Comments on Incentives To Adopt Improved Cybersecurity Practices

Terrence August
Rady School of Management
University of California, San Diego
La Jolla, CA 92093-0553
taugust@ucsd.edu

Tunay I. Tunca
Robert H. Smith School of Business
University of Maryland
College Park, MD 20742-1815
ttunca@rhsmith.umd.edu

April 29, 2013

1 Overview

In this commentary, we are aiming to provide insights and suggestions to utilize incentives to improve the adoption of cybersecurity practices by critical infrastructure providers. Our approach is two-fold: First, we will discuss the known research results in the academic literature on the subject. Second, based on our own existing research, we will provide some insights and suggestions on the problem on managing incentives to adopt cybersecurity practices within the existing legislative framework as well as through new legislation.

2 Insights from Existing Research

There is a growing body of studies that explore the management of incentives in cybersecurity. We will mention some insights from this body of research and later particularly focus on insights from studies on liability-based policies.

In a broader sense, cybersecurity falls into the concept of interdependent security, where actions and investment decisions of agents in a network of interconnected users impact the risk endured by the other agents. These agents could be other users (both individuals and firms), software and network providers, as well as providers of other critical infrastructure. In such environments, it has been argued that in order to best induce adoption of security measures, regulation and institutional coordination mechanisms may be needed (Kunreuther et al. 2002 and Kunreuther and Heal 2002).

A range of different policies and procedures are studied and suggested in the literature for improving cybersecurity. One way is the issuance of professional information security ratings on service providers

resembling financial credit ratings. It has been found that implementing such ratings does not always benefit service providers and customers – even those customers who demand highly secure business partners. On the other hand, adopting such ratings can benefit social welfare and it can be advisable to sanction and encourage such information security ratings (Zhou and Johnson 2010). Another approach suggested is software diversification in a network environment, as such a strategy can help alleviate the negative externalities associated with security interdependence. For this approach to be effective, software markets should be characterized by multiple products with few shared vulnerabilities (Chen et al. 2011). Another suggested way for improving cybersecurity is increased government enforcement against attackers and hackers. Png and Wang (2009) demonstrate that enforcement can lead to reduced attacker effort, and can be an effective overall policy for improved security.

As the gatekeepers of interconnectivity and by being the parties with greatest visibility and information, Internet Service Providers (ISP) play a critical role in maintaining cybersecurity. Therefore, an efficient and effective method for improving cybersecurity, and increasing compliance and adaptation of best cybersecurity practices, could be targeting ISP incentives. In the literature, security investments by ISPs have been studied and it has been argued that ISPs may lack incentives to maintain secure networks, pointing toward a need for regulation (Garcia and Horowitz 2007). Clayton (2010) posits that because of the lack of sufficient incentives for ISPs to help maintain the security of their customers, government may need to play a role in subsidizing the protection of customers' systems. In addition, a potential more proactive role for ISPs to improve cybersecurity has been examined as well. Wood and Rowe (2011) quantify the willingness-to-pay of consumers for added security packages offered by ISPs. They find support that consumers are willing to accept higher prices, security training, and account suspension in order to avoid the diverse impacts associated with unblocked security attacks.

Liability

The use of liability in cybersecurity is also a heavily discussed topic. A detailed discussion of this particular body of research can be found in August and Tunca (2011). Much of the gist of the intuition provided in this literature may apply to network providers such as ISPs as well. One commonly discussed suggestion is imposing loss liability on software vendors and providers. Arguments in favor of such a policy state that liability will provide economic incentives for vendors or providers to increase their investments in software security (Schneier 2004, Werth 2009). By investing more toward actions that improve software security such as debugging, testing, and fixing security flaws, a vendor or provider can reduce its liability exposure, i.e., payments for economic losses in case of a security breach (Kaner 1997, Ryan 2003, Cusumano 2004, Schneier 2008). A similar argument can be made for network infrastructure providers as well, considering that

malware and abnormal traffic monitoring and control; installation, updating and maintenance of security software and hardware at critical network gateways; and user training can all help reduce vulnerability of network infrastructure. On the other side of the argument, opponents of liability assert that imposing liability on producers and providers may stifle investments in software products (e.g., Heckman 2003, Joyce 2005, Ho 2009). It is also argued that the best recourse of action could be to directly improve the quality of software because the high costs of enforcing legal liability would be best applied toward improving security (Armour and Humphrey 1993).

