Safety in numbers?
The effect of network competition on cybersecurity

Carolyn Gideon
Fletcher School, Tufts University

Christiaan Hogendorn
Wesleyan University

TPUG at AEA Annual Meetings
January 4, 2015

Draft 3 (11/25/14)

Abstract

Economic incentives for security investment in elements of the Internet is of increasing concern. This paper contains an exploration of the incentives for Internet service providers (ISP)s to invest in security. The analysis focuses on the spillover effects of ISP security investments to other ISPs, which may be serving a different market or competing in the same market. The findings show that the nature of these spillover effects can change the effect competition in the ISP market has on incentives for investment in cybersecurity by the ISPs.

1. Introduction

Every user of the Internet confronts significant threats from cybercrime, including phishing, hacking, identity theft, malicious spam, and botnet infection. Some users must also confront targeted attacks and espionage. A recent RAND Corporation report describes how cybercrime has become a profitable industry with supporting services and software tools sold in a large black market (Ablon et al. 2014). Cybercrime flourishes because of underinvestment problems: digital information systems contain vulnerabilities including zero-day security flaws and out-of-date code. Network security design studies have shown that products at all layers of Internet service are released with security flaws that could have been fixed with existing technology. The system design community widely acknowledges that such security flaws are the result of insufficient economic incentives for efficient investment rather than lack of technological knowledge. As the gateway between end users and the Internet at large, Internet Service Providers (ISPs), including those that provide enterprise service as well as residential, are in a special position to help their customers defend against cybercrime and mitigate the underinvestment problems. ISPs have technological and cost advantages in enabling cybersecurity. This paper explores the economic incentives for security investment by ISPs. Specifically, the effect of market structure on ISP security investment decisions is studied.

Cybersecurity, or the decrease of risk from cyber attack, can be addressed at different levels of the Internet communication supply chain. The role of the ISP in cybersecurity is not obvious, not constant, and subject to some controversy. Clark, Berson and Lin (2014) point out that the end-

to-end argument in system design is based on an assumption that all IP-conforming packets are legitimate, and should not be treated differently by the transport providers. They note that "whether and how to violate the end-to-end principle in the name of security is an important policy issue today. How this issue is resolved will have profound implications for security." (p.18) Others have noted that the ISP is positioned to provide additional protection to individual users and small businesses in a cost effective way (Rowe et. al., 2011a, 2011b). For instance, ISPs have more knowledge and expertise than individual users and most small businesses, and thus can more effectively protect users' computers than the users can themselves. ISPs are also ideally placed to monitor traffic, which most do regularly. As the single bottleneck that all Internet traffic must pass through before reaching the end user's computer, one can also think of the ISP as a goalie, blocking the entrance to the end user when malicious content attempts to get through. Rowe et. al. (2011b) similarly use the analogy of the security booth at the entrance to a gated community. Yet this will often require an increased level of invasiveness on the part of the ISP, including deep packet inspection (DPI) in most instances. Most ISPs are reluctant to engage in this behavior. Some countries, such as South Korea, legally prohibit DPI by ISPs.

Many people think of their protection from cyberattacks as residing where their data is stored, their own computers and the databases of the websites they visit, rather than in the transit of packets. As such they can limit their web interactions to known and trusted sites and they can diligently maintain updated antivirus protection on their own machines. While these are important actions, they are often not sufficient in light of the spillovers that occur between the different layers of the Internet as well as between all the different interconnecting parties involved in any Internet transaction (or experience).

Many ISPs do provide some security services to their users. Some will monitor traffic to detect when a user's computer may be infected and acting as a bot or zombie. An ISP may then provide assistance in correcting the problem in the computer, or they may block the user with the infected computer to protect the network. Some ISPs provide their users with education regarding protection of their computers, sometimes offering antivirus software and instructions for installation.

This study addresses the question of how competition between ISPs affects their investment in and provision of cybersecurity. The ISPs' incentives to invest in cybersecurity are distorted by market failures. While much attention has been given to the impact of network effects, this paper focuses on the role of spillover effects and information asymmetry by developing a model that captures the impact of security investment on the probability of a successful attack.

The following section provides an analytic framework for thinking about cybersecurity at the ISP level. This is followed by the development of models of the security investment decisions made by ISPs in different market structure conditions. Section 4 then considers the effect of information asymmetries between ISPs and end users to depict how ISPs might compete for customers in one or more markets in price and unobserved security level.

