George Mason University School of Law
Working Paper Series

Year 2004 *Paper* 12

The Law and Economics of Cybersecurity: An Introduction

Mark F. Grady* Francesco Parisi†

*UCLA, grady@law.ucla.edu

†George Mason University, parisi@umn.edu

The Law and Economics of Cybersecurity: An Introduction

Mark F. Grady and Francesco Parisi

Abstract

One of the most controversial theoretical issues of our time is the governance of cybersecurity. Computer security experts, national security experts, and policy analysts have all struggled to bring meaningful analysis to cybersecurity; however, the discipline of law & economics has yet to be fully applied to the issue. This introduction presents work by leading national scholars who examine this complex national security challenge from a law and economics perspective. The focus spans from a discussion of pure market solutions to public-private issue analysis, providing a valuable basis for policy considerations concerning the appropriate governmental role on the issue of cybersecurity.

Mark Grady[1] -- Francesco Parisi[2]

The Law and Economics of Cybersecurity:

An Introduction[3]

Cybercrime imposes a large cost on our economy and is highly resistant to the usual methods of prevention and deterrence. Businesses spent about $8.75 billion to exterminate the infamous Love Bug. Perhaps far more important are the hidden costs of self-protection and losses from service interruption.

Unlike traditional crime, which terrorizes all, but has far fewer direct victims, cybercrime impacts the lives of virtually all citizens and almost every company. The Computer Security Institute and the FBI recently released the results of a study of 538 companies, government agencies and financial institutions. Eighty-five percent of the respondents reported having security breaches, 64% experienced financial loss as a result.[4] As this problem grows on a daily basis, it becomes imperative that society identify the most economically efficient way of fighting cybercrime. In this volume, the authors present a unique cross-section of views that attempt to identify the true problems of cybersecurity and present solutions that will help resolve these challenges. In the first section of the book, two authors outline some of the major problems of cybersecurity and explain how the provision of cybersecurity differs from traditional security models.

---

[1] Professor of Law and Director, Center for Law and Economics, University of California at Los Angeles, School of Law.
[2] Professor of Law and Director, Law and Economics Program, George Mason University, School of Law.
[3] Introduction to the volume by Mark Grady and Francesco Parisi (eds.), *The Law and Economics of Cybersecurity*, (forthcoming).
[4] Thurston Hatcher, *Survey: Costs of computer security breaches soar*. CNN, available at http://www.cnn.com/2001/TECH/internet/03/12/csi.fbi.hacking.report/. Visited on June 26, 2004.

Bruce Kobayashi examines the optimal level of cybersecurity as compared to traditional security. For example, while it might be more efficient to deter robbery in general, individuals may find it easier to simply put a lock on their door, thus diverting the criminal to a neighbor's house. Although in the general criminal context the government can act to discourage crime *ex ante* by implementing the sufficient level of punishment to deter the crime from occurring in the first place, this result is not so easily achieved in the world of cybercrime. Because the likelihood of detecting cybercrime is so low, the penalty inflicted would have to be of enormous magnitude to deter cybercrime.

In this context, companies can either produce private security goods that will protect their site by diverting the hacker to someone else or they can produce a public security good that will deter cybercrime in general. If the former route is chosen, an overproduction of private security will result that is economically inefficient. This occurs because each actor is taking individual measures that only protect him or herself, as opposed to acting collectively to stop the cyber attack in the first place. If collective action is utilized to produce public, security however, an underproduction will occur because companies will have an incentive to free-ride on the general security produced by others.

Kobayashi suggests utilizing a concept of property rights, whereby the security collective can exclude free-riders to eliminate this problem. Since security expenditures are not sufficiently novel or nonobvious to merit protection under patent or copyright law, Kobayashi suggests collective security action supported by contractual restrictions on members.

Peter Swire follows on Kobayahi's basic idea of collective action by introducing the notion of cooperation through disclosure. Swire attempts to answer the question of when disclosure may actually improve security. In probing this question, Swire develops a model that examines when an actor should choose between the Open Source Paradigm, which favors disclosure, and the Military Paradigm, which advocates secrecy. The Open Source Paradigm is based on three presumptions: attackers will learn little or nothing from disclosure; disclosure will prompt designers to improve the design of defenses; and disclosure will prompt other defenders to take action. The Military Paradigm departs from each of these presumptions and presupposes that attackers will learn much from the disclosure of vulnerabilities, that disclosure will not teach the designers anything significant about improving defenses and that disclosure will not prompt improvements in defense by others. From these two paradigms, Swire offers two further concepts that take a middle ground. The first, the Information Sharing Paradigm, reasons that while attackers will learn a lot from disclosure, the disclosure will prompt more defensive actions by others and will teach designers how to design better systems. For example, the FBI's disclosure of a terrorist "watch list" may enable people to be more attuned to who is a terrorist, but it does so at the cost of alerting terrorists to the fact that they are being scrutinized. The corollary of the Information Sharing Paradigm is the theory of Public Domain, which argues that while attackers will learn little to nothing from disclosure, disclosure will also not teach designers much and will not prompt many additional security steps by others.

