THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

An Overview of the Economics of Cybersecurity and Cybersecurity Policy

Joseph J. Cordes
Professor of Economics, Public Policy and Public Administration, and International Affairs
Trachtenberg School of Public Policy and Public Administration and Dept. of Economics
The George Washington University

Report GW-CSPRI-2011-6

June 1, 2011

Abstract

The design of effective policies to enhance and maintain cyber security must take into account a complex set of incentives facing not only the providers and users of the internet and computer software, but also those of potential attackers. Measures undertaken to defend against attacks must take into account that, like other forms of criminal and terrorist activity, the attackers are not passive agents (unlike nature in the case of natural hazards), and the design of effective policies must recognize, to the extent possible, that the defensive measures will elicit strategic responses from the attacker. There also are potentially serious incentive issues arising from classical problems of externalities and public good problems that encourage underinvestment in cyber security by private parties (e.g. businesses and software developers). Lastly, reducing the probability of cyber attacks and/or the consequences of cyber attacks is not costless. In principle, well-designed policies should balance benefits from defensive measures against their costs (which include important concerns about privacy). The paper examines how these questions can be addressed using fairly standard principles and tools from economic policy analysis and potential policy research questions.

Work supported by the Office of the Vice President for Academic Affairs and the School of Engineering and Applied Science of The George Washington University

Introduction

In May 2011, McKinsey and Company released a major study documenting the world-wide economic impact of the internet. A widely-cited statistic from the report is that on average, the internet has added between 3 and 4 percentage points to the gross domestic products of the economies of the developed world. In terms of the United States, this translates into additional total output of between $440 and $580 billion, or between $1400 and $1,900 per capita. This amount does not include what economists call the "consumer surplus" associated with the internet which, according to McKinsey equals on the order of $200 to $330 per year in economic value enjoyed by consumers.[1]

As the report goes on to note, based on its estimated economic value, the contribution of the internet to economic output is comparable to or exceeds that of each of the following sectors in the economy: transportation, education, communication, agriculture, utilities, and mining. These amounts do not directly measure the key role played by the internet in areas such as national security, or as intermediate inputs into other economic sectors.

Because of its considerable national importance, the internet poses a large and tempting target for criminal activities aimed at illegally extracting economic value from internet producers and consumers, as well as for terrorist activities aimed at inflicting economic or other harm on the United States through internet attacks. There is, therefore, broad social value, and also economic value, in identifying policies to reduce: (a) the likelihood of such attempts, (b) the likelihood that such attempts will succeed should they take place, and (c) the expected consequences of such activities.

This overview paper identifies some of the ways in which microeconomic policy analysis can contribute to a better understanding of how to craft cyber security policies. Although cyber security may seem to be a largely technical matter, there is a growing literature that recognizes the importance (some would say centrality) of understanding the key role of economic incentives. As noted by several authors:

"The economics of information security has recently become a thriving and fast-moving discipline . . . we find that incentives are becoming as important as technical design in achieving dependability." (Anderson and Moore, "The Economics of Information Security, 2006).

"*Economic analysis often addresses the underlying causes of security failures within a system, whereas a technical analysis will merely identify the mechanism!" (Steven Murdoch, 2010).*

The Demand and Supply of Cyber Security

The basic economic model of demand and supply provides a useful starting point. Figure 1, which is taken from Bauer and van Eeten (2009), presents a simple version of such a model in which it is assumed that there are two markets: a market for attacks populated by those who seek to breach cyber security and a market for security comprised of those who seek to thwart such breaches. A key insight is that both attackers and defenders need to devote scarce time and resources either to attacking or to defending, and that if both attackers and defenders strive to make rational decisions, at any moment there is some chosen volume of attacks, denoted by V, which depends in part on the amount of security S (left panel of Figure 1). Conversely, there is also some chosen level of security denoted by S that depends in part on the volume of attacks V (right panel of Figure 1).

One use of such a model is to examine what factors are likely to determine the chosen levels of V and S. More specifically, assuming that attackers and defenders make rational calculations, what factors will motivate attackers (defenders) to devote additional resources to attacks (defense against attacks)?

