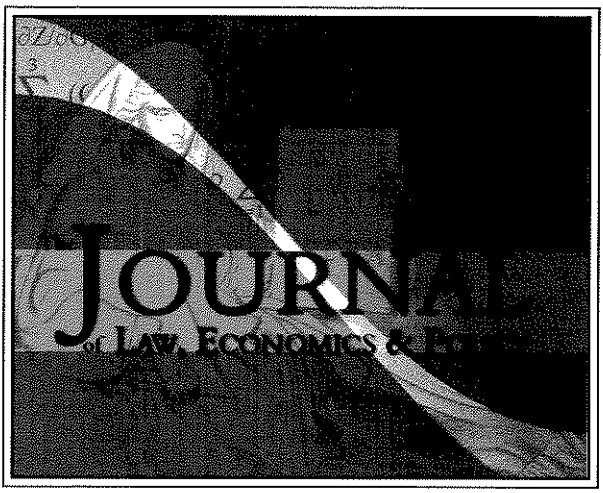
GEORGE MASON UNIVERSITY SCHOOL OF LAW




# IS CYBERSECURITY A PUBLIC GOOD? EVIDENCE FROM THE FINANCIAL SERVICES INDUSTRY

*Benjamin Powell, Ph.D.*

VOLUME 1 WINTER 2005 NUMBER 2

# IS CYBERSECURITY A PUBLIC GOOD? EVIDENCE FROM THE FINANCIAL SERVICES INDUSTRY

*Benjamin Powell, Ph.D.*[*]

The September 11, 2001, terrorist attacks on the United States heightened concerns about vulnerabilities to future attacks. One new area of concern is cyberterrorism: the possibility of terrorists using computers to attack our critical infrastructure electronically. The government has made efforts to better secure its own computer networks against terrorist hacking in the Pentagon, FBI, and other government agencies. Increasingly, however, the government has been concerned that the private sector is vulnerable to cyberterrorism. The private sector owns approximately 85 percent of the critical infrastructure in the U.S. (Deloitte 2004, p. 15). The government is concerned that a cyber attack on dams, trains, electrical grids, pipeline pumps, communications networks, or the financial services industry could cause significant physical or economic damage to the U.S. The policy question being asked is whether private businesses, when left to their own devices, provide enough cybersecurity or if some form of government involvement is justified.

Some policy makers are skeptical of the market's ability to provide enough cybersecurity. In a speech to the National Academy Conference on "Partnering Against Terrorism," Congressman Boehlert said, "Here is a case in which the government can't carry out its most basic mission—providing security—without the cooperation of the private sector. And here is a case in which the private sector will quickly need a range of products on which the market has never before put a premium—the classic market failure that calls out for government involvement" (Boehlert 2002). Similarly, in a February 2004 speech, Richard Clarke, the former counterterrorism czar for Bill Clinton and George W. Bush, said, "Last year was a market failure in cybersecurity, and 2004 doesn't look much better. In general, Internet Service Providers (ISPs) do nothing about security. The market

[*] Assistant Professor of Economics, San Jose State University; Director, Center for Entrepreneurial Innovation at The Independent Institute. E-mail: Benjamin.Powell@sjsu.edu. The author thanks Chris Cardiff, Anthony Gregory, and David Skarbek for excellent research assistance. Helpful comments from the participants at George Mason's Critical Infrastructure Project are gratefully acknowledged. The usual disclaimer applies.

isn't forcing the ISPs to do anything about security" (Ricadela 2004). Calls for government regulation of cybersecurity have accompanied these proclamations of "market failure." In 2003 the federal government published The National Strategy to Secure Cyberspace. The plan's three main goals are to prevent cyber attacks against America's critical infrastructure, reduce national vulnerability to cyber attacks, and minimize damage and recovery time from cyber attacks that do occur. The government needs to better consider the economics of cybersecurity before moving forward with any policies. Specifically, the government needs to examine if the market truly "fails" to provide the correct amount of cybersecurity. The government should also consider if it will be able to improve the situation or if "government failure" could be as pervasive as "market failure."