Swire reasons that different scenarios warrant different adherence to a particular security paradigm. Factors such as the number of attacks, the extent to which an attacker

learns from previous attacks and the extent of communication between attackers about their knowledge, will influence which model should be followed. In general, secrecy is always more likely to be effective against the first attack. While this might favor the Military Paradigm in physical security because of a low number of attacks and less communication between attackers, the same assumptions do not necessarily hold true in the realm of cybersecurity. Because cyber attacks can be launched repetitively and at minor expense, the Military Paradigm will provide little solace as secrets are soon learned and companies expend inordinate amounts of money attempting to retain their secrecy in vain. Further, as is true in traditional physical security, disclosure can often improve security by diverting an attack, presuming that your security is perceived as strong.

Swire further argues that there are two specific areas in which the presumptions of the Open Source paradigm do not hold true. First, private keys, combinations, and passwords should never be disclosed because doing so does little to promote security or enhance better security design, yet it obviously provides valuable information to the attacker. Additionally, Swire argues that surveillance techniques should not be disclosed because the attacker is unlikely to discover them during an attack and thus in the short-run, not disclosing surveillance will provide the defender with an additional source of security.

The second section of this volume Yochai Benkler argues that cybersecurity is best addressed by making system survivability the primary concern of security measures, rather than attempting to create impregnable cyber fortresses. By mobilizing excess capacity that users have on their personal devices, a network-wide, self-healing device

could be created. The already existing system of music-sharing offers a model of how this type of security could be achieved.

While the sharing of music files is admittedly controversial, the systems that have been put in place to make this a reality offer lessons for how broader cybersecurity can be achieved. Professor Benkler's proposal is based on three characteristics: redundant capacity; geographic and topological diversity; and the capacity for self-organization and self-healing based on a fully distributed system that in nowise depends on a single point that can in turn become the focus of failure. The music sharing industry has been hit by attacks a number of times and Napster even had its main center of data search and location shut-down. Nonetheless, the data survived because of the above characteristics. File sharing systems have allowed data and capacity to be transferred to where it is most needed, allowing it to survive even after repeated attacks. In many file-sharing systems, because the physical components are owned by end users, there is no network to shut-down when it is attacked, by cyberterrorism.

This same degree of survivability can also be seen in distributed computing, where it easier for a task to be shared by several computers, then to build one, very-fast computer. Benkler concludes the article by looking at different economic models that suggest when and how the lessons of file sharing can be put into practical implementation in order to achieve long-term survivability.

The article by Randy Picker examines whether and how security can best be achieved in an industry that is dominated by one company. Many people have come to believe that market dominancy by Microsoft compromises cybersecurity by creating a monoculture, a scenario in which common computer codes help spread virus easily,

software facilities are too integrated and thus lead to security lapses, and software is shipped too soon and thus is not adequately developed to address security needs. In this article, Picker attempts to address these criticisms, believing that they are misdirected and will lead to inefficient results.

Those who believe that the monoculture of Microsoft threatens security often liken the situation to the boll weevil epidemic in the early 1900s. Because farmers in the South only cultivated cotton, when an insect came by that attacked this crop, their fields and economies were both devastated. Opponents of monoculture believe that diversification helps insure against loss, whether it is in agriculture or the world of cybersecurity. Picker points out, however, that one of the primary problems with this logic is that it attempts to deal with the problem from the perspective of supply, rather than crafting demand-based solutions. Sure, the farmer can protect his crop by diversifying his cotton production with corn, but if there is no demand for the latter, the diversification is futile because consumers will not avail themselves of the corn anyway.

Picker's second criticism of the monoculture theorists is that they argue heterogeneity is the best way to address the massive collapse that can result when a virus invades an interconnected world. However, ensuring that different sectors use different operating systems and computers will not mean that all are protected. Rather, when an attack hits it will only shut down one sector instead of everyone. The only way to provide universal protection would be to have all work done on multiple systems, an inefficient solution to the problem. Picker advocates a security model that is very different from that proposed by the increased interconnection supported by Benkler. Picker instead advocates autarky, or purposefully severing some of the connection that

causes the massive shut-down in the first place. Picker argues that we need to accept the fact that interconnection is not always good. Which is economically more efficient: to have ten connected computers run ten different operating systems or to have ten isolated computers each running Windows?

