, and Nonprotected Consumers

25. Jg. (2013), Nr. 3

Autoren / Authors

Florian W. Bartholomae
Universität der Bundeswehr München / Bundeswehr University Munich
Institut für Ökonomie und Recht der globalen Wirtschaft / Department of Economics and Law of the Global Economy
Werner-Heisenberg-Weg 39
85577 Neubiberg – Germany
florian.bartholomae@unibw.de

Herausgeber / Editors

Bis zum Jahr 2008 (20. Jg.) erschien diese Reihe unter dem Titel:
Until 2008 published as:
„Diskussionsbeiträge des Instituts für Volkswirtschaftslehre der Universität der Bundeswehr München“.

Networks, Hackers, and Nonprotected Consumers

Florian W. Bartholomae

July 2013

Abstract

In this paper a network model is developed in which three players sequentially choose their strategies. In the first stage, a profit–maximizing network firm chooses the price and thus the size of the network. In the second stage the consumers decide whether to join in the network or not. In the last stage a hacker has the opportunity to hack the network and cause damage to the consumer. The success of hacking is based on the protection of the customers. Whereas in the first part of the paper this is given exogenously it is endogenized later on. In an extension, the utility of the hacker as well as the consumers includes psychological costs, thus allowing some further insights. Finally, policy implications are given implying better international cooperation of the law enforcement authorities.

Keywords: hacking ∘ network size ∘ cloud computing ∘ nonprotected consumers

JEL–classification: D03 ∘ L1 ∘ L86 ∘ K4

1 Introduction

The spread of high–speed Internet access as well as almost unlimited data storage has lead to significant changes in economic activities and the emergence of new business concepts. One recent innovation in business–to–business (as well as business–to–consumer) electronic commerce is cloud computing. Firms engaged in cloud computing offer computing services like storage and data processing to other firms and individuals.[1] There are several advantages of this service (Boss et al., 2007): Costs are reduced since only actual usage has to be paid and no further software is needed, which in turn reduces the requirements for provision of powerful computers; coordination and information costs are reduced since data and software is almost always and everywhere available. However, there are disadvantages as well (Abadi, 2009). One of them is the dependence on a third–party company and thus the danger of hold–up. In particular security issues have to be mentioned, since the data is not stored in a closed local area (within the company's area of influence) but on (sometimes untrusted) servers somewhere else that have to be accessed via the Internet (which itself increases security issues).

Besides companies also private persons store their data on third–party servers (even though they sometimes do not realize this). Data from almost every activity in the web is collected and stored. Especially the data collection activities of *Facebook* or *Google* are often a subject of great controversy. Furthermore, other companies have huge online data collections of their customers as well.

Both, companies as well as individuals, expose themselves to security issues. Many recent incidents have demonstrated this impressively: For instance, the hacking of Sony's Playstation network, the hacked Microsoft store in India, or the Chinese hacking attacks against many western firms. Hacking is one field of cybercrime,[2] *i.e.*, a crime that makes

[1] According to the NIST definition "Cloud computing is a model for enabling ubiquitous, convenient, on–demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Mell and Grance, 2009, 3)

[2] A brief history of hacking can be found in Leeson and Coyne (2005). Kshetri (2010) analyzes sev-

use of a computer network at some time (Kshetri, 2006, 33). This sort of crime differs from crime in "realspace". According to Katyal (2001), there are three important differences: It is quite cheap to commit cybercrime; further parties — such as the Internet Service Provider — are added to the "traditional perpetrator–victim scenario of crime" (Katyal, 2001, 1007); and most crimes stay unobservable to third or even second parties.

The structure of the paper is as follows: In the next section 2 the basic model is developed on which the first findings in section 3 are based. In section 4 the model is extended by endogenizing the probability of successful hacking. The motives for hacking and its effects on the previously derived results are analyzed in section 5. Finally, section 6 gives the conclusion.

2 Model Set–up

The analysis is based on a model introduced by Shy (2001, ch. 5.2). In his model (below referred to as standard network model[3]) he analyzes the profit–maximizing price setting of network firm. His analysis is extended in this paper by adding a third player, a hacker, besides the monopolistic network firm and its consumers.

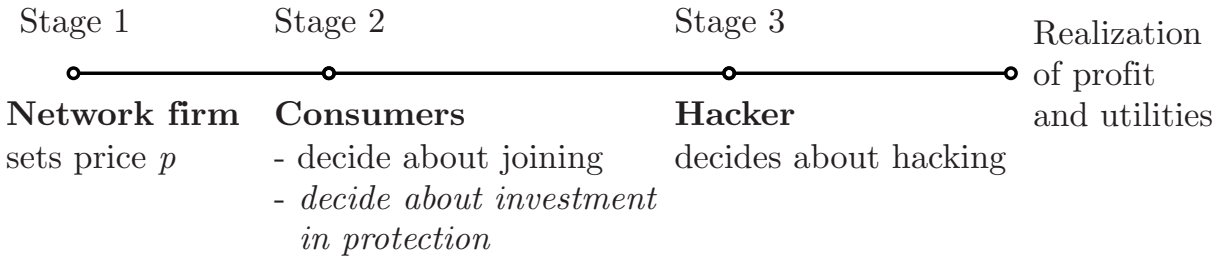
The model developed here consists of three stages, in which each of the three risk–neutral players — the network firm, the consumers and the hacker — decide about their strategies. The information structure is characterized as perfect and complete. In the first stage the firm decides about the price charged for the network service, which in turn determines the size of the network. In the second stage a mass of consumers decides, whether to join in the network or not. Consumers can be private individuals as well as firms using the cloud computing system of a third–party provider. Due to network effects three possible outcomes may arise: no one joins (stable equilibrium), a low (instable equilibrium) or a high number of consumers join (stable equilibrium). To avoid this problem

