DISCUSSION PAPER
SERIES IN
ECONOMICS AND
MANAGEMENT

Cybercrime and Cloud Computing – A Game Theoretic Network Model

Florian Bartholomae

Discussion Paper No. 17-05

GERMAN ECONOMIC ASSOCIATION OF BUSINESS
ADMINISTRATION – GEABA

Cybercrime and Cloud Computing

A Game Theoretic Network Model

Florian W. Bartholomae

Bundeswehr University Munich
85577 Neubiberg, Germany
florian.bartholomae@unibw.de

Abstract

In this paper a network model is developed in which three players sequentially choose their strategies. In the first stage, a profit-maximizing provider of cloud computing services chooses the price and thus the size of its user base (the network). In the second stage the consumers decide whether to use the service or not. In the last stage a hacker has the opportunity to force access into the cloud and cause damage to the consumers. The success of hacking is based on the hacking effort of the cyber-criminal, technical protection measurements installed by the provider, and the carefulness of the users. Several scenarios with different levels of data security and public prosecution of the hacker are analyzed. Especially for the case when no security measurements are available, a firm's strategy to limit the network size in order to render hacking unattractive is discussed in detail. Furthermore, in several extensions different motivations of the hacker as well as alternative competitive environments are included, thus allowing for 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 use of cloud computing services[1] has become an essential part of everyday life in private as well as in business context. Almost everyone that connects to the Internet is an user of cloud computing services like email services, on-line data storage or on-line tools (word processing, terminal services etc.). By using these services more or less confidential data are needed to use the service or to pay for it. Consumers are not always aware of the mass of data produced by them as data from almost every activity in the web is collected and stored on servers of cloud computing provides. Especially the data collection activities of *Facebook* or *Google* are often a subject of great controversy.

In business-to-business relations cloud computing becomes also more relevant as there are several advantages of this service (Boss et al., 2007, Armbrust et al., 2010, Nazir, 2012, Henneberger, 2016): 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; transaction costs like coordination and information costs are reduced as data and software is almost always and everywhere available. However, there are disadvantages as well especially with respect to security as 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) (Abadi, 2009, Bisong and Rahman, 2011, Hashizume et al., 2013) and of course there is the danger of hold-up as one has to rely on third party (Bamiah and Brohi, 2011). These risks cause many business to reassess carefully, whether to use the service at all (Mujinga and Chipangura, 2011). Furthermore, many advantages may also be seen as disadvantages, as "the data placed is easy to locate [and] to send across the communication channels of different countries" (Gangwar and Date, 2016, 889).

Many incidents in popular Online services have demonstrated this security issues impressively: For instance, the periodic hacking of Sony's Playstation network (in 2011 77 million accounts were affected) or the theft of credit card data of 134 million customers of the US firm Heartland Payment Systems.[2] In a recent study by Allianz (2017) on business risks, hacking and more generally cybercrime[3]

[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).

[3] Cybercrime is a crime that makes 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,

is one of the most important risks for firms. Almost three quarter of the participants in this study name 'hacker attacks' as main causes of cyber incidents.

In order to shed some light on the effects of hacking on the economy in general and the relevant participants (cloud computing provider and its customers) an extended network model is considered in the subsequent analysis. This framework is chosen since many cloud computing services generate more or less positive network externalities for their users as they allow for better (international) cooperation. In fact, many cloud computing services are network services (e.g. email) or have at least indirect network effects – *i.e.* a bigger user base allows for better support (forums, weblogs, communities etc.). Furthermore, the analysis is capable to capture costs beyond the pure monetary damage of the user: Due to increased danger of hacking additional users cause negative network externalities leading to lower economic activity and thus higher costs of hacking for the society.

The structure of the paper is as follows: In section 2 the basic set-up of the model is developed introducing the relevant players and the structure of the game. In section 3 the baseline case of a situation without hacking and the relevant situation with hacking are presented and explicitly analyzed in subsection 3.3. Section 4 discusses some extensions of the model to broaden the analysis. Finally, section 5 gives the conclusion.

2 Model Set-Up

The analysis is based on a model introduced by Shy (2001, ch. 5.2). In this model he analyzes the profit-maximizing price setting of a monopolistic network firm. This analysis is extended by adding a third player, a hacker, besides the monopolistic network firm – henceforth the cloud computing provider – and its consumers.

The model developed consists of three stages, in which each of the three risk-neutral players – the cloud computing provider, the consumers and the hacker – decide sequentially about their strategies. The information structure is characterized as perfect and complete. In the first stage the provider decides about the price charged for the cloud computing service, which in turn determines the size of the network. A monopolistic provider is assumed as for many cloud computing services demand sided external economies of scale prevail: Consumers tend to use well-known services because it is more likely that business partners or friends use this service as well. Thus, in most cloud computing services a dominant firm can

1007); and most crimes stay unobservable to third or even second parties. Kshetri (2010) analyzes several aspects of this special "industry". Besides cybercrime, cyberterrorism and hacking attacks against governments and institutions are of high importance to the economy as a whole, see e.g. Adams (2001).