This paper proceeds by first examining the economics of cybersecurity and its applicability to the defense against cyberterrorism. The financial services industry is regarded as one area of critical infrastructure requiring protection from cyberterrorism; it is therefore examined as a case study in section II to determine if the market is indeed failing. Section III considers the problems confronting government cybersecurity policy while focusing on the financial services industry and examines the potential for government failure. Section IV concludes.

## I. ECONOMICS OF CYBERSECURITY

Economists generally assume markets are relatively efficient. In the realm of cybersecurity, however, markets are often assumed to fail. At least one researcher (Anderson 2001) has pointed out that the incentives of the so-called "experts" in the area may cause this. Producers of information security technology may benefit financially if they can scare more people into purchasing security products. Similarly, professors competing for the latest homeland security grants may face incentives to overstate the problem. Despite these potential biases, simple economic models highlighting potential market failures in the provision of cybersecurity are worth considering.

The security of the entire Internet is affected by the security measures used by all individual Internet users (Anderson 2001). Because of this, cybersecurity is often assumed to be a "public good" that will be underprovided or fail to be provided at all in the private market. When firms or individuals have a greater level of cybersecurity, their computers are less likely to be hacked into and used to launch spam or other denial of services attacks (DOS). The security of one computer owner benefits other computer users by reducing the probability that they will be attacked through the first owner's computer. However, since individuals are not generally liable for the damage caused when a hacker takes over their computer, they

do not benefit personally from the increased security.[1] Since the user with the ability to provide the security does not benefit, they will fail to provide it. Other computer owners with access to the Internet face the same incentives, and everybody is worse off than they would be if everyone provided the security that had spillover benefits for everyone else. The incentives confronting an individual user could be modeled like the prisoner's dilemma game in Figure 1.

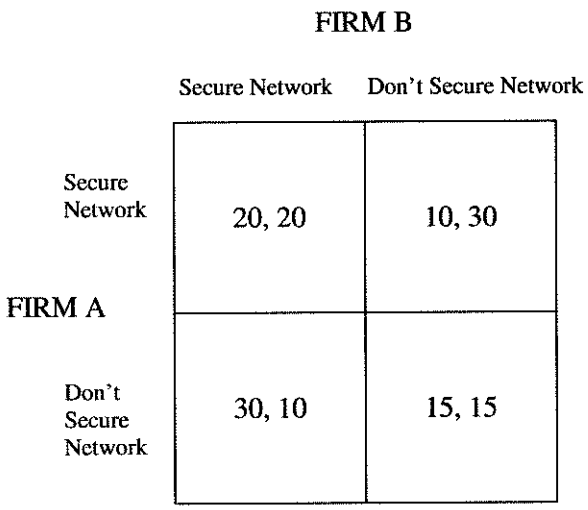



*Figure 1*

In this figure, "secure network" should be interpreted as a firm taking steps to prevent its computers from being used to launch attacks on other firms' computers. Thus, when one firm secures its network, the other firm receives the benefit. Since there is also some positive cost to securing their networks, neither firm has an incentive to do so. If both firms secured their networks, they would both be better off, in this case receiving a utility of "20." However, each firm only controls its own decision whether to secure its network or not. Firm B compares whether it would be better off securing its network or not depending on what A does. If firm A secures its network, B would receive 20 if it secured its own as well, but 30 if it did not, because it would still receive the benefit provided by A securing its network but would not bear the cost of securing its own. Similarly, if A does not secure its network, B would receive only 10 if it secured its own, because it would not be receiving the benefit of A's security but would be bearing the cost of securing its network. If B too did not secure its network, it would receive a higher utility of 15. Regardless of whether A does or does not

[1] Varian (2000) examines incentives under differing liability rules.

secure its network, B is better off not securing its own. The payoffs are symmetrical, so the same incentives confront firm A. The Nash equilibrium is for neither to secure its own network. This leaves them both with a utility of only 15. Both firms would clearly be better off if they could have coordinated and both secured their networks and received a utility of 20, but neither has an individual incentive to do this. Of course, with only two firms the transaction cost of bargaining to achieve the efficient outcome is fairly low, so the Coase theorem should hold and allow them to reach the efficient outcome (Coase 1960). However, in the real world these incentives face many firms and individuals. The transaction costs of bargaining between all computer users are likely high, so we would be stuck in the inefficient Nash outcome of 15, 15.