eral aspects of this special "industry". Beside cybercrime, cyberterrorism and hacking attacks against governments and institutions are of high importance to the economy as a whole, see e.g. Adams (2001).

[3]For an overview of network economics see Shy (2011).

of multiple equilibria, the assumption is made that consumers have perfect foresight, *i.e.*, consumers can correctly anticipate the number of other consumers joining in the network (Shy, 2001, 20).[4] In the third stage the hacker decides whether to hack the network or not. Finally, the payoffs are realized. The structure of the game, the players and their strategies are summarized in fig. 1.

Figure 1: Structure of the game, players and strategies.



The strategies of the players are now considered in more detail. The monopolistic network firm's profit function is given by

$$\pi = (p - c)N - F, \tag{1}$$

where p denotes the price of the network access, N the size of the network (*i.e.*, the number of users), c the marginal cost, and F the fixed cost of the network. The firm chooses the price of the network access.

The individual consumer's (expected) utility is given by

$$U_C = \begin{cases} (1-x)N - p & \text{if she joins (no hacking),} \\ (1-x)N - p - \chi D & \text{if she joins (hacking possible),} \\ 0 & \text{if she does not join,} \end{cases} \tag{2}$$

where the consumer's preference for the network x is uniformly distributed between 0

[4]Otherwise the monopolist has to deal with issues like the attraction of a "critical mass" of consumers, cf. Cabral et al. (1999).

and 1 with density η. That is, the higher x, the lower the utility of the network. The utility depends on the network size N as well, which is determined by ηx. If hacking takes place and is successful, the consumer incurs a damage D. This captures the loss of data as well as the damage following hacking like credit card fraud or identity theft. It may also include ransom that has to be paid to the hacker in order to regain access to one's data. For simplicity, all consumers suffer the same amount of damage. The share of nonprotected consumers is given by χ. These consumers are responsible of the security holes in the network due to careless handling of passwords, use of outdated software, lack of knowledge of how to handle with security issues, etc. The hacker is able to use this "open gates" to enter the network. Once the access is gained, the hacker is not only able to steal the data of the nonprotected consumers but also the data of all other network users. Thus in contrast to the standard network model, an additional network user has a negative externality on all other users, if she is nonprotected. In the first step, the share of nonprotected consumers is assumed to be exogenous. This lack of protection weakens the network security, thus influencing the probability of a successful hacking attempt. For simplicity I assume this probability to be χ as well. To sum up, if the consumer joins in the network and hacking is possible, she has to bear an expected damage of χD due to hacking.

Finally, the hacker decides whether to hack the network or not and thus his (expected) utility is given by

$$U_H = \begin{cases} \chi N v - \rho S & \text{if he hacks,} \\ 0 & \text{if he does not hack,} \end{cases} \tag{3}$$

where v denotes the value of the data of one network user to the hacker, that is the money he can earn from the (mis)use of her data. Again, the value of each consumer's data is likewise valuable to the hacker. It is plausible to assume $v < D$, *i.e.*, the hacker's value of the data is lower than the damage caused to the consumer. The consumer's damage

consists not only of the actual gain of the hacker[5] but also of additional costs arising from the need of additional insurance, reporting the crime, identification of the extent of the damage, going to court, etc. In the case of hacking — successful with probability χ — the hacker get caught with probability ρ (independent of hacking success) and is sentenced to pay a fine of S.

3 Baseline Case

First, I consider a scenario in which the share of nonprotected consumers is assumed to be given exogenously. The game is solved by backward induction in order to find the subgame perfect equilibrium.

In the last stage of the game the hacker decides, whether to hack the network or not. Given his utility specified in (3) utility from hacking is larger than utility from not hacking if

$$x \geq \tilde{x} \equiv \frac{\rho S}{v\chi\eta}, \tag{4}$$

since $N = \eta x$. Thus, $\tilde{x}$ describes the user threshold that determines the network size in order to generate a positive expected net value of the network for the hacker. Plausibly, if the expected fine increases, a larger network size, $\tilde{N} = \eta\tilde{x}$, is necessary, whereas a larger valuation of the network and/or a higher share of nonprotected users decreases the necessary network size.

Interestingly, there seems to be empirical evidence that this threshold should not be very high. First, there are many reasons, why the hacker's probability of getting caught is quite low. According to Kshetri (2006, 2010) law enforcement agencies are often inexperienced and/or overwhelmed. Furthermore, victims are often non–cooperative since they are afraid of losing reputation and therefore are even willing to pay ransom to criminals.