Picker concludes his article by suggesting that security concerns can be remedied through the use of liability rules. Imposing liability through tort law would, however, create headaches because it would be hard to sort out questions of fault and intervening cause among the developer, the cyber terrorist who unleashed the virus, and the end user who clicked when he shouldn't have done so. Likewise, requiring the purchase of mandatory insurance would be economically counterproductive. Rather, in his view, partial insurance that focuses on the first wave of consumers who face greater risks (from the less developed product), will lead to the economically most viable solution.

The second-half of the volume attempts to create regulatory solutions that will address the major problems of cybersecurity. The authors highlight the debate between public and private security with highly divergent positions. Amitai Aviram offers the perspective of private ordering as achieved through private legal systems (PLSs), institutions which aim to enforce norms when the law fails, neglects or chooses not to regulate behavior. Aviram's article gives a broad perspective to how PLSs are formed and then offers practical applications for the field of cybersecurity. Aviram reasons that PLSs cannot spontaneously form because new PLSs often cannot enforce cooperation. This gap occurs because the effectiveness of the enforcement mechanism depends on the provision of benefits by the PLS to its members, a factor that is non-existent in new PLSs. Thus, new PLSs tend to use existing institutions and regulate norms that are not

costly to enforce, ensuring gradual evolution rather than spontaneous formation. PLSs have widely existed throughout history. Literature about PLSs, however, has largely focused on how these organizations develop norms, rather than how these organizations come into existence in the first place.

In examining this question, Aviram starts with a basic paradox of PLS formation: in order to secure benefits to its members, a PLS must be able to achieve cooperation, but to achieve cooperation, a PLS must be able to give benefits to its members. This creates a chicken-and-egg situation. While this problem could be resolved through bonding members in a new PLS, bonding is often too expensive. Accordingly, PLSs tend to simply develop and evolve from existing institutions rather than developing spontaneously and independently.

In order to determine when, how and by whom a norm can be regulated, one must understand the cost of enforcing the norm. This in turn relies on fully comprehending the utility of the norm to the network's members, understanding the market structure of and among the members and understanding what gametype and payoffs have been set up by the norm for the network's members. Aviram introduces a variety of gametypes based on the expected payoffs to members. Some of the gametypes have higher enforcement costs, while others have lower. It is the games that have low enforcement costs that become the building blocks of PLSs, while those with high enforcement costs evolve gradually.

Aviram applies this concept to cybersecurity by looking at networks that aim to facilitate communication and sharing information among private firms. Unfortunately, these networks have been plagued by the traditional problems of any Prisoner's

Dilemma, in that members fear cooperation and divulging information because of worries about increased liability due to disclosure, risk of antitrust violations and the loss of proprietary information. Aviram sees part of the reason for the failure of these networks in that they are attempting to regulate norms with high-enforcement costs, without the sufficient background to do so. Aviram suggests restricting the membership of these networks so that they are not as broadly based as they presently are. This would allow norms to be developed among actors who have preexisting business connections that would facilitate enforcement (as opposed to the broad networks which currently exist and cannot enforce disclosure).

Neal Katyal's article takes a completely divergent view, reasoning that private ordering is insufficient and in many ways undesirable. Katyal argues that we must begin to rethink crime as merely harming an individual and begin to understand it for the harm it inflicts on the community. If rethinking is directed in this way, it tends to argue against solutions that favor private ordering. In turn, public enforcement should be favored. Katyal maintains that the primary harm to the community out of cyber attacks is not necessarily the effect on the individual. Indeed, often hackers only take action out of curiosity and some of their attacks do not actually affect the business' assets or profits in a direct sense. Rather, these attacks undermine the formation and development of networks. Katyal contends that society can therefore punish computer crimes, "even when there is no harm to an individual victim because of the harm in trust to the network. Vigorous enforcement of computer crime prohibitions can help ensure that the network's potential is realized."

Public enforcement is also defended because without governmental action to deter cybercrime, only wealthy companies will be able to afford to take the measures to protect themselves. Katyal compares the idea that private ordering should be used to resolve cybercrime to the notion of the government telling an individual that they will no longer prosecute car theft. Indeed, if the government adopted this policy car thefts might be fewer because fewer people would drive and those that did drive would take the precautions necessary to protect themselves from theft. While this might seem logical (and has even been used to a large extent in the realm of the cyber world,) it fails to take into account exogenous costs. For example, less driving may equal less utility, while greater security measures raises distributional concerns (i.e. can only the wealthy afford the security measures necessary to drive?).

Finally, Katyal suggests that to some extent private security measures may increase crime. This can be likened to the community where residents put gates around their homes and bars over their windows. It may deter crime for that individual, but, "it suggests that norms of reciprocity have broken down and that one cannot trust one's neighbor." This in turn leads those that abide by the law to leave the neighborhood, resulting in a higher crime rate. One of the primary reasons for public law enforcement is to put measures into place that are needed to protect the citizens, while averting sloppy and ill-performing private measures.