In the above analysis, all of the benefits of cybersecurity were external to the person providing the security. In reality, many of the benefits of cybersecurity accrue to the user of the security. Often the same security techniques that will secure your own private information, prevent your files from being destroyed by a virus, and prevent private financial loss are the same security techniques that benefit other computer users. Most forms of computer security create both private and public benefits. The above model highlighted why the market might fail to provide cybersecurity, but the empirical question that needs to be examined is whether the private benefits are great enough to cause individual firms and computer users to provide enough cybersecurity. If the costs of the security are high, the private benefits low, and the public benefits high, firms will underprovide cybersecurity on the market. If the costs are low and private benefits are high, firms will generally provide close to efficient levels of cybersecurity despite some positive externalities.

A word of caution is in order. In a predetermined model in which all private and public costs are known and specified in advance, it is trivial to solve the problem of finding the "optimal" level of cybersecurity and then compare what the private market provides to the theoretic optimal amount. However, it is impossible to know all the private and social costs and benefits in the real world. We know that 100 percent security is not likely to be the efficient outcome given the costs of achieving it. To observe any privately provided level of security and then deem it "market failure" because it does not conform to a predetermined optimum is unjustified. Instead, we must look at whether firms are providing security, and if so, how much, as well as whether they are increasing or decreasing their level of security.

The economic literature documents a second potential market failure in cybersecurity: the problem of information sharing and free riding. A number of papers explore this. Anderson (2001) looks at the incentives facing information sharers; Varian (2002) models the free rider problem and system reliability; Gordon et al. (2002) looks at information sharing by SB/ISOs; Gordon, Loeb, and Lucyshyn (2003) study the welfare implications of information sharing and the conditions necessary for information

sharing to increase computer security; and Schechter and Smith (2003) examine the benefits of sharing information to prevent security breaches.

The potential market failure in information sharing is a result of the incentive to free ride. The literature recognizes that if firms share information about security breaches and defenses against attacks, they can lower their security expenditures while maintaining or increasing their level of security. This sharing creates two potential problems. The first is that when a firm reports a security breach, it provides a benefit to other firms but may receive no reward itself. Thus, individual firms may fail to report breaches that would benefit others. The second potential market failure comes from the possibility of free riding on other firms' security innovations. If firms share security innovations and confront a common problem, individual firms may fail to deal with the problem because they hope they will get the benefit when another firm creates a security innovation to solve it. Because of this incentive to free ride, firms may not innovate as quickly as they should.

The key to potential market failures in information sharing is that the firm sharing the information does not benefit from sharing. This problem can be solved or at least reduced with appropriate incentive devices. Many information-sharing groups are private and can exclude non-members. Incentives for sharing would improve with the ability to kick out members suspected of holding back information (Tullock 1985). Other positive monetary incentives for sharing could also be offered. While the potential for free riding and underprovision of information sharing exists, there are benefits to be had by private groups if they can create the right incentive structure. As long as these groups are left private with the ability to make their own rules and exclude non-members, they will likely experiment to find ways to minimize the free rider problem.

Although a number of theoretic "market failures" are possible in the provision of cybersecurity, the market process may also work to solve these failures. In the next section we examine the financial services industry for evidence of market failure or success in the provision of cybersecurity.

## II. FINANCIAL SERVICES INDUSTRY CASE STUDY

A cyberterrorist attack on the financial services industry, part of the "critical infrastructure" of our economy, could ripple through the entire economy. Banks, investment firms, and insurance companies all store vast amounts of important data electronically, so the economic damage that could result from a cyber attack is high.[2] We use the Deloitte Touche Toh-

[2] Policy makers sometimes seem to draw a qualitative difference between general cybersecurity and cybersecurity of "critical infrastructure." From the economic point of view, only a quantitative difference exists. Some infrastructure may be deemed "critical" because if security failed, the dollar

matsu 2003 and 2004 Global Security Surveys of the financial services industry to examine how businesses in the financial services industry are protecting themselves from cyberterrorism. The survey respondents were information security executives at major banking, insurance, and financial services firms. Of the largest one hundred firms in each sector, more than 30 percent of the largest financial services firms, 20 percent of the largest banks, and 20 percent of the largest insurers responded to the survey.