[5]Besides other factors there is some redistribution from the consumer to the hacker, e.g. in case of ransom.

These factors negatively influence the probability of successful prosecution. Second, in some countries the fine for Internet crime is quite low or even non–existent (Kshetri, 2006, 37).[6] Therefore the numerator of (4) must be quite low as must $\tilde{x}$ which actually implies a big incentive for (rational) hacking even in small networks.

In the second stage consumers decide to join in the network if

$$p \leq \eta\hat{x}(1-\hat{x}) - \chi D. \tag{5}$$

This condition is only valid for the case of hacking, *i.e.*, (4) is fulfilled, $\hat{x} \geq \tilde{x}$. Otherwise, no damage incurs and (5) simplifies to $p \leq \eta\hat{x}(1-\hat{x})$ as in the standard network model (cf. Shy, 2001, 111).

As the firm chooses the price in the first period, (5) has to be reformulated to $\hat{x} = 0.5 + \sqrt{0.25 - (p+\chi D)/\eta}$.[7] The firm's profit in the first stage in case of hacking is given by

$$\pi_H = (p-c)\eta\left(\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{p+\chi D}{\eta}}\right) - F. \tag{6}$$

Maximizing with respect to the price and solving for the equilibrium price yields

$$p^{**} = \frac{\eta}{9}\left(1 + \sqrt{1 - \frac{3}{\eta}(c+\chi D)}\right) + \frac{1}{3}(c - 2\chi D) \tag{7}$$

The second solution of the quadratic equation has no economic relevance.[8] Since $\partial p^{**}/\partial D < 0$, the firm has to lower its price as the possible damage for the consumers from hacking increases.

[6] This is also problematic from another perspective, because this can lead to a shift of traditional crime activities to the web as punishing is disproportional (Katyal, 2001, 1005f).

[7] Since (5) is a quadratic equation, the reformulation yields two solutions. Since we know that the larger network size yields a stable equilibrium, the larger expression was chosen.

[8] The first order condition of (6) is given by $d\pi/dp = (2c - 6p + \eta - 4\chi D + \sqrt{\eta[\eta - 4(p+\chi D)]})/(2\sqrt{\eta[\eta + 4(p+\chi D)]})$, and the second order condition by $d^2\pi/dp^2 = 2\eta(c + 3p - \eta + 4\chi D)\{\eta[\eta - 4(p+\chi D)]\}^{-3/2}$. Only for the larger expression a negative second order condition is guaranteed.

The associated network size calculates to

$$N^{**} = \frac{\eta}{3}\left(1 + \sqrt{1 - \frac{3}{\eta}\left(c + \chi D\right)}\right), \tag{8}$$

and the firm's profit is given by

$$\pi^{**} = \frac{1}{27}(\eta + H)\left[\eta + H - 6\left(c + \chi D\right)\right] - F, \tag{9}$$

with $H = \sqrt{\eta\left[\eta - 3\left(c + \chi D\right)\right]}$. Considering this expression, the expected damage of the consumers has the same effect on profit as an increase in marginal cost of the firm.

Without hacking the profit–maximizing network price is

$$p^* = \frac{\eta}{9}\left(1 + \sqrt{1 - \frac{3c}{\eta}}\right) + \frac{c}{3} \tag{10}$$

and the associated network size is given by

$$N^* = \eta(1 + \sqrt{1 - 3c/\eta})/3. \tag{11}$$

The firm has the possibility to choose a price that limits the network size to a level where no hacking takes place, *i.e.* $x \leq \tilde{x}$. This price calculates to

$$p \geq \tilde{p} \equiv \frac{\rho S(v\eta\chi - \rho S)}{\eta(v\chi)^2} - \chi D. \tag{12}$$

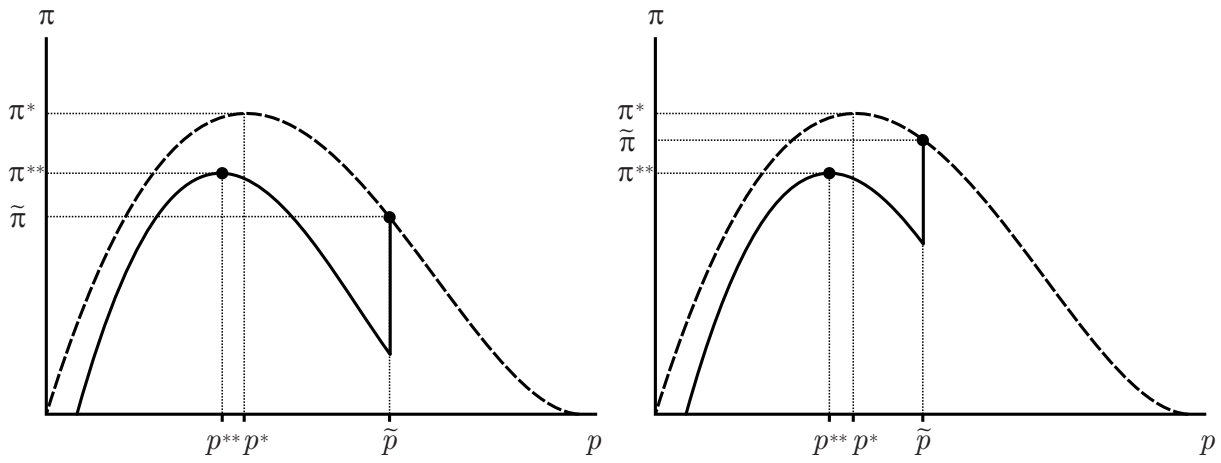
In this case profit is given by

$$\tilde{\pi} = \frac{\rho S\left[\rho S(v\eta\chi - 1) - \eta(v\chi)^2(c + \chi D)\right]}{\eta(v\chi)^3} - F. \tag{13}$$