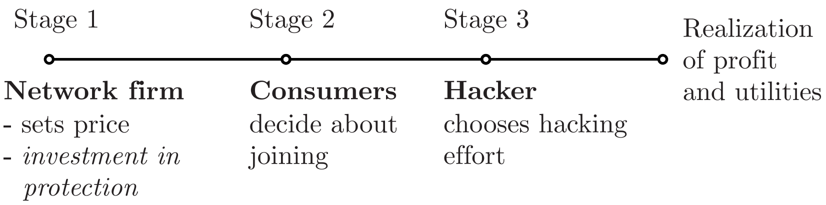

Figure 1: Structure of the game, players and strategies.

be found (*Microsoft*, *Google* etc.) Furthermore, the analysis is simplified. In the second stage a mass of consumers decides, whether to use the cloud computing service or not. Consumers can be private individuals as well as firms using the cloud computing system of the third-party provider. It is assumed that the cloud computing service generates positive network externalities for its users – either directly by improved (or even rendered possible) cooperation or indirectly by better support of a bigger community.[4] In case of firms these network effects may arise from improved and/or simplified cooperation between its employees or departments and its business partners. Due to this network effects three possible outcomes may arise: No one uses the service (stable equilibrium), a low (instable equilibrium) or a high number of consumers use the service (stable equilibrium). To avoid this problem of multiple equilibria, the assumption is made that consumers have perfect foresight, *i.e.*, consumers can correctly anticipate the number of other consumers using the cloud computing service (Shy, 2001, 20).[5] In the third stage the hacker decides whether to force access to the data in the cloud or not. Finally, the payoffs of all players are realized. The structure of the game, the players and their strategies are summarized in fig. 1.

Next, the basic strategies of all players are considered in more detail. The monopolistic cloud computing provider's profit function is given by

$$\pi = [p - k(c, \alpha)]N, \tag{1}$$

where p denotes the price of the service[6] and N the size of the network (*i.e.*, the number of users). Costs per user, $k(c, \alpha)$, depend on (constant) marginal cost, c, with $\partial k / \partial c > 0$, as well as all costs associated with network protection against hacking (like antivirus software and firewalls), which depend on the (technical) degree α, with $\partial k / \partial \alpha > 0$. This degree can take values between 0 (no protection measurements) and 1 (full protection).

[4] For a general overview of network economics see Shy (2011).

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

[6] A survey on pricing of cloud computing service can be found in Koehler et al. (2010).

The individual consumer's (expected) utility is given by[7]

$$U_C = \begin{cases} (1-x)N - p & \text{use of the service,} \\ (1-x)N - p - \rho D & \text{use of the service and being hacked,} \\ 0 & \text{no use of the service.} \end{cases} \tag{2}$$

The consumer's preference for the cloud computing service, x, is uniformly distributed between 0 and 1 with density η. That is, the higher x, the lower the utility of the service. Besides the individual preference, the utility depends on the network size N as well, which is determined by ηx. If hacking takes place and is successful with probability ρ, the consumer incurs a damage D. The expected damage ρD captures the loss of data as well as the damage following hacking like credit card fraud, identity theft or activities harming business opportunities. 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. This damage directly lowers the consumer's willingness to pay. This is in line with the findings of Gangwar and Date (2016) who show that security issues decrease the usefulness of cloud computing services for its customers.

In the last stage, the hacker decides whether to force access into the cloud or not;[8] thus his (expected) utility is given by

$$U_H = \begin{cases} \rho(e,s)Nv - F - e^2/2 & \text{if he hacks,} \\ 0 & \text{if he does not hack.} \end{cases} \tag{3}$$

Again, ρ denotes the probability of successful hacking. This probability depends on both, e, the effort the hacker assigns to his illegal activity, and s the share of non-protected consumers. The effort level can take values between 0 (no effort is made) and 1 (full effort is devoted to hacking). Non-protected 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.[9]

[7] Since only the decision of using the particular service is considered, outside options like building own private servers or refraining from any on-line activities are neglected. When considering the trade-off between a public an a private server one has to account for higher costs as a security environment has to be build by oneself but also that hackers may have less incentive to put effort into hacking as the server may not be known or the value of the data is too low. Furthermore, no network externalities emerge.

[8] According to the NIST definition "the term hacker is used to refer to people who either break into systems for which they have no authorization or intentionally overstep their bounds on systems for which they do have legitimate access" (see `http://tinyurl.com/NISTdef`).

[9] As Bamiah and Brohi (2011) point out, there may be a "malicious insider" in the provider firm as well. However, this possibility is not considered here.

The hacker is able to use these 'open gates' to gain access into the cloud service. Inside the cloud, the hacker is not only able to steal the data of the non-protected consumers but also the data of all other network users as the data is interconnected. Thus, in contrast to traditional network models, an additional network user has a negative externality on all other users, if she is non-protected. The hacker assigns a value v on the data of each network user, that is, the network's value for the hacker is given by Nv. If the hacker puts positive effort into hacking, he has to expect some fine F. This parameter captures both, the probability of getting caught and the fine set by the authorities.

The hacking effort raises the possibility of successful hacking and comes at cost of $e^2/2$ for the hacker. Additionally, the probability of a successful hacking attempt depends on the firm's protection measurements as well. Thus, the function can be specified as

$$\rho(e,s) = [1-(1-s)\alpha]e. \tag{4}$$

If the hacker choses the maximum effort ($e = 1$), hacking is successful with probability $1-(1-s)\alpha$ and therefore depends only on the security measurements and the share of non-protected consumers. As can be seen, non-protected consumers render security investments made by the cloud computing provider inefficient. If e.g. all consumers are non-protected, $s = 1$, security investments will have no restraining effect on the success of hacking – the best security measurements will not be effective, if the user leaves his access data unattended in public places. In contrast, if the firm does not care for network security and the hacker choses his maximum effort level, the hacker will be successful for sure.

