Information Economics and Policy 37 (2016) 42–51

Contents lists available at ScienceDirect

Information Economics and Policy

journal homepage: www.elsevier.com/locate/iep

Attack-prevention and damage-control investments in cybersecurity☆

Wing Man Wynne Lam

University of Liege (ULg), HEC Management School, Liege Competition and Innovation Institute (LCII), Belgium

ARTICLE INFO

Article history:
Received 1 November 2015
Revised 5 October 2016
Accepted 17 October 2016
Available online 19 October 2016

JEL classification:
K13
L1
L8,

Keywords:
Cybersecurity
Investment
Standard
Liability
Bilateral care

ABSTRACT

This paper examines investments in cybersecurity made by users and software providers with a focus on the latter's concerning attack prevention and damage control. I show that full liability, whereby the provider is liable for all damage, is inefficient, owing namely to underinvestment in attack prevention and overinvestment in damage control. On the other hand, the joint use of an optimal standard, which establishes a minimum compliance framework, and partial liability can restore efficiency. Implications for cybersecurity regulation and software versioning are discussed.

1. Introduction

New security concerns are constantly arising as privacy breaches proliferate and cyber attacks escalate. For example, a recent data breach at Dropbox has affected more than 68 million users.[1] And, as persistent are the rise of "ransomware" (a malicious program that encrypts files on the victim's computer and demands a fee before unlocking those files), the discovery of security flaws on smartphones, and the emergence of new security risks of the "Internet of Things" (e.g., hackers stealing sensitive data from owners of Internet-connected objects—from locks, lights, thermostats, televisions, refrigerators, and washing machines to cars). It is also common to see software providers releasing vulnerable alpha versions of their products before the more secure beta versions. Thus, a critical lag has emerged between software providers' investment in cybersecurity and today's rapidly evolving technological advances. This paper presents a model accounting for the investment incentives of the various parties affected by security concerns and analyzing the appropriate remediation when these incentives depart from the socially efficient level.

A prominent feature of the software industry is its fast development and release of new functionalities. Software products are therefore never free of bugs, and it is very common to observe multiple rounds of investments. To incorporate this feature, I consider a software provider that sells a software product—subject to potential security problems—and can invest in attack prevention and damage control to increase security. Attack-prevention investments, e.g., good infiltration detection and authentication technologies, reduce the probability of successful attacks (among others, phishing, denial-of-service, virus attacks). On the other hand, damage-control investments are remediation strategies, e.g., finding, testing, and fixing bugs reduces the probability that the hacker finds and exploits a bug before the provider does. Both types of investments are crucial to raising the security level of a product. For instance, Gartner predicts that both investments in attack prevention and damage control will continue to grow, as

☆ I thank the editor, Christiaan Hogendorn, and two anonymous referees for comments that significantly improved the paper. I thank Paul Belleflamme, Giacomo Calzolari, Jacques Crémer, Vincenzo Denicolò, Axel Gautier, Domenico Menicucci, Paul Seabright, and the participants at the LCII and CORE 2015 Digital Economy Workshop, the WEIS 2015 Conference, and the EALE 2015 Conference, the George Washington University 2016 Cybersecurity Workshop, as well as those at seminars at Télécom ParisTech and Saint-Louis University Brussels for their valuable comments. I also acknowledge the support of Toulouse School of Economics and University of Bologna at earlier stages of this research. All opinions expressed are strictly my own.

E-mail addresses: wingmanwynne.lam@ulg.ac.be, wynne1018@gmail.com

[1] See "Dropbox hack affected 68 million users," *BBC News*, August 31, 2016, available at http://www.bbc.com/news/technology-37232635.

http://dx.doi.org/10.1016/j.infoecopol.2016.10.003
0167-6245/

organizations focusing just on one have not been successful in increasing security.[2]

Software users can also invest in security. If the provider finds and discloses a bug, then users can adopt various defenses (among others, user-side encryption, firewalls, virus detection techniques, intrusion detection systems, data-loss prevention features) against online attacks. Not all users, however, whether enterprise and home users, take preventive measures even when software providers disclose bug information. Kaspersky Lab reports that hackers often use exploits for known vulnerabilities against enterprises because enterprises are slow to apply patches. For example, the use of exploits for office software vulnerabilities against enterprise users is three times as frequent as that against home users.[3] Symantec (2016) also reports that more than 75% of websites Symantec scanned contained unpatched vulnerabilities in 2015, with very little improvement over the past three years. We capture the lack of precautionary actions by assuming that there are costs of taking precaution. Furthermore, depending on the magnitude of these costs, a user is either a layman or an expert: actions are more costly for the former than for the latter. For example, the costs of taking precautions vary between different types of enterprise users. While financial services, telecommunication sectors, utilities and government departments have far more resources to hire security professionals to maintain and manage top-notch security tools, smaller companies have relatively limited budgets to that effect. Hence, their engineers may not have a keen understanding about the state-of-the-art security, which results in higher learning costs than their more advanced counterparts. For short, there are three types of investments: the provider's attack-prevention investment reduces the attack occurring probability (once an attack occurs, it causes damage to both the provider and the users), whereas the provider's bug-fixing investment and user precautionary actions limit the extent of the damage.