As the price was chosen accordingly, the network size is $\tilde{N} = \eta\tilde{x}$.

Proposition 3.1 *Although compared to the non–hacking scenario in case of hacking the*

Figure 2: Comparison of profits.



price for the network access will be lower in order to compensate the consumers for the potential damage, the network size will be lower. Under certain conditions the price will be higher because the resulting limitation of the networks size prevents hacking, allowing the monopolistic network firm a higher profit.

Proof Hacking will take place, if condition (4) is fulfilled. Comparison of (7) and (10) shows that the price in case of hacking will be lower, if the consumer's expected damage, χD, has a positive value. Furthermore, comparison of (11) with (8) shows that the network size in case of hacking is lower as long as χD is positive.

The network firm has the possibility to render hacking unattractive by limiting its network size and avoiding that $x \geq \tilde{x}$ is met. This is profitable if $\pi^* \geq \tilde{\pi}$, *i.e.*, (13) is larger than (9). Since the formal comparison is tedious, fig. 2 illustrates the main findings. The continuous curve describes the network firm's profits in case of hacking and the dashed curve describes profits if no hacking occurs. The profit level $\tilde{\pi}$ is associated with two prices. However, only the higher price guarantees a limitation of the network size, thus this price will be chosen by the firm. The firm decides only for this price $\tilde{p}$, if it is higher compared to both p^{**} as well as p^* (otherwise $\tilde{p}$ would have no limiting effect). In case of $\tilde{p} < p^*$ the profit–maximizing price would ensure that no hacking would occur since the network size is too small to be profitable for the hacker.

In the situation depicted on the left side of fig. 2 hacking is not prevented by the firm, whereas in the situation on the right side the firm decides for the network size limiting price $\tilde{p}$ in order to prevent hacking and increase profit. □

Proposition 3.2 *In case of hacking, the consumer's expected total damage will be totally born by the monopolistic network firm. Hacking does eventually decrease total welfare.*

Proof Equation (9) showed that expected damage actually increases marginal cost. Thus, profit in case of hacking compared to the hacking–free case decreased by $N \times \Delta c$. Since $\Delta c = \chi D$, the difference in profits is $N\chi D$, *i.e.*, the profit is reduced by overall expected damage of the consumers and the firm indirectly bears their burden — thus there is a perfect pass–trough from the consumers to the monopolistic network firm.

The change in total welfare caused by hacking, ΔWF, can be calculated as the difference between the hacker's utility gain (see (3)) and the firm's profit loss,

$$\Delta \text{WF} = \chi N(v - D) - \rho S. \tag{14}$$

The first term is positive, if the hacker's (personal) valuation of the data is larger than the consumer's damage. This term may be called the "expected net gain from hacking". As $v < D$ (implying a negative "gain") overall welfare will be reduced by hacking. □

In a next step, it is analyzed what optimal fine a legislative authority should set in order to prevent hacking, allowing firms not to carry this over with its price setting. This critical fine can be calculated by the threshold for hacking given by (4) and the profit–maximizing threshold user indirectly given by (8), $x^{**} = N^{**}/\eta$. Both thresholds have to be equal, *i.e.*, the hacker has no incentive to hack at the optimal (profit–maximizing) network size,

$$S \geq \frac{v\chi}{3\rho}\left(\eta + \sqrt{\eta[\eta - 3(c + \chi D)]}\right). \tag{15}$$

Thus, when setting a fine, the legislative authority should take the following factors into account: First, the observable monetary value of the network should serve as a basis. The revenue of the provider can be used as a proxy for this value, which should be highly correlated with the hacker's valuation of the network. Second, the damage done by the hacker should increase the fine. The damage should be estimated quite liberal in order to include not only the (observable) explicit costs, but also the implicit costs for the user. Third, the fine could be lower, as the probability of catching the hacker increases. However, due to international hackers beyond a national authority's jurisdiction as well as overwhelmed criminal prosecution, the probability tends to be quite low, making a higher fine even more necessary.

4 Consumers' Decision for Protection

Now every consumer has the possibility of investing I in order to prevent hacking. The assumption is made that the higher the consumer's preference for the network, the higher the willingness to invest in order to prevent hacking. Disutility from investment is given by xI, which implies heterogeneity in investment costs. This assumption seems plausible since consumers differ in their computer literacy and show different costs in securing their network accounts. The specification implies further that an individual with the highest valuation at $x = 0$ has no disutility from investment. This specification keeps the analysis tractable and is justified because a higher preference for network and computer services may also promote computer skills and lowers the investment costs.