The value v of the data is the money amount which the hacker can earn from the (mis)use of the user's data. The relation between this value and the damage done to the consumer is given by

$$D = (1+d)v. \tag{5}$$

The parameter d captures the user's additional costs beyond the pure redistribution from the user to the hacker like ransom or business secrets. These additional costs arise from the need of extra insurance, reporting the crime, identification of the extent of the damage, going to court, etc.[10] As $d > 0$ it follows that $D > v$.

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

3 Scenario Analysis

Based on the general model set-up, two specifications are considered in the following two subsections. The third subsection discuses the findings in more detail.

3.1 Set-Up without Hacking

If no hacking takes place, the game consists of only two stages, where the cloud computing provider decides first about the price to gain access to its service and the consumers decide second, whether to use the service or not. Applying the concept of backward induction and starting with the consumers, they will join if

$$p \leq \eta \hat{x}(1-\hat{x}) \quad \text{or} \quad \hat{x} = \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{p}{\eta}} \tag{6}$$

Note that there are two solutions for the demand function but only the larger one guarantees a stable optimum (cf. Shy, 2001, 112). Since without hacking, only marginal costs are relevant, $k(c,\alpha) = c$, the firm's profit in the first stage is

$$\pi = (p-c)\eta \left(\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{p}{\eta}} \right). \tag{7}$$

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

$$p^* = \frac{\eta}{9}\left(1 + \sqrt{1 - \frac{3c}{\eta}}\right) + \frac{c}{3}, \tag{8}$$

the associated network size is given by

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

and profit by

$$\pi^* = \frac{\eta}{27}\left(1 + \sqrt{1 - \frac{3c}{\eta}}\right)\left[\eta\left(1 + \sqrt{1 - \frac{3c}{\eta}}\right) - 6c\right]. \tag{10}$$

3.2 Set-Up with Hacking

Now hacking is possible. In the last stage of the game the hacker decides first, how much effort he puts into forcing access into the cloud. Maximizing his utility, (3), considering (4) results in the effort level

$$e^{Opt} = [1-(1-s)\alpha]vN. \tag{11}$$

Second, he must consider, whether this effort leads to higher utility than refraining from the illegal activity. That is, some threshold of the network $\tilde{N}$ results which gives the minimum network size in order to generate a positive expected utility for the hacker,

$$N \geq \tilde{N} \equiv \frac{\sqrt{2F}}{[1-(1-s)\alpha]v}. \tag{12}$$

Plausibly, if the expected fine increases, this threshold rises as well, whereas a larger valuation of the data, a higher share of non-protected users and/or less security investments made by the cloud computing provider decrease the minimum network size. Thus, the users and the provider have to face the probability of hacking

$$\rho = \begin{cases} [1-(1-s)\alpha]^2 vN & N \geq \tilde{N} \\ 0 & N < \tilde{N}. \end{cases} \tag{13}$$

In the second stage consumers decide to use the cloud computing service, if

$$p \leq \eta\hat{x}[(1-\hat{x}) - [1-(1-s)\alpha]^2(1+d)v^2]. \tag{14}$$

This condition is only valid for the case of hacking, *i.e.*, (12) is fulfilled, $\eta\hat{x} = \hat{N} \geq \tilde{N}$, otherwise all results from subsection 3.1 apply. For simplification of (14) substitute

$$\Lambda \equiv [1-(1-s)\alpha]^2(1+d)v^2. \tag{15}$$

Thus, Λ captures the additional damage done to the cloud computing users, d, the value of the data, v, and the probability of successful hacking if maximum effort is chosen by the hacker, $[1-(1-s)\alpha]$. If hacking takes place, Λ thus shows the decrease in the user's maximum willingness to pay.

The first order condition of (14) with respect to Λ turns out to be negative which implies several interesting findings, as Λ positively depends on s, d, and v: Obviously, the firm has to lower its price as the possible damage for the consumers from hacking increases. This can be the case, if either the additional damage done to the consumers, d, increases or the share of non-protected consumers, $1-s$, grows. In contrast, quite counterintuitive seems the result that the more valuable the data, the users store in the cloud, v, the lower the price the provider may charge. This follows from the fact that more valuable data also increases the overall value of the network for the hacker leading to higher hacking effort.

As the firm chooses the price in the first period, (14) has to be reformulated to $\hat{x} = 0.5(1-\Lambda) + \sqrt{0.25(1-\Lambda) - p/\eta}$.[11] The provider's profit in the first stage in case of hacking is given by

$$\pi_H = [p - k(c,\alpha)]\eta \left(\frac{1-\Lambda}{2} + \sqrt{\frac{1-\Lambda}{4} - \frac{p}{\eta}} \right). \tag{16}$$

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

$$p^{**} = \frac{(1-\Lambda)\eta}{9} \left(\frac{2+\Lambda}{2} + \sqrt{\frac{(4-\Lambda)(1-\Lambda)}{4} - \frac{3k(c,\alpha)}{\eta}} \right) + \frac{k(c,\alpha)}{3} \tag{17}$$

The second solution of the quadratic equation has no economic relevance.[12] The associated network size calculates to

$$N^{**} = \frac{\eta(1-\Lambda)}{3} \left(1 + \sqrt{1 - \frac{3k(c,\alpha)]}{\eta(1-\Lambda)^2}} \right), \tag{18}$$

and obviously the network size decreases in Λ.[13] Finally, the firm's profit is given by

$$\pi^{**} = \frac{\Omega}{27} \left[(1-\Lambda)\Omega - 6k(c,\alpha) \right], \tag{19}$$

with $\Omega = \eta(1-\Lambda)\left(1 + \sqrt{1 - 3k(c,\alpha)/[\eta(1-\Lambda)^2]}\right)$.[14] It comes as little surprise that the provider's profit negatively depends on Λ that lowers both, price and demand.