To eliminate potential investment inefficiencies, the regulator can ideally impose the optimal levels of attack-prevention and damage-control investments whenever both investments are observable and verifiable. In reality, however, it is difficult to monitor a provider's investment in bug discovery and bug fixing: because the objective is to find hitherto unknown vulnerabilities, the success of discovery, which depends on rapidly evolving attack and defense technologies, is largely uncertain. On the contrary, attack-prevention investment is relatively easy to monitor as its objective is to defend against known vulnerabilities. For instance, new software products can be tested for known vulnerabilities to ensure that they are secure before they can be released on the market. Thus, I assume that the regulator can regulate directly attack-prevention—but not damage-control—investment by setting a standard (i.e., a minimum level of security). In practice, there are different types of security standards—such as encryption standards, security breach notification standards, IT continuity standards—set by the National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS) in the U.S. and more widely by the International Organization for Standards (ISO) and Internet Engineering Task Force (IETF). Similarly, in the banking industry, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides guidelines that the regulator can use to assess whether bank security is good enough to prevent certain known attacks. Damage-control investment, the success of which is hard to predict, can be regulated indirectly by liability rules. Liability rules, which are governed by the tort system, state the amount of damage each party is liable for. For example, software users may file lawsuits against software providers for security breaches, data leakage, and infringement of privacy, and if providers are proven to have caused harm, they will be held accountable for user damage.

Clearly, if the provider is not responsible for damage harming users, its investment incentives will be suboptimal. In the existing literature on bilateral care—where both the provider and the users can undertake one type of investment to reduce the expected damage—conventional wisdom suggests that strict liability with a defense of contributory negligence—under which the provider is fully liable only if the user is not negligent—yields the optimal investment (Brown, 1973). I, however, show that when the provider undertakes multiple types of investments, its investment incentives can still be suboptimal even when it has full liability. In particular, the provider underinvests in attack prevention and overinvests in damage control. The reason is that the provider does not take into account the precautionary costs of the users, which gives it too much incentive to search for bugs. Moreover, because attack-prevention and bug-detection investments are substitutes, allowing providers to fix security problems later increases the likelihood of releasing a less secure software product in the first place. This result is akin to the practice of software versioning in the software industry, where providers first release versions of products that are prone to security issues and then fix these problems only at later stages (see Section 5.2). Interestingly, a partial liability rule (or more precisely, the provider bears a fine/reimbursement that is smaller than user damage level) with an optimal standard can restore the first-best outcome. And this result is consistent with the view taken by some security experts: Bruce Schneier, for instance, argued that

> "100% of the liability should not fall on the shoulders of the software vendor, just as 100% should not fall on the attacker or the network owner. But today, 100% of the cost falls directly on the network owner, and that just has to stop."[4]

The important implications of these results are that the regulator can implement similar standards of security as other, already regulated, industries such as automotive and aviation, and implement policies that help users reduce their costs of taking precautions. For instance, since not all users apply patches immediately after their introduction (home users may ignore security risk warnings, while enterprise users may not apply patches in a timely manner because of time constraints), policies that help synchronize patch release and adoption cycles can be useful (see Section 4.1). Furthermore, I show that increasing the number of expert users improves social welfare. On the other hand, it may exacerbate the under- and over-investment problems, which has important implications for user education in the software industry. The difference between private and social investment incentives arises from two sources of inefficiency. The first is that the provider does not pay fully for the damage, and the total amount of damage is decreasing in the number of expert users. The second source of inefficiency is that the provider ignores the precautionary costs of the users, and the total cost of precaution is increasing in the number of expert users. When the provider bears substantial liability for user damage, the second source of inefficiency dominates. These results suggest that if the objective of the government is to improve social welfare, it would be desirable to provide more support and training in the area of cybersecurity so that users become more competent in managing security threats. If its objective, however, is to alleviate inefficiencies in investments, then the government needs to be careful about increasing the number of

[2] See "Gartner says Worldwide Information Security Spending will grow 7.9% to reach $81.6 billion in 2016," *Gartner Press Release*, August 9, 2016, available at http://www.gartner.com/newsroom/id/3404817.

[3] See "Evolution of cyber threats in the corporate sector," *Kaspersky Security Bulletin 2015*, December 10, 2015, available at http://bit.ly/2bQ4Q1C.

[4] See Schneier (2007).