2. Conceptual framework

Nature of the threat

Although there is a great deal of concern over cyberwarfare, cyberespionage, and cyberterrorism, combatting these is largely a matter of national security policy. In contrast, cybercrime is an ongoing, widely dispersed activity that has many economic characteristics.

Cybercriminals most commonly make small attacks that produce a small gains. But they operate at very large scale, so that the total gain may be quite large. Examples of cybercrimes include selling illegal goods, using illegal methods to sell legal goods (e.g. sending spam e-mail), stealing information like credit card numbers or passwords for financial gain, and holding digital property at ransom (e.g. denial of service (DoS) or locking files).

Cybercrime has evolved into an industry in its own right, complete with supporting services and vertical supply chains (Levchenko et al. 2011 provide a detailed analysis of the spam value chain). A crucial input to cyberscrime is the provision of a large number of Internet Protocol (IP) addresses. Since every individual attack is traceable to an IP, cybercriminals must somehow hijack legitimate IPs. Furthermore, it is easy to block an IP that is an identifiable source of illegal activity, so cybercriminals generally need a large number of IPs and to use each IP relatively lightly. This is usually done by running malware on a large number of individual Internet-connected computers, creating a botnet that can be remotely controlled. Alternatively, cybercriminals may knowingly cooperate to share seemingly legitimate IPs. In either case, the IPs are ultimately registered to an ISP, so that ISP could potentially either be held responsible for a cybercrime or take measures against it.

Layers and investments

One can simplify by thinking of Internet service as consisting of three important levels: the end user, the ISP and the content provider. Each has a role in providing cybersecurity. End users and content providers are similar in the sense that both are edge nodes and both have computers that might be compromised. Content providers are distinguished by being more vulnerable to direct attack (DoS, stealing large lists of passwords or credit card numbers) and by their scale which permits different types of security investments. ISPs operate in the middle moving traffic between end users and content providers.

At each layer, agents can make investments to improve cybersecurity. End users can take action at both their local machine level and their local network. On their local machines they can engage in avoidance behaviors or "digital hygiene" (not downloading malware, running a firewall) and preventative measures (running a regular antivirus scan, using easily secured operating systems and applications, connecting to the Internet less [e.g. in coffee shops or when the computer is not being used], providing information about files and sites causing cybersecurity breaches to interested parties). At the local network level, end users can purchase a router with additional firewall capabilities, require high encryption standards for their wireless networks, and disable wireless sharing.

Content providers can take similar measures as end users, but they will often do so at scale with the help of IT professionals. For this reason, content provider computers are much less likely to be part of botnets, though still prone to data theft. Content providers may also purchase services from content delivery networks (CDNs). Although CDNs are primarily designed to deliver a faster, more responsive service to end users, they also offer significant cybersecurity advantages.

In particular, they can act as a "heat sink" for DoS attacks, limiting the potential damage and exhausting the resources of a DoS attacker.

The investments that ISPs can make include monitoring their networks for evidence of cybersecurity breaches, actively notifying or denying service to customers causing cybersecurity breaches, using more secure protocols at the Internet and application layers, and encouraging cybersecurity-promoting behaviors by end-users (through education or providing/upselling software) (Rowe and Wood 2013). The monitoring of network traffic for cybersecurity reasons is controversial because it involves inspecting, including potentially deep packet inspecting, and filtering customers' traffic. This introduces both network neutrality and privacy concerns.

Effects on ISPs of cybersecurity investments
For ISPs, the benefits of cybersecurity investments fall into five categories:

1. *Reducing direct attacks on ISPs*. ISPs themselves operate extensive administrative systems storing credit card numbers, passwords, and customer information. These may be attacked just like any other content provider. In addition, ISPs' routers and other infrastructure systems are potentially vulnerable to attack. However this latter form of attack is difficult and more dangerous in terms of detection, so it does not appear to be a major vector for financially-motivated cybercriminals (though it is a major concern for cyberwarfare and cyberterrorism).

2. *Reducing traffic due to cybersecurity breaches*. Botnets and particularly DoS attacks can generate a lot of network traffic. Potentially this could increase infrastructure costs for ISPs. However, there is no evidence of this as a current motivation for cybersecurity investments by ISPs.