Formal economic modeling of the problem has also yielded further insights. Government imposition of vendor risk sharing may lead to more secure, higher quality software products (Kim et al. 2010). It has also been argued that software liability is effective at making producers increase security quality when consumers are heterogeneous in their sensitivities to quality, whereas it is ineffective if consumers are more homogeneous (Kim et al. 2011). Among the papers in this literature, August and Tunca (2011) particularly focuses on analyzing the effect of liability in a network setting characterized by interdependent risks. In this case, software users impose negative externalities on one another which alters the effectiveness of liability schemes. Further, this study demonstrates that the users' ability to shield themselves from risk as well as reduce the externality they impose on others by maintaining their own systems' security, in the presence of software security vulnerabilities, should be taken into account when setting liability policies in a network environment. The insights garnered from August and Tunca (2011) offer recommendations on the structuring of cybersecurity incentives. An in-depth discussion follows in Section 3 of this document.

3 Structuring Incentives for Cybersecurity

In the current network environment with security risk interdependencies, there are serious incentive problems among various actors whose decisions impact the overall security of the cyber infrastructure; the risks associated with attacks on this infrastructure are growing in number and potential impact; and the importance of the role of regulation is increasingly understood and debated. However, answering how regulation or innovative cybersecurity incentives can actuate a shift toward preferable outcomes, such as an increasingly secure cyber infrastructure and higher social surplus associated with such public resources, is still not well understood and requires more formal economic analysis. In the following, we provide some recommendations and general insights that are based on our current understanding distilled from our recent research.

There is a host of regulatory policies and incentives that can be targeted at improving cybersecurity including:

- Liability on economic losses associated with cyber attacks

- Issuing and enforcing standards on any processes or practices affecting cybersecurity
- Subsidies and cost-sharing mandates to encourage more appropriate and secure usage of technologies
- Taxes and penalties that target and discourage potentially high risk behavior by users
- Subsidies for improved technology design for cybersecurity risk diversification

These policies and incentives can be categorized based on whether they apply in the long run or short run. Those targeting the long run (e.g., liability and standards) aim to improve the security associated with technologies that are eventually produced by encouraging better investments in security. Those targeting the short run (e.g., subsidies on software and infrastructure security maintenance and good practices) apply to existing products and technologies and aim to immediately impact the manner in which they are deployed to improve cybersecurity; in other words, the inherent security associated with the products and technologies is held fixed in short-run settings. Those targeting the long run (e.g., imposing and maintaining software and network security standards) aim to create incentives on software and infrastructure providers to invest in reducing the vulnerability of their products and offerings.

We begin by discussing these short-run settings. In August and Tunca (2006), we study networks exhibiting security interdependence where software and/or network usage is priced by a provider. In these networks, users can also incur individual protection investments to reduce their cybersecurity risk. Given a short-run setting, the inherent security properties of the network are fixed, but users influence the actual security level that realizes based on their behavior. We examine several different policies and incentive structures aimed at increasing cybersecurity: (i) government imposed mandates on network users to maintain their own security (e.g., requiring user to protect their systems by applying security patches and investing in other defensive measures), (ii) subsidies to elicit improved security maintenance set by vendors and service providers behavior by network users, (iii) government-specified subsidies that must be provided by network owners to elicit improved security maintenance behavior by network users, and (iv) government-specified taxes on network usage. We study this set of incentives for (a) privately provided software and networks where the network owner charges for use, and (b) socially provided software and networks that are free to use.

Insights and recommendations that can be derived from August and Tunca (2006) on how to incentivize firms, users and infrastructure providers are as follows: For case (a), government-imposed mandates are likely to be ineffective if generally applied to the entire network user base. An open question is whether or not targeted mandates could be beneficial, particularly for specific network users who also are critical infrastructure providers or network users that interact with these providers. In short-run settings where the network has a high inherent security risk and the cost for network users to protect themselves is

also high, subsidies to incentivize security maintenance by users are likely to be beneficial to both social welfare and even network owner profits. In certain cases, network owners will not have natural incentives to provide subsidies, but it is in the best interest of government to specify subsidies to be provided by network owners. Otherwise, cybersecurity risk will be too high, and social welfare will be depressed as a result. When user protection costs are low, incentive provision can be unnecessary. In this case, network users will make security choices that are more aligned with socially optimal decisions. For freely provided networks or case (b), the recommended cybersecurity incentives can be significantly different. In this case, a usage tax on network users is the most beneficial policy instrument which helps reduce the amount of cybersecurity risk faced on the network. The tax effectively discourages the activity of users with high-risk behavior, which, in turn, can help reduce risk because of the security interdependence that exists between users. Network user cost protection subsidies can still play role but are less effective than taxes except for security environments with both low inherent security risk and low costs of user protection.