Such analysis is useful for providing insights both about how a range of factors, including, but not limited to policy and legal decisions, affect incentives for attackers and defenders to choose the volume of attacks, V, and the volume of security, S. Just as important, the model also provides insights about how both attacks and security will change in response to changes in the costs and/or rewards facing both attackers and defenders. Such analysis is the precursor to examining more normative questions. Namely, what is the privately optimal amount of investment in cyber security? Is this amount the same as the socially optimal amount? What is the role of public policy in fostering socially optimal investments in cyber security?

The Simple Analytics of Cyber Security

In Figure 1, the left panel shows the “demand” and “supply” of cyber crime conditional on the amount of security, S, and the right panel shows the demand and supply of cyber security conditional on the volume of cyber crime (which can be taken to stand not only for cyber criminal activities such as internet fraud, but also more terrorist-oriented activities aimed at the internet). The model provides the following broad insights.

- At any given moment, one can represent the “state of play” as one characterized by choices made by attackers about the volume of attacks, V, conditional on choices about security, S, made by defenders; and on choices about security made by defenders, S, that are conditional on the volume of attacks, V, chosen by attackers.

- Given some level of security, attackers balance the cost of additional attacks against the benefits from additional attacks. For analytical purposes, one can imagine an “equilibrium” in which the number of attacks is the point at which the marginal benefit from the additional attack just equals the marginal cost (left hand panel).

- Similarly, given some level of attack volume, defenders balance the cost of attaining additional security against the benefits from the added security. As in the market for attacks, one can imagine an equilibrium in which the chosen level of security, S, is the point at which the marginal benefit from increments of security just equals the marginal cost (right hand panel).

- The chosen volume of attacks, V, depends on the attack supply and attack demand curves, which depend on the chosen level of security. For example, other things remaining constant, changes in the environment that increase security, S, shift the cost of cyber attacks upward and reduce the desired volume of attacks. Factors that could lead to greater security might include public policy decisions and technology. Or, private or public investments that reduce the impact of successful attacks would shift the attack benefit curve downward, reducing the reward, and hence the incentive for attacks.

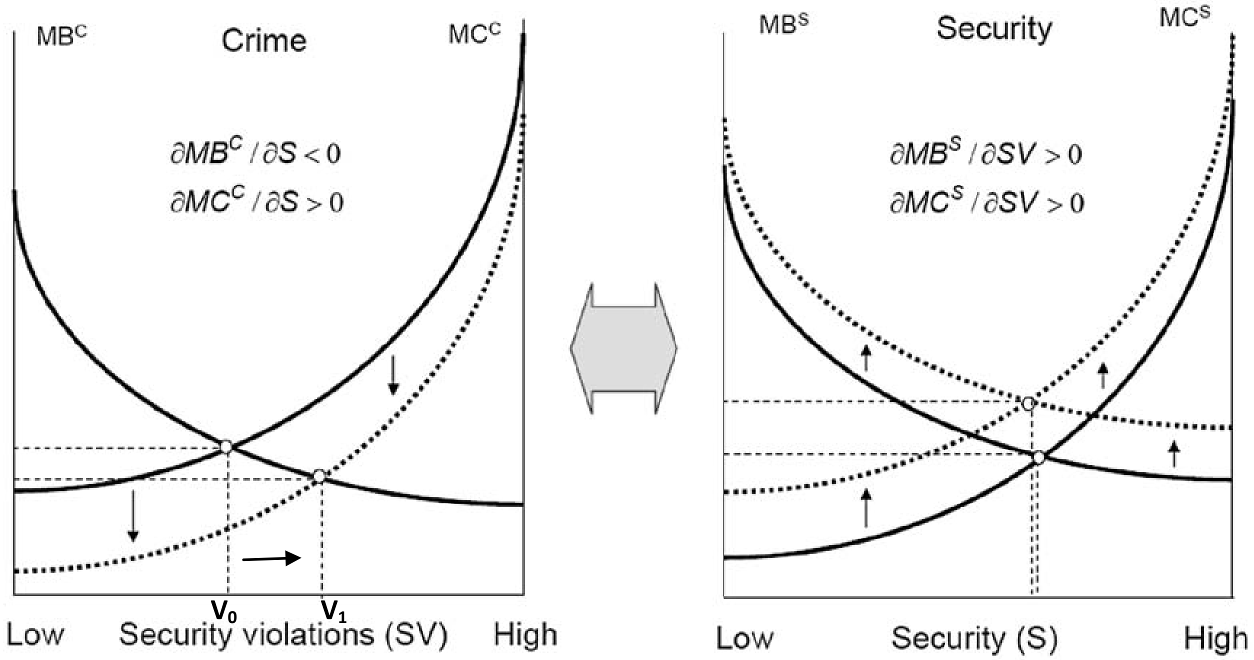
- Similarly, the chosen volume of security is the result of benefit cost balancing by defenders, and the level of security can increase or decrease in response to factors that reduce (increase) costs of security and/or increase (reduce) the benefits from greater security. For example, other things remaining constant, technological innovations that reduce the cost of defending against cyber attacks would shift the cost of cyber security downward, which initially would lead to an increase in cyber security. This effect would be reinforced in the market for cyber attacks because a higher level of cyber-security would raise the cost of attacks, thereby reducing the desired volume of attacks. This change, in turn, would have “second-order effects” in the market for cyber security by reducing somewhat both the benefits of cyber-security measures and further reducing the costs of defending against them.