If there were a massive market failure to provide cybersecurity in the financial services industry, we would expect little investment in cybersecurity, lack of industry concern in providing it, and little use of security products. If, however, cybersecurity provides large private benefits, we might observe the opposite. If the financial services industry responds to heightened threats by increasing security staffing, increasing budgets, and using new technology, then there is reason to believe that the private benefits to security induce firms to provide it despite some publicness characteristics.

The point of this section is not to prove the "optimality" of the current level of security provided in the financial services industry, but only to emphasize the widespread investment in and use of technology to highlight the market's ability to provide security despite publicness characteristics. Testing for "market failure" by examining current provision compared to an optimum is impossible. To know the optimal level of security (or any other good in the market), we would have to know all the costs and benefits to all market participants under ever changing conditions at every point in time. But this information is not available because it is decentralized, subjective, and often tacit or inarticulate knowledge that cannot be made available to analysts (Hayek 1945). This is why the market process is a discovery procedure in which the optimal pattern of resource use is constantly evolving and being discovered anew (Hayek 1978).

In examining financial services companies, we find most do make large investments in cybersecurity. In the U.S., financial services companies spend between 6 and 7 percent of their entire information technology budgets on security (Deloitte 2004: 20). Most firms have an upper level executive dedicated to cybersecurity. Sixty one percent of respondents to the Deloitte survey in 2003 had a Chief Security Officer or a Chief Information Security Officer (p. 10). The survey summarized the financial services industry view of cybersecurity as follows: "Executives rank security as a high priority and security initiatives are seen as a good investment. Security is a business issue driven by shareholder value, customers' perception, brand and reputation protections, legal and regulatory compliance, vulnerability and sustainability" (2004, p. 15).

---

value of damages would be much greater than the losses from damages in non-"critical" infrastructure. From an economic efficiency standpoint, holding probability of breach constant, we should hope to see greater security in industries and firms where the expected dollar value of damages is higher.

Financial companies' investment in cybersecurity has translated into widespread use of many security technologies. The percent of financial firms that have fully deployed or are piloting various defenses are: 85 percent use intrusion detection/prevention systems, nearly 100 percent use anti-virus software, 40 percent use smart cards, and 20 percent use biometrics (Deloitte 2004, p. 24). These are all increases over the percent of firms using them in 2003. Other widely used technologies include public key infrastructure (30 percent), virtual private networks (70 percent), content filtering/monitoring (60 percent), and single sign-on (30 percent).

With significant budgets, widespread use of technology, and upper level executives devoted to cybersecurity in the financial services industry, we would expect that if businesses found themselves not earning enough of a private return on these investments because of publicness characteristics, they would shrink their investments and staffing. However, we observe financial firms increasing or maintaining their cybersecurity budgets. The Deloitte survey found that from 2003 to 2004, fewer than 10 percent of firms had reduced their security budget, while 25 percent of firms retained their previous security budget. More than 63 percent of firms reported a security budget increase. Of these, more than 20 percent experienced a 0 to 5 percent budget increase, just under 15 percent experienced a 5 to 10 percent budget increase, just under 15 percent of firms had a 10 to 20 percent increase, and about 13 percent of firms had a security budget increase greater than 20 percent (2004, p. 20). U.S. firms experienced the greatest budget growth (2004, p. 20). Increasing budgets have also translated into larger security staffs. Forty-seven percent of respondents reported that their IT security staffing levels had increased in the last year, while 29 percent remained unchanged and only 19 percent reported decreases (2003, p. 14).

Security executives seem confident that their cybersecurity spending is appropriate. Only 10 percent of respondents felt their organizations' spending on security was "inadequate," and when asked to characterize their organizations' investments in security, 84 percent classified it as on plan or catching up while only 8 percent felt it was falling behind (2003, p. 14).