In August and Tunca (2011), we further study whether liability policy should play a role in network environments with interdependent cybersecurity risk. In this study, we also differentiate between cases where a known patch or remedy is not available for users to protect their systems ("zero-day" threats) and those where such remedies are available and hence the users have had opportunities to take precautionary measures to protect their systems (non zero-day threats). First, in a short-run setting we find that imposing liability for economic losses incurred by network users onto the network provider is particularly detrimental when the security properties of the network are fixed in the short run. In this case, the network provider will raise price to restrict usage and reduce its exposure to liability on these potential security losses. The network provider's behavior in response to liability policy in short-run settings leads to outcomes that are welfare inferior to the status quo.

In August and Tunca (2011), we also study long-run settings where network providers have the ability to respond to policy and cybersecurity incentives by adapting their security investments in products. We again examine several incentives aimed at increasing cybersecurity: (i) network provider liability on economic losses caused by cybersecurity attacks on network users, (ii) government-specified subsidies that must be provided by network owners to elicit improved security maintenance behavior by network users, and (iii) government-specified security investment levels to be maintained by network providers (i.e., enforced cybersecurity standards). First, it is important to note that the aggregate security of the network depends on both the security investment level of the network owner/operator as well as the individual security protection decisions made by the network users because of security interdependence. Second, the network owner already has incentives to invest in security because (a) less users will subscribe to riskier networks which hurts owner revenues, and (b) a more secure network can also be coupled with a higher price which helps boost revenues. As a result, when examining a policy such as government-imposed network owner

liability on economic losses, what matters is to what extent does such a policy marginally impact the owner's security investment beyond that which it already has incentives to make.

In comparing these three classes of incentives, it is generally the case that loss liability is the least effective policy and it often backfires, leading to reduced investments in cybersecurity by network owners. Liability always directly impacts the upside benefit of serving additonal network users; on this side of the trade-off, a network owner will try to reduce the number of network users it serves, which can reduce social welfare. We find that a regulatory approach involving cybersecurity standards and an incentives approach involving network user security protection subsidies can be the preferred approach under different market conditions. Cybersecurity standards tend to perform best in high risk network environments where network users can shield themselves from most of the security risk by incurring protection costs. In such conditions, the equilibrium investments in security made by network owners are often insufficient, and security standards can help address their misaligned incentives. On the other hand, consider high risk network environments where users are still exposed to sizable systemic security risk even when fully protecting themselves. In these cases, if the cost of protection is not too high, providing additional incentives to encourage network users to invest and protect is welfare superior. However, if the cost of user protection is prohibitively high, these subsidies would necessarily need to be quite large, in which case a cybersecurity standards approach remains preferred.

Interestingly, we demonstrate in August and Tunca (2011) that it is not necessarily the case that having the network owner make larger investments in cybersecurity is beneficial to social welfare. In fact, because both these product/technology investments made by network owners and protection investments made by users are types of cost that affect the aggregate security level of the system, it can sometimes be more efficient for the costs to be allocated at the network user level. In such cases, the protection investments made by network users act as substitutes to the investments made by network owners. For example, we see this outcome realize in high security risk environments where network users can almost fully shield themselves from security risk by incurring substantial protection costs. Under these market conditions, it is more efficient to engender greater investments at the protection level by inducing network users to incur these costs by providing subsidies. The network owner naturally reduces its security investment in the network, but the aggregate effect on cybersecurity is beneficial to welfare.

Another strategy to reduce cybersecurity risk is to design network products and technologies to take advantage of the benefits of risk diversification. When the interdependent cybersecurity risk faced by network users can be made idiosyncratic to the network being used, a network provider has incentives to design and offer multiple variants of its network product to benefit from risk diversification. August et al. (2013) craft an economic model to formally examine these risk diversification benefits and find that, in high security risk environments, social welfare can increase substantially by offering multiple network variants.

However, the average per-user economic losses associated with security decrease only when the cost of protection incurred by users is high. When these costs are low, average per-user security losses actually increase even though social welfare still improves by increasing the aggregate usage of the diversified networks.