Although the simple model does not, by itself, identify specific cyber security policy measures, it provides several broad insights that help inform the design of public policy intended to enhance cyber security.

- The model shows that ultimately the level of cyber security, S, depends on a wide range of incentives facing producers of internet services (defenders against cyber-attacks) and cyber-attackers. For defenders, the relevant incentives are: (1) the economic payoff to cyber-security, and (2) the economic cost of cyber security; while for cyber-attackers the relevant incentives are: (3) the economic (or political) gain from cyber attacks, and (4) the economic costs of attacks. This carries with it the basic, but important implication that there are multiple points of influence of public policy on the ultimate level of cyber security. Examples of the different incentives that can either enhance or reduce cyber security are presented in Table 1 (Bauer and van Eeten, 2009).

- Second, the model illustrates the importance of recognizing linkages between the behavior of both attackers and defenders in assessing the effects of policies. Consider for example, the case in which some external factor reduces the cost of attacks. As indicated in the left-hand panel, the immediate consequence would be to increase the equilibrium volume of attacks. However, this in turn would also increase both the benefits of defending against attacks, and also the costs of mounting such defenses. In the specific case shown in Figure 1, these two effects in the market for cyber security are shown as roughly cancelling each other out, in which case the overall level of cyber security (as measured by the volume of attacks) would decline, unless defenders were willing to invest additional resources in cyber defenses over and above those that would be privately optimal in response to the initial increase volume of attacks from V_0 to V_1.

Figure 1: The "Markets" for Cyber Attacks and Cyber Defense: Bauer and van Eeten (Telecommunications Policy, 2009


MB^C
Crime
MC^C
$\partial MB^C / \partial S < 0$
$\partial MC^C / \partial S > 0$
V_0
V_1
Low
Security violations (SV)
High
MB^S
Security
MC^S
$\partial MB^S / \partial SV > 0$
$\partial MC^S / \partial SV > 0$
Low
Security (S)
High

MB^C … marginal benefits of crime, MC^C … marginal cost of crime,
MB^S … marginal benefits of security, MC^S … marginal cost of security,
SV … level of security violations, S … level of security

Incentives to Enhance (Reduce) Security (Bauer and van Eeten)		
Actor	**Security-Enhancing**	**Security-Reducing**
ISP Provider	Cost of customer support	Cost of security measures
	Cost of abuse management	Cost of customer acquisition
	Cost of blacklisting	Legal provisions shielding ISPs
	Loss of reputation, brand damage	
	Cost of infrastructure expansion	
	Legal provisions requiring security	
Software Vendors	Cost of vulnerability patches	Cost of software development & testing
	Loss of reputation	Benefits of functionality
		Benefits of compatibility
		Licensing w.ith hold harmless clauses
3rd party providers	Benefits of on-line transactions growth	Cost of security measures
	Trust in on-line transactions	Benefits of usability of the service
	Loss or reputation, brand damage	
Users	Exposure to and costs of cyber crime	Cost of security products