Additionally the assumption is made that in the case of hacking, the probability of the hacker's success to hack a nonprotected consumer is 1, whereas in the case of a careful consumer this probability is 0.[9] Since the investment is only necessary, if hacking is possible, a consideration of the non–hacking case is skipped. With all these modifications,

[9]This assumption is in line with Cremonini and Nizovtsev (2006) who show that a hacker chooses that system that is less protected compared to all others.

(2) changes to

$$U_C = \begin{cases} (1-x)N - p - \chi D & \text{if she joins and gets hacked,} \\ (1-x)N - p - xI & \text{if she joins and invests,} \\ 0 & \text{if she does not join.} \end{cases} \tag{16}$$

According to the modified utility function, the consumer invests in security, if

$$(1-x)N - p - xI \geq (1-x)N - p - \chi D \quad \Leftrightarrow \quad x_I \leq \chi D/I. \tag{17}$$

The threshold user is given by $x \leq \hat{x} \equiv 0.5\left(1 + \sqrt{\mu[\mu - 4(p + \chi D)]}/\mu\right)$. For low values of x, *i.e.*, a high valuation of the network, investment is always better compared to the situation of getting hacked, since the investment barely reduces utility compared to the expected damage of hacking. The critical value x_I decreases as the expected damage decreases — the consumer is less willing to invest in security even if the damage itself would be large. This is in line with Huang et al. (2008) who show that risk–averse firms only invest in security if the potential damage reaches a certain level.

Proposition 4.1 *If security is costly, there will always be a share of nonprotected consumers regardless of the level of expected damage or security investment costs.*

Proof For a given network size with threshold consumer x, the share of nonprotected consumers χ is given by $1 - x_I/x$ or

$$\chi = \frac{xI}{D + xI}. \tag{18}$$

This implies reasonable results: An increase in the costs of security increases the share disproportionately, whereas an increase in the damage from hacking reduces the share (disproportionately as well). The share of nonprotected consumers can never be 0 if

$I > 0$. In this case some consumers with $x > 0$ would not invest, since they would not fear getting hacked. The share would increase. □

Considering (18), the network firm's profit function, (6), changes to[10]

$$\pi_{H,I} = \left[\eta x(1-x) - \frac{xI}{D+xI}D - c\right]\eta x - F. \tag{19}$$

The first order condition is given by

$$\frac{\partial \pi}{\partial x} = \eta[\eta x(2-3x) - c] - \eta D x I \frac{2D+xI}{(D+xI)^2}. \tag{20}$$

The resulting user threshold is given by $x^*_\chi(\eta, c, I, D)$, which determines the networks size $N^*_\chi = \mu x^*_\chi$ as well as $p^*_\chi(\eta, c, I, D)$.[11] The effects of the variables are comprehensible: An increase in η increases the network size, whereas an increase in c, I or D decreases the network size. Since the network size, (8), decreases in χ and the endogenized χ increases in I, a decrease of x in I is obvious. However, the negative effect of D dominates its correcting effect on χ.

Changes in the exogenous variables show the expected effects on the network's price, as well. An increase in the marginal cost increases the price chosen by the network firm. An increase in D or the investment costs forces the monopolistic firm to lower its price (see (7)) since it has to consider that the network is rendered more unattractive to its customers.

Proposition 4.2 *High costs of security measurements to prevent hacking may lead to a collapse in the network size.*

[10] For a more compact mathematical expression, the profit was formulated as a function of x instead of p. However, in the setting of a monopolistic firm maximization of $\pi(x)$ with respect to x and then calculation of p is identical to maximization of $\pi(p)$ with respect to p and solving for the price.

[11] In fact this maximization problem yields four extensive solutions. However, it is possible to formalize the effects of the exogenous variables on x without considering the explicit solution. This is done in the appendix.

Proof The optimal network size, ηx_χ^*, has to be evaluated in the modified hacking condition given in (4),

$$x \geq \tilde{x}_\chi \equiv \frac{\rho S}{v\eta} \frac{D + x_\chi^* I}{x_\chi^* I}. \tag{21}$$

An increase in I also increases $\tilde{x}_\chi$.[12] This seems quite counterintuitive: Intuitively, if less consumers invest in security, the change of successful hacking increases, whereby the (probably) low value of the network is offset. However, since higher security costs render these measurements unattractive, more consumers remain nonprotected and thus the danger of getting hacked for the network users increases. This reduces the overall network size and thus the value for the hacker, respectively. In fact this dynamic is similar to the collapse of the market in Akerlof (1970)'s market for lemons example ending in a situation, in which no consumer joins and thus no hacker hacks. □

There is evidence that the necessary investments of the victims are low as it may only imply better training of the users (Kshetri, 2006, 38). Obviously, it is also in the interest of the network firm to design its service in the first place in a way that low security costs are ensured, since this in turn increases its profit.