[11] Since (14) is a quadratic equation, the reformulation yields two solutions. As only the larger network size yields a stable equilibrium, this expression was chosen.

[12] Again, only for the larger expression a negative second order condition and thus a profit maximum is guaranteed.

[13] Since Λ is always in relation to η, formulated in casual way, 'hacking reduces the user density.'

[14] Note that for $\Lambda = 0$, this expression would become $H = \eta\left(1 + \sqrt{1 - 3k(c,\alpha)/\eta}\right)$ yielding the same profit as in (10).

3.3 Analysis and Discussion

To simplify the analysis we start with a scenario where either no technical protection by the cloud computing provider is possible, $\alpha = 0$, or all consumers are non-protected, $s = 1$ – in this situation any investment in network security, neither costly nor free of cost, would make sense.[15] As long as condition (12), $N \geq \sqrt{2F}/v$, is fulfilled, the hacker will put effort into forcing access into the network – in this situation the level of effort corresponds to the probability of a successful hacking attempt (see (4)). Comparison of (8) with (17) shows that the price in case of hacking will be lower, if the data of the user has some positive value, *i.e.*, $\Lambda = (1+d)v^2 > 0$. Furthermore, comparison of (9) with (18) shows that the number of users will be lower in case of hacking for the same reason.

Proposition 1 *If the provider does not invest in security and there is danger of hacking, the price for the cloud computing service is lower while less users are willing to use the service.*

If no technical hacking prevention is possible, the cloud computing provider still has the possibility to render hacking unattractive by limiting its network size and avoiding that $N \geq \tilde{N}$ is met. At this threshold profit would be

$$\tilde{\pi} = \frac{2F}{v^2}\left(1 - \frac{\sqrt{2F}}{\eta v} - \frac{cv}{\sqrt{2F}}\right) \tag{20}$$

which depends positively on F. Thus, profit is in the end determined by public authorities who decide about the expected fine.

Thus, the limitation strategy is profitable if $\tilde{\pi} \geq \pi^{**}$, *i.e.*, (20) is larger than (19). Since the formal comparison is tedious, fig. 2 illustrates the main findings. The continuous curve describes the cloud computing provider's profit in case of hacking and the dashed curve describes profit when no hacking takes place. As can be seen, the profit in case of hacking is always lower compared to the situation without this possibility. The difference between both profits is ΛN^2 so that profit in case of hacking will be lower the higher the value of the data and the higher the

[15] However, investment would nevertheless reduce the probability of hacking: As investment in security increases costs per user, the profit-maximizing network will be smaller. Thus, the value of the network will be smaller which decreases the effort the cyber-criminal puts into forcing access to the data. Thus, probability of hacking would decrease – not because of higher technical difficulties for the hacker but because of a less attractive network. Despite this fact, increasing its costs only to irritate the hacker without having the direct positive effect of a higher willingness to pay of its consumers may not be a good idea for a profit-maximizing provider.

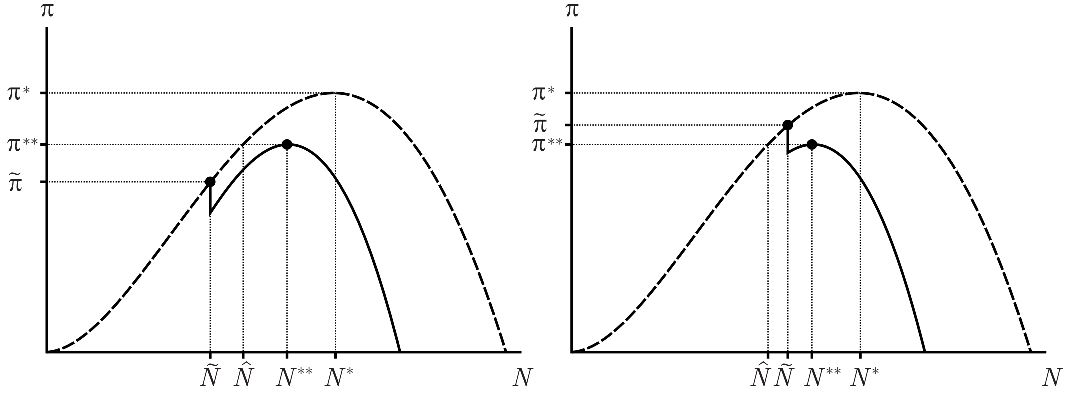

Figure 2: Comparison of profits: Limitation of network size may increase profit.

additional damage done to the cloud computing users.[16] If costs per user as well as d and v are positive, it may turn out that profit in case of a limitation of the network is higher than in a situation without any restriction (as depicted on the right side of the figure). However, if the hacking preventing size is too small, the loss in profit would be too big implying that a profit-maximizing provider would refrain from limitation. This consideration suggests that there exists some threshold of the network size $\hat{N}$ in the mass of $\tilde{N}$ which leads to a higher profit if the user base is limited. This threshold is depicted in fig. 2 as well. Note that $\hat{N}$ is found by searching for the smallest network size that leads in a situation without hacking to the highest possible profit in the case of hacking, π^{**}. That is, the cloud computing provider will limit its network size if $\hat{N} \leq \tilde{N} \leq N^*$; both, in cases $\tilde{N} < \hat{N}$ and $\hat{N} > N^*$, no limitation will take place as the chosen user base ensures a profit maximum. $\hat{N}$ will be higher, the higher costs per user as this lowers in general the profit-maximizing network size and thus makes smaller user bases more attractive. In contrast, the threshold will be higher, the higher the value of the stored data and the damage done to the consumers.