What is the Socially Optimal Amount of Cyber Security

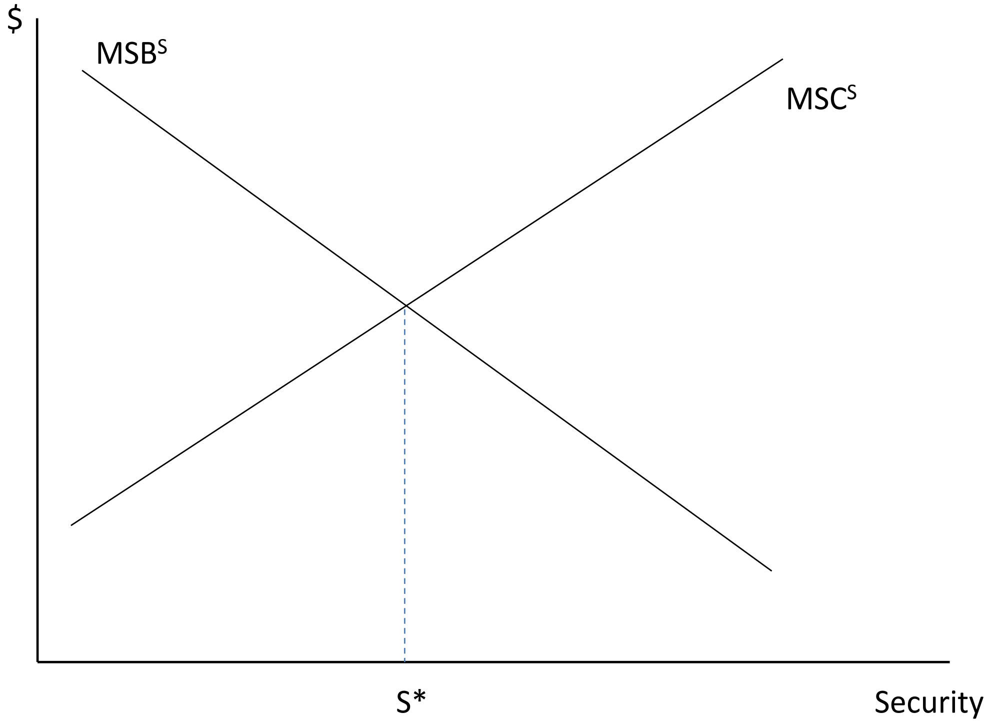
The simple model sketched out in Figure 1 also provides a basis for defining, at least in principle, the concept of a socially optimal amount of cyber security. Figure 2 provides a simple graphical exposition. In Figure 2, the $\mathbf{MSC}^{\mathbf{S}}$ line is similar to the security supply curve in Figure 1, with the important modification that it stands for the marginal social cost of attaining additional increments of cyber-security. Social cost includes not only the private cost of cyber-security measures that are directly borne by private parties, but any and all other resource costs that are incurred. For example, the social cost of enhanced encryption of on-line financial records would include not only the direct costs of developing, installing, and maintaining the more secure system borne by the financial institutions making the investment in the enhanced encryption, but also any costs that third parties needed to make in order to adapt their own systems to the new system. Similarly the $\mathbf{MSB}^{\mathbf{S}}$ schedule stands for the marginal social benefit derived from additional increments of cyber security. Social benefit includes not only the benefits of cyber security measures that are received by those investing in such measures, but any and all benefits flowing to other parties. For example, the social benefit from investing in greater cyber security by institution A would include the direct benefits from enhanced security to A plus any benefits from greater security at site A that might spillover to other parties as a result of improved security at A.

The basic social optimality principle holds that, in principle, the optimal amount of cyber-security is the amount at which the additional social benefit from investing in the next unit of greater security just equals the marginal cost of doing so. Although this amount is not easily observable or measurable in practice, it nonetheless provides useful guidance for cyber security in two ways.

- The concept of social optimality when linked with the concept of private market failure, provides a useful framework for identifying circumstances in which private markets fail to provide the incentives needed for private actors to make socially (as distinct from privately) optimal choices about how much to spend on cyber security. These circumstances define a class of cases in which public policy interventions have the potential to improve the allocation of resources to cyber security.

- Closely related to the above point, the social optimality principle provides a measurement framework for empirically evaluating whether public actions aimed at cyber security --- for example, through regulations mandating cyber-security standards --- have social benefits that are commensurate with their social cost.

Figure 2: How Much Should Society Spend on Cyber Security?



Private Market Failure and Cyber Security

In the marketplace for cyber security depicted in Figure 1, the chosen level of cyber security is assumed to be determined by decentralized, and often uncoordinated, decisions made by private producers and consumers. An important public policy question is that of whether such decisions are likely to result in the socially optimal amount of cyber security depicted above in Figure 2.