Budgets, technology, and employees are all allocated to cybersecurity, as are upper level planning resources. Eighty-one percent of firms report that risk management is part of strategic planning, and 16 percent report that risk management is informally considered. Only 3 percent report that they have no strategy in place around risk, and no firms report that it is not considered at all (2004, p. 23). The Deloitte survey also found that "[i]n terms of respondents who have a comprehensive IT disaster recovery/business continuity plan in place the survey highlighted the following: 91 percent of respondents say that their organizations have one, 54 percent characterize themselves as 'very confident' that their backups either work or are being stored off site in accordance with policy" (2004, p. 25). Both of these numbers were increases from 2003.

All of the investment in cybersecurity translates into confidence among many in the financial services industry that they are up to the task of providing cybersecurity. When asked about their organizations' readiness to face cybersecurity threats, 50 percent of respondents stated that their organization was either well skilled and had the competency to respond or that staff supplementation or outsourcing was being used to gain that competency. Another 30 percent recognized that they were missing some skills but said they were adequately closing the gap. Fewer than 3 percent of organizations felt that they were missing skills and had large gaps (2004, p. 19). The survey concluded, "The majority of respondents are confident that their networks are protected from cyber attacks (e.g. DOS attack, malicious code, sabotage, etc.)" (2004, p. 23).

Non-survey evidence also suggests that businesses are receiving private benefits and possibly even overproviding cybersecurity. Campbell et al. (2003) found that security breaches can decrease the market value of firms by a statistically significant level. Soo Woo (2000) estimates that firms actually overinvest in cybersecurity. He finds a return on investment in security of around 20 percent, which is lower than the 30 percent return on investment required for most information technology investments at the time of his study.

A final concern of market failure that includes but is not limited to the financial services industry is that knowledge of damaging viruses is not communicated to those at risk of attack. However, since many people could benefit from an advanced warning, a major private incentive exists to provide it. In fact, the media, through traditional print, television, and radio stories, as well as Internet news sites, frequently warn about viruses. Since viewers and listeners value the information, providing the information increases ratings or circulation. A cursory search of Lexis Nexis for articles in major U.S. news sources from October of 2003 to October of 2004 for the words "computer virus, computer hacker, Mydoom, Sasser" turned up 755 articles. Surely many other articles were published in other forms of media and smaller circulation papers.

If cybersecurity were a purely public good, we would not see the private sector devoting so many dollars, employees, and planning resources or employing so many technologies to provide cybersecurity. There must be enough of a private return to cybersecurity to cause firms to invest so much in it. If the publicness characteristics of cybersecurity were very troubling, we would not likely see the industry continue to devote more resources to security. In general, firms do not appear to be free riding or holding off for other companies to innovate. In fact, the Deloitte survey reports that "US respondents felt that their competitors had no relevance to the way they operated or spent their money" (2004, p. 10).

The market is providing cybersecurity in the financial services industry; a complete "market failure" has not occurred. The policy question of

All of the investment in cybersecurity translates into confidence among many in the financial services industry that they are up to the task of providing cybersecurity. When asked about their organizations' readiness to face cybersecurity threats, 50 percent of respondents stated that their organization was either well skilled and had the competency to respond or that staff supplementation or outsourcing was being used to gain that competency. Another 30 percent recognized that they were missing some skills but said they were adequately closing the gap. Fewer than 3 percent of organizations felt that they were missing skills and had large gaps (2004, p. 19). The survey concluded, "The majority of respondents are confident that their networks are protected from cyber attacks (e.g. DOS attack, malicious code, sabotage, etc.)" (2004, p. 23).

Non-survey evidence also suggests that businesses are receiving private benefits and possibly even overproviding cybersecurity. Campbell et al. (2003) found that security breaches can decrease the market value of firms by a statistically significant level. Soo Woo (2000) estimates that firms actually overinvest in cybersecurity. He finds a return on investment in security of around 20 percent, which is lower than the 30 percent return on investment required for most information technology investments at the time of his study.