5 Types of Hackers and Psychological Costs

The analysis so far did not investigate the hacker's motives and their potential implications on the analysis. According to Leeson and Coyne (2005) there are several motives for hacking. They differentiate "good hackers", "bad hackers", and "greedy hackers". "Good hackers" simply seek the challenge of hacking a system or have rather noble aims like making the world a better place, whereas "bad hackers" seek for notoriety and fame in

[12] The effects of changes in the other variables are plausible: A rise in D increases the critical hacking value, since more consumers invest in security measurements and thus rendering hacking unsuccessful. Increases in the marginal costs of the network firm, the probability of getting caught or in the fine raise the necessary network size, whereas an increase in the value of the data decreases the threshold $\tilde{x}_\chi$.

their (hacking) community. The last group, "greedy hackers", want to earn income from their activities. They use the data for credit card fraud, sell the data or are even hired by other criminals. According to this classification, only the last type of hacker was considered in the previous analysis.

To explicitly take account for the other types of hacker, the utility in case of hacking (see (3)) is modified to $\chi N\theta v - (1+\psi_h)\rho S$. The parameter $\theta \in [0,\infty)$ was added to describe the hacker's (personal) valuation of the data beyond their monetary value. This valuation varies across the three types of hackers: The "good hacker" should be described by $\theta < 1$ or even $\theta = 0$, since he has no intention to (mis)use the data; the "bad hacker" has some extra intrinsic motivation for hacking and thus valuates his success higher than his monetary gain, *i.e.* $\theta > 1$; the "greedy hacker" is only interested in the money he can earn and thus $\theta = 1$ (the previous specification).

Furthermore, $\psi_h \in [0,\infty)$ is introduced. This parameter denotes the hacker's additional psychological costs of the fine.[13] These may arise from direct confrontation with his victims or his insight of damage caused by him. This costs also depend on the type of the hacker: Whereas a "greedy" as well as a "bad" hacker may incur only low psychological costs (low ψ_h)[14], a "good" hacker may suffer from large costs, since he does not want to harm anyone in the first place.[15]

The concept of (additional) psychological costs is also introduced in the specification of the user's utility. If the consumer joins and her account is hacked, her utility changes to $(1-x)N - p - (1+\psi_c)\chi D$ (second case of (2)). In this case, the parameter $\psi_c \in [0,\infty)$ denotes the consumer's psychological costs of the damage, *i.e.*, for $\psi_c = 0$ the individual only bears the actual damage and has no further costs (the original specification),

[13]The modification of the hacker's utility is quite similar to the cost–benefit calculus of Kshetri (2006, 36ff). In line with him, the value of the network vN catches monetary as well as psychological benefits. The perceived fine $(1+\psi_h)S$ catches monetary as well as psychological costs of committing the crime, and ρ catches the probability of arrest as well as of conviction.

[14]A "bad hacker" could even show a lack of understanding that hacking is unlawful even implying $\psi_h < 0$, however, I do not explicitly consider this case.

[15]In the original specification, no psychological costs were considered, $\psi_h = 0$.

whereas for $\psi_c > 0$ she suffers from costs beyond the pure monetary damage.[16] This additional psychological costs include e.g. fear of future hacking, loss of sense of security or exaggerated attention in future transactions.

This modifications allow some interesting further insights. The threshold derived in (4) changes to

$$x \geq \tilde{x}_\psi \equiv (1 + \psi_h)\rho S/\theta v \chi \eta, \tag{22}$$

that is, the more the criminal suffers from psychological costs, the higher $\tilde{x}$. These costs appear to be quite low as there is no physical contact between the offender and the victim which probably could change general moral behavior (Johnson, 2004, 32).[17] As the perceived damage of the consumers increases, they are less willing to pay a high price for using the network, *i.e.*, (5) changes to $p \leq \eta\hat{x}(1 - \hat{x}) - (1 + \psi_c)\chi D$.

The modifications allow to state the following proposition (a more general formulation of theorem 2):

Proposition 5.1 *If the firm is confronted with a "bad hacker", its profit is reduced the most compared to the hacking–free scenario, whereas in case of a "good hacker" the profit reduction is least. If the consumers face psychological costs from hacking, the network firm's profit is reduced by more than expected monetary damage. In total, overall welfare will be further reduced by psychological costs.*

Proof Since a "good hacker" faces higher psychological costs than the "bad hacker", his perceived fine is larger. Additionally his valuation of the data is lower. According to (22) both factors increase the threshold for hacking and make hacking less likely. If the firm

[16] According to Taylor and Mayhew (2002) indirect costs from crime can be up to 70% or so of direct costs.

[17] Furthermore, if we relax the assumption of risk neutrality, the incentive for hacking increases further. As Becker (1968, 178) and Becker (1995, 6) note, criminals are "risk takers, not risk avoiders."

decides to render hacking unattractive, its profit is given by

$$\tilde{\pi} = \frac{\sigma\left[\sigma\left(v\eta\chi - \sigma\right) - \left(c + \psi_c\chi D\right)\eta(\theta v\chi)^2\right]}{\eta(\theta v\chi)^3} - F, \tag{23}$$

with $\sigma = (1+\psi_h)\rho S$. Again, in case of a "good hacker" ($\psi_h > 0$), profit will be larger.