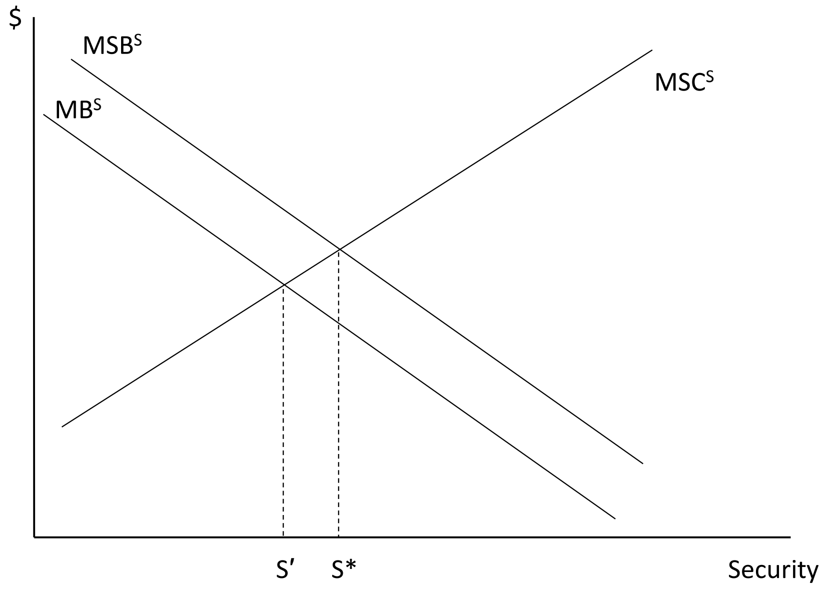
A further contribution of microeconomic policy analysis is to identify cases in which balancing of private benefits and costs in the market for cyber security is not likely to lead to a balancing of social benefits and costs, as shown in Figure 2. An extensive literature in public economics has identified a number of plausible situations in which benefits and costs in private markets will fail to account for all of the social benefits and costs; and these situations can arise in the market of cyber security.

Figure 3 depicts the case in which private investments in cyber security are less than the social benefits. In such cases, leaving cyber security to the market place is predicted to result in under-investment in cyber security. Three important cases in which a situation such as that shown in Figure 3 can arise are network externalities, prisoner's dilemma, and public goods aspects of private security investments.

Network Externalities

In a widely cited paper, Katz and Shapiro argue that the adoption of new technologies often follows an S-shaped adoption curve characterized by initial slow adoption, and then more rapid deployment once a critical mass of users is reached. It has been argued that cyber security technologies follow a similar pattern. Namely, initially the benefits of early adoption of new cyber security technologies may be less than the cost until a critical mass of users is reached. This situation creates incentives for potential users to wait until the new technology is adopted. Of course, if everyone waits, the technology is not adopted. The example of the slow adoption of better (more secure) internet protocols is cited as an example. In terms of Figure 3, early adopters of technologies with network externalities derive private benefits from early adoption, but they do not capture the external benefits associated with their adoption, causing them investment in less than the socially optimal amount S*.

Figure 3: Underinvestment in Cyber Security



Public Security Goods

Another area of potential private market failure occurs in the case of public security goods. Examples of such goods include information concerning: the nature and frequency of past attacks; pending attacks; vulnerabilities to attacks; options for defending against attacks.

An important property of such information is that it is what economists term non-rival in consumption; once the good (information) is produced, all potential users can consume the knowledge (and its benefits) without reducing its availability to others. If such good are made available to anyone without regard to whether the user contributes toward the provision of such goods (the property of nonexclusion), one has a classic example of a pure public good, which in turn creates incentives for potential beneficiaries of such goods to act as free-riders, and can lead to under provision.

Information Asymmetries and Lemons Problems

Cyber security technologies also present cases of goods with quality attributes that can be difficult to verify by potential consumers. More importantly, information about such attributes is often apt to be distributed asymmetrically so that, for example, vendors of software that is purported to protect against cyber attacks may know more than potential buyers about its effectiveness, or lack thereof. Such cases create "lemons problems" when a superior technology is costlier to produce than an inferior technology, but potential consumers have no way of knowing whether the costlier alternative is also the better alternative, compared with cheaper but also less-effective alternatives. It has been shown that in such cases, a possible outcome is that the higher quality alternative may eventually be driven from the market (or attain a smaller market share than warranted) by cheaper and less effective alternatives if potential buyers have difficulty verifying the true quality differences. The same concept has been applied to examine the incentives for adopting "good" vs. "bad" website privacy policies when information about quality is imperfect, and asymmetrically distributed.