A final concern of market failure that includes but is not limited to the financial services industry is that knowledge of damaging viruses is not communicated to those at risk of attack. However, since many people could benefit from an advanced warning, a major private incentive exists to provide it. In fact, the media, through traditional print, television, and radio stories, as well as Internet news sites, frequently warn about viruses. Since viewers and listeners value the information, providing the information increases ratings or circulation. A cursory search of Lexis Nexis for articles in major U.S. news sources from October of 2003 to October of 2004 for the words "computer virus, computer hacker, Mydoom, Sasser" turned up 755 articles. Surely many other articles were published in other forms of media and smaller circulation papers.

If cybersecurity were a purely public good, we would not see the private sector devoting so many dollars, employees, and planning resources or employing so many technologies to provide cybersecurity. There must be enough of a private return to cybersecurity to cause firms to invest so much in it. If the publicness characteristics of cybersecurity were very troubling, we would not likely see the industry continue to devote more resources to security. In general, firms do not appear to be free riding or holding off for other companies to innovate. In fact, the Deloitte survey reports that "US respondents felt that their competitors had no relevance to the way they operated or spent their money" (2004, p. 10).

The market is providing cybersecurity in the financial services industry; a complete "market failure" has not occurred. The policy question of whether we should expect government failure if it tried to provide cybersecurity remains.



## III. GOVERNMENT FAILURE AND THE FINANCIAL INDUSTRY

If there are public benefits that firms do not take into account, then the possibility remains that the government could be needed to provide the difference between the optimal level of cybersecurity and the level the private sector voluntarily provides.

It is impossible to determine the optimal level of cybersecurity and then compare it to what the private market has provided, because public goods are not bought and sold on the market. Clearly cybersecurity has costs, and making cyberspace 100 percent secure is unlikely to be optimal. As one survey respondent put it, "There is no such thing as 100 percent security. Security is not only a technology issue but a management issue as well" (2003, p. 17). Governments are simply not in a position to calculate the optimal number of resources that should be devoted to cybersecurity.

An inefficient level of cybersecurity can occur with either under- or overprovision. The market is often accused of underproviding security, but overprovision, in which security spending exceeds the expected value of losses from breaches, is likely to occur when government regulators determine the level of security. Even with the efficient level of cybersecurity, some costly breaches will occur. These will cause public relations problems for the bureaucrats in charge of regulating security, so they will likely seek to minimize breaches even if it means forcing firms to overspend on security. The costs of preventing breaches will be slower innovation rates and more expensive products and services, but these costs are largely unnoticed by the public, while costly breaches are not. The incentive problem is much the same as the one facing regulators at the FDA, which has been long recognized in the economics literature (Peltzman 1973, 1974).

Government regulators will also lack the information necessary for error correction that market participants possess. When an individual firm provides too much security, it gets feedback from the market in its profit and loss statements. It can compare itself to other firms making different decisions and see that security provisions should be reduced. When regulators mandate security provision levels for all firms, this type of error correction information is not available, since the innovative and competitive process of different companies providing different levels of security is stifled. Of course, some feedback is available if regulations are far too costly; an entire industry could go bankrupt, for instance. This informational feedback is not as precise as what a decentralized, competitive market provides, so overprovision is less likely to be detected.

The problem of calculating the efficient level of security, the incentive to overregulate, and the lack of precise feedback all make government failure likely. But even if we look at specific instances of how the market

might fail to provide enough security in the financial services industry, we find that U.S. policy is unlikely to be able to fix these problems.

Former homeland security czar Tom Ridge stated the problem by saying, "Anywhere there is a computer . . . whether in a corporate building, a home office or a dorm room . . . if that computer isn't secure, it represents a weak link. Because it only takes one vulnerable system to start a chain reaction that can lead to devastating results" (Ridge 2003). If his statement is true and literally any unsecured computer poses a threat, then U.S. policymakers cannot correct the public good problem of cybersecurity. For U.S. policy to be effective, the externality would have to be external to individual firms and users but internal to the United States. However, the Internet spans national boundaries and there are millions of computer users overseas. Computers in foreign countries can be used to launch attacks on U.S. critical infrastructure as easily as computers within the U.S. Since it is neither practical nor desirable to cut off all U.S. computer users from the world's Internet, U.S. policy could not possibly hope to secure cyberspace in the U.S. if an externality between all computer users exists.