Katyal concludes by arguing that not all cybercrimes can be punished and not all can be punished the same way. If the police were to go after every person who committed a cybercrime, it would lead to public panic and further erode the community

of trust. Additionally, some crimes, like unleashing a worm in a network, may be more serious than a more minor cyber trespass.

Lichtman and Posner's article attempts to move beyond the debate of public versus private enforcement that was discussed in the previous chapter by creating a solution that relies on private measures, enforced and promoted by publicly imposed liability. The authors acknowledge that vast security measures have been taken both publicly and privately to address the problem of cybersecurity. However, these measures have not sufficiently addressed the harm because the perpetrators of crime are often hard to identify and when they can be, often lack the resources to compensate for their actions. Accordingly, the authors advocate adopting a system that imposes liability on Internet service providers (ISPs) for harm caused by their subscribers. The authors argue that this liability regime is similar to much of tort law which holds third parties accountable when they can control the actions of judgment-proof tortfeasors. While this idea may run parallel to the common law, the authors acknowledge the fact that it appears to run counter to modern legislation which aims to shield ISPs from liability. However, even in these laws, the roots of vicarious liability can be seen by the fact that immunity is often tied to the ISP taking voluntary steps to control the actions of its subscribers.

One of the objections that the authors see to their proposal is very similar to the problem of private enforcement that Katyal discusses in the previous article. Shielding ISPs from liability, like failing to publicly enforce cyber security, will give end users an incentive to develop and implement their own security devices. Lichtman and Posner counter that this argument does not suggest that ISPs should not face liability, but that their liability should be tailored to, "encourage service providers to adopt the precautions

that they can provide most efficiently, while leaving any remaining precautions to other market actors." Indeed, just as auto drivers are not given immunity from suit based on the argument that the pedestrian could avoid an accident by staying at home, the same should hold true in the cyber world.

The second criticism to this proposal is that it might cause ISPs to overreact by unnecessarily excluding too many innocent but risky subscribers in the name of security. Increased security may indeed drive up costs and drive away marginal users, but likewise users may be driven away by insecurity in the cyber arena. Posner and Lichtman also believe that the danger of increased cost to ISPs can be alleviated by offering tax breaks to ISPs based on their subscriber base, prohibiting state taxation of sales tax on internet transactions, or subsidizing the production of internet service to underserved populations. Problems of virus traveling across several ISPs can be resolved through joint and several liability, while the fear that no one individual will be harmed enough by cybercrime to bring suit, can be resolved through class action lawsuits or suits initiated by a state's attorney general.

The most cognizable concern about the liability plan, however, is the worry that it would be ineffective in a global community, where a cybercriminal can simply reroute his or her attack through a country with less stringent security laws. Posner and Lichtman answer this concern by arguing that global regimes can be adopted to exclude internet packets from states with bad laws. As countries like the U.S. adopted ISP liability, it would spread to other nations.

Trachtman picks up on this final concern that Lichtman and Posner raised and is common to many internet security problems and proposals; the notion of global

cybersecurity and its accompanying questions of jurisdiction and international organization. This problem has become even more acute with the development of organized cyberterrorism, as evidenced by the cyberterrorism training camps ran by Al Qaeda when the Taliban controlled Afghanistan. Throughout his paper, Trachtman examines the same question that was seen in the Aviram, Katyal and Posner/Lichtman articles; to what extent is government regulation necessary to achieve cybersecurity? Trachtman acknowledges that private action suffers to some extent from the inability to exclude free-riders and other collective action problems. Trachtman suggests that private action may be sufficient to resolve some forms of cybercrime, but it clearly will not work to eliminate all cyberterrorism. There are areas that warrant international cooperation, including the (i) limitation of terrorist access to networks, (ii) *ex ante* surveillance of networks in order to interdict or repair injury, (iii) *ex post* identification and punishment of attackers, and (iv) establishment of more robust networks that can survive attack.

Once you have moved past the question of whether private or public action should be favored, you must look to the issue of whether local action is sufficient. Cybercrime proposes unique jurisdictional questions because actions in one country may have effects in another. If the host country will not enforce laws against the cybercriminals, how can the victim country stop the attack? This issue of ambiguous jurisdiction is one of the failures of modern international law in this area. This would seem to suggest that international cooperation should take place. Trachtman suggests creating an umbrella organization that has jurisdiction over these matters and can act transnationally. Trachtman concludes by offering a variety of game theory presentations that exhibit when and how international cooperation can best occur in the realm of cybersecurity.

The authors in this volume have attempted to provide a source for better understanding the dilemmas and debates over how cybersecurity is best provided. Whether it is through private legal systems or public enforcement or a combination of the two, society can scarcely wait in finding new and more efficient tools in the war on cybercrime.