Coordination Failures

Lastly, researchers have identified cases in which coordination failures among private parties seeking to defend against cyber attacks can lead to sub-optimal outcomes. Table 2 illustrates one possibility that would lead to under investment in cyber security relative to the outcome. Table 2 is an example of a simple prisoner's dilemma involving two entities seeking to defend against cyber attack. The outcome in which each entity invests in cyber security (20, 20) is superior to that in which neither invests (15, 15). However, if neither party knows with certainty what the other party will do, the privately optimal strategy is for neither to invest – in the hope that the other party will. Of course if both parties engage in this behavior, neither will invest, and the privately optimal strategy leads to the socially inferior outcome (neither invests). The privately (but not socially optimal) strategy would be to not invest, and attempt to free-ride on investment of the other party. The prisoner's dilemma outcome results when each party chooses the latter strategy, which results in the inferior payoff (compared to that when both invest) of (15, 15).

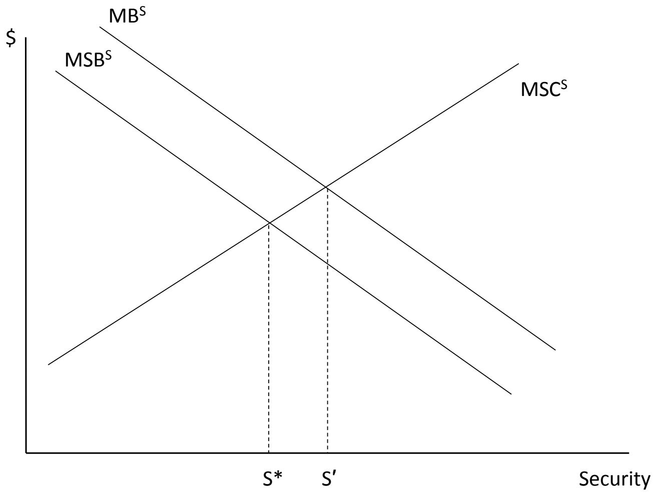
Table 2: Prisoner's Dilemma Security Game Payoff		
	Firm B	
Firm A	**Secure Network**	**Don't Security Network**
Secure Network	(20,20)	(10, 30)
Don't Secure Network	(30, 10)	(15, 15)

Source: Powell (2001)

Private Security Actions and Threat Shifting

Interestingly, coordination failures also have the potential to result in over-investment in cyber-technologies that have the effect of shifting threats from protected sites onto others. This is the case of private security goods that lower likelihood of successful attacks on individual sites, but not on the whole system. Such investments shift threats but do not reduce them in the aggregate. Uncoordinated investments in private security goods may actually lead to overspending on cyber security from a social standpoint. Individual providers have an incentive to spend because it reduces the likelihood of a successful threat on *their* site, even if such spending does not lower the likelihood of a successful attack occurring somewhere else in the system.

Figure 3: Overspending on Cyber Security



Policy Responses

In each of the above cases, the underlying problem is that what is privately optimal in the private marketplace need not be socially optimal. The fact that markets cannot always be counted on to produce socially efficient outcomes creates a potential role for public policy to achieve a better outcome. The range of policy options range from those that involve little or no active intervention by the government in the production and use of cyber security to more intrusive intervention.

Minimal/Low Intervention

An important role of public policy can simply be to see to it that legal rules provide the right incentives. For example, private parties are more likely to invest in cyber-security if they must also bear some of the cost of cyber-security failures. A classic illustration is that of legal rules assigning liability for cyber breaches such as identify theft and/or cyber financial theft. Americans take it for granted that banks and other financial institutions are responsible for making good most losses associated with such occurrences. Such is not, however, the case in much of Europe where institutions are not as responsible. Not surprisingly, as several analysts have noted, the American legal approach has created stronger incentives for American financial institutions than their European counterparts to invest in measures to minimize the likelihood of such breaches.