3. *Gain of customers due to perceptions of cybersecurity*. An individual ISP could gain customers due to improved cybersecurity if end users either increase use of the Internet or switch from a different ISP that they perceive as less secure. At present, there is no evidence that consumers acknowledge a role for their ISP in cybersecurity. A survey of Internet guides to selecting an ISP did not turn up evidence of cybersecurity as a criterion. Even Consumer Reports did not evaluate ISPs in their cybersecurity reviews, instead focusing on antivirus and firewall software. A recent Department of Homeland Security report specifically recommends subsidies and incentives for ISPs because consumers either don't perceive or misperceive the effects of ISP cybersecurity investments (Department of Homeland Security 2013).

4. *Reducing Legal Responsibility for Damage from Cyberattacks.* At present, ISPs do not bear legal responsibility for damage from cyberattacks in the US. American federal cybersecurity regulations do not apply to ISPs. On the state level, California Assembly Bill 1950, passed in 2004, does require that all businesses that "obtain personal information about a California resident...implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure." Other state-level security breach notification laws also require that consumers are notified by businesses in the event of a security breach. Neither of these sets of laws have yet been invoked in a court case against a business, let alone an ISP, and this invocation would act as the key test for determining the definition of "reasonable security procedures and practices". The FCC's

Communications Security, Reliability and Interoperability Council have developed their own best practices for cybersecurity for ISPs, but ISPs have repeatedly resisted and expressed loud opposition to attempts to create formal federal cybersecurity regulations (Gross 2012).

Outside the United States, countries generally promote best practices and information coordination amongst ISPs but do not regulate. Spamhaus identifies many ISPs worldwide, including multiple ISPs in Japan, a country that possesses this best practices/coordination model, with multiple "current known spam issues," and accuses them of "knowingly hosting illegal spam operations," but no known action is forthcoming from these countries' governments (likely an example of the tragedy of the commons, as these operations only cause network disruption in aggregate).

5. *Reducing Peer Sanctions for Cyberinsecurity*. Probably the most important consequence for an ISP of having infected computers in its network is the possibility of being blocked by other ISPs. When it appears that traffic from a particular IP or range of IPs is malicious, other ISPs may contact either the host ISP or the relevant Certificate Authority, and may ultimately block traffic from those IPs. This can be costly for the host ISP which effectively offers poor or no service to those IPs. The host ISP may have to intervene to disinfect the computers at its customers' locations, incurring substantial costs. That said, this peer pressure system is not entirely effective because there are "rogue" or "gray" ISPs that exist in part to support shady activities, and there are also very large ISPs which may be "too big to block" even if they host large numbers of infected computers (van Eeten et al. 2010).

Based on the above survey, two conclusions emerge for modeling of ISP payoffs from cybersecurity investments. First, it appears that the benefits and costs of such investments are not related to the prices or market shares of ISPs since customers do not perceive ISPs as being players in the security arena. This means that ISP benefits and costs are additive terms in the payoff function and do not interact with demand. Second, it also appears that cybersecurity investments and costs are not related to other costs born by the ISP since they have little impact on the amount of traffic carried. Thus, it is accurate to include additively separable terms for the benefits and costs of cybersecurity investments in ISP payoff functions.

Spillovers

The effects of botnets and other cybersecurity breaches create an Internet-wide pollution. While the source of any one attack is a particular ISP, the harms spill out globally. Thus, the effects of cyberinsecurity are partly a global commons problem analogous to environmental pollution. Unlike with the environment, however, it is possible to withdraw from the pollution simply by blocking large ranges of IP addresses (at the cost of interconnectivity). This means that if cybersecurity breaches become sufficiently costly, there is the danger of balkanization of the Internet.

Turning to ISP cybersecurity investments specifically, investment by a particular ISP, has four types of benefits:

1. *A benefit to end-users who enjoy greater security*. This can be considered an externality as long as end users do not recognize that the benefit comes from ISP decisions.
2. *A benefit to content providers*. Since content providers are usually more sophisticated about

cybersecurity than end users, there may be more opportunities for ISPs to internalize this benefit through pricing. However, since the benefit accrues in large part to content providers that are not customers of the investing ISP, this is still largely a positive externality.
3. *A benefit to the ISP itself*. This is the one effect that one can expect will be fully internalized.
4. *A benefit to other ISPs*. This is also a positive externality, but one that may be more subject to commons management by the community of ISPs. In particular, if ISPs are very large, they may find ways of partially internalizing inter-ISP cybersecurity measures.