Proposition 2 *If the minimum size necessary to make the network attractive for hacking exceeds a critical size, limitation of the user base to this size is profitable for the cloud computing provider as a higher network price and profit is feasible.*

Now let there be only protected users, $s = 0$, and full investment in security, $\alpha = 1$. In this situation there would be no hacking since the possibility of a successful hacking attempt would be 0 as stated by (4). However, this would be

[16] For any N, profit without hacking is in general $[N(1-N/\eta)-k(c)]N$ and with hacking $[N(1-N/\eta-\Lambda)-k(c,\alpha)]N$. Thus, profit in case of hacking will be lower by $[\Lambda N + k(\alpha)]N$.

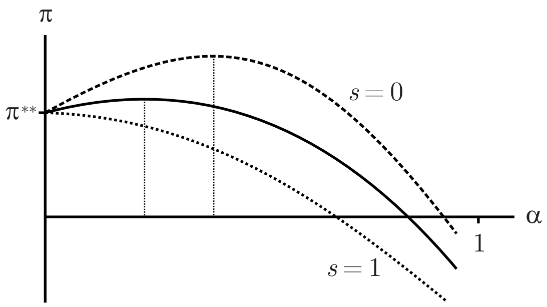

Figure 3: Profit-maximizing level of protection.

advantageous only in the case if investment in security is free of cost. Otherwise the provider faces some trade-off: On the one side, investment increases the users' willingness to pay as the probability of hacking is reduced.[17] On the other side, this advantage comes at extra costs per user that have to be born in order to install the security measurements. Independent of the exact specification, neither full security measurements ($\alpha = 1$) nor no investment ($\alpha = 0$) is advantageous. Although a positive investment will never allow for the first best solution since protection is costly, it will nevertheless increase the profit in case of hacking as higher security is valued by the users of cloud computing, that is, the user base will be larger as well as all users are also willing to pay a higher price for the service. Obviously, the higher the costs of security measurements, the lower the chosen level of protection. However, if the assumption of only protected consumers is abandoned, *i.e.* there is a positive share of non-protected consumers, this investment significantly decreases and may in the most extreme case – all consumers are non-protected – rendered completely inefficient and thus be zero for sure. This relationship is also reflected in the equations: (14) shows that the user's willingness to pay increases in α, if this is not countered by non-protected consumers, $s = 0$.

Fig. 3 summarizes the results. The upper dashed curve shows the change in the provider's profit if all users are protected while the level of protection, α, is increased. The lower continuous curve shows profit for a moderate share of non-protected consumers while the lowest dotted curve shows profit if all users are non-protected. As can be seen for $s = 1$ profit cannot be increased beyond the initial profit without any security measurements, π^{**}. The lower the share of non-protected consumers the higher the profit-increasing level of security measurements.

Proposition 3 *The network provider will only invest in security measurements if*

[17] Or as Gangwar and Date (2016, 900) state: "Countermeasures and preventive measure to avoid security risk will increase usefulness of cloud computing."

there are some protected consumers. However, he will never choose full protection even if all consumers would take data security seriously.

How does hacking affect welfare? Since the monopolistic cloud computing provider completely skims consumer surplus, social benefit consists of the profit of the firm as well as of the hacker's utility. That is welfare would only increase, if the hacker's gain in utility exceeds the firm's loss in profit. The hacker's utility at any attractive network size $N > \tilde{N}$ is given by (3) considering (4) and (11),

$$U_H = \frac{1}{2}\left[[1-(1-s)\alpha]vN\right]^2 - F. \tag{21}$$

Subtracting from this expression the firm's loss in profit, the change in social benefit results:

$$\Delta\text{WF} = -\frac{1}{2}\left[[1-\alpha(1-s)]\,vN\right]^2(1+2d) - k(\alpha)N - F \tag{22}$$

Obviously, this expression is negative for any network size and thus social benefit is always decreased by hacking. The gain from the hacker cannot compensate for the loss in the user base and the reduced willingness to pay. Note that the hacker's criminal activity has not to be successful – only the expected damage is considered by the consumers even in case of a non-successful attempt (with possibility $1-\rho$). However, since only the mere existence of a hacker or more precisely a network value attractive for hacking has a negative effect on the consumer's willingness to pay, overall welfare is reduced.

Proposition 4 *The possibility of hacking decreases total welfare.*

In a next step, it is analyzed which (optimal) fine a legislative authority should set. Basically, this discussion is based on the results yielding to propositions 2 and 4. The hacker will only pursue his illegal activity if his resulting utility is positive. Thus, reformulation of (21) gives

$$F \geq \frac{1}{2}\left[[1-(1-s)\alpha]vN\right]^2 \tag{23}$$

This equation is a transformation of (12) and shows the minimum fine needed to ensure a network of size N. Thus, when setting a fine, the legislative authority must take the following factors into account: First, the observable (monetary) value of the data 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 may be estimated quite liberal in order to include not only the (observable) explicit costs, but also the implicit costs for the user. Third, the share of protected consumers and the level of network security play a crucial role: The higher both parameters, the lower the necessary fine, as the hacker faces more difficulties to force access into the network and thus may rather refrain from hacking.

