STANFORD UNIVERSITY

CRACKING CYBERSECURITY

By DAVID (WEI) JIA

STANFORD, CALIFORNIA

May 6, 2012

Executive Summary

Introduction and Motivation

Because of the tremendous impact and importance of cyberspace in our daily lives, the government must protect cyberspace and guarantee its security to ensure the liberty of our citizens. The government must utilize not only stick and carrot economic policies to incentivize the free market, but also enact security compliance and liability laws to overcome the inherent network externalities of cybersecurity.

Market Forces and Economic Incentives

Economic incentives have proven to be successful in helping correct the free market towards a particular policy position. Most firms do not benefit economically from enhanced security, so governmental economic policies can incentivize firms to invest more in product security. However, economic incentives and the free market are not sufficient. This is because:

- Security is essentially a public good because the benefits of security are only perceived and are highly distributed. This leads to negative network externalities.
- Firms are not likely to enhance security because they are more focused on features, whose potential benefits far outweigh economic incentives for security.
- Firms have a tendency to presume that the cybersecurity enacted by intermediary firms, such as Internet Service Providers (ISP), will suffice in guaranteeing their own security.
- Cybersecurity products have a first mover disadvantage because a firm only benefits if all other firms are using the product: RSA would not work if only one firm implemented it.

Cyberspace Compliance and Liability

Because of the inherent inadequacies of market policies, we recommend that the government also enact security compliance standards for different industries with the following features:

- Have industry-specific compliance laws that firms in a particular industry must meet.
- Formulate these laws through an open rulemaking process, with input from and collaboration with industry leaders.
- Standards can also be driven by the private sector through industry associations.

In addition, we also recommend liability laws to incentivize firms to be more self-motivated to prevent cybersecurity failures. We recommend the following features:

- Firms that are found negligent to their duties to build and maintain secure systems are penalized with an explicit cost.
- The explicitness of this cost will help firms internalize the full risk of a security failure.
- Firms can be liable for both direct harm and for recovery costs.
- Larger liability costs can be addressed by an insurance network. The due diligence process will be shifted from the government to a more efficient cybersecurity insurance network.

Introduction and Motivation

In recent years, cyberspace has affected the lives of practically every U.S. citizen. We depend on this vastly complex platform for economic prosperity and to satisfy our most basic needs. Because of this wide-reaching nature of cyberspace, we must secure and protect it from cyberattacks and sophisticated adversaries who wish to jeopardize the freedom, safety, and welfare of our citizens. The President has identified cybersecurity as one of the top priorities of his administration and directed a 60-day review of current U.S. cyberspace security policies. This "Cyberspace Policy Review" recommends a range of ways to strengthen our cybersecurity policy. In the current report, we would like to highlight and call attention to a particular recommendation: the need for public and private sector collaboration in securing cyberspace.

In cyberspace, because of the intertwined nature of incentives and responsibilities that are spread among the public and private sectors, "[t]he Federal government cannot succeed in [securing cyberspace] if it works in isolation" (Hathaway 17). The majority of the national information infrastructure is owned and operated by private sectors entities. At the same time, these entities depend on government policies and programs to give them tools to succeed in their respective markets. With such distributed and interconnected ownerships, responsibilities, and incentives, collaboration between the public and private sector is not only important but also necessary. Thus, to secure cyberspace, the government must enact non-compulsory stick and carrot economic policies to properly incentivize the market, and also work with industry leaders to formalize security compliance and liability laws to ensure cybersecurity without impeding technological progress.

Economic Incentives

Although not enough on their own, economic incentives from the government are important and useful in securing cyberspace. In the past, the government has successfully used economic policies that leverage market forces towards specific policy positions to incentivize key corporate decisions in many industries. As Pfleeger mentions in his testimony to the House Armed Services Committee, "[t]here are both public and private precedents for such incentives, such as tax incentives and insurance discounts" (Pfleeger). The government has already successfully utilized corporate tax credits to incentivize the use of green technology (Bram). So it is not a far cry to suppose that such policies would also be effective in incentivizing companies to build proper cybersecurity systems in the software market. While customer centric companies may choose to build security into their product "when the customer demands [it]," some of the most innovative companies in the market choose only "good-enough security" (RAND). For these companies, "innovation…is the key to avoiding or preventing security problems…[a]s a result, security takes a back seat to performance…and is not the key determinant of a product's success" (RAND). To make it more economically worthwhile for market innovators as well as customer-oriented companies to adopt good security practices, the government must enact economically favorable policies to incentivize these market actors.