The exact nature of the spillover depends on the technology of cyberdefense. Varian (2004) discusses three possible payoff cases. In **total effort**, cybersecurity depends on the sum (or average) investment of the ISPs. In **weakest link**, it depends on the investment of the least secure ISP, and in **best shot** it depends on the investment of the most secure ISP. As Varian notes, which of these cases best represents the nature of the payoff for security investment depends on the technology that relates the specific investments of the networks involved to outcomes.

3. Models of ISP security investment with spillovers

Consider a very simple model of ISP profit maximization for both monopoly and duopoly in order to observe the effect of market structure on security investment. For Internet service, this is complicated by the transit that may occur between multiple monopolies in different geographies. Previous models of spillover effects in security make use of strong assumptions regarding the effectiveness of security investment (Kunreuther and Heal, 2003). This paper assumes that despite investments in cybersecurty, costly attacks may still occur. Such attacks are included as probabilistic events, with the probability of attack declining with investments in security.

Consider two cities, each with N households. Assume a fixed market size, so that all N households in both cities subscribe to a broadband connection as long as the monthly price is below some upper limit $\bar{p}$. such that if $p \leq \bar{p}$ then no household will drop service.

Any broadband provider *i* in either city earns per-customer profit:

$$\Pi_i = \alpha_i(p_i\text{-}c) - Y(s_i,s_j)A - s_i^2, \qquad (1)$$

Where α_i is ISP_I's market share, p_i is ISP_I's price, c is the variable cost of serving a customer, Y is the probability of a cyber attack on the ISP's network, and it is a function of ISP_I's chosen level of security s_i, and A is the cost to an ISP of a successful cyber attack on its network, and s_i^2 is the cost of investing in security level s_i. $Y(s_i,s_j)$ is assumed to be a continuous function in the range of (0,1) and increasing in s_i and s_j.

The ISP will choose its price, p_i, and its level of security, s_i, to maximize its profits. Its choice of security level, s_i, will be based on the simple first order condition:

$$\frac{\partial \pi_i}{\partial s_i} = -AY'(s_i) - 2s_i = 0 \qquad (2)$$

This shows that the nature of the impact of an ISP's security investment on the probability of a successful attack determines the ISP's security investment decision.

In general, assume the probability of a cyber attack on the ISP's network has three linear components: (i) the direct effect of a single user's transactions that could result in infection (γs_i), (ii) the indirect effect of infection from another user on the same ISP's network ($\beta n_i s_i$), and (iii) the indirect effect of infection from a user of another ISP's network ($\delta n_j s_j$), resulting in:

$$Y(s_i,s_j) = \gamma s_i + \beta n_i s_i + \delta n_j s_j + z, \text{ with} \quad (3)$$
$$\gamma, \beta, \delta < 0 \text{ and}$$
$$z \text{ sufficiently large that } 0 \leq Y(s_i) \leq 1.$$

Thus the probability of a successful attack on an ISP's network will decrease with increased investment in security as follows:

$$Y'(s_i,s_j) = \gamma + \beta n_i < 0. \quad (4)$$

This base model provides a basis for considering the ISP's choice of security level in different market structures. The first is a monopolist that operates in both cities. In all other market structures considered, ISPs will choose their levels of security in a simultaneous game to depict the strategic interdependent nature of their security investments. In some cases they will also choose their prices in a sequential game.

One two-city monopolist

The ISP who provides broadband service as a monopolist in both markets will choose its security level in each network as shown above. In this extreme case of a single monolithic network, security level is chosen in isolation of the action of other networks, as there are none. The impact of security investment on probability of a successful attack then reduces to:

$$Y(s^M) = \gamma s^M + \beta n s^M + z, \text{ with}$$

$$Y'(s^m) = \gamma + \beta n < 0.$$

Substituting into equation (2) above results in the first-order condition:

$$s^M = \frac{-A(\gamma+\beta n)}{2} \quad (5)$$

As seen above, the level of security chosen by the single monopolist over all markets is the level that minimizes its own expected cost of cyber attack, with no consideration of any external effects of security (positive or negative) on the network users. In this simplest case the ISP's incentive to invest in security is based on the reduction of its own costs of a cyber attack on the network. While increased security creates a benefit to users who will have a lower expected cost of an attack, there is no demand effect of the security level chosen, though this assumption is relaxed below. Also, in this case the improved security of the network is a function solely of the ISP's own investment, with no spillover effects from the investment of other ISPs as it has no interconnection with other ISPs. This assumption will also be relaxed below when considering different possible natures of ISP security investment.