When we observe the activities of major financial firms worldwide, we find that U.S. firms are already providing greater levels of cybersecurity than foreign firms. The Deloitte survey found that

> [w]ith the largest security staff and the greatest number of financial institutions with security strategies, it is not surprising that the U.S. reported that they were likely spending more on security than any other part of the world, given the events of the last few years. They also felt that they were prepared to take higher risks and be the leaders in adopting new forms of technology. This is a similar finding to last year, when US respondents felt that their competitors had no relevance to the way they operated or spent their money (2004, p. 10).

In 2003, the survey similarly found that U.S. firms are

> early adopters of technology, and characterize the level of risk that their organizations strive to achieve as "effective and efficient." Respondents from the United States show the highest level of BCP/DRP development, maintenance and testing over the past 12 months, which comes as no surprise given the events of September 11, 2001 (2003, p. 9).[3]

Any U.S. policy requiring greater cybersecurity from financial firms in the U.S. would likely have little impact on the industry's protection from cyberterrorism launched through third-party computers. Since U.S. firms are already providing higher levels of cybersecurity than foreign firms, any cyber attack launched on the financial services industry that first requires breaching an individual firm's security before being launched on other firms would likely come from outside of U.S. borders. Protection for individual

---

[3] BCP stands for Business Community Plan; DRP stands for Disaster Recovery Plan.

firms against such an attack once launched from inside the financial services industry is almost certainly a private good already being provided.

Even if most of the relevant externalities between firms were caused by low cybersecurity in the U.S., it is not clear that government policy could fix one of the major sources of weakness. Many breaches that threaten companies come not from technical problems or lack of investment but from simple human carelessness. As one survey respondent said, "The behavioral aspects are as worrying as the technical aspects. Everyone has to understand that it is their personal responsibility to manage risk and assets" (2003, p. 18). More specifically, another respondent even claimed that humans are *the* weakest link: "We feel that the biggest threat to us is security awareness, or lack of it. One person who opens a virus-laden attachment can cause a lot of damage. People are the weakest link. Technology can only help reduce risks to a point" (2003, p. 12). In 2004 yet another respondent claimed, "Lack of internal security awareness is still one of our biggest threats. Technology can reduce risks to a point but it is people who are the weakest link" (2004, p. 17). Direct regulation is unlikely to be able to address lax behavior.

Although the focus of this paper has been on the market's ability to provide cybersecurity and the potential that government failure could be worse than market failure, other reforms with less potential for government failure can be considered. If spillover costs of lax security between computer users are significant, legal reform to internalize the externalities could be pursued. This could involve reforming negligence standards so that computer owners could be held liable when their computer is hacked into and used to attack others. This type of reform would better address lax behavior by creating proper incentives. It would leave the market's discovery procedure in place. It would not require government to calculate the optimal level of security or give officials the incentive to over-regulate. Interventions other than legal reforms to internalize externalities would make government failure likely.

Even if the market underprovides cybersecurity, direct government regulations are unlikely to help achieve the optimal level. Government regulators have no way to know the optimal level of security. Given their incentives, they would likely force companies to invest too much and would lack the feedback mechanism to force them to revise their judgments. Most of the relevant externalities that need to be corrected exist outside of the U.S. When attempting to eliminate security breaches, policy is unlikely to directly impact one of the greatest sources of risk, lax individual behavior.

## IV. CONCLUSION

Cyberterrorism against private critical infrastructure is not a problem that should be considered separately from ordinary private cybersecurity.

As Green (2002) wrote, "There is no such thing as cyberterrorism—no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity." Even Richard Clarke, Bush's Cybersecurity Czar, admitted, "To date, we've never seen any of the officially designated terrorist groups engage in a cyberattack against us." (Green 2002).

Green observes that this "is not to say that cybersecurity isn't a serious problem—it's just not one that involves terrorists . . . the real danger is from the criminals and other hackers who did $15 billion in damage to the global economy last year using viruses, worms, and other readily available tools" (2002). This is consistent with how the financial services industry perceived cybersecurity. Fewer than five percent of respondents ranked cyberterrorism as a high threat, but viruses and worms were overwhelmingly ranked the greatest threat with more than 70 percent of respondents giving them the highest threat rating (2004, p. 22).