There are several ways to enact these economic incentives. Here, we provide a few of them. A simple but not immediately obvious economic sanction is for the government to leverage its own role as a purchaser of cyber technology. The government can use its significant market buying power to incentivize software vendors to implement security in their products. This can be done by "[refusing] to deal with system providers whose products and services are demonstrably insecure, unsafe or undependable," and "[insisting] that critical systems…must be accompanied by solid, up-to-date formal arguments describing why the systems are secure and

dependable" (Pfleeger). The government is already taking advantage of similar economic sanctions in other markets such as nuclear power (Pfleeger). Secondly, the state and federal government should enact data breach notification laws that would create more transparency of security failures. Under these laws, firms would be required to make publicly available any incident that results in the compromise of personal data (Pfleeger). This would provide an economic incentive for customer sensitive firms to create products that are better able to secure their clients' personal information. According to a study at The Brookings Institution, "46 states and the District of Columbia have [such laws]," and several proposals have already been made to create a data breach law on the national level (Friedman 13). These laws can be enforced with a reporting system whereby an individual or organization that feels a violation has occurred can file a complaint with the designated office of the state. The Better Business Bureau has used an identical reporting model to effectively enforce business-customer trust. In addition, the government can extend liability statutes to also cover cybersecurity failure to make it even more economically costly for corporations to ignore security (Pfleeger).

Why Economic Incentives Are Not Enough

Even though economic incentives are useful, utilizing market forces alone is not sufficient in solving the problem of cybersecurity in our current socioeconomic ecosystem. To understand why, let us build a framework through which to understand the security decisions that companies face. First, we note that a company acting rationally would only invest resources in a certain endeavor if it sees potential returns. In terms of risk prevention, this means that a company would choose to invest in security only if not doing so would result in a loss that is larger than the preventative investment. Yet, as Friedman duly notes in his report on

cybersecurity, even with the existence of negative economic repercussions, “this risk might be smaller than a systematic attempt to prevent potential breaches” (Friedman 8). In other words, a firm often perceives the cost associated with a security failure to be less than the cost of systematically building preventative measures. Furthermore, even when the cost of a security failure is high, companies do not always fully internalize the risk until it actually happens (Friedman 8). In fact, this is more true than not. When a firm perceives that enough other intermediary firms have invested adequately in security to keep the likelihood of infection of the entire system low, it may choose not to act securely because the firm believes that it is already “protected by the secure actions of others” (Pfleeger). A simple example is when a small company, by not keeping up-to-date firewall software, ignores the broader implications of a computer worm attack because the firm assumes that the Internet Service Provider (ISP) has already enacted sufficient cybersecurity to prevent such risks.

In this model, security can be viewed as a public good because investing in security does not necessarily guarantee security and only reduces the likelihood of a failure. Regardless of a single firm’s total amount of cybersecurity investment, security depends on the decisions of many external actors. Firms therefore perceive security investment as having only distributed benefits. Thus, the negative externalities of investment often times outweigh the perceived benefits of security failure prevention, causing any single firm acting alone to be less likely to invest in sound cybersecurity. Empirically, this “herd immunity” effect of cybersecurity has been widely studied and verified in academic publications (Friedman 8, Pfleeger).

Moreover, adverse network effects also hinder investment in cybersecurity. Information technology is often most beneficial when each actor in the system shares the same standard and platform for interconnectivity (Friedman 9). Although this has been an extremely important

driving force in software adoption, the rise of a less diverse technological ecosystem has made it easier and more valuable for attackers. In a more singular system, attackers are able to focus all of their efforts on exploiting a single system containing a massive number of users instead of being forced to understand an overabundance of disparate systems with much fewer users on each system. In this natural way, the free market simply leads to a more insecure cyberspace.

While most technological innovations reap significant benefits from being the first mover, many security innovations derive little benefits to being first in the market (Friedman 10). This is because "network security products often do not improve overall security until other users adopt them" (Friedman 10). Unlike most software products, there is no inherent or obvious comparative advantage to implementing a novel security system when others do not implement it. RSA would lose practically all of its value if only one or a few firms decided to implement it. In this way, the value of cybersecurity has become binary in the context of the entire market.

Often times, a firm's desire to create innovative products, become first movers, and receive windfall profits far outweighs the time and effort required to receive governmental economic benefits by implementing security standards. Thus, if actors were making individual decisions on the free market, even with economic incentives, many security innovations would never become adopted. Market forces alone, though important in their own right, have therefore failed to sufficiently incentivize cybersecurity adoption.

Cybersecurity Compliance and Liability

To address the inherent flaws of pure market mechanisms and inadequacies of economic incentives, we recommend that the government enact security compliance regulations and liability laws that will ensure a more secure cyberspace. First, the government should enact laws

of basic cybersecurity compliance specific to each major industry that produces technological products. A panel of experts can be gathered for each industry to determine what basic security needs suffice to protect the individual rights of the end user. There can also be umbrella clauses that cover multiple industries, and more specific ones that deal with only particular industries. Because of their potentially overarching effects, these standards should be formulated through an open rulemaking policy by collaborating with and considering the inputs of industry leaders. Industry players already agree that cybersecurity compliance regulation is important (Friedman 12, Weatherford). In fact, James Barnett Jr., chief of the FCC's Public Safety and Homeland Security Bureau, was cited in an article saying that "major networking companies serving 80 percent of the nation's Internet users have agreed to adopt [security legislations]" (Jackson). Therefore, congress should be poised to act on these legislations (Weatherford).