Basically, this implies a very specific measurement and so only the 'optimal' network size has to be found. From the perspective of a firm, any network size larger than $\hat{N}$, *i.e.* a lower user base that ensures higher profit than if hacking takes place, would be welcome – as was already addressed in the discussion of (20). With respect to welfare, N should be N^* so that there is no negative effect from hacking at all. Furthermore, with respect to effectiveness, N^* also determines the maximum fine as some higher fine would have no effect on the network size as well as welfare.

Proposition 5 *By setting an adequate fine, public authorities can lower the danger of hacking and thus increase welfare. When doing so, the value of the data, the caused damage and the users' as well as the providers' level of protection have to be taken into account.*

Nevertheless, determination of an optimal fine is not that easy in reality. First, what was not considered in this analysis are the costs of the punishment or the costs of preceding prosecutions, respectively. A tougher proceeding rises costs which have to be financed by e.g. increased taxes paid by society. Thus, governments face the trade-off, whether the users' and providers' gains justify higher costs for the society. Second, due to international hackers beyond a national authority's jurisdiction as well as overwhelmed criminal prosecution, the probability of catching the hacker is quite low and so is the fine he has to expect. There are many reasons, why the probability of getting caught is 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. These factors negatively influence the probability of successful prosecution.[18] Second, in some countries even the fine for Internet crime itself is quite low or non-existent (Kshetri, 2006, 37).[19]

[18] As a study by Germany's digital association points out, only every fifth commercial victim of cybercrime contacts public authorities (bitkom, 2016).

[19] 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).

4 Extensions

In the following two subsections, some extensions to the basic model are given that shed some light on the question how consumers themselves or competition can help to overcome problems of hacking.

4.1 Consumers' Decision for Protection

So far it was assumed that a share of consumers is protected. This will now be relaxed, so that consumers can decide whether they want to protect themselves or not. It is assumed that the higher the consumer's preference for the cloud computing service, the higher the willingness to invest in order to prevent hacking. This is in line with bitkom (2016) which highlight that more technophile users (low x) have better security measurements. 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.

Additionally, the assumption is made that while the hacker forces access into the cloud he only can get access to the data of the non-protected users but not to the safe data of the protected users. Since the investment is only necessary if hacking is possible, consideration of the non-hacking scenario is skipped, *i.e.*, $N \geq \tilde{N}$ is presumed as well. Based on these modifications, (2) changes to

$$U_C = \begin{cases} (1-x)N - p - \rho D & \text{use of the service and being hacked,} \\ (1-x)N - p - xI & \text{use of the service and invest,} \\ 0 & \text{no use of the service.} \end{cases} \tag{24}$$

According to this modified utility function, a user invests in security if

$$(1-x)N - p - xI \geq (1-x)N - p - \rho D. \tag{25}$$

This condition results in $x_I \leq \rho D/I$. Considering (i) the probability of hacking, (13); (ii) the relation between the mass of users that invest in security, N_I, and the share of protected users, $s = 1 - N_I/N$; and (iii) the assumption, that the relevant network size for the hacker is reduced by the amount of protected consumers, $N - N_I$, the following condition results which determines the protected user base given N,

$$N_I = \frac{1}{I}\left(1 - \alpha\frac{N_I}{N}\right)^2 (1+d)v^2(N - N_I)\eta. \tag{26}$$

If the firm does not invest in security, $\alpha = 0$, condition (26) solves to

$$1 - s = \frac{(1+d)v^2\eta}{I + (1+d)v^2\eta}. \tag{27}$$

This allows for several reasonable results. First, the share of protected consumers $1-s$ increases as the costs of protection I decrease. Obviously, if costs are $I = 0$ all consumers will choose to be protected. However, in this case condition (26) is violated since no hacking could take place any more as the number of accounts that can be hacked is $N - N_I = 0$. If investment costs are low enough to ensure that $N - N_I \leq \tilde{N}$ no hacking will take place as well[20] – *i.e.*, there exists some investment level $\tilde{I}$ which ensures $N_I \geq N - \tilde{N}$. A lower level than $\tilde{I}$ has no effect on the network size and will not encourage more consumers to invest since the danger of hacking is eliminated by the positive externality of the already protected users on the network size. Second, more users are willing to invest in their personal security, if the value of the data v increases and/or more additional damage d occurs. While the first increases the motivation of the hacker to force access into the cloud, the second increases the motivation of the users to protect their data.[21]

As the firm increases its investment in protection and assuming this would have no effect on N, less consumers would invest in personal security, thus there is a substitutive relationship between technical network security and personal precaution. Since N increases in α as well, the effects are not that clear. Nevertheless, the share of users investing in personal protection decreases. In addition, – as already stated in proposition 5 – the (expected) fine and the level of protection are substitutes as well, that is, the higher the fine the less effort the hacker puts into his criminal activity and thus, the less users are willing to invest in protection measurements.