Two one-city monopolies
Now consider two ISPs, each operating in one city only such that each city has a monopolist but the monopolists are different firms with different ownership. ISP 1 has market share $\alpha_0 = 1$ in City A and ISP 2 has market share $\alpha_0 = 1$ in City B. Each firm will set its price independently according to the monopoly profit-maximizing price of as in the above case.

Security of the networks, though, is characterized by strategic interdependence as the security level of ISP 1's network will affect the probability of attack for ISP 2, and vice versa. Thus, even though the ISPs operate in separate discrete markets, they choose their security levels in a simultaneous game.

The ISPs now maximize profits

$$\Pi_i = p_i\text{-}c - Y(s_i,s_j)A - s_i^2,$$

Where the probability of a successful attack is represented by the simple equation (3) above.

Based on the first-order condition equation (2) above the resulting investment in security is:

$$s_i = \frac{-A(\Upsilon+\beta n_i)}{2} \qquad (6)$$

Note that while this appears to be the same first-order condition as in the two-city monopoly case in equation (5) above, the investment is now smaller because $n_i < n$. Thus the simple version of security investment effect on probability of attack results in a reduction of security investment when a monopolist ISP in a market connects with another market's monopolist ISP rather than itself.

When considering more specific possible relationships between the ISPs' security investments, including potential spillover effects, the effect of interconnecting with an independent monopoly ISP from the other market on the probability of attack and on the ISP's security investment depends on the nature of the spillover effects. In this situation, Best-Shot and Weakest-Link spillover effects, as described above, will not fully apply, as the networks, while interconnecting, do not overlap. In this case Best-Shot spillover effects will apply only to that traffic that crosses between networks. The traffic that flows between users of the lower security network will experience the lower level of security only, and have the associated probability of attack.

Therefore, if the ISPs are each monopolists in different cities, neither can fully depend on the other's security for their network, as some traffic will circulate within their own network only, making the Total Effort case more relevant to the two monopoly cities, using Varian's (2004) most simple specification, represented above by equation (3). Since traffic from the other city will go through the recipient's own ISP, then:

$$When\ s_i \geq s_j,\ \ Y(s_i, s_j) = \Upsilon s_i + \beta n_i s_i\ + \delta\, n_j s_i + z,\ and$$

$$Y'(s_i) = \Upsilon + \beta n_i \ + \delta\, n_j,$$

or, essentially:

$$Y'(s_i) = \Upsilon + \beta n \text{ (since } n_i+n_j=n).$$

However,

$$\text{When } s_i < s_j,\ Y(s_i, s_j) = \Upsilon s_i + \beta n_i\, s_i \ + \delta\, n_j\, s_j + z, \text{ and}$$

$$Y'(s_i) = \Upsilon + \beta n_i.$$

Substituting into the fisrt-order condition in equation (2) above:

$$s_i = \frac{-A(\Upsilon+\beta n_i)}{2}, \text{ if } s_i < s_j, \text{ and}$$

$$s_i = \frac{-A(\Upsilon+\beta n)}{2}, \text{ if } s_i \geq s_j.$$

This shows that if ISP *i* invests more in security than ISP *j*, then its security investment is the same as the two-city monopolist investment. When ISP *i* invests less in security than ISP *j*, the ISPs will engage in a simultaneous game where each chooses either a high or low level of security investment.

It is reasonable to think that the relationship between individual security investments and the security outcomes may be structurally different than in this simplest Total Effort Case. Consider the alternative form:

$$Y(s_i) = \Upsilon s_i + \beta\, n_i\, s_i + \delta\, n_j s_j s_i + \ z,$$
$$\text{with } \beta<0,\ \delta<0, \text{ and}$$
$$z \text{ sufficiently large that } 0 \leq Y(s_i) \leq 1.$$

$$Y'(s_i) = \ \Upsilon + \beta n_i \ + \delta\, n_j s_i.$$

.