However, one drawback of having a compliance model alone is that it shifts a firm's incentive from reducing the overall security risk of the entire system to reducing the possibility of sanctions from not complying with the standard (Friedman 12). To address this, we suggest enacting explicit liability laws to further prompt companies to realize their greater security responsibility. By maintaining explicit costs of liabilities, these laws will "force companies to internalize the full cost of an attack" (Friedman 13). In the case of larger costs, companies can turn to insurance as an option to address liability. This shifts much of the due diligence responsibilities from the government to a more efficient insurance network as they would be naturally incentivized to deter firms from security failures (Friedman 13). This has already been proven to be a successful system in many industries such as automobile and motorcycle insurance. We could create a cybersecurity insurance industry much like existing ones, where companies pay a premium that is correlated with their level of security risks and quality of

security implemented. The insurance network would also have a set of basic industry-wide security compliance standards that must be met for a company to qualify.

In a recent example, Global Payments, one of the world's largest payment processors had as many as 10 million debit and credit card numbers leaked, and faced billions of dollars in liabilities charges from the failure (Janezic). Under the existing system, this unrealistic liability charge could potentially force Global Payments, a crucial player in the payment processing industry, to declare bankruptcy overnight. This would disrupt millions of businesses that depend on their services to operate. Under our proposed system, Global Payments would be protected by insurance companies from liability costs associated with security failures, given that the failure occurred under adherence to strict security compliance laws. More importantly, compensation from the insurance company would be able to cover personal damages for which Global Payments might otherwise not be able to pay. Insurance companies would also be able to force their clients to comply with stricter security standards and implement a higher level of security to reduce future risks of failure. Our current system of compliance is not sufficient for many industries like the credit card processing industry. Much like regulations in the early automobiles industry, we must constantly revise and update our cybersecurity laws to make them better suited for the current socioeconomic ecosystem.

Finally, we affirm that even though compliance and liability laws are essential to securing our cyber-frontier, they have their own risks, and they do not necessitate the complete removal of stick and carrot economic incentives. While it may be important to have stricter compliance laws and heavier liability penalties in some industries that deal with sensitive information such as banking and payment processing, it would make more sense to enact economic incentives for fledgling firms or industries where cybersecurity failures do not lead to as much inherent

damage. With compliance and liability laws, we must also take heed in our choice of severity. Too loose would reduce their effectiveness, but too strict would hinder entrepreneurs and scare away potential investors. This choice of severity depends on the potential security risks of each particular industry and must be decided on a case-to-case basis.

Conclusion

Cybersecurity is a complex and salient issue, characterized by the interweaving of responsibilities and incentives between the private and public sectors. To successfully address this problem, the government must take a multi-pronged approach. While creating policies to provide economic incentives to private sector entities for implementing up-to-date cybersecurity standards, the government must enact security compliance and liability laws without hindering technological innovations. To do this, we recommend a balance of economic incentives and compliance and liability laws that would fit the needs of each particular industry.

Bibliography

Hathaway, Melissa: “Cyberspace Policy Review”.

Pfleeger, Shari Lawrence, What Should the Department of Defense’s Role in Cyber Be? Testimony to House Armed Service Committee Subcommittee on Emerging Threats and Compatibilities, 11 February 2011.

Cybersecurity Economic Issues: Corporate Approaches and Challenges to Decisionmaking, RAND Corporation.

Rowe, R. Brent, Gallaher, Michael P. “Private Sector Cyber Security Investment Strategies: An Empirical Analysis”, March 2006.

van Eeten, Michael J. G., Bauer, Johannes M. “Economics of Maleware Security Decisions, Incentives and Externalities”, STI Working Paper 2008/1 May, 29, 2008, JT03246705

Jackson, William, “‘No one would tolerate’ Internet Crime Rates in Physical World, FCC Official Says” *Government Computer News* March 29, 2012, accessed May 5, 2012. < http://gcn.com/Articles/2012/03/29/House-Cybersecurity-hearing-FCC-official-its-not-working.aspx>

Weatherford, Mark “The Private Sector Agrees, We Need to Improve Cybersecurity Now” *Department of Homeland Security* March 6, 2012, accessed May 5, 2012. < http://blog.dhs.gov/2012/03/private-sector-agrees-we-need.html>

Janezic, Richard “Global Payments Breach in 2011; New Visa, MasterCard alerts” *Midsize Insider* May 7, 2012, accessed May 5, 2012 < http://midsizeinsider.com/en-us/article/global-payments-breach-in-2011-new-visa>

Friedman, Allan “Economic and Policy Frameworks for Cybersecurity Risks” Center for Technology Innovation at Brookings Institute, July 21, 2011.

Bram, Thursday "Tax Breaks for Going Green" *Wise Bread* February 16, 2010, accessed May 17, 2012 http://www.openforum.com/idea-hub/topics/money/article/tax-breaks-for-going-green-1>