Proposition 6 *If personal security is costly, there is always a share of careless consumers. The share will be lower the higher the risk of hacking, however, it will be lower, the better the technical network security installed by the cloud computing provider. Furthermore, there is a critical level of investment costs which lead to a situation without hacking.*

The profit of the firm also depends negatively on the users' investment costs. If these costs decrease, more users protect themselves which has a positive effect

[20] 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.

[21] This is in line with Huang et al. (2008) who show that even risk-averse firms only invest in security if the potential damage reaches a certain level.

on the network size – as the hacker finds the network less attractive more users join and thus the user base increases which has a positive effect on the willingness to pay. This affects the firm's profit positively although investment of the power users (those with low values of x) lowers their valuation of the service.

4.2 Types of Hackers and Psychological Costs

The analysis so far did not investigate the hacker's motives besides the pure economic interest. However, there are different types of hacker whose motivations differ significantly. This has implications for our analysis since the types have different valuations of the network and perceived costs. Leeson and Coyne (2005) differentiate three types of hackers, "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 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 $\rho N\theta v-(1+\psi_h)F-e^2/2$. The parameter $\theta\in[0,\infty)$ was added to describe the hacker's (personal) valuation of the data beyond their pure 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 initial specification).

Furthermore, the psychological parameter $\psi_h\in[0,\infty)$ is introduced. This parameter denotes the hacker's additional psychological costs of the fine.[22] It may arise from direct confrontation with his victims or his insight of the damage caused by him. Again, the parameter depends on the type of the hacker: Whereas a "greedy" as well as a "bad" hacker may incur only low psychological costs (low ψ_h),[23] a "good" hacker may suffer from large costs, since he does not want to harm anyone in the first place.

[22] The modification of the hacker's utility is quite similar to the cost-benefit consideration of Kshetri (2006, 36ff). In line with him, the value of the network $N\theta v$ catches monetary as well as psychological benefits. The perceived expected fine $(1+\psi_h)F$ catches monetary and psychological costs of committing the crime as well as the probability of arrest and of conviction.

[23] A "bad hacker" could even show a lack of understanding that hacking is unlawful even implying $\psi_h\geq-1$, however, such a situation is not explicitly considered here. In case of a "greedy" hacker

The concept of (additional) psychological costs is also introduced in the specification of the user's utility. If the consumer uses the cloud computing service and the account is hacked, her utility changes to $(1-x)N-p-\rho(1+\psi_c)D$ (second case of (2)). In this situation, 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), whereas for $\psi_c > 0$ she suffers from costs beyond the pure monetary damage. 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 for some interesting further insights. The threshold derived in (12) changes to

$$N \geq \tilde{N}_\psi \equiv \frac{\sqrt{2(1+\psi_h)F}}{[1-(1-s)\alpha]\theta v}, \tag{28}$$

that is, the more the criminal suffers from psychological costs, the higher $\tilde{N}_\psi$. 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).[24] In contrast, a higher valuation of the hacker, θ, decreases the threshold. Thus, a "bad hacker" with low or no additional psychological costs and high personal valuation of the data might be willing to force access into the cloud at almost any user base. A "good hacker" with higher qualms may only become active, if the network is really big (or he has not to fear any prosecution).

As the perceived damage of the consumers increases, they are less willing to pay a high price for using the network, *i.e.*, (14) changes to $p \leq \eta\hat{x}[(1-\hat{x})-(1+\psi_C)\theta\Lambda]$. Obviously, all of these modifications allow to state the following proposition:

Proposition 7 *If a provider of cloud computing services is confronted with a "bad hacker", network size and profit is reduced the most compared to a situation without hacking, whereas in case of a "good hacker" the reductions are least. In total, overall welfare will be further reduced by psychological costs.*

the parameter may also be low, if he is part of a criminal organization that supports him and his family in case of conviction. Thus, he even may neglect any costs.

[24] 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."

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

$$F_\psi \geq \frac{1}{2(1+\psi_H)}\left[[1-(1-s)\alpha]\theta vN\right]^2. \tag{29}$$

Comparison with (23) 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.

4.3 Repeated Game and Competition

Propositions 1 and 2 showed that it is not always in the interest of the cloud computing provider to prevent hacking as allowing for hacking still generates higher profits. However, this may result from the fact that a one-shot game was considered. But what happens, if an infinite planning horizon of the provider is considered, *i.e.*, the considered game is repeated infinitely? As consumers that were hacked in the past may lose trust in the security of their data, it seems plausible to assume that these consumers leave the network for good. Nevertheless it can also be argued that some victims stay because they value the benefits of the network higher compared to their suffered damage, while some of those who were not hacked leave as they are afraid to be future victims. For simplicity, let the probability of successful hacking ρ also denote the share of those who leave, *i.e.*, each period profits of a provider that does not prevent hacking will be reduced by ρ, $\pi^*_{t+1} = (1-\rho)\pi^*_t$. As usual, future profits have to be discounted by some factor δ. Therefore, a firm will not prevent hacking if $\sum_{t=0}^{\infty}\delta^t(1-\rho)^t\pi^* \geq \sum_{t=0}^{\infty}\delta^t\tilde{\pi}$, that is the net present value of profits in case of hacking is larger than the net present value of profits in case of limitation.[25] This condition can be reformulated to $\pi^* \geq [1+\rho\delta/(1-\delta)]\tilde{\pi}$ for $\delta(1-\rho) < 1$. As δ or $(1-\rho)$ increase, the provider is less likely to ignore hacking. However, as noted previously, $\tilde{N}$ might be quite low or even close to zero and thus $\tilde{\pi}$ as well. Therefore, even with an infinitely planning horizon, a firm may found itself in a better situation if it does not prevent hacking.