4 Summary of Recommendations and Suggestions

In summary, our recommendations for incentivizing ISPs among critical infrastructure providers, other network providers and direct internet usage enablers, coming from the insights and implications from our research can be summarized in the following table (Table 1):

	(a) Short Run		*(b) Long Run*	
Optimal Policy	Low maintenance cost	High maintenance cost	Low maintenance cost	High maintenance cost
Low zero-day risk	No Extra Liability	Maint. Subsidies	Standards	Standards
High zero-day risk	Maint. Subsidies	No Extra Liability	Maint. Subsidies	Standards

Table 1: Recommended policy for various security landscapes and investment scenarios (adapted from August and Tunca 2011).

An important point to keep in mind for the above table is that the cost of enforcing security standards should be taken into account before choosing that policy as in certain cases those costs can be prohibitive. In such cases, maintenance subsidies can be the best alternative. For other critical infrastructure providers that are users of the cyber-infrastructure rather than being providers, the main insights that come from research imply that employing loss liability may not be the best and cost sharing policies such as maintenance subsidies are likely to be more helpful. However, future research that particularly focuses on the effect and the role of non-ISP critical infrastructure providers would be helpful in providing further and clarifying insights and recommendations.

References

Armour, J. and W. S. Humphrey (1993, Aug). Software product liability. Software Engineering Institute, Carnegie Mellon University.

August, T., M. F. Niculescu, and H. Shin (2013). Cloud implications on software network structure and security risks. Working Paper. University of California, San Diego, Georgia Institute of Technology.

August, T. and T. I. Tunca (2006). Network software security and user incentives. *Management Science 52*(11), 1703–1720.

August, T. and T. I. Tunca (2011). Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science 57*(5), 934–959.

Chen, P., G. Kataria, and R. Krishnan (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly 35*(2), 397–422.

Clayton, R. (2010). Might governments clean-up malware? In *Proceedings of the Ninth Workshop on Economics of Information Security*, Harvard University, Cambridge, MA, USA.

Cusumano, M. A. (2004). Who is liable for bugs and security flaws in software? *Communications of the ACM 47*(3), 25–27.

Garcia, A. and B. Horowitz (2007). The potential for underinvestment in internet security: implications for regulatory policy. *Journal of Regulatory Economics 31*(1), 37–55.

Heckman, C. (2003). Two views on security software liability: Using the right legal tools. *IEEE Security & Privacy*, 73–75.

Ho, V. (2009, Jun). EU software liability law could divide open source. *CNET News*.

Joyce, E. (2005, Feb). More regulation for the software industry? *EnterpriseITPlanet.com*.

Kaner, C. (1997, Oct). Software liability. Pacific Northwest Software Quality Conference.

Kim, B. C., P. Chen, and T. Mukhopadhyay (2010). An economic analysis of the software market with a risk-sharing contract. *International Journal of Electronic Commerce 14*(2), 7–39.

Kim, B. C., P. Chen, and T. Mukhopadhyay (2011). The effect of liability and patch release on software security: The monopoly case. *Production and Operations Management 20*(4), 603–617.

Kunreuther, H. and G. M. Heal (2002). Interdependent security: The case of identical agents. Working Paper, Columbia Univ.

Kunreuther, H., G. M. Heal, and P. R. Orszag (2002). Interdependent security: Implications for homeland security policy and other areas. *The Brookings Institution, Policy Brief #108*.

Png, I. and Q.-H. Wang (2009). Information security: User precautions, attacker efforts, and enforcement. *Proceedings of the 42nd Hawaii International Conference on System Sciences*, 1–11.

Ryan, D. J. (2003). Two views on security software liability: Let the legal system decide. *IEEE Security & Privacy*, 70–72.

Schneier, B. (2004, Oct). Information security: How liable should vendors be? *Computerworld*.

Schneier, B. (2008, Jul). Software makers should take responsibility. *The Guardian*.

Werth, C. (2009, Jul). Software crackdown. *Newsweek*.

Wood, D. and B. Rowe (2011). Assessing home internet users demand for security: Will they pay ISPs? In *Proceedings of the Tenth Workshop on Economics of Information Security*, George Mason University, Fairfax, VA, USA.

Zhou, Z. Z. and M. E. Johnson (2010). The impact of professional information risk ratings on vendor competition. Working Paper, Rady School of Management, University of California, San Diego, Tuck School of Business, Dartmouth College, Hanover, NH.