Cyberterrorism against private critical infrastructure is not a problem that requires special government attention. According to the evidence examined here, the government should not be concerned with any general market failure in the provision of cybersecurity. While some aspects of cybersecurity have certain "publicness characteristics," we find many ways in which private orderings in the market provide security despite theoretical problems. Examining the financial services industry, part of the critical infrastructure of our economy, we find no evidence of a pervasive market failure to provide cybersecurity. Instead, we find widespread use of many technologies, increasing budgets, and innovation in adopting new technology. When compared to firms in other countries, financial firms in the U.S. are early adopters and generally better prepared for cyber attacks than foreign competitors. Since any externality created by unsecured computers is not limited by national boundaries, it is unlikely that U.S. policy could correct for such an externality anyway. Cybersecurity is being provided in the private sector, and it is best left free of cumbersome government regulations that may prevent private voluntary orderings from continuing to innovate to secure cyberspace.

## REFERENCES

Anderson, Ross (2001) "Unsettling Parallels Between Security and the Environment." http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt.

Anderson, Ross (2001) "Why Information Security is Hard—An Economic Perspective." In: Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, LA.

Boehlert, Sherwood (2002) Speech to National Academy Conference on Partnering Against Terrorism. October 3. Accessed Sept. 8, 2004. http://www.house.gov/boehlert/nationalacademyspeech1003a.htm.

Campbell, K; Gordon, Lawrence; and Loeb, Martin (2003) "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." *Journal of Computer Security*. Vol. 11, No. 3, pp. 431–448.

Coase, Ronald (1960) "The Problem of Social Cost." *Journal of Law and Economics*. Vol. 3 pp.1–44.

Deloitte, Touche, and Tohmatsu (2003) 2003 *Global Security Survey*. http://www.deloitte.com/gfsi.

Deloitte, Touche and Tohmatsu (2004) 2004 *Global Security Survey*. http://www.deloitte.com/gfsi.

Gordon, Lawrence; Loeb, Martin; and Lucyshyn, William (2002) "An Economics Perspective on the Sharing of Information Related to Security Breaches: Concepts and Empirical Evidence." In: Proceedings of the First Workshop on Economics and Information Security, May 16–17, University of California, Berkeley.

Gordon, Lawrence, Martin Loeb, and William Lucyshyn. 2003. Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy* 22:461–485.

Green, Joshua. 2002. "The Myth of Cyberterrorism." *Washington Monthly*, November. http://www.washingtonmonthly.com/features/2001/0211.green.html.

Hayek, Frederic. 1945. "The Use of Knowledge in Society." *American Economic Review*. 35:519–530.

Hayek, Frederic. 1978. "Competition as a Discovery Procedure." In *New Studies in Philosophy, Politics, Economics and the History of Ideas*. Chicago, IL: University of Chicago Press.

Peltzman, Samuel. 1973. "An Evaluation of the Consumer Protection Legislation: The 1962 Drug Amendments." *Journal of Political Economy*. 81:1049–91.

Peltzman, Samuel. 1974. *Regulation of Pharmaceutical Innovation: The 1962 Amendments*. Washington, American Enterprise Institute for Public Policy Research.

Ricadela, Aaron. 2004. Market Failure is to Blame for Security Problems. *Security Pipeline*. Feb 27. http://www.securitypipeline.com/trends/showArticle.jhtml?articleId=18201051&printableArticle=true.

Ridge, Tom. 2003. Speech at the National Cyber Security Summit. December 3. http://www.us-cert.gov/press_room/detail/RidgeSummitSpeech.html.

Schechter, S. and Smith, C. 2003. "How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems Networks." In: Proceedings of the Financial Cryptography Conference, January 27-30, Cosier, Guadeloupe.

Tullock, Gordon. 1985. "Adam Smith and the Prisoner's Dilemma." Quarterly Journal of Economics. 402: 1073-81.

Varian, Hal. 2002. "System Reliability and Free Riding." In: Proceedings of the First Workshop on Economics and Information Security. May 16-17. University of California, Berkeley.