Other possible policy responses involving minimal to low intervention in private markets include: ensuring that there are no legal barriers to cooperation among stakeholders in providing cyber security; facilitating the creation of uniform codes and standards; and encouraging voluntary private sector institutions to facilitate cooperation and collective action. In each of these cases, the public sector serves more as a facilitator to shape market incentives, with minimal use of its regulatory powers and or financial resources.

More Active Intervention

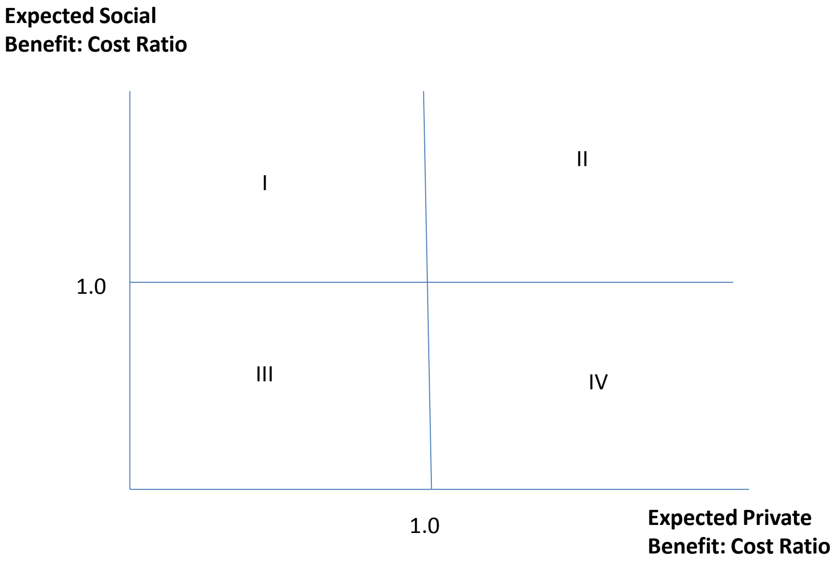
Government also can undertake more active measures to foster greater cyber security. Examples include explicit regulation of private behavior to either require that certain security measures be undertaken, or to enjoin other kinds of actions that are believed to weaken cyber security. Budgetary resources can also be used to encourage greater private investment in cyber security. Public funding can be provided to support government investments in basic and possibly some forms of applied R&D in cyber security; and some observers have suggested that the producer be provided with explicit financial incentives in the form of tax credits to encourage more spending.

Table 3 below provides a simple taxonomy of possible government actions based both on the degree of government intrusion into private market decisions and which side of "market" is affected by the public policy, and Table 4 provides a simple classification of cases when more or less activist government policies are appropriate.

Table 3: A Simple Taxonomy of Cyber Security Policies		
	Policy Tools Affecting the Cost of Cyber Security Measures	**Policy Tools Affecting the Benefits of Cyber Security Measures**
Minimal Market Intervention	Creation of standards, voluntary organizations	Legal liability rules, government procurement standards
Moderate Market Intervention	Government funded R&D; Demonstration Projects	Public private partnerships
Active Market Intervention	Explicit financial incentives (tax credits to lower costs)	Government regulation

The basic message of Figure 4 is that the need for more or less active government involvement in the realm of cyber-security depends on (a) the mix of "private" and "public" benefit. Roughly speaking, the higher the ratio of public to private benefit the stronger the case for policy activism. In the case of public benefits, an additional factor is whether these benefits are more commercial in nature or whether they have more to do with national security.

Figure 4: Public vs. Private Actions



Summary and Future Research

The discussion above demonstrates that standard tools of microeconomics can, and have been, applied to the analysis and evaluation of policies for achieving greater cyber security. Microeconomic policy analysis provides a range of analytical models for examining observed behavior as well as a framework for identifying and analyzing policy options that is rich and varied.

There are a number of areas in which future research can strengthen what is already known about the nexus between economics and cyber-security.

- From the perspective of policy analysis, much of the current literature is case-specific. Specific policy applications are scattered throughout, often as brief examples. More work is needed to turn conceptual insights from this literature into practical policies.

- Policy analysis of cyber-security options can learn from the evolution of policy in other areas, most notably environmental policy and homeland security policy.

- Cyber security policy analysis can also benefit by drawing on insights from the research of Nobel Economics Laureate Elinor Ostrom which focuses on the development of voluntary institutions as response to private market failure.

- Insights can also be gained by comparative analysis of policies in other countries, especially the European Union.