This reflects a direct effect of an ISP's security investment on its own network as well as an additional combined effect of the combined security investments of both ISPs, similar in concept to the total effort case described above. Substituting into the first-order condition in equation (2) above:

$$s_i = \frac{-A(\Upsilon+\beta n_i+ \delta n_j s_j)}{2}.$$

The result is that a monopolist ISP will increase its security investment with the security investment of the interconnecting monopolist ISP, as

$$\frac{\partial s_i}{\partial s_j} = -\frac{A\delta n_j}{2} > 0.$$

This is a surprising result as one would expect the ISPs to free-ride on the other's security investment. When moving from the single multi-city monopoly to the connection of geographically discrete monopolists there is a change in the security level of each network. The direction of this change in investment will depend primarily on the other ISP's level of security level:

$$s_i - s^M = -\frac{An_i(\delta s_j - \beta)}{2}.$$

If $s_i = 0$, then:

$$s_i - s^M = \frac{A\beta n_i}{2} < 0, .$$

or $s_i < s^M$. As s_i increases, s_i will increase, at some point exceeding the two-city monopolist's security level. This implies that increases in the ownership of territories of monopolist ISPs can bring a decrease in the level of security compared to if the ISP was connecting to a different firm's network.

Two two-city duopolies

Finally, consider two ISPs competing in both City A and City B. Now, the firms are directly competing for customers when they choose their prices and security levels. Competition occurs as follows: First, the two firms receive a starting market share in each market, α_0 for ISP 1 and 1 - α_0 for ISP 2. Then ISP 1 and ISP 2 set their prices, p_1 and p_2 and security levels s_1 and s_2. Finally, the broadband subscribers choose their provider according to demand function

$$\alpha_1 = \alpha_0 - \theta(p_1 - p_2),$$

where α_0 is the initial market share for ISP1, 1- α_0 is the initial market share for ISP2. Now α_1 will denote ISP 1's market share after any reallocation of users based on the price difference between the ISPs. ISP 2's market share after all such switching between networks is 1- α_1.

Note that users respond to a difference in prices but the assumption that demand does not respond to security is maintained. The users then exchange traffic in a completely symmetric way without any difference between the cities or the providers.

Continuing our assumption of symmetric firms, the starting market share is $\alpha_0 = 0.5$ for ISP 1, and thus for ISP 2. The two ISPs each have first order conditions for price and security.

Note that security does not enter into this equation, so one can solve for the symmetric Nash equilibrium in prices

$$p_1 = p_2$$

Since each ISP charges the same price, each firm will maintain their initial market share of one half in each city.

The first-order condition for the choice of security level is unchanged from the prior case above, as the security decision remains orthogonal to the price. Thus the security levels chosen in the symmetric two-city duopolies is the same as the security levels chosen in the two one-city monopolies case above. One implication is that if customers are not considering security in their choice of ISP, then maintaining different ISPs as monopolists in different geographic markets improves security above the single multi-market monopolist case as much as having duopoly in each of the markets. One also sees that security does not improve when two monopolists in discrete markets compete with each other in both markets.

It is important to note that this result is dependent on the assumption that users are not choosing between ISPs based on the level of security provided. This may in fact be the case, as Rowe et al (2011a) and Rowe & Wood (2013) found that the vast majority of home broadband users did not consider security an important factor when selecting their ISP. However, it is also reasonable to think that end users are becoming increasingly aware and concerned about their risks as they shift more of their personal and financial activity to cloud based applications and the media highlights attacks of greater magnitude and frequency. This case is considered below with consideration of the information asymmetry between the ISPs and the users.

Vertical spillovers

The above cases considered some of the potential horizontal spillovers of security investments between ISPs and how that effects an ISP's choice of security level in its network. It is also possible that the ISPs choice of security level is sensitive to vertical spillovers from either end users or content providers. In fact, one would expect that a higher level of security investment by end users will reduce the probability of cyber attack on the ISP's network sufficiently to reduce the ISP's profit-maximizing security investment. Similarly, a higher level of vigilant security exercised by content providers may reduce the ISP's security choice, all else equal. The above models of security choice as a function of other ISPs' security choices assumes constant levels of security for both end-users and content providers.

4. Models of ISP security investment with information asymmetries

Rowe et al (2011a) shows that broadband users value security and are willing to pay their ISPs for increases in security provided. Now consider the effect of competition on ISP security choices when there are demand effects based on consumers' willingness to pay for additional security as well as their limited ability to assess the relative security levels of competing ISPs.