Another important aspect that was not considered due to simplification of the analysis is competition. While competition lowers the prices of the cloud computing service and boosts overall welfare by increasing the network (Shy, 2001, 117) – at least if there is some compatibility between the systems – it has a further

[25] Please note that since in the case of hacking, the network size decreases over time, this size will eventually led to a size that is unattractive for hackers. That is $\pi^* = \tilde{\pi}$ and so in all later periods both strategies generate the same profit, thus rendering this flow of profits irrelevant.

positive effect in this setting. As Cremonini and Nizovtsev (2006) argue in a similar context, a hacker has to take the possibility of attacking other systems into account as well. If there are such possibilities, Internet criminals must consider opportunity costs of not switching to another system and thus to run the risk to lose potential higher values. They found that a hacker chooses that system which is less protected compared to all others. In line with this argumentation our analysis has shown that the relative value of the networks matter as well. Thus, a small network or a good protected network has a lower risk of attracting a hacker – or in context of this model, the threshold $\tilde{N}$ increases in a competitive setting.

5 Conclusion

This paper extended a standard network model by introducing a third player, the hacker, and applying it to the context of widely used cloud computing services. It was shown that the potential damage caused by the cyber-criminal reduced the user base, the profit of the cloud computing provider as well as overall welfare. Although the provider may limit its user base to a size at which 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. The possibility of improving the network security or more care by the consumers does not eliminate the problem since additional costs baffle incentives yielding and incomplete prevention of hacking. Furthermore, the negative welfare effect caused by hacking may be underestimated due to neglect of psychological costs of the consumers as well as additional motives of the hackers that even may render some strategies for prevention ineffective.

All in all this suggests an important policy implication. 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. In this case the hacker will always force access into the network and no provider 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 (costly) 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 that more and more depends on data security and safe data exchange.

References

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

Adams, J. (2001): “Virtual Defense,” *Foreign Affairs*, 80, 98–112.

Allianz (2017): “Allianz Risk Barometer – Top Business Risks 2017,” Munich, URL `http://tinyurl.com/AllianzRiskBarometer`.

Armbrust, M., A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2010): “A View of Cloud Computing,” *Communications of the ACM*, 53, 50–58.

Bamiah, M. A. and S. N. Brohi (2011): “Seven Deadly Threats and Vulnerabilities in Cloud Computing,” *International Journal of Advanced Engineering Sciences and Technologies*, 9, 87–90.

Becker, G. S. (1968): “Crime and Punishment: An Economic Approach,” *Journal of Political Economy*, 76, 169–217.

Becker, G. S. (1995): “The Economics of Crime,” *Cross Sections*, Fall, 8–15.

Bisong, A. and S. M. Rahman (2011): “An Overview of the Security Concerns in Enterprise Cloud computing,” *International Journal of Network Security & Its Applications*, 3, 30–45.

bitkom (2016): “Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie,” Berlin, URL `http://tinyurl.com/bitkom2016`.

Boss, G., P. Malladi, D. Quan, L. Legregni, and H. Hall (2007): “Cloud Computing,” .

Cabral, L. M., D. J. Salant, and G. A. Woroch (1999): “Monopoly pricing with network externalities,” *International Journal of Industrial Organization*, 17, 199–214.

Cremonini, M. and D. 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).

Gangwar, H. and H. Date (2016): “Critical Factors of Cloud Computing Adoption in Organizations: An Empirical Study,” *Global Business Review*, 17, 886–904.

Hashizume, K., D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez (2013): “An Analysis of Security Issues for Cloud Computing,” *Journal of Internet Services and Applications*, 4, 5.

Henneberger, M. (2016): “Covering peak demand by using cloud services – An economic analysis,” *Journal Of Decision Systems*, 25, 118–135.

Huang, C. D., Q. Hu, and R. 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, 793–804.

Johnson, D. G. (2004): “Ethics On-Line,” in R. A. Spinello and H. T. Tavani, eds., *Readings in CyberEthics*, Jones and Bartlett Publishers, Inc., chapter 1, 2 edition, 30–39.

Katyal, N. K. (2001): “Criminal Law in Cyberspace,” *University of Pennsylvania Law Review*, 149, 1003–1114.

Koehler, P., D. Ma, A. Anandasivam, and C. Weinhardt (2010): “Customer heterogeneity and tariff biases in Cloud computing,” in *Proceedings of the International Conference on Information Systems 2010*.

Kshetri, N. (2006): “The Simple Economics of Cybercrimes,” *Security & Privacy, IEEE* , 4, 33–39.

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

Leeson, P. T. and C. J. Coyne (2005): “The Economics of Computer Hacking,” *Journal of Law, Economics & Policy*, 1, 511–532.

Mell, P. and T. Grance (2009): “The NIST definition of cloud computing,” *National Institute of Standards and Technology*, 53, 50, NIST.

Mujinga, M. and B. Chipangura (2011): “Cloud computing concerns in developing economies,” in *Proceedings of the 9th Australian Information Security Management Conference,*.

Nazir, M. (2012): “Cloud Computing: Overview & Current Research Challenges ,” *IOSR Journal of Computer Engineering*, 8, 14–22.

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

Shy, O. (2011): “A Short Survey of Network Economics,” *Review of Industrial Organization*, 38, 119–149.

Taylor, N. and P. 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.