As expected damage changes to $(1+\psi_c)\chi D$, the markup on marginal cost in (9) changes accordingly, thus hacking decreases profit by $(1+\psi_c)\chi N D$. Therefore, for $\psi_c > 0$ the firm has not to bear the pure monetary damage but the perceived damage of the consumers.

According to theorem 2, the change in total welfare calculates to

$$\Delta\mathrm{WF}_\psi = \left[\chi N(\theta v - D) - \rho S\right] - \left(\chi N\psi_c D + \psi_h\rho S\right). \tag{24}$$

The first bracket shows the actual welfare change of hacking, whereas the second bracket depicts the psychological costs. The actual welfare change is similar to (14) except for θ which has a positive effect on welfare by increasing the net gain from hacking. This effect only emerges in case of a "bad hacker". Psychological cost decrease welfare in any case, thus offsetting any positive effect of hacking and decreasing welfare even beyond (14). □

The existence of psychological costs and different types of hackers also have an effect on the optimal fine,

$$S_\psi \geq \frac{\theta v\chi\eta}{3(1+\psi_h)\rho}\left(1 + \sqrt{\eta[\eta - 3(c + (1+\psi_c)\chi D)]}\right). \tag{25}$$

Comparison with (15) suggests that potential low psychological costs of committing Internet crimes like hacking should be considered, thus leading to a fine much higher compared to the network's value. To a certain extent, this may also deter "bad hackers" who — from a pure monetary point of view — may act quite irrational.

6 Conclusion

This paper extended the standard network model by introducing a third player, the hacker. It was shown that the damage caused by this cyber–criminal reduces the network size, the profit of the network firm as well as overall welfare. Although the network firm may set a higher price to limit its network to a size where it becomes unattractive for the hacker, it will have in almost no case the incentive to do so as its profit would be reduced dramatically. This is caused by the fact that the maximum network size that is necessary to render hacking unattractive is very low due to many institutional problems. Furthermore, the negative welfare effect caused by hacking may be underestimated due to neglect of psychological costs of the consumers (as well as of the hackers).

An important policy implication arises. It is necessary to have the possibility to sentence the hacker to render hacking unattractive in some cases. The higher the expected fine, the less likely a hacker decides to hack. Therefore a problem arises, if there is no possibility to sentence the hacker.[18] In this case the hacker will always hack the network and no firm has the possibility to prevent hacking if it limits the network size. Furthermore, no network user can count on a deterrence of the hacker and has to invest in security measurements on herself. As this problem is obvious in an international context, a global legal cooperation is required. Many industrialized countries are already working on such international cooperations (Kshetri, 2006, 35) to encounter this type of crime that can have severe effects on the economy.

[18] This is the case, if $\rho S = 0$ in (4).

Appendix

Although (20) is explicitly solvable, the expression is very complicated. Since only in the effects of changes in the exogenous variables on the user threshold or the network size, respectively, are of interest, it is more convenient to apply the implicit function theorem.

The first order condition of (20) (*i.e.*, the second order condition of the profit maximization problem) with respect to x is given by

$$\frac{\partial^2 \pi}{\partial x^2} = 2\eta^2 \left[1 - 3x - \frac{D^3 I}{\eta(D+xI)^3}\right]. \tag{A1}$$

The first order conditions with respect to all other variables are given by

$$\frac{\partial^2 \pi}{\partial x \partial D} = -\left[I^2 x^2 (3D+xI)\eta\right]/(D+xI)^3 \tag{A2}$$

$$\frac{\partial^2 \pi}{\partial x \partial I} = -\left(2D^3 x\eta\right)/(D+xI)^3 \tag{A3}$$

$$\frac{\partial^2 \pi}{\partial x \partial c} = -\eta \tag{A4}$$

$$\frac{\partial^2 \pi}{\partial x \partial \eta} = \left\{[2x\eta(2-3x) - c](D+xI)^2 - DxI(2D+xI)\right\}/(D+xI)^2. \tag{A5}$$

Thus the relevant derivatives calculate to

$$\frac{\partial x}{\partial D} = -\frac{(xI)^2(3D+xI)}{2D^3 I + 2(3x-1)(D+xI)^3\eta} \tag{A6}$$

$$\frac{\partial x}{\partial I} = \frac{D^3 x}{\eta(D+xI)^3\left\{1 - 3x - D^3 I/[\eta(D+xI)^3]\right\}} \tag{A7}$$

$$\frac{\partial x}{\partial c} = 1/\left\{2\eta\left\{1 - 3x - D^3 I/[\eta(D+xI)^3]\right\}\right\} \tag{A8}$$

$$\frac{\partial x}{\partial \eta} = \frac{c(D+xI)^2 + DxI[2D+xI] + 2x(3x-2)(D+xI)^2\eta}{2(D+xI)^2\eta^2\left\{1 - 3x - D^3 I/[\eta(D+xI)^3]\right\}}. \tag{A9}$$

In the relevant parameter range, $1 - 3x - D^3 I/[\eta(D+xI)^3]$ is negative, therefore $\partial x/\partial I$ and $\partial x/\partial c$ are negative as well. Also $\partial x/\partial I < 0$. Since the numerator of $\partial x/\partial I$ is negative, the whole expression turns out to be positive.