If end users value security and consider the relative security of competing providers when choosing an ISP, ISPs will attempt to convince users of their superior security. Yet security is often an unobservable characteristic when perfect security is unobtainable. While users cannot directly observe a network's security level, they often can observe an incident of successful cyber attack. Users will tend to associate successful attacks with lower levels of security despite the fact that there is always a probability of successful attack in even the most secure network.

When a costly characteristic of a service is unobservable to users and known only to the providers, there is the possibility of the lemons problem. If a user cannot determine if an ISP has a high level of security, he will not be willing to pay for a hgh level of security as he may only be getting a low level of security. If the user is not willing to pay for the unobserved high level of security, the ISP will be unwilling to provide a high level of security as its cost will exceed what the user will pay. This results in only lowlevels of security being provided by the market. (Akerlof, 1970).

While such information asymmetry inherent in the problem of assessing the security level of an ISP, the lemons market result is not inevitable. It may be possible for the ISPs with high levels of security to signal their quality in a way that creates a more efficient equilibrium despite the remaining positive probability of a successful attack. (Spence, 1973).

5. Conclusion and policy implications

This paper explored the effect of market structure on incentives for ISPs to invest in cybersecurity using simple theoretical models of ISP competition. The results show that horizontal spillovers from the investment of other ISPs, either competing or not, can change the incentives for security investment. Even the interconnection with a different noncompeting ISP in a geographically distinct market can increase the incentive to provide increased security. Meanwhile, the existence of a competing ISP within the same market may or may not change the incentives for security investment. If users do not respond to differences in security levels when choosing an ISP, competition will not impact the incentive. Such lack of demand effect may be due to low value for security, low expectation that security, though valued, will come from the ISP versus another level of service provision, or from information asymmetries with inadequate signaling ability of a high-security ISP.

One interesting implication of these findings relates to the nature of ISP consolidation and anti-trust review. ISPs seeking to gain additional markets through merger (such as the proposed Comcast Time-Warner transaction) will argue that the addition of new monopoly or near-monopoly markets will not reduce competition as the number of broadband providers within each market does not change. However, the above findings show there still may be welfare reduction from a lower level of security offered by the ISPs. In particular, two monopolist ISPs in distinct markets will increase their security levels in response to the level of the other interconnecting monopolist ISPs. This suggests there may be need for broader review of such mergers, beyond the existing anti-trust competition reduction standards.

REFERENCES

Ablon, Lillian, Libicki, Martin, Golay, Andrea. 2014. Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar. Santa Monica: RAND.

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

Clark, David, Berson, Thomas, and Lin, Herbert S., editors. 2014. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.* Washington DC: The National Academies Press.

Department of Homeland Security, Executive Order 13636: Improving Critical Infrastructure Cybersecurity, Incentives Study Analytic Report, June 12, 2013.

Grant Gross, Grant. 2012. "ISPs: No New Cybersecurity Regulations Needed," PCWorld, March 7.

Kunreuther, Howard and Heal, Geoffrey. 2003. "Interdependent security." Journal of Risk and Uncertainty. 26: 231.

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., ... & Savage, S. (2011, May). Click trajectories: End-to-end analysis of the spam value chain. In Security and Privacy (SP), 2011 IEEE Symposium on (pp. 431-446). IEEE.

Rowe, B., & Wood, D. (2013). Are Home Internet Users Willing to Pay ISPs for Improvements in Cyber Security?. In Economics of Information Security and Privacy III (pp. 193-212). Springer New York.

Rowe, Brent, Wood, Dallas, Reeves, Doug, and Braun, Fern. 2011a. "Economic Analysis of ISP Provided Cyber Security Solutions." Institute for Homeland Security Solutions. June.

Rowe, Brent, Wood, Dallas, Reeves, Doug, and Braun, Fern. 2011b. "The Role of Internet Service Providers in Cyber Security." Institute for Homeland Security Solutions. June.

Spence, Michael. 1903. "Job Market Signaling." *Quarterly Journal of Economics*. 87 (3): 355-374.

Van Eeten, M., Bauer, J. M., Asghari, H., Tabatabaie, S., & Rand, D. (2010). The role of internet service providers in botnet mitigation: An empirical analysis based on spam data (No. 2010/5). OECD Publishing.

Varian, H. (2004). System reliability and free riding. In Economics of information security (pp. 1-15). Springer US.