- Empirical work on the effects of actual government policies is still relatively sparse. Important empirical questions about the effects of cyber security policies include: How does regulation affect the development and use of cyber security technologies? How can one measure the social costs and benefits of investments in cyber security? Based on the development of such measures, what are the measured benefits and costs of greater investment in cyber security?[2]

[1] This amount is the additional utility, measured in dollars that consumers derive from what McKinsey calls "the exceptional value that consumers place on internet services such as e-mail, social networks, search facilities, and on-line reservation services, among others."

[2] An example of such research is Khana and Liginal (2007).

References

Anderson Ross and Moore, Tyler, 2006. "The Economics of Information Security" *Science* 314(27) pp. 610-613.

Anderson, Ross: Economics and Information Security Resource Page: http://www.cl.cam.ac.uk/~rja14/econsec.html#Homepages

Asaf, Dan, 2007. "Government Intervention in Information Infrastructure Provision."

In Goetz and Shinoi, eds. Critical Infrastructure Protection. IFIP International Federation for Information Processing, Volume 65 / 2002 - Volume 292 / 2009.

Bauer, Johannes M. and van Eeten, Michael J.G, 2009. "Cybersecurity: Stakeholder Incentives, externalities, and policy options," *Telecommunications Policy* 33, pp. 706-719.

Camp, L. Jean and Wolfram, Catherine, 2004. "Pricing Security: A Market in Vulnerabilities" Economics of Information Security, Vol 12.

Gandal, Neil, 2006. "An Introduction fo Key Themes in the Economics of Cyber Security." Unpublished paper, Tel Aviv University and CEPR.

Keshtri, Nir, 2009. "Positive Externality, Increasing Returns, and the Rise in Cybercrimes." Communications of the ACM 52(12), pp. 141-144.

Khansa, Lara and Liginlal, Divakaran, 2007. "The Influence of Regulations on Innovation in Information Security." *AMCIS 2007 Proceedings.* Paper 180.

Kobayashi, Bruce, 2005. "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods." Law and Economics Working Paper Series, George Mason University Law School.

Murdoch, Steven, 2010. *Security Economics*. Presentation on Feb. 26, 2010.

National Vulnerability Database: http://nvd.nist.gov/statistics.cfm.

Powell, Benjamin, 2004. “Is Cybersecurity a Public Good; Evidence from the Financial Services Industry.” Unpublished working paper, San Jose State University.

Vila, Greenstad, and Molnar, 2003. “Why We Can’t be Bothered to Read Privacy Policies: Models of Privacy as a Lemon’s Market.” Paper presented at the Fifth International Conference on Electronic Commerce (ICEC 2003), Pittsburgh, PA.

Joseph J. Cordes

Professor of Economics, Public Policy and Public Administration, and International Affairs
Trachtenberg School of Public Policy and Public Administration and Dept. of Economics
The George Washington University

Professor Cordes received his Ph.D.in Economics from the University of Wisconsin, Madison in 1977. He has been on the faculty of The George Washington University since 1975. He was a Brookings Economic Policy Fellow in the Office of the Assistant Secretary for Tax Policy, US Treasury Department in 1980-81. From 1989-1991 he was Deputy Assistant Director for Tax Analysis at the Congressional Budget Office. Professor Cordes currently directs the University's Ph.D. Program in Public Policy, and is an Associate Scholar at the Urban Institute. Professor Cordes is a member of the National Tax Association, and the American Economic Association.

Dr. Cordes is co-editor of the *Encyclopedia of Taxation and Tax Policy* (Urban Institute Press). He has published articles on tax policy, government regulation, and government spending in *Economic Inquiry*, *Journal of Economic Perspectives*, *Journal of Public Economics*, *Journal of Finance*, *Journal of Law and Economics*, *National Tax Journal*, *Public Finance*, *Research Policy*, *Eastern Economic Journal*, *Journal of Policy Analysis and Management*, *Journal of Urban Economics*, *Space Policy*, and the *American Economic Review*. He has been a contributor to *The Economics of Technological Change on Employment and Growth* (Ballinger), *State Taxation of Business* (Praeger), *Labor Market Adjustments in the Pacific Basin* (Kluwer-Nijhof), *Cooperative Research and Development: The Industry-University-Government Relationship* (Kluwer-Nijhof), and *Readings in Public Policy* (Basil Blackwell).