References

Abadi, Daniel J. (2009) 'Data management in the cloud: Limitations and opportunities.' *IEEE Data Engineering Bulletin* 32(1), 3–12

Adams, James (2001) 'Virtual Defense.' *Foreign Affairs* 80(3), 98–112

Akerlof, George A. (1970) 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism.' *The Quarterly Journal of Economics* 84(3), 488–500

Becker, Gary S. (1968) 'Crime and Punishment: An Economic Approach.' *Journal of Political Economy* 76(2), 169–217

__ (1995) 'The Economics of Crime.' *Cross Sections* Fall, 8–15

Boss, Greg, Padma Malladi, Dennis Quan, Linda Legregni, and Harold Hall (2007) 'Cloud Computing'

Cabral, Luis M.B., David J. Salant, and Glenn A. Woroch (1999) 'Monopoly pricing with network externalities.' *International Journal of Industrial Organization* 17, 199–214

Cremonini, Marco, and Dmitri Nizovtsev (2006) 'Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies.' Proceedings of 5th Workshop on the Economics of Information Security (WEIS 2006), Cambridge (UK)

Huang, C. Derrick, Qing Hu, and Ravi S. Behara (2008) 'An economic analysis of the optimal information security investment in the case of a risk-averse firm.' *International Journal of Production Economics* 114(2), 793–804

Johnson, Deborah G. (2004) 'Ethics On-Line.' In *Readings in CyberEthics,* ed. Richard A. Spinello and Herman T. Tavani, 2 ed. (Jones and Bartlett Publishers, Inc.) chapter 1, pp. 30–39

Katyal, Neal Kumar (2001) 'Criminal Law in Cyberspace.' *University of Pennsylvania Law Review* 149(4), 1003–1114

Kshetri, Nir (2006) 'The Simple Economics of Cybercrimes.' *Security & Privacy, IEEE* 4(1), 33–39

__ (2010) *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (Heidelberg: Springer)

Leeson, Peter T., and Christopher J. Coyne (2005) 'The Economics of Computer Hacking.' *Journal of Law, Economics & Policy* 1(2), 511–532

Mell, Peter, and Timothy Grance (2009) 'The NIST definition of cloud computing.' *National Institute of Standards and Technology* 53(6), 50. NIST

Shy, Oz (2001) *The Economics of Network Industries* (Cambridge: Cambridge University Press)

__ (2011) 'A Short Survey of Network Economics.' *Review of Industrial Organization* 38(2), 119–149

Taylor, Natalie, and Pat Mayhew (2002) *Financial and Psychological Costs of Crime for Small Retail Businesses* number 229. In 'Trends & Issues in Crime and Criminal Justice.' (Australian Institute of Criminology)

In dieser Reihe sind zuletzt erschienen / Recently published:

2013

25/02 **Sauer, Beate und Friedrich L. Sell**, Is the Eurozone not a Monetary Union, but an Extraordinary Exchange Rate Union?

25/01 **Sell, Friedrich L. und David C. Reinisch**, How do Beveridge and Phillips curves in the Euro Area behave under the stress of the World Economic Crisis?

2012

24/02 **Sell, Friedrich L. und David C. Reinisch**, Anmerkungen zum Monopson am Arbeitsmarkt: Der Zeithorizont macht den Unterscheid

24/01 **Sell, Friedrich L. und Felix Stratmann**, Verteilungs(un)gleichgewicht in Deutschland: Zweieinhalb theoretische Konzepte und fünf empirische Belege

2011

23/02 **Sell, Friedrich L. und Beate Sauer**, A Further View on Current Account, Capital Account and Target2 Balances: Assessing the Effect on Capital Structure and Economic Welfare

23/01 **Sell, Friedrich L. und Felix Stratmann**, Downs' ökonomische Theorie der Demokratie 2.0: Politische Präferenzen und Gleichheitsaversion

2010

22/03 **Morasch, Karl**, Intermediation by Heterogeneous Oligopolists

22/02 **Sell, Friedrich L.**, Desempleo, desajuste en el mercado laboral („mismatch") e inflación: un modelo integrativo

22/01 **Sell, Friedrich L.**, Die Weltwirtschaftskrise als Exempel der Überinvestitionstheorie: Komplementäre Erklärungsansätze von v. Hayek/Garrison und Minsky

2009

21/03 **Bartholomae, Florian W., Karl Morasch und Rita Orsolya Tóth**, Smart Entry in Local Retail Markets for Electricity and Natural Gas

21/02 **Sell, Friedrich L. und Felix Stratmann**, Equity Aversion, Inequality Aversion and Economic Welfare: On the Macroeconomic Substantiation of Microeconomic Utility Functions

21/01 **Bartholomae, Florian W. und Alina M. Popescu,** Regional Income Distribution and Human Capital Formation. A Model of Intergenerational Education Transfer in a Global Context

Universität der Bundeswehr München
Fachgruppe Volkswirtschaftslehre an der
Fakultät für Wirtschafts- und Organisationswissenschaften
D – 85577 Neubiberg